I

(Seadusandlikud aktid)

MÄÄRUSED

EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2022/2554,

14. detsember 2022,

mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011

(EMPs kohaldatav tekst)

EUROOPA PARLAMENT JA EUROOPA LIIDU NÕUKOGU,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 114,

võttes arvesse Euroopa Komisjoni ettepanekut,

olles edastanud seadusandliku akti eelnõu liikmesriikide parlamentidele,

võttes arvesse Euroopa Keskpanga arvamust ([1]),

võttes arvesse Euroopa Majandus- ja Sotsiaalkomitee arvamust ([2]),

toimides seadusandliku tavamenetluse kohaselt ([3])

ning arvestades järgmist:

(1) Info- ja kommunikatsioonitehnoloogia (IKT) toetab digiajastul keerukaid süsteeme, mida kasutatakse igapäevases tegevuses. See tagab majanduse toimimise olulistes sektorites, sealhulgas finantssektoris, ja parandab siseturu toimimist. Suurem digiteerimine ja omavaheline seotus võimendavad ka IKT-riski, mis muudab ühiskonna tervikuna ja eelkõige finantssüsteemi küberohtude või IKT-katkestuste suhtes kaitsetumaks. IKT-süsteemide üldlevinud kasutus ning ulatuslik digiteerimine ja ühendatus on tänapäeval liidu finantssektori ettevõtjate tegevuse põhielemendid, kuid nende digitaalset kerksust ei ole veel hästi käsitletud ega nende laiematesse tegevusraamistikesse integreeritud.

(2) Viimastel aastakümnetel on IKT kasutamine omandanud finantsteenuste osutamisel keskse rolli, kusjuures praegu on see kõigi finantssektori ettevõtjate tüüpiliste igapäevaste funktsioonide toimimise jaoks kriitilise tähtsusega. Digiteerimine hõlmab praegu näiteks makseid, mille puhul kasutatakse sularaha ja paberipõhiste meetodite asemel üha rohkem digilahendusi, väärtpaberite kliirimist ja arveldamist, elektroonilist ja algoritmkauplemist, laenuandmis- ja rahastamistehinguid, vastastikust laenuandmist, krediidireitinguid, kahjukäsitlust ja *back office*'i tegevust. IKT kasutamine on muutnud ka kindlustussektorit – alates kindlustustehnoloogia kaudu internetis

([1]) ELT C 343, 26.8.2021, lk 1.
([2]) ELT C 155, 30.4.2021, lk 38.
([3]) Euroopa Parlamendi 10. novembri 2022. aasta seisukoht (*Euroopa Liidu Teatajas* seni avaldamata) ja nõukogu 28. novembri 2022. aasta otsus.

teenuseid pakkuvate kindlustusvahendajate esilekerkimisest kuni kindlustuslepingute digitaalse sõlmimiseni. Kogu finantssektor on muutunud valdavalt digitaalseks, kuid digiteerimine on süvendanud ka seoseid ja sõltuvust nii finantssektori sees kui ka finantssektori ja kolmandate isikute taristu ja kolmandast isikust teenuseosutajate vahel.

(3) Euroopa Süsteemsete Riskide Nõukogu (ESRN) kinnitas süsteemset küberriski käsitlevas 2020. aasta aruandes, et finantssektori ettevõtjate, finantsturgude ja finantsturutaristu suur omavaheline seotus ning eelkõige nende IKT-süsteemide omavaheline sõltuvus võivad kujutada endast süsteemset nõrkust, sest lokaalsed küberintsidendid võivad kanduda kiiresti liidu mis tahes ühest ligikaudu 22 000 finantssektori ettevõtjast üle kogu finantssüsteemile, olenemata geograafilistest piiridest. Finantssektoris toimuvad tõsised IKTga seotud rikkumised ei mõjuta ainult üksikuid finantssektori ettevõtjaid. Need soodustavad ka lokaalselt nõrkuse edasi kandumist finantsülekannete kanaleid pidi ja võivad avaldada negatiivset mõju liidu finantssüsteemi stabiilsusele, näiteks põhjustades likviidsuse väljavoolu ning üldiselt vähendada kindlustunnet ja usaldust finantsturgudesse.

(4) IKT-riskile on viimastel aastatel pööranud tähelepanu rahvusvahelised, liidu ja riiklikud poliitikakujundajad, reguleerivad asutused ja standardeid kehtestavad asutused eesmärgiga suurendada digitaalset kerksust, kehtestada standardeid ja koordineerida regulatiivset või järelevalvetööd. Rahvusvahelisel tasandil püüavad Baseli pangajärelevalve komitee, makse- ja arveldussüsteemide komitee, finantsstabiilsuse nõukogu, finantsstabiilsuse instituut ning G7 ja G20 anda eri jurisdiktsioonide pädevatele asutustele ja turukorraldajatele vahendeid oma finantssüsteemi kerksuse suurendamiseks. Seda tööd on ajendanud ka vajadus võtta IKT-riski igakülgselt arvesse omavahel tihedalt seotud ülemaailmse finantssüsteemi kontekstis ning püüda saavutada asjakohaste parimate tavade suurem kooskõla.

(5) Hoolimata sihipärasest liidu ja riiklikust poliitikast ja seadusandlikest algatustest on IKT-risk jätkuvalt probleem liidu finantssüsteemi tegevuskerksuse, suutlikkuse ja stabiilsuse jaoks. 2008. aasta finantskriisile järgnenud reformidega tugevdati peamiselt liidu finantssektori vastupanuvõimet ning sooviti kaitsta liidu konkurentsivõimet ja stabiilsust majanduse, usaldatavusnõuete ja turukäitumise seisukohast. Kuigi IKT turvalisus ja digitaalne kerksus on operatsiooniriski osa, on finantskriisijärgses regulatiivses tegevuskavas nendele vähem keskendutud ning neid on arendatud ainult mõnes liidu finantsteenuste poliitika ja regulatiivse maastiku lõigus või ainult üksikutes liikmesriikides.

(6) Komisjoni 8. märtsi 2018. aasta teatises „Finantstehnoloogia tegevuskava: konkurentsivõimelisema ja innovatiivsema Euroopa finantssektori poole“ rõhutati, et väga oluline on muuta liidu finantssektor vastupidavamaks, sealhulgas tegevuslikust vaatenurgast, et tagada selle tehnoloogiline ohutus ja hea toimimine ning kiire taastumine IKTga seotud rikkumistest ja intsidentidest, võimaldades kokkuvõttes tulemuslikku ja sujuvat finantsteenuste osutamist kogu liidus, muu hulgas pingelistes olukordades, säilitades samal ajal tarbijate ja turu usalduse ja kindlustunde.

(7) 2019. aasta aprillis esitasid Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1093/2010 ([4]) asutatud Euroopa Järelevalveasutus (Euroopa Pangandusjärelevalve) (EBA), Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1094/2010 ([5]) asutatud Euroopa Järelevalveasutus (Euroopa Kindlustus- ja Tööandjapensionide Järelevalve)

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

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

(EIOPA) ning Euroopa Parlamendi ja nõukogu määrusega (EL) nr 1095/2010 ([6]) asutatud Euroopa Järelevalveasutus (Euroopa Väärtpaberiturujärelevalve) (ESMA) (koos „Euroopa järelevalveasutused“) ühiselt tehnilise nõuande, milles kutsuti üles kasutama rahanduse valdkonnas IKT-riski puhul ühtset lähenemisviisi ja soovitati proportsionaalselt tugevdada finantsteenuste sektori digitaalset tegevuskerksust liidu valdkondliku algatuse kaudu.

(8) Liidu finantssektorit reguleerib ühtne reeglistik ja juhib Euroopa Finantsjärelevalve Süsteem. Sätteid digitaalse tegevuskerksuse ja IKT turvalisuse kohta ei ole aga veel täielikult või järjepidevalt ühtlustatud, kuigi digitaalne tegevuskerksus on digiajastul finantsstabiilsuse ja turu usaldusväärsuse tagamiseks määrava tähtsusega ja ei ole vähem oluline kui näiteks ühised usaldatavus- või turukäitumisstandardid. Seepärast peaks ühtse reeglistiku ja järelevalvesüsteemiga hõlmama ka digitaalse tegevuskerksuse, tugevdades pädevate asutuste volitusi, et võimaldada neil teha järelevalvet IKT-riski juhtimise üle finantssektoris, eesmärgiga kaitsta siseturu usaldusväärsust ja tõhusust ning hõlbustada selle nõuetekohast toimimist.

(9) Õigusnormide erinevused ja ebaühtlane riiklik regulatiivne või järelevalvealane lähenemine IKT-riskile takistab finantsteenuste siseturu toimimist ning pärsib asutamisvabaduse sujuvat kasutamist ja piiriüleselt tegutsevate finantssektori ettevõtjate teenuste osutamist. Moonutatud võib olla ka eri liikmesriikides tegutsevate sama tüüpi finantssektori ettevõtjate vaheline konkurents. See on nii eelkõige valdkondades, kus liidu tasandil ühtlustamine on olnud väga piiratud (näiteks digitaalse tegevuskerksuse testimine) või kus ühtlustamist ei ole toimunud (näiteks kolmandast isikust tuleneva IKT-riski seire). Erinevused, mis tulenevad riiklikul tasandil kavandatud arendustest, võivad tekitada uusi siseturu toimimist takistavaid tõkkeid ning kahjustada turuosalisi ja finantsstabiilsust.

(10) IKT-riski puudutavate sätete üksnes osalise käsitlemise tõttu liidu tasandil esineb siiani lünki või kattuvusi olulistes valdkondades, nagu IKT intsidentidest teatamine ja digitaalse tegevuskerksuse testimine, ning ebaühtlust, mis tuleneb lisanduvatest lahknevatest riiklikest normidest või kattuvate normide mittekulutõhusast kohaldamisest. See on eriti kahjulik sellisele IKT-mahukale sektorile nagu finantssektor, sest tehnoloogiariskid ei tunne piire ja finantssektor osutab oma teenuseid piiriüleselt nii liidu sees kui ka väljaspool. Piiriüleselt tegutsevatel või mitme tegevusloaga (ühel finantssektori ettevõtjal võib näiteks olla pangandus-, investeerimisühingu ja makseasutuse litsents, millest igaühe on välja andnud erinev pädev asutus ühes või mitmes liikmesriigis) eraldiseisvatel finantssektori ettevõtjatel on operatiivselt keeruline ise järjepidevalt ja kulutõhusalt IKT-riski käsitleda ja IKT intsidentide negatiivset mõju leevendada.

(11) Kuna ühtse reeglistikuga ei ole kaasnenud laiahaardelist IKT- või operatsiooniriski raamistikku, tuleb kõigi finantssektori ettevõtjate digitaalse tegevuskerksuse põhinõudeid rohkem ühtlustada. Kui finantssektori ettevõtjad arendavad nendele põhinõuetele tuginedes IKT-suutlikkust ja üldist kerksust, et tulla toime tegevuse katkestustega, aitaks see säilitada liidu finantsturgude stabiilsust ja usaldusväärsust ning seega tagada liidus investorite ja tarbijate kaitse kõrge taseme. Kuna käesoleva määruse eesmärk on edendada siseturu sujuvat toimimist, peaks see tuginema Euroopa Liidu toimimise lepingu (ELi toimimise leping) artikli 114 sätetele, nagu neid tõlgendab Euroopa Liidu Kohus (Euroopa Kohus) oma väljakujunenud praktikas.

(12) Käesoleva määrusega soovitakse konsolideerida ja ajakohastada IKT-riskiga seotud nõuded osana operatsiooniriski nõuetest, mida seni on käsitletud eraldi eri liidu õigusaktides. Kuigi nendes õigusaktides käsitleti finantsriski peamisi kategooriaid (nt krediidirisk, tururisk, vastaspoole krediidirisk ja likviidsusrisk, turukäitumise risk), ei käsitletud neis nende vastuvõtmise ajal põhjalikult kõiki tegevuskerksuse komponente. Kuigi kõnealustes liidu õigusaktides käsitleti operatsiooniriski norme põhjalikumalt, keskenduti sageli traditsioonilisele kvantitatiivsele riski käsitlevale lähenemisviisile (kehtestades IKT-riski hõlmamiseks kapitalinõuded), mitte sihipärastele kvalitatiivsetele normidele, millega nähakse ette kaitsmise, avastamise, piiramise, taastamise ja parandamise suutlikkus IKT intsidentide puhul

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

või teatamise ja digitaalse testimise suutlikkus. Nendes õigusaktides sooviti peamiselt käsitleda ja ajakohastada usaldatavusnõuete täitmise järelevalve, turu usaldusväärsuse või turukäitumise põhinorme. IKT-riski käsitlevate eri normide konsolideerimisel ja ajakohastamisel tuleks kõik finantssektori digiriski käsitlevad sätted esimest korda koondada sidusal viisil ühte õigusakti. Käesoleva määrusega kõrvaldatakse seega mõningate eelnevate õigusaktide lüngad või ebaühtlus, muu hulgas neis kasutatud terminoloogia osas, ning osutatakse sõnaselgelt IKT-riskile, kehtestades sihipärased normid IKT-riski juhtimise suutlikkuse, intsidentidest teatamise, tegevuskerksuse testimise ja kolmandast isikust tuleneva IKT-riski seire kohta. Käesoleva määrusega tuleks seetõttu ühtlasi suurendada teadlikkust IKT-riskist ning tunnistada, et IKT intsidendid ja vähene tegevuskerksus võivad ohustada finantssektori ettevõtjate usaldusväärsust.

(13) Finantssektori ettevõtjad peaksid kasutama IKT-riski käsitlemisel sama lähenemisviisi ja samu põhimõtetel põhinevaid norme, võttes arvesse oma suurust ja üldist riskiprofiili ning oma teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust. Sidusus aitab suurendada usaldust finantssüsteemi vastu ja säilitada selle stabiilsust, eelkõige ajal, mil IKT-süsteemidest, -platvormidest ja -taristust sõltutakse suurel määral, millega kaasneb suurem digirisk. Lisaks peaks esmase küberhügieeni järgimine minimeerima IKT-katkestuste mõju ja kulusid ning hoidma seega ära majandusele suurte kulude tekkimise.

(14) Määrus aitab vähendada regulatiivset keerukust, edendab järelevalvealast ühtsust ja suurendab õiguskindlust ning aitab samuti piirata nõuete täitmisega seotud kulusid, eelkõige piiriüleselt tegutsevate finantssektori ettevõtjate puhul, ja vähendada konkurentsimoonutusi. Seepärast on finantssektori ettevõtjate digitaalse tegevuskerksuse ühtse raamistiku kehtestamine määrusega kõige asjakohasem viis tagada, et liidu finantssektor kohaldab kõiki IKT-riski juhtimise komponente ühetaoliselt ja sidusalt.

(15) Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/1148 ([7]) oli esimene liidu tasandil kehtestatud horisontaalne küberturvalisuse raamistik, mida hakati kohaldama ka kolme liiki finantssektori ettevõtjate – krediidiasutused, kauplemiskohad ja kesksed vastaspooled – suhtes. Kuna direktiivis (EL) 2016/1148 sätestati mehhanism oluliste teenuste operaatorite identifitseerimiseks riiklikul tasandil, jäävad üksnes teatavad krediidiasutused, kauplemiskohad ja kesksed vastaspooled, keda liikmesriigid sellisena identifitseerisid, tegelikult direktiivi kohaldamisalasse, ja nemad on seetõttu kohustatud täitma selles sätestatud IKT turvalisuse ja intsidentidest teatamise nõudeid. Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2555 ([8]) on sätestatud ühine kriteerium selle kohaldamisalasse kuuluvate üksuste kindlaksmääramiseks (suuruse ülempiiri reegel), jättes selle kohaldamisalasse ka kolme liiki finantssektori ettevõtjad.

(16) Kuna käesoleva määrusega tõstetakse digitaalse kerksuse eri komponentide ühtlustamise taset, kehtestades IKT-riski juhtimise ja IKT intsidentidest teatamise suhtes nõuded, mis on kehtivas finantsteenuseid käsitlevas liidu õiguses sätestatud nõuetega võrreldes rangemad, on kõnealuse kõrgema taseme puhul tegemist suurema ühtlustamisega ka võrreldes direktiivis (EL) 2022/2555 sätestatud nõuetega. Sellest tulenevalt on käesolev määrus direktiivi (EL) 2022/2555 suhtes *lex specialis*. Samal ajal on äärmiselt oluline tagada, et finantssektor ja liidu horisontaalne küberturvalisuse raamistik, nagu see on praegu sätestatud direktiivis (EL) 2022/2555, oleksid endiselt tugevalt seotud, et tagada kooskõla liikmesriikides vastu võetud küberturvalisuse strateegiatega ning võimaldada teavitada finantsjärelevalveasutusi küberintsidentidest, mis mõjutavad teisi nimetatud direktiiviga hõlmatud sektoreid.

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

([8]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ja millega muudetakse määrust (EL) nr 910/2014 ja direktiivi (EL) 2018/1972 ning tunnistatakse kehtetuks direktiiv (EL) 2016/1148 (küberturvalisuse 2. direktiiv) (vt käesoleva *Euroopa Liidu Teataja* lk 80).

(17) Vastavalt Euroopa Liidu lepingu artikli 4 lõikele 2 ja ilma et see piiraks Euroopa Kohtu tehtavat kohtulikku kontrolli, ei tohiks käesolev määrus mõjutada liikmesriikide vastutust seoses riigi põhifunktsioonidega, mis puudutavad avalikku julgeolekut, riigikaitset ja riigi julgeoleku tagamist, näiteks seoses sellise teabe esitamisega, mis oleks vastuolus riigi julgeoleku kaitsmisega.

(18) Selleks et võimaldada sektoritevahelist õppimist ja võtta tulemuslikult arvesse muude sektorite kogemusi küberohtudega tegelemisel, peaksid direktiivis (EL) 2022/2555 osutatud finantssektori ettevõtjad jääma nimetatud direktiivi nn ökosüsteemi (näiteks koostöörühm ning küberturbe intsidentide lahendamise üksused). Euroopa järelevalveasutused ja riiklikud pädevad asutused peaksid nimetatud direktiivi raames saama osaleda strateegilise poliitika aruteludes ning koostöörühma tehnilises töös, vahetada teavet ja teha täiendavat koostööd nimetatud direktiivi kohaselt määratud või loodud ühtsete kontaktpunktidega. Käesoleva määruse kohased pädevad asutused peaksid konsulteerima ja tegema koostööd ka küberturbe intsidentide lahendamise üksustega. Samuti peaks pädevatel asutustel olema võimalik küsida tehnilist nõu direktiivi (EL) 2022/2555 kohaselt määratud või asutatud pädevatelt asutustelt ning kehtestada koostöökord, mille eesmärk on tagada tõhusad kiire reageerimise koordineerimismehhanismid.

(19) Võttes arvesse tugevaid seoseid finantssektori ettevõtjate digitaalse ja füüsilise kerksuse vahel, on käesolevas määruses ning Euroopa Parlamendi ja nõukogu direktiivis (EL) 2022/2557 ([9]) vaja elutähtsate teenuste osutajate toimepidevuse ühtset käsitust. Kuna finantssektori ettevõtjate füüsilist kerksust käsitletakse terviklikult käesoleva määrusega hõlmatud IKT-riski juhtimise ja teatamiskohustuse raames, ei tuleks direktiivi (EL) 2022/2557 III ja IV peatükis sätestatud kohustusi kõnealuse direktiivi kohaldamisalasse kuuluvate finantssektori ettevõtjate suhtes kohaldada.

(20) Pilvteenuse osutajad on üks direktiiviga (EL) 2022/2555 hõlmatud digitaristu kategooria. Käesoleva määrusega loodavat liidu järelevaatamisraamistikku (edaspidi „järelevaatamisraamistik“) kohaldatakse kõigi kriitilise tähtsusega kolmandast isikust IKT-teenuste, sealhulgas pilvteenuse osutajate suhtes, kes osutavad IKT-teenuseid finantssektori ettevõtjatele, ja seda tuleks pidada direktiivi (EL) 2022/2555 kohase järelevalve täienduseks. Käesoleva määrusega loodud järelevaatamisraamistik peaks hõlmama pilvteenuse osutajaid, kuni puudub liidu horisontaalne raamistik, millega oleks asutatud digitaalne järelevaatamisasutus.

(21) Selleks et säilitada täielik kontroll IKT-riski üle, on finantssektori ettevõtjatel vaja laiahaardelist suutlikkust, et võimaldada tugevat ja tulemuslikku IKT-riski juhtimist, ning erimehhanisme ja -korda kõigi IKT intsidentide käsitlemiseks ja tõsistest IKT intsidentidest teavitamiseks. Samuti peaks finantssektori ettevõtjatel olema kehtestatud IKT-süsteemide, -kontrollide ja -protsesside testimise ning kolmandast isikust tuleneva IKT-riski juhtimise kord. Finantssektori ettevõtjate digitaalse tegevuskerksuse miinimumnõudeid tuleks muuta rangemaks, võimaldades samal ajal teatavatel finantssektori ettevõtjatel, eelkõige mikroettevõtjatel ja sellistel finantssektori ettevõtjatel, kelle suhtes kohaldatakse lihtsustatud IKT-riski juhtimise raamistikku, kohaldada nõudeid proportsionaalselt. Selleks et hõlbustada proportsionaalset ja tõhusat, pädevate asutuste töökoormuse vähendamise vajadusega arvestavat järelevalvet tööandja kogumispensioni asutuste üle, tuleks selliste finantssektori ettevõtjate suhtes kohaldatavas asjakohases riiklikus järelevalvekorras võtta arvesse nende suurust ja üldist riskiprofiili ning nende teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust, isegi kui ületatakse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/2341 ([10]) artiklis 5 sätestatud asjakohaseid lävesid. Eelkõige tuleks järelevalvetegevuses keskenduda vajadusele käsitleda tõsiseid riske, mis on seotud konkreetse üksuse IKT-riski juhtimisega.

([9]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2557, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ (vt käesoleva *Euroopa Liidu Teataja* lk 164).

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

Pädevad asutused peaksid samuti olema tähelepanelikud selliste tööandja kogumispensioni asutuste järelevalve suhtes, kes kooskõlas direktiivi (EL) 2016/2341 artikliga 31 annavad olulise osa oma põhitegevusest, nagu varade valitsemine, kindlustusmatemaatilised arvutused, raamatupidamisarvestus ja andmehaldus, edasi teenuseosutajatele, ning tegema nende üle järelevalvet proportsionaalselt.

(22) IKT intsidentidest teatamise läved ja taksonoomia on riiklikul tasandil väga erinevad. Kuigi Euroopa Parlamendi ja nõukogu määrusega (EL) 2019/881 ([11]) asutatud Euroopa Liidu Küberturvalisuse Ameti (ENISA) ja direktiivi (EL) 2022/2555 kohase koostöörühma tehtava asjakohase töö kaudu võib jõuda üksmeelele, esineb lävede kehtestamise ja taksonoomia kasutamise valdkonnas jätkuvalt lahknevaid käsitusi või need võivad ülejäänud finantssektori ettevõtjate puhul tekkida. Selliste lahknevuste tõttu peavad finantssektori ettevõtjad täitma mitmeid nõudeid, eelkõige kui nad tegutsevad mitmes liikmesriigis ja kuuluvad finantskontserni. Lisaks võivad need lahknevused takistada selliste uute ühetaoliste või tsentraliseeritud liidu mehhanismide loomist, mis kiirendaksid teatamisprotsessi ja toetaksid kiiret ja sujuvat pädevate asutuste vahelist teabevahetust, mis on äärmiselt oluline IKT-riski käsitlemiseks suurte rünnete korral, millel võivad olla süsteemsed tagajärjed.

(23) Selleks et vähendada teatavate finantssektori ettevõtjate halduskoormust ja potentsiaalselt dubleerivaid teatamiskohustusi, tuleks lõpetada Euroopa Parlamendi ja nõukogu direktiivi (EL) 2015/2366 ([12]) kohaste intsidentidest teatamise reeglite kohaldamine käesoleva määruse kohaldamisalasse kuuluvate makseteenuse pakkujate suhtes. Sellest tulenevalt peaksid krediidiasutused, e-raha asutused, makseasutused ja kõnealuse direktiivi artikli 33 lõikes 1 osutatud kontoteabe teenuse pakkujad käesoleva määruse kohaldamise alguskuupäevast teavitama käesoleva määruse kohaselt kõigist tegevust või turvalisust mõjutavatest maksetega seotud intsidentidest, millest on varem teatatud nimetatud direktiivi kohaselt, olenemata intsidendi seotusest IKTga.

(24) Selleks et võimaldada pädevatel asutustel täita järelevalveülesandeid, saades täieliku ülevaate IKT intsidentide laadist, sagedusest, olulisusest ja mõjust, ning tõhustada asjaomaste avaliku sektori asutuste, sealhulgas õiguskaitse- ja kriisilahendusasutuste vahelist teabevahetust, tuleks käesolevas määruses sätestada kindel IKT intsidentidest teatamise kord, mille kohaselt käsitletakse asjakohaste nõuetega praeguseid lünki finantsteenuseid käsitlevas õiguses, ning kõrvaldada kulude vähendamiseks olemasolevad kattuvused ja dubleerimine. On oluline IKT intsidentidest teatamise korda ühtlustada, kohustades kõiki finantssektori ettevõtjaid teavitama oma pädevaid asutusi käesolevas määruses sätestatud ühtse ja ühtlustatud raamistiku abil. Lisaks peaks Euroopa järelevalveasutustel olema õigus täpsustada veelgi IKT intsidentidest teatamise raamistiku asjakohaseid elemente, nagu taksonoomia, tähtajad, andmekogumid, vormid ja kohaldatavad läved. Täieliku kooskõla tagamiseks direktiiviga (EL) 2022/2555 peaks finantssektori ettevõtjatel olema lubatud asjaomast pädevat asutust olulistest küberohtudest vabatahtlikult teatada, kui küberoht mõjutab nende arvates finantssüsteemi, teenusekasutajaid või kliente.

(25) Finantssektori teatavates allsektorites on digitaalse tegevuskerksuse testimise nõudeid välja töötatud, kehtestades raamistikke, mis ei ole alati täielikult omavahel kooskõlas. See võib kahekordistada piiriüleste finantssektori ettevõtjate kulusid ja muudab digitaalse tegevuskerksuse testimise tulemuste vastastikuse tunnustamise keerukaks, mis omakorda võib siseturgu killustada.

([11]) Euroopa Parlamendi ja nõukogu 17. aprilli 2019. aasta määrus (EL) 2019/881, mis käsitleb ENISAt (Euroopa Liidu Küberturvalisuse Amet) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimist ja millega tunnistatakse kehtetuks määrus (EL) nr 526/2013 (küberturvalisuse määrus) (ELT L 151, 7.6.2019, lk 15).

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

(26) Lisaks, kui IKT-testimist ei nõuta, jääb nõrkus avastamata, mis seab finantssektori ettevõtja IKT-riski ohtu ning kokkuvõttes tekitab suurema riski finantssektori stabiilsusele ja usaldusväärsusele. Ilma liidu sekkumiseta jääks digitaalse tegevuskerksuse testimine ebaühtlaseks ning puuduks süsteem IKT-testimise tulemuste vastastikuseks tunnustamiseks eri jurisdiktsioonides. Ühtlasi, kuna on ebatõenäoline, et finantssektori muudes allsektorites võetaks mõistlikus ulatuses vastu testimisskeeme, jääksid nad ilma testimisraamistiku võimalikust kasust seoses IKT nõrkuse ja -riskide avastamise ning kaitsevõime ja talitluspidevuse testimisega, mis aitavad suurendada tarbijate, tarnijate ja äripartnerite usaldust. Nende kattuvuste, lahknevuste ja lünkade kõrvaldamiseks tuleb sätestada koordineeritud testimiskorda käsitlevad normid ja seeläbi edendada selliste finantssektori ettevõtjate puhul süvatestimise vastastikust tunnustamist, kes täidavad käesoleva määruse kriteeriume.

(27) Finantssektori ettevõtjate sõltuvus IKT-teenuste kasutamisest tuleneb osaliselt nende vajadusest kohaneda tekkiva konkurentsivõimelise digitaalse maailmamajandusega, et suurendada oma tegevuse tõhusust ja vastata tarbijate nõudlusele. Sellise sõltuvuse laad ja ulatus on viimastel aastatel pidevalt muutunud ning aidanud vähendada kulusid finantsvahenduses ja võimaldanud finantstegevuse puhul äritegevust laiendada ja skaleerida, andes samal ajal mitmesugused IKT-vahendid keerukate siseprotsesside juhtimiseks.

(28) IKT-teenuste kõnealust laialdast kasutust näitavad keerukad lepingud, millest tulenevalt on finantssektori ettevõtjatel sageli raske leppida kokku lepingutingimustes, mis oleksid kohandatud vastavalt usaldatavusstandarditele või muudele regulatiivsetele nõuetele, mida nende suhtes kohaldatakse, või kasutada teatavaid õigusi, nagu pääsu- või auditeerimisõigused, isegi juhul, kui viimased on nende lepingutes kindlaks määratud. Lisaks ei ole paljude selliste lepingutega ette nähtud piisavaid kaitsemeetmeid, mis lubaksid tegevuse edasiandmise protsesse täies ulatuses seirata, mistõttu ei saa finantssektori ettevõtja seonduvaid riske hinnata. Peale selle, kuna kolmandast isikust IKT-teenuste osutajad osutavad sageli standardteenuseid eri tüüpi klientidele, ei ole sellised lepingud alati piisavad finantssektoris osalejate individuaalsete või erivajaduste rahuldamiseks.

(29) Kuigi finantsteenuseid käsitlev liidu õigus sisaldab teatavaid üldiseid norme tegevuse edasiandmise kohta, ei ole lepingulise aspekti seire liidu õiguses täielikult sätestatud. Kuna puuduvad selged ja kohandatud liidu standardid, mida kohaldatakse kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingute suhtes, on IKT-riski väline allikas põhjalikult käsitlemata. Sellest tulenevalt on vaja kehtestada teatavad peamised põhimõtted, mis suunavad seda, kuidas finantssektori ettevõtjad juhivad kolmandast isikust tulenevat IKT-riski, ja mis on eriti olulised, kui finantssektori ettevõtjad kasutavad kolmandast isikust IKT-teenuste osutajaid, et toetada oma kriitilise tähtsusega või olulisi funktsioone. Neid põhimõtteid peaksid toetama peamised lepingulised õigused, mis puudutavad mitut lepingute täitmise ja lõpetamisega seotud elementi, eesmärgiga tagada teatavad minimaalsed kaitsemeetmed, et toetada finantssektori ettevõtjate võimet seirata tulemuslikult kogu kolmandast isikust teenuseosutajate tasandil tekkivat IKT-riski. Kõnealused põhimõtted täiendavad tegevuse edasiandmise suhtes kohaldatavat valdkondlikku õigust.

(30) Praegu on ilmne teatav ühtsuse ja ühtlustamise puudumine seoses kolmandast isikust tuleneva IKT-riski ja kolmandast isikust IKT-teenuste osutajatest sõltuvuse seirega. Tegevuse edasiandmise käsitlemisel on küll tehtud jõupingutusi (näiteks EBA 2019. aasta suunised tegevuse edasiandmise kohta ja ESMA 2021. aasta suunised pilvteenuse osutajatele tegevuse edasiandmise kohta), kuid laiemat probleemi, mis on seotud sellise süsteemse riski kõrvaldamisega, mille võib tekitada finantssektori seotus piiratud arvu kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega, ei ole liidu õiguses piisavalt käsitletud. Normide puudumist liidu tasandil süvendab asjaolu, et ei ole volitusi ja vahendeid käsitlevaid riiklikke norme, mis võimaldaksid finantsjärelevalveasutustel saada hästi aru sõltuvusest kolmandast isikust IKT-teenuste osutajatest ja seirata piisaval määral riske, mis tulenevad kolmandast isikust IKT-teenuste osutajatest sõltuvuse kontsentratsioonist.

(31) Võttes arvesse potentsiaalset süsteemset riski, mis kaasneb tegevuse ulatuslikuma edasiandmisega ja kolmandast isikust IKT-teenuste osutajate kontsentratsiooniga, ning asjaolu, et riiklikud mehhanismid ei ole piisavad, et tagada finantsjärelevalveasutustele asjakohased vahendid kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatel esineva IKT-riski tagajärgede kvantifitseerimiseks, kvalifitseerimiseks ja leevendamiseks, on vaja kehtestada asjakohane järelevaatamisraamistik, mis võimaldaks pidevalt seirata selliste kolmandast isikust IKT-teenuste osutajate tegevust, kes on finantssektori ettevõtjate jaoks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad, tagades samal ajal, et säilib muude kui finantssektori ettevõtjatest klientide konfidentsiaalsus ja turvalisus. Kuigi kontsernisisese IKT-teenuste osutamisega kaasnevad spetsiifilised riskid ja eelised, ei tohiks seda automaatselt pidada vähem riskantseks kui IKT-teenuste osutamist väljaspool finantskontserni asuvate teenuseosutajate poolt ning seetõttu tuleks selle suhtes kohaldada sama õigusraamistikku. Kui aga IKT-teenuseid osutatakse sama finantskontserni piires, võib finantssektori ettevõtjatel olla suurem kontroll kontsernisiseste teenuseosutajate üle, mida tuleks üldises riskihindamises arvesse võtta.

(32) Kuna IKT-risk on muutumas üha komplekssemaks ja keerukamaks, sõltuvad head IKT-riski avastamise ja ennetamise meetmed suurel määral ohte ja nõrkust puudutava teadmuse regulaarsest jagamisest finantssektori ettevõtjate vahel. Teabe jagamine aitab tekitada suuremat teadlikkust küberohtudest. See omakorda suurendab finantssektori ettevõtjate suutlikkust hoida ära küberohtude muutumist tegelikeks IKT intsidentideks ning võimaldab finantssektori ettevõtjatel tõhusamalt piirata IKT intsidentide mõju ja kiiremini taastuda. Näib, et liidu tasandi suuniste puudumisel on sellist teadmuse jagamist pärssinud mitu tegurit, eelkõige ebakindlus seoses selle kooskõlaga andmekaitse-, monopolidevastaste ja vastutusnormidega.

(33) Lisaks takistavad kasuliku teabe jagamist kahtlused selle kohta, millist liiki teavet saab teiste turuosaliste või muude kui järelevalveasutustega (näiteks ENISAga analüütilise sisendi andmiseks või Europoliga õiguskaitse otstarbel) jagada. Seepärast on teabe jagamise ulatus ja kvaliteet praegu endiselt piiratud ja killustunud, asjakohane teabevahetus on peamiselt lokaalne (riiklike algatuste kaudu) ning puuduvad kogu liitu hõlmavad ühtsed teabe jagamise kokkulepped, mis oleks kohandatud vastavalt integreeritud finantssüsteemi vajadustele. Seepärast on oluline neid sidekanaleid tugevdada.

(34) Finantssektori ettevõtjaid tuleks julgustada teabe jagamise kokkulepetes osalemise kaudu vahetama omavahel küberohte käsitlevat teavet ja teadmust ning kasutama kollektiivselt oma individuaalseid teadmisi ja praktilisi kogemusi strateegilisel, taktikalisel ja operatiivsel tasandil, et suurendada oma suutlikkust küberohte piisavalt hinnata ja seirata, end nende eest kaitsta ja neile reageerida. Seepärast tuleb liidu tasandil võimaldada mehhanismide loomist vabatahtlikult teabe jagamise kokkulepete jaoks, mis usaldusväärses keskkonnas sõlmimise korral aitaksid finantssektori kogukonnal ennetada küberohte ja reageerida neile ühiselt, piirates kiiresti IKT-riski levikut ja takistades võimalikku ülekandumist finantskanalite kaudu. Need mehhanismid peaksid olema kooskõlas kohaldatavate liidu konkurentsiõiguse normidega, mis on esitatud komisjoni 14. jaanuari 2011. aasta teatises „Suunised Euroopa Liidu toimimise lepingu artikli 101 kohaldatavuse kohta horisontaalkoostöö kokkulepete suhtes“, ning liidu andmekaitsenormidega, eelkõige Euroopa Parlamendi ja nõukogu määrusega (EL) 2016/679 ([13]). Mehhanismid peaksid toimima lähtuvalt kõnealuse määruse artiklis 6 sätestatud ühe või mitme õigusliku aluse rakendamisest näiteks olukorras, kus isikuandmete töötlemine on vajalik vastutava töötleja või kolmanda isiku õigustatud huvi korral, nagu on osutatud kõnealuse määruse artikli 6 lõike 1 punktis f, ning olukorras, kus isikuandmete töötlemine on vajalik vastutava töötleja seadusjärgse kohustuse täitmiseks või see on vajalik avalikes huvides oleva ülesande täitmiseks või vastutava töötleja avaliku võimu teostamiseks, nagu on osutatud vastavalt kõnealuse määruse artikli 6 lõike 1 punktides c ja e.

([13]) Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119, 4.5.2016, lk 1).

(35) Selleks et säilitada kogu finantssektori digitaalne tegevuskerksus ja pidada samal ajal sammu tehnoloogia arenguga, tuleks käesolevas määruses käsitleda igat liiki IKT-teenustest tulenevaid riske. Selleks tuleks käesoleva määruse kontekstis IKT-teenuste määratlust tõlgendada laialt, hõlmates IKT-süsteemide kaudu ühele või mitmele sise- või väliskasutajale pidevalt osutatavaid digi- ja andmeteenuseid. See määratlus peaks hõlmama näiteks OTT-teenuseid (inglise keeles '*over the top*' services), mis kuuluvad elektroonilise side teenuste kategooriasse. Määratlusest tuleks välja jätta üksnes selliste tavapäraste analoogtelefoniteenuste piiratud kategooria, mis kvalifitseeruvad kanalikommutatsiooniga üldkasutatava telefonivõrgu teenuseks, lauatelefoniteenuseks, analoogtelefonsideks või püsivõrgu liini telefoniteenuseks.

(36) Hoolimata käesoleva määrusega ette nähtud laiast kohaldamisalast, tuleks digitaalse tegevuskerksuse normide kohaldamisel võtta arvesse finantssektori ettevõtjate suuruse ja üldise riskiprofiili märkimisväärseid erinevusi. Üldpõhimõte on see, et finantssektori ettevõtjad peaksid IKT-riski juhtimise raamistiku rakendamiseks ressursside ja suutlikkuse jaotamisel võtma oma IKTga seotud vajaduste puhul igakülgselt arvesse oma suurust ja üldist riskiprofiili ning oma teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust; pädevad asutused peaksid aga jätkama sellise jaotuse hindamist ja läbivaatamist.

(37) Direktiivi (EL) 2015/2366 artikli 33 lõikes 1 osutatud kontoteabe teenuse pakkujad kuuluvad sõnaselgelt käesoleva määruse kohaldamisalasse, võttes arvesse nende tegevuse eripära ja sellest tulenevaid riske. Lisaks kuuluvad käesoleva määruse kohaldamisalasse e-raha asutused ja makseasutused, mille suhtes kohaldatakse Euroopa Parlamendi ja nõukogu direktiivi 2009/110/EÜ ([14]) artikli 9 lõike 1 ning direktiivi (EL) 2015/2366 artikli 32 lõike 1 kohast erandit, isegi kui neile ei ole antud direktiivi 2009/110/EÜ kohast tegevusluba e-raha väljastamiseks või kui neile ei ole antud direktiivi (EL) 2015/2366 kohast tegevusluba makseteenuste osutamiseks ja täitmiseks. Samal ajal ei kuulu käesoleva määruse kohaldamisalasse Euroopa Parlamendi ja nõukogu direktiivi (EL) 2013/36/EL ([15]) artikli 2 lõike 5 punktis 3 osutatud postižiiroasutused. Makseasutuste puhul, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 kohast erandit, e-raha asutuste puhul, mille suhtes kohaldatakse direktiivi 2009/110/EÜ kohast erandit, ning direktiivi (EL) 2015/2366 artikli 33 lõikes 1 osutatud kontoteabe teenuse pakkujate puhul peaks pädev asutus olema direktiivi (EL) 2015/2366 artikli 22 kohaselt määratud pädev asutus.

(38) Kuna suurematel finantssektori ettevõtjatel võib olla rohkem ressursse ning nad saavad kiiresti eraldada vahendeid juhtimisstruktuuride arendamiseks ja luua mitmesuguseid äristrateegiaid, peaksid ainult need finantssektori ettevõtjad, kes ei ole mikroettevõtjad käesoleva määruse tähenduses, olema kohustatud kehtestama keerukama juhtimiskorra. Sellistel ettevõtjatel on paremad vahendid, et luua eelkõige spetsiaalsed juhtimisfunktsioonid kolmandast isikust IKT-teenuste osutajatega sõlmitud järelevalvekokkulepete või kriisijuhtimise jaoks, korraldada IKT-riski juhtimine vastavalt kolme kaitseliiniga mudelile või võtta kasutusele sisemine riskijuhtimis- ja kontrollimudel ning võimaldada siseauditeid oma IKT-riski juhtimise raamistiku puhul.

(39) Mõned finantssektori ettevõtjad saavad kasu eranditest või nende suhtes kohaldatakse liidu asjaomase valdkondliku õiguse alusel väga leebet õigusraamistikku. Selliste finantssektori ettevõtjate hulka kuuluvad Euroopa Parlamendi ja nõukogu direktiivi 2011/61/EL ([16]) artikli 3 lõikes 2 osutatud alternatiivsete investeerimisfondide valitsejad, Euroopa Parlamendi ja nõukogu direktiivi 2009/138/EÜ ([17]) artiklis 4 osutatud kindlustus- ja edasikindlustusandjad ning tööandja kogumispensioni asutused, kes haldavad pensioniskeeme, millel ei ole kokku rohkem kui 15 liiget.

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

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

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

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

Neid erandeid silmas pidades ei oleks selliste finantssektori ettevõtjate lisamine käesoleva määruse kohaldamisalasse proportsionaalne. Lisaks tunnistatakse käesolevas määruses kindlustusvahendusturu struktuuri eripära, mistõttu ei tohiks käesolevat määrust kohaldada kindlustusvahendajate, edasikindlustusvahendajate ja kõrvaltegevusena pakutava kindlustuse vahendajate suhtes, kes kvalifitseeruvad mikroettevõtjateks või väikesteks ja keskmise suurusega ettevõtjateks.

(40) Kuna direktiivi 2013/36/EL artikli 2 lõike 5 punktides 4–23 osutatud üksused on kõnealuse direktiivi kohaldamisalast välja jäetud, peaks liikmesriikidel olema võimalik otsustada jätta käesoleva määruse kohaldamisalast välja kõnealused üksused, kes asuvad nende territooriumil.

(41) Selleks, et viia käesolev määrus vastavusse Euroopa Parlamendi ja nõukogu direktiivi 2014/65/EL ([18]) kohaldamisalaga, on lisaks asjakohane jätta käesoleva määruse kohaldamisalast välja kõnealuse direktiivi artiklites 2 ja 3 osutatud füüsilised ja juriidilised isikud, kellel on lubatud osutada investeerimisteenuseid ilma direktiivi 2014/65/EL kohast tegevusluba saamata. Direktiivi 2014/65/EL artikliga 2 jäetakse kõnealuse direktiivi kohaldamisalast välja ka üksused, mis kvalifitseeruvad käesoleva määruse kohaldamisel finantssektori ettevõtjateks, näiteks väärtpaberite keskdepositooriumid, investeerimisfondid ning kindlustus- ja edasikindlustusandjad. Käesoleva määruse kohaldamisalast kõnealuse direktiivi artiklites 2 ja 3 osutatud isikute ja üksuste väljajätmine ei peaks hõlmama kõnealuseid väärtpaberite keskdepositooriume, investeerimisfonde ning kindlustus- ja edasikindlustusandjaid.

(42) Liidu valdkondliku õiguse alusel kohaldatakse mõne finantssektori ettevõtja suhtes nende suuruse või osutatavate teenustega seotud põhjustel leebemaid nõudeid või erandeid. Kõnealune finantssektori ettevõtjate kategooria hõlmab väikeseid ja mitteseotud investeerimisühinguid, väikeseid tööandja kogumispensioni asutusi, mille asjaomane liikmesriik võib direktiivi (EL) 2016/2341 kohaldamisalast välja jätta kõnealuse direktiivi artiklis 5 sätestatud tingimustel, ning mis haldavad pensioniskeeme, millel ei ole kokku rohkem kui 100 liiget, ning asutusi, mille suhtes kohaldatakse direktiivi 2013/36/EL kohast erandit. Seepärast on kooskõlas proportsionaalsuse põhimõttega ja liidu valdkondliku õiguse mõtte säilitamiseks asjakohane kohaldada nende finantssektori ettevõtjate suhtes samuti käesoleva määruse kohast lihtsustatud IKT-riski juhtimise raamistikku. Neid finantssektori ettevõtjaid hõlmava IKT-riski juhtimise raamistiku proportsionaalsust ei tohiks muuta regulatiivsete tehniliste standarditega, mille töötavad välja Euroopa järelevalveasutused. Lisaks on kooskõlas proportsionaalsuse põhimõttega asjakohane kohaldada käesoleva määruse kohast lihtsustatud IKT-riski juhtimise raamistikku direktiivi (EL) 2015/2366 artikli 32 lõikes 1 osutatud makseasutuste ja direktiivi 2009/110/EÜ artiklis 9 osutatud e-raha asutuste suhtes, kellele on tehtud erand neid liidu õigusakte ülevõtvas liikmesriigi õiguses, samal ajal kui makseasutused ja e-raha asutused, kellele ei ole tehtud erandit kooskõlas liidu valdkondlikku õigust ülevõtva liikmesriigi õigusega, peaksid järgima käesolevas määruses sätestatud üldraamistikku.

(43) Samuti ei tohiks finantssektori ettevõtjatelt, kes kvalifitseeruvad mikroettevõtjateks või kelle suhtes kohaldatakse käesoleva määruse kohast lihtsustatud IKT-riski juhtimise raamistikku, nõuda järgmist: sellise funktsiooni loomist, mille abil seiratakse kolmandast isikust IKT-teenuste osutajatega sõlmitud IKT-teenuste kasutamise kokkuleppeid; kõrgema juhtkonna liikmele vastutuse andmist seonduva riski ja asjakohaste dokumentide üle järelevaatamise eest; vastutuse panemist IKT-riski juhtimise ja järelevaatamise eest kontrollifunktsioonile ning sellise kontrollifunktsiooni asjakohase sõltumatuse taseme tagamist, millega välditakse huvide konflikti; IKT-riski juhtimise raamistiku dokumenteerimist ja selle läbivaatamist vähemalt kord aastas; IKT-riski juhtimise raamistiku regulaarsete siseauditite võimaldamist; pärast oma võrgu- ja infosüsteemide taristus ja protsessides oluliste muudatuste tegemist põhjalike hindamiste läbiviimist; korrapäraste riskianalüüside tegemist IKT pärandsüsteemide kohta; IKT reageerimis- ja taastekavade rakendamise suhtes sõltumatute siseauditite tegemise võimaldamist; kriisijuhtimisfunktsiooni rakendamist, talitluspidevuse ning reageerimis- ja taastekavade testimise laiendamist, et hõlmata esmase IKT-taristu ja varurajatiste puhul ümberlülitusstsenaariume; taotluse korral pädevate asutuste teavitamist tõsiste IKT intsidentide tekitatud hinnangulisest aastasest kogukulust ja -kahjust, et oleks olemas IKT-alane varusuutlikkus; pädevate asutuste teavitamist muudatustest, mis tehti pärast IKT intsidendi järgseid kontrolle; asjaomase

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

tehnoloogia arengu pidevat jälgimist; käesoleva määrusega ette nähtud IKT-riski juhtimise raamistiku lahutamatu osana tervikliku digitaalse tegevuskerksuse testimise programmi loomist ning kolmandast isikust tulenevat IKT-riski käsitleva strateegia vastuvõtmist ja korrapärast läbivaatamist. Lisaks tuleks mikroettevõtjatelt üksnes nõuda, et nad hindaksid IKT-alase varusuutlikkuse vajadust üksnes oma riskiprofiili alusel. Mikroettevõtjad peaksid saama kasu paindlikumast korrast seoses digitaalse tegevuskerksuse testimise programmidega. Tehtavate testide liiki ja sagedust kaaludes peaksid nad leidma õige tasakaalu digitaalse tegevuskerksuse kõrge taseme säilitamise eesmärgi, olemasolevate ressursside ja oma üldise riskiprofiili vahel. Mikroettevõtjad ja finantssektori ettevõtjad, kelle suhtes kohaldatakse käesoleva määruse kohast lihtsustatud IKT-riski juhtimise raamistikku, tuleks vabastada nõudest teha IKT-vahendite, -süsteemide ja -protsesside süvatestimist, mis tugineb ohuteabel põhinevale läbistustestimisele, sest sellist testimist tuleks nõuda ainult finantssektori ettevõtjatelt, kes täidavad käesoleva määruse kriteeriume. Arvestades mikroettevõtjate piiratud suutlikkust, peaks neil olema võimalik leppida kolmandast isikust IKT-teenuste osutajaga kokku finantssektori ettevõtja pääsu-, kontrolli- ja auditeerimisõiguste delegeerimises kolmandast isikust IKT-teenuste osutaja poolt määratud sõltumatule kolmandale isikule tingimusel, et finantssektori ettevõtja saab asjaomaselt kolmandalt isikult igal ajal nõuda kolmandast isikust IKT-teenuste osutaja tegevuse kohta asjakohast teavet ja kinnitust.

(44) Kuna ainult neid finantssektori ettevõtjaid, kes on digitaalse kerksuse süvatestimiseks kindlaks määratud, tuleks kohustada tegema ohuteabel põhinevaid läbistusteste, peaksid selliste testide tegemisega kaasnevaid haldusprotsesse teostama ja rahalisi kulusid kandma väike osa finantssektori ettevõtjaid.

(45) Selleks et tagada ühest küljest finantssektori ettevõtjate äristrateegiate ja teisest küljest IKT-riski juhtimise täielik kooskõla ja üldine vastavus, tuleks finantssektori ettevõtjate juhtorganeid kohustada täitma otsustavat ja aktiivset rolli IKT-riski juhtimise raamistiku ning üldise digitaalse tegevuskerksuse strateegia suunamises ja kohandamises. Lisaks sellele, et juhtorganite kasutatav lähenemisviis peaks keskenduma IKT-süsteemide kerksuse tagamise viisidele, peaks see hõlmama inimesi ja protsesse selliste põhimõtete kaudu, mis edendab ettevõtja igal tasandil kõigi töötajate suurt teadlikkust küberriskidest ja pühendumust tagada kõigil tasanditel range küberhügieen. See, et kokkuvõttes on finantssektori ettevõtja IKT-riski juhtimise eest vastutav juhtorgan, peaks olema selle laiahaardelise lähenemisviisi üldpõhimõte, mis peaks väljenduma juhtorgani pidevas osalemises IKT-riski juhtimise seire kontrollis.

(46) Põhimõte, et juhtorgan vastutab täielikult ja lõplikult finantssektori ettevõtja IKT-riski juhtimise eest, käib käsikäes vajadusega tagada finantssektori ettevõtja jaoks selline IKTga seotud investeeringute tase ja üldeelarve, mis võimaldab finantssektori ettevõtjal saavutada digitaalse tegevuskerksuse kõrge taseme.

(47) Käesolevas määruses lähtutakse asjakohastest küberriski juhtimise rahvusvahelistest, riiklikest ja valdkondlikest parimatest tavadest, suunistest, soovitustest ja käsitustest ning edendatakse põhimõtteid, mis hõlbustavad IKT-riski juhtimise üldise struktuuri kujundamist. Seega, kui finantssektori ettevõtjate loodud põhisuutlikkus vastab käesolevas määruses sätestatud mitmesuguste IKT-riski juhtimise funktsioonide (kindlaksmääramine, kaitse ja ennetamine, avastamine, reageerimine ja taastamine, õppimine ja arenemine ning teabevahetus) täitmiseks vajaminevale, peaks finantssektori ettevõtjatele jääma võimalus kasutada teisiti piiritletud või kategoriseeritud IKT-riski mudeleid.

(48) Selleks et muutuva küberohtude maastikuga sammu pidada, peaks finantssektori ettevõtjatel olema ajakohastatud IKT-süsteemid, mis on usaldusväärsed ja millel on suutlikus mitte ainult teenuste osutamiseks vajaliku andmetöötluse tagamiseks, vaid ka piisava tehnoloogilise kerksuse kindlustamiseks, mis võimaldab neil piisavalt toime tulla halvenenud turutingimustest või muudest ebasoodsatest olukordadest tuleneva täiendava töötlemisvajadusega.

(49) Tõhusaid talitluspidevuse ja taastekavasid on vaja selleks, et finantssektori ettevõtjad saaksid kohe ja kiiresti lahendada IKT intsidendid, eelkõige tulla toime küberrünnetega, piirates kahju ja seades prioriteediks tegevuse jätkamise ja taastemeetmed kooskõlas oma varunduspõhimõtetega. Siiski ei tohiks selline tegevuse jätkamine kuidagi seada ohtu võrgu- ja infosüsteemide terviklust ja turvalisust või andmete kättesaadavust, autentsust, terviklust ja konfidentsiaalsust.

(50) Kuigi käesoleva määrusega lubatakse finantssektori ettevõtjatel määrata oma taasteaja ja taastekünnise eesmärgid kindlaks paindlikult ja seega asjaomaste funktsioonide laadi ja kriitilist tähtsust ning konkreetseid ärivajadusi täielikult arvesse võttes, tuleks määrusega siiski nõuda, et kõnealuste eesmärkide seadmisel hinnataks võimalikku kogumõju turu tõhususele.

(51) Küberrünnete toimepanijad kalduvad saama rahalist tulu otse allika juures, tuues seega finantssektori ettevõtjate jaoks kaasa märkimisväärseid tagajärgi. Selleks et takistada seda, et IKT-süsteemid kaotavad oma tervikluse või ei ole kasutatavad, ning seega hoida ära andmetega seotud rikkumisi ja füüsilise IKT-taristu kahjustumist, tuleks märkimisväärselt parandada ja sujuvamaks muuta seda, kuidas finantssektori ettevõtjad teavitavad tõsistest IKT intsidentidest. IKT intsidentidest teavitamist tuleks ühtlustada kõigi finantssektori ettevõtjate jaoks kehtestatava nõudega esitada raporteid vahetult ainult oma asjaomastele pädevatele asutustele. Kui finantssektori ettevõtja üle teevad järelevalvet mitu riiklikku pädevat asutust, siis peaksid liikmesriigid määrama raporti adressaadiks ühe pädeva asutuse. Nõukogu määruse (EL) nr 1024/2013 ([19]) artikli 6 lõike 4 kohaselt oluliseks liigitatud krediidiasutused peaksid esitama raporti riiklikele pädevatele asutustele, kes peaksid seejärel edastama raporti Euroopa Keskpangale (EKP).

(52) Selline otsene teavitamine peaks võimaldama finantsjärelevalveasutustele kohest juurdepääsu tõsiseid IKT intsidente käsitlevale teabele. Finantsjärelevalveasutused peaksid omakorda edastama tõsiste IKT intsidentide üksikasjad avaliku sektori asutustele, kes ei ole finantssektori asutused (näiteks pädevad asutused ja ühtsed kontaktpunktid direktiivi (EL) 2022/2555 tähenduses, riiklikud andmekaitseasutused ning kuritegelikku laadi tõsiste IKT intsidentide puhul õiguskaitseasutused), et suurendada selliste asutuste teadlikkust kõnealustest intsidentidest ning küberturbe intsidentide lahendamise üksuste puhul hõlbustada kohasel viisil viivitamatu abi osutamist finantssektori ettevõtjatele. Lisaks peaks liikmesriikidel olema võimalik kindlaks määrata, et finantssektori ettevõtjad peaksid ise esitama sellist teavet avaliku sektori asutustele, mis ei kuulu finantsteenuste valdkonda. Need teabevood peaksid võimaldama finantssektori ettevõtjatel kiiresti saada kasu kõnealuste asutuste asjakohasest tehnilisest panusest, nõuannetest parandusmeetmete kohta ja edasistest järelmeetmetest. Teavet tõsiste IKT intsidentide kohta tuleks edastada vastastikku: finantsjärelevalveasutused peaksid edastama finantssektori ettevõtjale kogu vajaliku tagasiside või suunised ning Euroopa järelevalveasutused peaksid jagama anonüümitud andmeid intsidendiga seotud küberohtude ja ilmnenud nõrkuse kohta, et aidata kaasa laiemale ühisele kaitsele.

(53) Kuigi kõigil finantssektori ettevõtjatel peaks olema intsidentidest teavitamise kohustus, ei eeldata, et see kohustus mõjutaks kõiki ettevõtjaid samamoodi. Et hõlmata üksnes tõsiseid IKT intsidente, tuleks asjakohaseid olulisuse lävesid ning teavitamise tähtaegu sobivalt kohandada Euroopa järelevalveasutuste väljatöötatavatel regulatiivsetel tehnilistel standarditel põhinevates delegeeritud õigusaktides. Lisaks tuleks teavitamiskohustuse tähtaegade kehtestamisel arvesse võtta finantssektori ettevõtjate eripära.

(54) Käesoleva määrusega tuleks nõuda, et krediidiasutused, makseasutused, kontoteabe teenuse pakkujad ja e-raha asutused teavitaksid kõigist tegevust või turvalisust mõjutavatest maksetega seotud intsidentidest, millest on varem teatatud direktiivi (EL) 2015/2366 alusel, olenemata intsidendi seotusest IKTga.

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

(55) Euroopa järelevalveasutustele tuleks teha ülesandeks hinnata IKT intsidentidest teavitamise võimaliku liidu tasandil tsentraliseerimise teostatavust ja tingimusi. Sellise tsentraliseerimise puhul kasutataks tõsistest IKT intsidentidest teavitamisel ühist ELi keskust, mis võtab asjaomased raportid vahetult vastu ja teavitab automaatselt riiklikke pädevaid asutusi või tsentraliseeriks üksnes riiklike pädevate asutuste edastatud asjaomased raportid ning täidaks seega koordineerivat rolli. Euroopa järelevalveasutustele tuleks teha ülesandeks koostada EKP ja ENISAga konsulteerides ühisaruanne, milles uuritakse ühise ELi keskuse loomise teostatavust.

(56) Selleks et saavutada digitaalse tegevuskerksuse kõrge tase ja lähtudes nii asjaomastest rahvusvahelistest standarditest (näiteks G7 põhielemendid ohuteabel põhineva läbistustestimise jaoks) kui ka liidus rakendatavatest raamistikest, näiteks TIBER-EUst, (inglise keeles „Threat Intelligence-based Ethical Red Teaming“) peaksid finantssektori ettevõtjad oma IKT-süsteeme ja IKT ülesandeid täitvaid töötajaid korrapäraselt testima, et teha kindlaks nende tulemuslikkus ennetada, avastada, reageerida ja taastada eesmärgiga tuvastada võimalik IKT nõrkus ja sellega tegeleda. Kajastamaks finantssektori ettevõtjate küberturvalisuse alase valmisoleku taseme erinevust finantssektori eri allsektorites ja nende vahel, peaks testimine hõlmama mitmesuguseid vahendeid ja meetmeid alates põhinõuete hindamisest (näiteks nõrkuse hindamine ja skaneerimine, avatud lähtekoodiga tarkvara analüüsimine, võrgu turvalisuse hindamine, lünkade analüüsimine, füüsilise turvalisuse ülevaatamine, küsimustikud ja skaneerimistarkvara lahendused, teostatavuse korral lähtekoodi ülevaatamine, stsenaariumipõhine testimine, ühilduvuse testimine, jõudlustestid või läbivtestimine) süvatestimiseni ohuteabel põhineva läbistustestimise kaudu. Selline süvatestimine peaks olema nõutav üksnes selliste finantssektori ettevõtjate puhul, kes on IKT seisukohast piisavalt küpsed, et kõnealuseid teste mõistlikult teha. Käesoleva määruse kohaselt nõutavad digitaalse tegevuskerksuse testid peaksid seega olema käesoleva määruse kriteeriume täitvate finantssektori ettevõtjate (näiteks suured, süsteemselt olulised ja IKT seisukohast küpsed krediidiasutused, börsid, väärtpaberite keskdepositooriumid ja kesksed vastaspooled) puhul nõudlikumad kui muude finantssektori ettevõtjate puhul. Samal ajal peaks digitaalse tegevuskerksuse testimiseks ohuteabel põhinev läbistustestimine olema asjakohasem selliste finantssektori ettevõtjate puhul, kes tegutsevad põhiliste finantsteenuste allsektorites (nagu maksed, pangandus ning kliiring ja arveldus) ning kellel on süsteemne roll ja vähem asjakohane muude allsektorite puhul (nagu varahaldurid ja reitinguagentuurid).

(57) Finantssektori ettevõtjad, kes on seotud piiriülese tegevusega ning kasutavad liidus oma asutamis- või teenuste osutamise vabadust, peaksid oma päritoluliikmesriigis vastama süvatestimise nõuetele (st ohuteabel põhinevad läbistustestid), mis peaks hõlmama IKT-taristut kõigis jurisdiktsioonides, kus piiriülene finantskontsern liidus tegutseb, võimaldades seega sellistel finantskontsernidel kanda asjaomaseid IKT testimiskulusid ainult ühes jurisdiktsioonis.

(58) Selleks et tugineda teatavate pädevate asutuste poolt juba omandatud eksperditeadmistele, eelkõige seoses TIBER-EU raamistiku rakendamisega, peaks käesolev määrus võimaldama liikmesriikidel määrata ühe avaliku sektori asutuse, kes vastutab riiklikul tasandil kõigi ohuteabel põhinevate läbistustestidega seotud küsimuste eest finantssektoris, või pädevad asutused, kes sellise määramise puudumisel delegeeriksid ohuteabel põhinevate läbistustestidega seotud ülesannete täitmise mõnele muule riiklikule finantssektori pädevale asutusele.

(59) Kuna käesoleva määrusega ei nõuta finantssektori ettevõtjatelt, et nad käsitleksid kõiki kriitilise tähtsusega või olulisi funktsioone ühe ohuteabel põhineva läbistustesti raames, peaks finantssektori ettevõtjatel olema vabadus otsustada, millised kriitilise tähtsusega või olulised funktsioonid ja mitu sellist funktsiooni tuleks kõnealuse testiga hõlmata.

(60) Käesoleva määruse tähenduses peaks ühine testimine, mis hõlmab mitme finantssektori ettevõtja osalemist ohuteabel põhinevas läbistustestimises ja mille suhtes kolmandast isikust IKT-teenuste osutaja saab sõlmida otse lepingu välistestijaga, olema lubatud üksnes juhul, kui võib põhjendatult eeldada, et avaldub kahjulik mõju selliste teenuste kvaliteedile või turvalisusele või selliste teenustega seotud andmete konfidentsiaalsusele, mida kolmandast isikust IKT-teenuste osutaja osutab klientidele, kes ei kuulu käesoleva määruse kohaldamisalasse. Ühise testimise suhtes tuleks samuti kohaldada kaitsemeetmeid (juhtimine ühe määratud finantssektori ettevõtja poolt, osalevate finantssektori ettevõtjate arvu kohandamine), et tagada testimise põhjalikkus asjaomaste finantssektori ettevõtjate jaoks, kes vastavad käesoleva määruse kohaselt ohuteabel põhineva läbistustestimise eesmärkidele.

(61) Selleks et kasutada ära ettevõtja tasandil olemasolevaid sisemisi ressursse, tuleks käesoleva määrusega lubada kasutada ohuteabel põhineva läbistustestimise tegemiseks sisetestijaid, tingimusel et järelevalveasutus on selleks loa andnud, puudub huvide konflikt ning perioodiliselt vahetatakse sise- ja välistestijaid (iga kolme testi järel), nõudes samal ajal, et ohuteabel põhineva läbistustestimise puhul oleks ohuteabe andja alati finantssektori ettevõtjast sõltumatu. Vastutus ohuteabel põhineva läbistustestimise tegemise eest peaks jääma täielikult finantssektori ettevõtja kanda. Ametiasutuste väljastatud tõendid peaksid teenima üksnes vastastikuse tunnustamise eesmärki ega tohiks välistada järelmeetmeid finantssektori ettevõtja IKT-riski taseme suhtes, samuti ei tuleks neid tõendeid käsitada järelevalvealase kinnitusena finantssektori ettevõtja IKT-riski juhtimise ja leevendamise suutlikkusele.

(62) Selleks et tagada kolmandast isikust tuleneva IKT-riski usaldusväärne seire finantssektoris, on vaja sätestada põhimõtetel põhinevad normid, et suunata finantssektori ettevõtjaid sellise riski seirel, mis tekib seoses kolmandast isikust IKT-teenuste osutajatele edasi antud funktsioonidega, eelkõige kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenustega, ning üldisemalt igasuguse sõltuvuse puhul kolmandast isikust IKT-teenuste osutajatest.

(63) Selleks et tulla toime IKT-riski eri allikate keerukusega, võttes samal ajal arvesse finantsteenuste sujuvat osutamist võimaldavate tehnoloogiliste lahenduste pakkujate paljusust ja mitmekesisust, peaks käesolev määrus hõlmama mitmesuguseid kolmandast isikust IKT-teenuste osutajaid, sealhulgas pilv-, tarkvara- ja andmeanalüüsiteenuste osutajaid ning andmekeskuse teenuste osutajaid. Samuti, kuna finantssektori ettevõtjad peaksid tõhusalt ja sidusalt tuvastama ja juhtima igat liiki riske, sealhulgas finantskontserni raames hangitud IKT-teenuste kontekstis, tuleks selgitada, et käesoleva määruse kohaselt tuleks kolmandast isikust IKT-teenuste osutajateks pidada ka ettevõtjaid, kes kuuluvad finantskontserni ja osutavad IKT-teenuseid peamiselt oma emaettevõtjale või oma emaettevõtja tütarettevõtjatele või filiaalidele, samuti finantssektori ettevõtjaid, kes osutavad IKT-teenuseid teistele finantssektori ettevõtjatele. Lisaks, võttes arvesse arenevat makseteenuste turgu, mis sõltub üha enam keerukatest tehnilistest lahendustest, ning pidades silmas uusi makseteenuste liike ja makselahendusi, tuleks makseteenuste ökosüsteemi osalisi, kes pakuvad maksete töötlemise toiminguid või käitavad maksetaristuid, samuti käsitada käesoleva määruse kohaselt kolmandast isikust IKT-teenuste osutajatena, välja arvatud keskpangad makse- või väärtpaberiarveldussüsteemide käitamisel ning avaliku sektori asutused, kui nad osutavad IKTga seotud teenuseid riigi funktsioonide täitmise kontekstis.

(64) Finantssektori ettevõtjal peaks igal ajal olema täielik vastutus oma käesoleva määruse kohaste kohustuste täitmise eest. Finantssektori ettevõtjad peaksid kohaldama proportsionaalset lähenemisviisi kolmandast isikust IKT-teenuste osutaja tasandil tekkinud riski seireks, võttes igati arvesse oma IKTga seotud sõltuvuse laadi, ulatust, keerukust ja olulisust, teenuste kriitilist tähtsust või olulisust, lepingutega hõlmatud protsesse või funktsioone ja hoolika hindamise põhjal võimalikku mõju finantsteenuste jätkumisele ja kvaliteedile ettevõtja ja kontserni tasandil, nagu on asjakohane.

(65) Sellise seire puhul tuleks kasutada kolmandast isikust tulenevat IKT-riski käsitlevat strateegilist lähenemisviisi, mille formaliseerimiseks on finantssektori ettevõtja juhtorgan võtnud vastu spetsiaalse kolmandast isikust tuleneva IKT-riski strateegia, mis rajaneb iga kolmandast isikust IKT-teenuste osutajatest sõltuvuse pideval uurimisel. Selleks et suurendada järelevalvealast teadlikkust IKT valdkonna sõltuvusest kolmandatest isikutest ning pidades silmas käesoleva määrusega loodud järelevaatamisraamistiku kontekstis tehtava töö täiendavat toetamist, tuleks kõigilt finantssektori ettevõtjatelt nõuda, et nad peaksid teaberegistrit, mis sisaldab kõiki lepinguid kolmandast isikust IKT-teenuste osutaja pakutavate IKT-teenuste kasutamise kohta. Finantsjärelevalveasutustel peaks olema võimalik nõuda täielikku registrit või paluda selle konkreetseid osi ning seega hankida olulist teavet, et saada laiem arusaam finantssektori ettevõtjate IKTga seotud sõltuvusest.

(66) Lepingute ametlikku sõlmimist peaks toetama ja sellele peaks eelnema põhjalik lepingueelne analüüs, mille keskmes on eelkõige kavandatava IKT-lepinguga toetatavate teenuste kriitiline tähtsus või olulisus, järelevalveasutuse vajalik luba või muud tingimused ja võimalik seonduv kontsentratsioonirisk, ning kolmandast isikust IKT-teenuste osutajate valimise ja hindamise protsessis tuleks samuti rakendada hoolsusmeetmeid ning hinnata võimalikke huvide konflikte. Lepingute puhul, mis käsitlevad kriitilise tähtsusega või olulisi funktsioone, peaksid finantssektori ettevõtjad võtma arvesse seda, kas kolmandast isikust IKT-teenuste osutajad kasutavad kõige ajakohasemaid ja kõrgema tasemega infoturbestandardeid. Lepingute lõpetamise aluseks peaksid olema vähemalt sellised asjaolud, mis annavad tunnistust puudujääkidest kolmandast isikust IKT-teenuste osutaja tasandil, eelkõige õigusaktide või

lepingutingimuste olulisest rikkumisest, lepingutega ette nähtud funktsioonide täitmise võimalikku muutmist tõendavatest asjaoludest, kolmandast isikust IKT-teenuste osutaja üldise IKT-riski juhtimise nõrku kohti käsitlevatest tõenditest või asjaoludest, mis viitavad asjaomase pädeva asutuse suutmatusele teha finantssektori ettevõtja üle tulemuslikku järelevalvet.

(67) Selleks et käsitleda kolmandast isikust IKT-teenuste osutajate kontsentratsiooniriski süsteemset mõju, edendatakse käesoleva määrusega tasakaalustatud lahendust, mis seisneb kõnealuse kontsentratsiooniriski paindlikus ja järkjärgulises käsituses, sest jäikade ülempiiride või rangete piirangute kehtestamine võib pärssida äritegevust ja piirata lepinguvabadust. Finantssektori ettevõtjad peaksid oma kavandatud lepinguid põhjalikult hindama, et teha kindlaks kõnealuse riski tekkimise tõenäosus, ning analüüsima muu hulgas põhjalikult alltöövõtulepinguid, eelkõige juhul, kui need on sõlmitud kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajatega. Selles etapis ja selleks, et saavutada tasakaal lepinguvabaduse kaitsmise kohustuse ja finantsstabiilsuse tagamise kohustuse vahel, ei peeta sobivaks näha ette norme, mis käsitlevad kolmandast isikust IKT-teenuste osutajatega seotud rangeid ülempiire ja piiranguid. Järelevaatamisraamistiku kontekstis peaks käesoleva määruse kohaselt määratud juhtiv järelevaatamisasutus pöörama seoses kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega erilist tähelepanu sellele, et mõista täielikult vastastikuse sõltuvuse ulatust ja avastada konkreetsed olukorrad, kus kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suur kontsentratsioon liidus avaldab tõenäoliselt survet liidu finantssüsteemi stabiilsusele ja usaldusväärsusele, ning pidama dialoogi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega, kui selline konkreetne risk on kindlaks tehtud.

(68) Selleks et korrapäraselt hinnata ja seirata kolmandast isikust IKT-teenuste osutaja suutlikkust osutada finantssektori ettevõtjale turvaliselt teenuseid, avaldamata negatiivset mõju ettevõtja digitaalsele tegevuskerksusele, peaksid olema ühtlustatud mitmed kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingute peamised elemendid. Selline ühtlustamine peaks hõlmama minimaalselt valdkondi, mis on olulised selleks, et võimaldada finantssektori ettevõtjal täiel määral seirata riske, mis võivad tuleneda kolmandast isikust IKT-teenuste osutajast, pidades silmas finantssektori ettevõtja vajadust kindlustada oma digitaalne kerksus, sest ta sõltub suurel määral talle osutatud IKT-teenuste stabiilsusest, funktsionaalsusest, kättesaadavusest ja turvalisusest.

(69) Käesoleva määruse nõuetega kooskõla saavutamise eesmärgil lepingute üle uusi läbirääkimisi pidades peaksid finantssektori ettevõtjad ja kolmandast isikust IKT-teenuste osutajad tagama, et oleksid hõlmatud käesoleva määrusega ette nähtud peamised lepingusätted.

(70) Käesolevas määruses sätestatud mõiste „kriitilise tähtsusega või oluline funktsioon“ hõlmab Euroopa Parlamendi ja nõukogu direktiivi 2014/59/EL ([20]) artikli 2 lõike 1 punktis 35 sätestatud „kriitiliste funktsioonide“ määratlust. Seega on direktiivi 2014/59/EL kohaselt kriitilisteks funktsioonideks peetavad funktsioonid hõlmatud kriitilise tähtsusega funktsioonide määratlusega käesoleva määruse tähenduses.

(71) Olenemata IKT-teenustega toetatava funktsiooni kriitilisest tähtsusest või olulisusest tuleks lepingutes esitada eelkõige funktsioonide ja teenuste täielik kirjeldus ning kõnealuste funktsioonide täitmise ja andmete töötlemise kohad ning teenustasemete kirjeldused. Muud hädavajalikud elemendid, mis võimaldavad finantssektori ettevõtjal seirata kolmandast isikust tulenevat IKT-riski, on järgmised: lepingusätted, milles täpsustatakse, kuidas kolmandast isikust IKT-teenuste osutaja tagab isikuandmetele ligipääsetavuse, nende kättesaadavuse, tervikluse, turvalisuse ja kaitse; sätted, milles määratakse kindlaks asjaomased tagatised, et võimaldada andmetele juurdepääs, nende taastamine ja tagastamine kolmandast isikust IKT-teenuste osutaja maksejõuetuse, kriisilahenduse või äritegevuse

([20]) Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta direktiiv 2014/59/EL, millega luuakse krediidiasutuste ja investeerimisühingute finantsseisundi taastamise ja kriisilahenduse õigusraamistik ning muudetakse nõukogu direktiivi 82/891/EMÜ ning Euroopa Parlamendi ja nõukogu direktiive 2001/24/EÜ, 2002/47/EÜ, 2004/25/EÜ, 2005/56/EÜ, 2007/36/EÜ, 2011/35/EL, 2012/30/EL ja 2013/36/EL ning määruseid (EL) nr 1093/2010 ja (EL) nr 648/2012 (ELT L 173, 12.6.2014, lk 190).

lõpetamise korral; sätted, millega kohustatakse kolmandast isikust IKT-teenuste osutajat andma abi osutatavate teenustega seotud IKT-intsidentide puhul ilma lisakuludeta või eelnevalt kindlaksmääratud hinnaga; sätted, mis käsitlevad kolmandast isikust IKT-teenuste osutaja kohustust teha täielikku koostööd finantssektori ettevõtja pädevate asutuste ja kriisilahendusasutustega, ning sätted, mis käsitlevad lepingu lõpetamise õigust ja sellega seonduvat lepingu lõpetamise minimaalset etteteatamistähtaega vastavalt pädevate asutuste ja kriisilahendusasutuste ootustele.

(72) Lisaks sellistele lepingusätetele ja tagamaks, et finantssektori ettevõtjatel on täielik kontroll kõigi muudatuste üle, mis toimuvad kolmanda isiku tasandil ning võivad kahjustada nende IKT turvalisust, tuleks kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamist käsitlevates lepingutes samuti kindlaks määrata järgmine: täielikud teenustasemete kirjeldused koos täpsete kvantitatiivsete ja kvalitatiivsete tulemuseesmärkidega, et võimaldada põhjendamatu viivituseta asjakohaste parandusmeetmete võtmist, kui kokkulepitud teenustasemeid ei saavutata; kolmandast isikust IKT-teenuste osutaja asjaomased etteteatamistähtajad ja teatamiskohustus selliste sündmuste puhul, mis võivad oluliselt kahjustada kolmandast isikust IKT-teenuste osutaja võimet osutada vastavaid IKT-teenuseid; kolmandast isikust IKT-teenuste osutaja suhtes kohaldatav nõue rakendada ja testida ettevõtte talitluspidevuse plaane ning kasutada IKT-turvameetmeid, -vahendeid ja -põhimõtteid, mis võimaldavad teenuseid turvaliselt osutada ning osaleda ja teha täielikku koostööd finantssektori ettevõtja tehtavas ohuteabel põhinevas läbistustestis.

(73) Kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamist käsitlevad lepingud peaksid samuti hõlmama sätteid, millega antakse finantssektori ettevõtjale või määratud kolmandale isikule pääsu-, kontrolli- ja auditeerimisõigused ja õigus teha koopiaid, mis on äärmiselt olulised vahendid finantssektori ettevõtja pidevas seires kolmandast isikust IKT-teenuste osutaja tegevuse üle ning mida täiendab kõnealuse teenuseosutaja täielik koostöö kontrollide ajal. Ka finantssektori ettevõtja pädeval asutusel peaks olema õigus teadete alusel kontrollida ja auditeerida kolmandast isikust IKT-teenuste osutajat tingimusel, et kaitstakse konfidentsiaalset teavet.

(74) Sellistes lepingutes tuleks samuti näha ette spetsiaalsed väljumisstrateegiad, mis võimaldavad eelkõige kohustuslikke üleminekuperioode, mille jooksul kolmandast isikust IKT-teenuste osutajad peaksid jätkama asjaomaste teenuste osutamist, et vähendada katkestuste riski finantssektori ettevõtja tasandil või võimaldada viimasel lülituda tulemuslikult ümber muude kolmandast isikust IKT-teenuste osutajate teenuste kasutamisele või hakata kasutama ettevõtjasiseseid lahendusi, olenevalt osutatud IKT-teenuse keerukusest. Lisaks peaksid direktiivi 2014/59/EL kohaldamisalasse kuuluvad finantssektori ettevõtjad tagama, et asjaomased IKT-teenuste lepingud on nende finantssektori ettevõtjate kriisilahenduse korral püsivad ja täielikult täidetavad. Seega peaksid kõnealused finantssektori ettevõtjad kooskõlas kriisilahendusasutuste ootustega tagama, et asjaomased IKT-teenuste lepingud oleksid kriisilahendusele vastupidavad. Kuni need finantssektori ettevõtjad jätkavad oma maksekohustuste täitmist, peaksid nad lisaks muudele nõuetele tagama, et asjaomased IKT-teenuste lepingud sisaldavad sätteid, mis käsitlevad restruktureerimise või kriisilahenduse olukorras lepingute mittelõpetamist, mittepeatamist ja muutmata jätmist.

(75) Lisaks võib avaliku sektori asutuste või liidu institutsioonide välja töötatud lepingu tüüptingimuste vabatahtlik kasutamine, eelkõige selliste lepingu tüüptingimuste kasutamine, mille komisjon on töötanud välja pilvteenuste jaoks, olla finantssektori ettevõtjatele ja kolmandast isikust IKT-teenuste osutajatele mugavam, suurendades täielikus kooskõlas finantsteenuseid käsitlevas liidu õiguses sätestatud nõuete ja ootustega nende õiguskindlust seoses pilvteenuste kasutamisega finantssektoris. Lepingu tüüptingimuste väljatöötamine tugineb meetmetele, mida kavandati juba 2018. aasta finantstehnoloogia tegevuskavas, mis näitas komisjoni kavatsust julgustada ja hõlbustada selliste lepingu tüüptingimuste väljatöötamist, mida finantssektori ettevõtjad saaks kasutada pilvteenuste edasiandmisel, lähtudes valdkonnaüleste pilvteenuste sidusrühmade jõupingutustest, mida komisjon on finantssektori osalusel edendanud.

(76) Selleks et edendada järelevalvealaste käsituste ühtlustamist ja tõhusust finantssektorile kolmandatest isikutest tuleneva IKT-riski käsitlemisel ning tugevdada selliste finantssektori ettevõtjate digitaalset tegevuskerksust, kes sõltuvad finantsteenuste osutamist toetavate IKT-teenuste puhul kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatest, ning seega aidata säilitada liidu finantssüsteemi stabiilsust ja finantsteenuste siseturu usaldusväärsust, tuleks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes kohaldada liidu järelevaatamisraamistikku. Kuigi järelevaatamisraamistiku loomine on põhjendatud liidu tasandil meetmete võtmisest saadava

lisaväärtusega ning IKT-teenuste kasutamise tähtsuse ja eripäraga finantsteenuste osutamisel, tuleks samal ajal meelde tuletada, et see lahendus tundub sobiv üksnes käesoleva määruse kontekstis, mis puudutab konkreetselt finantssektori digitaalset tegevuskerksust. Sellist järelevaatamisraamistikku ei tohiks siiski pidada liidu järelevalve uueks mudeliks muus finantsteenuste ja -tegevuse valdkonnas.

(77) Järelevaatamisraamistikku tuleks kohaldada ainult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes. Sellepärast tuleks luua määramismehhanism, et võtta arvesse finantssektori sellistest kolmandast isikust IKT-teenuste osutajatest sõltuvuse ulatust ja laadi. See mehhanism peaks hõlmama kvantitatiivsete ja kvalitatiivsete kriteeriumide kogumit, millega kehtestatakse järelevaatamisraamistikuga hõlmamise aluseks olevad kriitilise tähtsuse parameetrid. Selle hindamise täpsuse tagamiseks ja kolmandast isikust IKT-teenuste osutaja organisatsioonilisest struktuurist olenemata peaksid sellised kriteeriumid suuremasse kontserni kuuluva kolmandast isikust IKT-teenuste osutaja puhul võtma arvesse kogu kolmandast isikust IKT-teenuste osutaja kontserni struktuuri. Ühelt poolt peaks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatel, kes ei ole nende kriteeriumide põhjal automaatselt sellisena määratud, olema võimalik otsustada vabatahtlikult kohaldada järelevaatamisraamistikku, kuid teiselt poolt tuleks need kolmandast isikust IKT-teenuste osutajad, kelle suhtes juba kohaldatakse ELi toimimise lepingu artikli 127 lõikes 2 osutatud Euroopa keskpankade süsteemi ülesannete täitmist toetavaid järelevaatamismehhanismi raamistikke, selle kohaldamisalast välja jätta.

(78) Sarnaselt tuleks järelevaatamisraamistiku kohaldamisalast välja jätta ka finantssektori ettevõtjad, kes osutavad IKT-teenuseid teistele finantssektori ettevõtjatele, kuuludes ise käesoleva määruse kohaselt kolmandast isikust IKT-teenuste osutajate kategooriasse, kuna nende suhtes juba kohaldatakse asjaomase finantsteenuseid käsitleva liidu õigusega kehtestatud järelevalvemehhanisme. Asjakohasel juhul peaksid pädevad asutused oma järelevalvetegevuse raames võtma arvesse IKT-riski, mida põhjustavad finantssektori ettevõtjatele IKT-teenuseid osutavad finantssektori ettevõtjad. Olemasolevate kontserni tasandi riskiseiremehhanismide tõttu tuleks sama erandit kohaldada ka nende kolmandast isikust IKT-teenuste osutajate suhtes, kes osutavad teenuseid peamiselt oma kontserni ettevõtjatele. Need kolmandast isikust IKT-teenuste osutajad, kes osutavad IKT-teenuseid ainult ühes liikmesriigis üksnes selles liikmesriigis tegutsevatele finantssektori ettevõtjatele, tuleks nende piiratud tegevuse ja piiriülese mõju puudumise tõttu samuti määramismehhanismi kohaldamisalast välja jätta.

(79) Finantsteenuste valdkonnas toimunud digiüleminek on toonud kaasa IKT-teenuste kasutamise ja neile tuginemise enneolematul tasemel. Kuna finantsteenuste osutamine ilma pilvteenuseid, tarkvaralahendusi ja andmetega seotud teenuseid kasutamata on muutunud mõeldamatuks, on liidu finantsökosüsteem muutunud lahutamatult sõltuvaks teatavatest IKT-teenuste osutajate teenustest. Mõned neist teenuseosutajatest, kes on IKT-põhiste tehnoloogiate arendamisel ja rakendamisel novaatorid, täidavad olulist rolli finantsteenuste osutamisel või on integreeritud finantsteenuste väärtusahelasse. Seega on nad omandanud liidu finantssüsteemi stabiilsuse ja usaldusväärsuse seisukohast kriitilise tähtsuse. Selline laialdane sõltuvus kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate teenustest koos erinevate turuosaliste infosüsteemide vastastikuse sõltuvusega tekitab otsese ja potentsiaalselt tõsise riski liidu finantsteenuste süsteemile ja finantsteenuste osutamise järjepidevusele, kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaid peaksid mõjutama tegevushäired või olulised küberintsidendid. Küberintsidentidele on omane võime paljuneda ja levida kogu finantssüsteemis märkimisväärselt kiiremas tempos kui muud liiki riskid, mida finantssektoris seiratakse, ning need võivad kanduda teistesse sektoritesse ja ületada geograafilisi piire. Need võivad areneda süsteemseks kriisiks, kus usaldus finantssüsteemi vastu väheneb reaalmajandust toetavate funktsioonide katkemise või suure finantskahju tõttu, saavutades taseme, millele finantssüsteem ei suuda vastu pidada või mis nõuab jõuliste šokkidega toimetuleku meetmete kasutuselevõttu. Selleks et vältida selliste stsenaariumide realiseerumist ning seeläbi liidu finantsstabiilsuse ja finantsilise usaldusväärsuse ohustamist, on oluline ühtlustada kolmandatest isikutest tuleneva IKT-riskiga seotud järelevalvetavasid, eelkõige uute normide abil, mis võimaldavad liidul korraldada järelevaatamise kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle.

(80) Järelevaatamisraamistik sõltub suurel määral koostöö tasemest juhtiva järelevaatamisasutuse ja sellise kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja vahel, kes osutab finantssektori ettevõtjatele finantsteenuste osutamist mõjutavaid teenuseid. Edukas järelevaatamine eeldab muu hulgas juhtiva järelevaatamisasutuse suutlikkust viia tõhusalt läbi seiremissioone ja kontrolle, et hinnata kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate kasutatavaid reegleid, kontrolle ja protsesse ning hinnata nende tegevuse võimalikku kumulatiivset mõju finantsstabiilsusele ning finantssüsteemi usaldusväärsusele. Samal ajal on väga oluline, et kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad järgiksid juhtiva järelevaatamisasutuse soovitusi ja lahendaksid väljendatud mureküsimused. Kuna finantsteenuste pakkumist mõjutavaid teenuseid osutavate kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate poolse koostöö puudumine, nagu oma ruumidele juurdepääsu andmisest või teabe esitamisest keeldumine, jätaks juhtiva järelevaatamisasutuse lõpuks ilma olulistest vahenditest kolmandatest isikutest tuleneva IKT-riski hindamisel ning võib negatiivselt mõjutada finantsstabiilsust ja finantssüsteemi usaldusväärsust, on vaja ette näha ka proportsionaalne karistuste rakendamise kord.

(81) Seda arvesse võttes ei tohiks raskused kolmandas riigis asutatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele määratud sunniraha sissenõudmisel seada ohtu juhtiva järelevaatamisasutuse vajadust määrata sunniraha, et sundida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaid täitma käesolevas määruses sätestatud läbipaistvuse ja juurdepääsuga seotud kohustusi. Selleks et tagada selliste karistuste täitmisele pööramine ja võimaldada kiiresti kasutusele võtta menetlused, millega on tagatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate kaitseõigus määramismehhanismi ja soovituste andmise kontekstis, peaksid kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad, kes osutavad finantssektori ettevõtjatele finantsteenuste pakkumist mõjutavaid teenuseid, olema kohustatud säilitama liidus piisava äritegevuse. Tulenevalt järelevaatamise laadist ja võrreldavate korralduste puudumisest muudes jurisdiktsioonides, puuduvad sobivad alternatiivsed mehhanismid, mis tagaksid selle eesmärgi saavutamise tõhusa koostöö kaudu, mida tehakse kolmandate riikide finantsjärelevalveasutustega seoses selliste digitaalsete operatsiooniriskide mõju seirega, mis kaasnevad süsteemset laadi kolmandast isikust IKT-teenuste osutajatega, kes kvalifitseeruvad kolmandas riigis asutatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajateks. Selleks et jätkata IKT-teenuste osutamist liidu finantssektori ettevõtjatele, peaks kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutaja, mis on kooskõlas käesoleva määrusega määratud kriitilise tähtsusega teenuseosutajaks, 12 kuu jooksul alates sellisest määramisest tegema kõik vajalikud korraldused, et tagada liidus enda registreerimine äriühinguna, asutades tütarettevõtja, nagu see on määratletud liidu õigustikus, nimelt Euroopa Parlamendi ja nõukogu direktiivis 2013/34/EL ([21]).

(82) Liidus tütarettevõtja asutamise nõue ei tohiks takistada kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajal osutada IKT-teenuseid ja nendega seotud tehnilist tuge väljaspool liitu asuvate rajatiste ja taristu kaudu. Käesoleva määrusega ei kehtestata andmete lokaliseerimise kohustust, sest sellega ei nõuta, et andmeid tuleb säilitada või töödelda liidus.

(83) Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatel peaks olema võimalik osutada IKT-teenuseid kõikjalt maailmas, mitte tingimata või mitte ainult liidus asuvatest ruumidest. Järelevaatamistegevus peaks esmalt toimuma liidus asuvates ruumides ja suhtlemise teel liidus asuvate ettevõtjatega, sealhulgas kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate poolt käesoleva määruse kohaselt asutatud tütarettevõtjatega. Siiski ei pruugi selline liidus toimuv tegevus olla piisav selleks, et juhtival järelevaatamisasutusel oleks võimalik täielikult ja tõhusalt oma käesolevast määrusest tulenevaid ülesandeid täita. Juhtival järelevaatamisasutusel peaks seetõttu olema võimalik teostada oma asjakohaseid järelevaatamisvolitusi ka kolmandates riikides. Nende volituste teostamine kolmandates riikides peaks võimaldama juhtival järelevaatamisasutusel kontrollida rajatisi, mille kaudu kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja IKT-teenuseid või tehnilise toe teenuseid tegelikult osutab või haldab, ning peaks andma juhtivale järelevaatamisasutusele põhjalikud ja praktilised teadmised kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja IKT-riski juhtimisest. Juhtiva järelevaatamisasutuse kui liidu asutuse võimalus teostada volitusi väljaspool liidu territooriumi peaks olema igakülgselt piiritletud asjakohaste tingimustega, eelkõige asjaomase kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja nõusolekuga. Samuti tuleks kolmanda riigi asjaomaseid ametiasutusi teavitada juhtiva järelevaatamisasutuse tegevusest tema territooriumil ning neil ei tohiks

([21]) Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta direktiiv 2013/34/EL teatavat liiki ettevõtjate aruandeaasta finantsaruannete, konsolideeritud finantsaruannete ja nendega seotud aruannete kohta ja millega muudetakse Euroopa Parlamendi ja nõukogu direktiivi 2006/43/EÜ ning tunnistatakse kehtetuks nõukogu direktiivid 78/660/EMÜ ja 83/349/EMÜ (ELT L 182, 29.6.2013, lk 19).

olla selle suhtes vastuväiteid. Tõhusa rakendamise tagamiseks ning ilma et see piiraks liidu institutsioonide ja liikmesriikide vastavat pädevust, peavad sellised volitused ühtlasi tuginema täielikult halduskoostöö kokkulepetele, mis sõlmitakse asjaomase kolmanda riigi asjakohaste ametiasutustega. Seetõttu peaks käesolev määrus võimaldama Euroopa järelevalveasutustel sõlmida asjakohaste kolmanda riigi ametiasutustega halduskoostöö kokkuleppeid, millega ei tohiks luua muid õiguslikke kohustusi liidu ja selle liikmesriikide jaoks.

(84) Juhtiva järelevaatamisasutusega suhtlemise hõlbustamiseks ja piisava esindatuse tagamiseks peaksid kontserni kuuluvad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad määrama ühe juriidilise isiku oma koordineerimiskeskuseks.

(85) Järelevaatamisraamistik ei tohiks piirata liikmesriikide pädevust teha ise järelevaatamis- või seiremissioone seoses kolmandast isikust IKT-teenuste osutajatega, kes ei ole käesoleva määruse kohaselt määratud kriitilise tähtsusega IKT-teenuste osutajaks, kuid keda võib riiklikul tasandil käsitada olulistena.

(86) Selleks et võimendada finantsteenuste valdkonna mitmetasandilist institutsioonilist ülesehitust, peaks Euroopa järelevalveasutuste ühiskomitee jätkuvalt tagama üldise sektoritevahelise koordineerimise kõigis IKT-riskiga seotud küsimustes kooskõlas oma küberturvalisust puudutavate ülesannetega. Teda peaks toetama uus allkomitee (edaspidi „järelevaatamisfoorum"), kes valmistab ette nii kriitilise tähtsusega kolmandatest isikutest IKT-teenuste osutajatele suunatud individuaalseid otsuseid kui ka ühissoovituste tegemist – eelkõige kriitilise tähtsusega kolmandatest isikutest IKT-teenuste osutajate järelevaatamiskavade võrdlemise kohta – ning teeb kindlaks IKT kontsentratsiooniriskiga seotud probleemide lahendamise parimad tavad.

(87) Selle tagamiseks, et kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle tehtaks liidu tasandil asjakohast ja tõhusat järelevaatamist, sätestatakse käesolevas määruses, et juhtivaks järelevaatamisasutuseks võib määrata ükskõik millise kolmest Euroopa järelevalveasutusest. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja individuaalsel määramisel ühele kolmest Euroopa järelevalveasutusest tuleks lähtuda ülekaaluka osa asjaomase Euroopa järelevalveasutuse vastutusvaldkonda kuuluvates finantssektorites tegutsevate finantssektori ettevõtjate hindamisest. Selline käsitus peaks tagama järelevaatamisfunktsioonide täitmisest johtuvate ülesannete ja kohustuste tasakaalustatud jaotuse kolme Euroopa järelevalveasutuse vahel ning kasutama parimal viisil ära kõigi kolme Euroopa järelevalveasutuse inimressursse ja tehnilisi eksperditeadmisi.

(88) Juhtivatele järelevaatamisasutustele tuleks anda vajalikud volitused, et teha uurimisi, viia kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate ruumides ja asukohtades läbi kohapealseid ja kaugkontrolle ning saada täielikku ja ajakohastatud teavet. Need volitused peaksid võimaldama juhtival järelevaatamisasutusel saada tegeliku ülevaate finantssektori ettevõtjatele ja kokkuvõttes liidu finantssüsteemile kolmandatest isikutest tuleneva IKT-riski liigist, mõõtmest ja mõjust. Euroopa järelevalveasutustele järelevaatamises juhtiva rolli andmine on eeltingimus, et saada aru IKT-riski süsteemsest mõõtmest rahanduses ja seda käsitleda. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate mõju liidu finantssektorile ja kaasnevast IKT kontsentratsiooniriskist tulenevad võimalikud probleemid vajavad kollektiivset käsitlust liidu tasandil. Mitme auditi samaaegne läbiviimine ja pääsuõiguste samaaegne kasutamine eraldi paljude pädevate asutuste poolt nendevahelise vähese koordineerimisega või koordineerimiseta ei võimaldaks finantsjärelevalveasutustel saada liidus kolmandast isikust tulenevast IKT-riskist täielikku ja põhjalikku ülevaadet ning tekitaks ka liiasust, koormust ja keerukust kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele, kui nende kohta esitataks arvukalt seire- ja kontrollitaotlusi.

(89) Kriitilise tähtsusega teenuseosutajaks määramise olulise mõju tõttu tuleks käesoleva määrusega tagada, et kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate õigusi järgitakse kogu järelevaatamisraamistiku rakendamisel. Enne kriitilise tähtsusega teenuseosutajaks määramist peaks sellistel teenuseosutajatel olema näiteks õigus esitada juhtivale järelevaatamisasutusele põhjendatud avaldus, mis sisaldab kogu asjakohast teavet nende määramisega seotud hindamiseks. Kuna juhtival järelevaatamisasutusel peaks olema õigus esitada soovitusi IKT-riski küsimuste ja sobivate parandusmeetmete kohta, mille hulka kuulub õigus esitada vastuväiteid teatavate lepingute suhtes, mis kokkuvõttes mõjutavad finantssektori ettevõtja või finantssüsteemi stabiilsust, tuleks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele samuti anda võimalus esitada enne asjaomaste soovituste lõplikku vormistamist selgitusi, milles käsitletakse soovituses kavandatud lahenduste oodatavat mõju tarbijatele, kes on

käesoleva määruse kohaldamisalast välja jäävad ettevõtjad, ning sõnastada lahendused riskide leevendamiseks. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad, kes ei nõustu soovitustega, peaksid esitama põhjendatud selgituse oma kavatsuse kohta soovitusega mitte nõustuda. Kui sellist põhjendatud selgitust ei esitata või kui seda peetakse ebapiisavaks, peaks juhtiv järelevaatamisasutus avaldama avaliku teate, milles kirjeldatakse kokkuvõtlikult nõuete täitmata jätmist.

(90) Seoses finantssektori ettevõtjate usaldatavusnõuete täitmise järelevalvega peaks pädevate asutuste ülesannete hulka kindlasti kuuluma juhtiva järelevaatamisasutuse antud soovituste sisulise täitmise kontrollimine. Pädevatel asutustel peaks olema võimalik nõuda, et finantssektori ettevõtjad võtaksid lisameetmeid juhtiva järelevaatamisasutuse soovitustes kindlaks tehtud riskide käsitlemiseks, ning nad peaksid esitama aegsasti sellekohased teatised. Kui juhtiv järelevaatamisasutus esitab soovitusi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele, kelle üle tehakse järelevalvet direktiivi (EL) 2022/2555 alusel, peaks pädevatel asutustel olema vabatahtlikkuse alusel ja enne lisameetmete võtmist võimalik konsulteerida kõnealuse direktiivi kohaste pädevate asutustega, et edendada koordineeritud lähenemisviisi kõnealuste kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega tegelemisel.

(91) Järelevaatamise käigus tuleks juhinduda kolmest tegevuspõhimõttest, mille eesmärk on tagada: a) juhtiva järelevaatamisasutuse rolli täitvate Euroopa järelevalveasutuste vaheline tihe koordineerimine ühise järelevaatamisvõrgustiku kaudu; b) kooskõla direktiiviga (EL) 2022/2555 loodud raamistikuga (kõnealuse direktiivi kohaste organite vabatahtliku konsulteerimise kaudu, et vältida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele suunatud meetmete dubleerimist) ning c) hoolsusmeetmete kohaldamine, et minimeerida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate poolt klientidele, kes on käesoleva määruse kohaldamisalast välja jäävad ettevõtjad, osutatavate teenuste katkemise võimalikku riski.

(92) Järelevaatamisraamistik ei tohiks mingil viisil või mingis osas asendada finantssektori ettevõtjatele kehtestatud nõuet juhtida ise riske, mis kaasnevad kolmandast isikust IKT-teenuste osutajate kasutamisega, sealhulgas nende kohustust seirata pidevalt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega sõlmitud lepinguid. Sarnaselt ei tohiks järelevaatamisraamistik mõjutada finantssektori ettevõtjate täielikku vastutust kõigi käesolevas määruses ja asjakohastes finantsteenuseid käsitlevates õigusaktides sätestatud juriidiliste kohustuste järgimise ja täitmise eest.

(93) Selleks et vältida dubleerimist ja kattuvust, peaksid pädevad asutused hoiduma üksi selliste meetmete võtmisest, mille eesmärk on seirata kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate riske, ning nad peaksid sellega seoses tuginema asjakohase juhtiva järelevaatamisasutuse hinnangule. Kõik meetmed tuleks igal juhul eelnevalt koordineerida ja kokku leppida juhtiva järelevaatamisasutusega järelevaatamisraamistiku kohaste ülesannete täitmise kontekstis.

(94) Selleks et edendada ühtlustamist rahvusvahelisel tasandil seoses parimate tavade kasutamisega kolmandast isikust IKT-teenuste osutajate digiriski juhtimise läbivaatamisel ja seirel, tuleks Euroopa järelevalveasutusi julgustada sõlmima koostöökokkuleppeid kolmandate riikide asjaomaste järelevalve- ja reguleerivate asutustega.

(95) Selleks et kasutada ära pädevates asutustes operatsiooni- ja IKT-riskile spetsialiseerunud töötajate eripädevust, tehnilisi oskusi ja eksperditeadmisi, peaksid kolm Euroopa järelevalveasutust ja vabatahtlikkuse alusel direktiivi (EL) 2022/2555 kohased pädevad asutused ning juhtiv järelevaatamisasutus toetuma riikide järelevalvealasele suutlikkusele ja järelevalvealastele teadmistele ning looma spetsiaalsed uurimisrühmad iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja jaoks, moodustades valdkondadevahelisi rühmi, et toetada järelevaatamistegevuse, sealhulgas kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üldiste uurimiste ja kontrollide ning kõigi vajalike järelmeetmete ettevalmistamist ja elluviimist.

(96) Kuigi järelevaatamisülesannetega kaasnevaid kulusid rahastataks täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele kehtestatud tasudest, tekib Euroopa järelevalveasutustel enne järelevaatamisraamistiku tegevuse algust tõenäoliselt kulusid seoses eelseisvat järelevaatamist toetavate sihtotstarbeliste IKT-süsteemide rakendamisega, kuna selliseid sihtotstarbelisi IKT-süsteeme on vaja eelnevalt arendada ja kasutusele võtta. Käesolevas määruses sätestatakse seega hübriidrahastamise mudel, mille kohaselt järelevaatamisraamistikku kui sellist rahastataks täielikult tasudest ning Euroopa järelevalveasutuste IKT-süsteemide arendamist liidu ja riiklike pädevate asutuste osamaksetest.

(97) Pädevatel asutustel peaksid olema kõik nõutavad järelevalve-, uurimis- ja karistuste määramise volitused, et tagada oma käesolevas määruses sätestatud kohustuste nõuetekohane täitmine. Nad peaksid põhimõtteliselt avaldama teateid määratud halduskaristuste kohta. Kuna finantssektori ettevõtjad ja kolmandast isikust IKT-teenuste osutajad võivad olla asutatud eri liikmesriikides ja nende üle võivad järelevalvet teha erinevad pädevad asutused, tuleks käesoleva määruse kohaldamist hõlbustada, tehes ühelt poolt tihedat koostööd asjakohaste pädevate asutuste vahel, sealhulgas EKPga seoses talle nõukogu määrusega (EL) nr 1024/2013 antud eriülesannetega, ning teiselt poolt konsulteerides Euroopa järelevalveasutustega vastastikuse teabevahetuse ja asjakohase järelevalvetegevuse kontekstis abistamise kaudu.

(98) Selleks et täpsustada kolmandast isikust IKT-teenuste osutajate kriitilise tähtsusega teenuseosutajateks määramise kvantitatiivseid ja kvalitatiivseid kriteeriume ja ühtlustada järelevaatamistasusid, peaks komisjonil olema õigus võtta kooskõlas Euroopa Liidu toimimise lepingu artikliga 290 käesoleva määruse täiendamiseks vastu delegeeritud õigusakte, milles täpsustatakse veelgi süsteemset mõju, mida kolmandast isikust IKT-teenuste osutaja maksejõuetuks muutumine või tegevuse katkemine võib avaldada finantssektori ettevõtjatele, kellele ta IKT-teenuseid osutab; selliste globaalsete süsteemselt oluliste ettevõtjate või muude süsteemselt oluliste ettevõtjate arvu, kes sõltuvad asjaomasest kolmandast isikust IKT-teenuste osutajast; konkreetsel turul tegutsevate kolmandast isikust IKT-teenuste osutajate arvu; andmete teise kolmandast isikust IKT-teenuste osutajasse migreerimise ja IKT alase töömahu sinna üleviimise kulusid ning järelevaatamistasude summat ja nende maksmise viisi. On eriti oluline, et komisjon viiks oma ettevalmistava töö käigus läbi asjakohaseid konsultatsioone, sealhulgas ekspertide tasandil, ja et kõnealused konsultatsioonid viidaks läbi kooskõlas 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes ([22]) sätestatud põhimõtetega. Eelkõige selleks, et tagada delegeeritud õigusaktide ettevalmistamises võrdne osalemine, peaksid Euroopa Parlament ja nõukogu saama kõik dokumendid liikmesriikide ekspertidega samal ajal ning nende ekspertidel peaks olema pidev juurdepääs komisjoni eksperdirühmade koosolekutele, millel arutatakse delegeeritud õigusaktide ettevalmistamist.

(99) Regulatiivsed tehnilised standardid peaksid tagama käesolevas määruses sätestatud nõuete järjepideva ühtlustamise. Asutustena, kellel on põhjalikud eriteadmised, peaksid Euroopa järelevalveasutused töötama komisjonile esitamiseks välja regulatiivsete tehniliste standardite eelnõud, mis ei hõlma poliitilisi valikuid. Regulatiivsed tehnilised standardid tuleks töötada välja IKT-riski juhtimise, tõsistest IKT intsidentidest teatamise ja testimise valdkonnas ning seoses kolmandatest isikutest tuleneva IKT-riski usaldusväärse seire põhinõuetega. Komisjon ja Euroopa järelevalveasutused peaksid tagama, et kõik finantssektori ettevõtjad saavad kõnealuseid standardeid ja nõudeid kohaldada viisil, mis on proportsionaalne nende suuruse ja üldise riskiprofiiliga, nende teenuste, tegevuse ja toimingute laadi, ulatuse ja keerukusega. Komisjonil peaks olema õigus võtta need regulatiivsed tehnilised standardid vastu rakendusaktidega vastavalt ELi toimimise lepingu artiklile 290 ning kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

(100) Selleks et soodustada tõsistest IKT intsidentidest ja tegevust või turvalisust mõjutavate maksetega seotud tõsistest intsidentidest teavitamise raportite võrreldavust ning tagada läbipaistvus seoses lepingutega, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate IKT-teenuste kasutamist, peaksid Euroopa järelevalveasutused töötama välja rakenduslike tehniliste standardite eelnõud, millega kehtestatakse finantssektori ettevõtjate jaoks standardmallid, -vormid ja -menetlused tõsisest IKT intsidendist ja tegevust või turvalisust mõjutavast maksetega seotud tõsisest intsidendist teavitamiseks ning standardmallid teaberegistri jaoks. Nende standardite väljatöötamisel peaksid Euroopa järelevalveasutused võtma arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust. Komisjonil peaks olema õigus võtta need rakenduslikud tehnilised standardid vastu rakendusaktidega vastavalt ELi toimimise lepingu artiklile 291 ning kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 15.

([22]) ELT L 123, 12.5.2016, lk 1.

(101) Kuna Euroopa Parlamendi ja nõukogu määrustes (EÜ) nr 1060/2009, ([23]) (EL) nr 648/2012, ([24]) (EL) nr 600/2014 ([25]) ja (EL) nr 909/2014 ([26]) sisalduvatel regulatiivsetel ja rakenduslikel tehnilistel standarditel põhinevate delegeeritud õigusaktide ja rakendusaktidega on juba täpsustatud täiendavaid nõudeid, on asjakohane anda Euroopa järelevalveasutustele kas individuaalsed või ühiskomitee kaudu ühised volitused esitada komisjonile regulatiivsed ja rakenduslikud tehnilised standardid selliste delegeeritud õigusaktide ja rakendusaktide vastuvõtmiseks, millega võetakse üle ja ajakohastatakse kehtivaid IKT-riski juhtimise norme.

(102) Kuna käesoleva määrusega ning Euroopa Parlamendi ja nõukogu direktiiviga (EL) 2022/2556 ([27]) kaasneb täieliku kooskõla tagamiseks selliste IKT-riski juhtimist käsitlevate sätete konsolideerimine, mis sisalduvad mitmes liidu finantsteenuste õigustiku määruses ja direktiivis, sealhulgas määrustes (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014 ja (EL) nr 909/2014 ning Euroopa Parlamendi ja nõukogu määruses (EL) 2016/1011, ([28]) tuleks kõnealuseid määruseid muuta selgitamaks, et kohaldatavad IKT-riskiga seotud sätted on sätestatud käesolevas määruses.

(103) Sellest tulenevalt tuleks kitsendada selliste operatsiooniriskiga seotud asjakohaste artiklite kohaldamisala, mille kohaselt võeti määrustes (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 sätestatud õiguse alusel vastu delegeeritud õigusakte ja rakendusakte, pidades silmas eesmärki tuua käesolevasse määrusesse üle kõik digitaalse tegevuskerksuse aspekte hõlmavad sätted, mis praegu sisalduvad kõnealustes määrustes.

(104) Potentsiaalset süsteemset küberriski, mis on seotud selliste IKT-taristute kasutamisega, mis võimaldavad maksesüsteemide toimimist ja maksete töötlemise toimingute osutamist, tuleks liidu tasandil igakülgselt käsitleda digitaalse kerksuse ühtlustatud normides. Selleks peaks komisjon kiiresti hindama vajadust vaadata läbi käesoleva määruse kohaldamisala, viies sellise läbivaatamise kooskõlla direktiivis (EL) 2015/2366 ette nähtud põhjaliku läbivaatamise tulemustega. Viimasel kümnendil toimunud arvukad ulatuslikud ründed näitavad, et maksesüsteemid on muutunud avatuks küberohtudele. Maksesüsteemid ja maksete töötlemise toimingud on omandanud liidu finantsturgude toimimise jaoks kriitilise tähtsuse, olles makseteenuste ahelas kesksel kohal ja tugevalt seotud üldise finantssüsteemiga. Selliste süsteemide vastu suunatud küberründed võivad põhjustada tõsiseid äritegevuse häireid, millel on otsene mõju peamistele majandusfunktsioonidele, nagu maksete hõlbustamine, ja kaudne mõju seotud majandusprotsessidele. Kuni liidu tasandil ei ole kehtestatud ühtlustatud korda ning maksesüsteemide käitajate ja töötlevate ettevõtjate järelevalvet, võivad liikmesriigid sarnaste turutavade kohaldamiseks võtta eeskuju käesolevas määruses sätestatud digitaalse tegevuskerksuse nõuetest, kui nad kohaldavad norme selliste maksesüsteemide käitajate ja töötlevate ettevõtjate suhtes, kelle üle tehakse järelevalvet nende enda jurisdiktsioonis.

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

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

([25]) Euroopa Parlamendi ja nõukogu 15. mai 2014. aasta määrus (EL) nr 600/2014 finantsinstrumentide turgude kohta ning millega muudetakse määrust (EL) nr 648/2012 (ELT L 173, 12.6.2014, lk 84).

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

([27]) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta direktiiv (EL) 2022/2556, millega muudetakse direktiive 2009/65/EÜ, 2009/138/EÜ, 2011/61/EL, 2013/36/EL, 2014/59/EL, 2014/65/EL, (EL) 2015/2366 ja (EL) 2016/2341 seoses finantssektori digitaalse tegevuskerksusega (vt käesoleva *Euroopa Liidu Teataja* lk 153).

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

(105) Kuna käesoleva määruse eesmärki, nimelt reguleeritud finantssektori ettevõtjate kõrge digitaalse tegevuskerksuse taseme saavutamine, ei suuda liikmesriigid piisavalt saavutada, sest see eeldab paljude erinevate liidu ja riiklike õigusnormide ühtlustamist, küll aga saab seda meetme ulatuse ja toime tõttu paremini saavutada liidu tasandil, võib liit võtta meetmeid kooskõlas Euroopa Liidu lepingu artiklis 5 sätestatud subsidiaarsuse põhimõttega. Kõnealuses artiklis sätestatud proportsionaalsuse põhimõtte kohaselt ei lähe käesolev määrus nimetatud eesmärgi saavutamiseks vajalikust kaugemale.

(106) Euroopa Andmekaitseinspektoriga konsulteeriti kooskõlas Euroopa Parlamendi ja nõukogu määruse (EL) 2018/1725 ([29]) artikli 42 lõikega 1 ning ta esitas arvamuse 10. mail 2021, ([30])

ON VASTU VÕTNUD KÄESOLEVA MÄÄRUSE:

I PEATÜKK

Üldsätted

Artikkel 1

Reguleerimisese

1. Digitaalse tegevuskerksuse ühtlaselt kõrge taseme saavutamiseks sätestatakse käesolevas määruses ühetaolised nõuded, mis käsitlevad finantssektori ettevõtjate äriprotsesse toetavate võrgu- ja infosüsteemide turvalisust:

a) finantssektori ettevõtjate suhtes kohaldatavad nõuded, mis puudutavad

   i) info- ja kommunikatsioonitehnoloogia (IKT) riskide juhtimist;

   ii) pädevate asutuste teavitamist tõsistest IKT intsidentidest ja vabatahtlikkuse alusel olulistest küberohtudest;

   iii) artikli 2 lõike 1 punktides a–d osutatud finantssektori ettevõtjate poolt pädevate asutuste teavitamist tegevust või turvalisust mõjutavatest maksetega seotud tõsistest intsidentidest;

   iv) digitaalse tegevuskerksuse testimist;

   v) küberohte ja -nõrkust puudutava teabe ja teadmuse jagamist;

   vi) meetmeid kolmandast isikust tuleneva IKT-riski usaldusväärseks juhtimiseks;

b) kolmandast isikust IKT-teenuste osutajate ja finantssektori ettevõtjate vahel sõlmitud lepinguid käsitlevad nõuded;

c) normid järelevaatamisraamistiku loomiseks ja toimimiseks selliste kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate jaoks, kes osutavad teenuseid finantssektori ettevõtjatele;

d) normid, mis käsitlevad pädevate asutuste koostööd ning pädevate asutuste poolset järelevalvet ja nõuete täitmise tagamist kõigis käesoleva määrusega hõlmatud küsimustes.

2. Mis puudutab finantssektori ettevõtjaid, keda käsitatakse elutähtsate või oluliste üksustena vastavalt riigisisestele õigusnormidele, millega on üle võetud direktiivi (EL) 2022/2555 artikkel 3, siis käesolevat määrust käsitatakse nimetatud direktiivi artikli 4 kohaldamisel valdkondliku liidu õigusaktina.

3. Käesoleva määrusega ei piirata liikmesriikide vastutust seoses riigi põhifunktsioonidega avaliku julgeoleku, riigikaitse ja riikliku julgeoleku tagamisel kooskõlas liidu õigusega.

([29]) Euroopa Parlamendi ja nõukogu 23. oktoobri 2018. aasta määrus (EL) 2018/1725, mis käsitleb füüsiliste isikute kaitset isikuandmete töötlemisel liidu institutsioonides, organites ja asutustes ning isikuandmete vaba liikumist, ning millega tunnistatakse kehtetuks määrus (EÜ) nr 45/2001 ja otsus nr 1247/2002/EÜ (ELT L 295, 21.11.2018, lk 39).

([30]) ELT C 229, 15.6.2021, lk 16.

Artikkel 2

Kohaldamisala

1. Ilma et see piiraks lõigete 3 ja 4 kohaldamist, kohaldatakse käesolevat määrust järgmiste üksuste suhtes:

a) krediidiasutused;

b) makseasutused, sealhulgas sellised makseasutused, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 kohast erandit;

c) kontoteabe teenuse pakkujad;

d) e-raha asutused, sealhulgas sellised e-raha asutused, mille suhtes kohaldatakse direktiivi 2009/110/EÜ kohast erandit;

e) investeerimisühingud;

f) krüptovarateenuse osutajad, kes on saanud tegevusloa vastavalt Euroopa Parlamendi ja nõukogu määrusele, mis käsitleb krüptovaraturge ning millega muudetakse määruseid (EL) nr 1093/2010 ja (EL) nr 1095/2010 ja direktiive 2013/36/EL ja (EL) 2019/1937 (edaspidi „krüptovaraturgude määrus“), ja varapõhiste tokenite emitendid;

g) väärtpaberite keskdepositooriumid;

h) kesksed vastaspooled;

i) kauplemiskohad;

j) kauplemisteabehoidlad;

k) alternatiivsete investeerimisfondide valitsejad;

l) fondivalitsejad;

m) aruandlusteenuste pakkujad;

n) kindlustus- ja edasikindlustusandjad;

o) kindlustusvahendajad, edasikindlustusvahendajad ja kõrvaltegevusena pakutava kindlustuse vahendajad;

p) tööandja kogumispensioni asutused;

q) reitinguagentuurid;

r) kriitilise tähtsusega võrdlusaluste haldurid;

s) ühisrahastusteenuse osutajad;

t) väärtpaberistamise registrid;

u) kolmandast isikust IKT-teenuste osutajad.

2. Käesoleva määruse kohaldamisel nimetatakse lõike 1 punktides a–t osutatud üksusi koos finantssektori ettevõtjateks.

3. Käesolevat määrust ei kohaldata järgmiste suhtes:

a) direktiivi 2011/61/EL artikli 3 lõikes 2 osutatud alternatiivsete investeerimisfondide valitsejad;

b) direktiivi 2009/138/EÜ artiklis 4 osutatud kindlustus- ja edasikindlustusandjad;

c) tööandja kogumispensioni asutused, mis haldavad pensioniskeeme, millel ei ole kokku rohkem kui 15 liiget;

d) füüsilised või juriidilised isikud, kelle suhtes kohaldatakse direktiivi 2014/65/EL artiklite 2 ja 3 kohast erandit;

e) kindlustusvahendajad, edasikindlustusvahendajad ja kõrvaltegevusena pakutava kindlustuse vahendajad, kes on mikroettevõtjad või väikesed või keskmise suurusega ettevõtjad;

f) direktiivi 2013/36/EL artikli 2 lõike 5 punktis 3 osutatud postižiiroasutused.

4. Liikmesriigid võivad käesoleva määruse kohaldamisalast välja arvata direktiivi 2013/36/EL artikli 2 lõike 5 punktides 4–23 osutatud üksused, mis asuvad nende vastaval territooriumil. Kui liikmesriik seda võimalust kasutab, teatab ta sellest ja kõigist hilisematest muudatustest komisjonile. Komisjon teeb selle teabe üldsusele kättesaadavaks oma veebisaidil või muul kergesti juurdepääsetaval viisil.

Artikkel 3

Mõisted

Käesolevas määruses kasutatakse järgmisi mõisteid:

1) „digitaalne tegevuskerksus“ – finantssektori ettevõtja suutlikkus luua, tagada ja vaadata läbi oma tegevuse terviklikkust ja usaldusväärsust, tagades kas otseselt või kaudselt kolmandast isikust IKT-teenuste osutajate pakutavate teenuste kasutamise kaudu kogu IKTga seotud suutlikkuse, mida on vaja selliste võrgu- ja infosüsteemide turvalisuse käsitlemiseks, mida finantssektori ettevõtja kasutab ning mis toetavad finantsteenuste jätkuvat osutamist ja nende kvaliteeti, sealhulgas katkestuste vältel;

2) „võrgu- ja infosüsteem“ – direktiivi (EL) 2022/2555 artikli 6 punktis 1 määratletud võrgu- ja infosüsteem;

3) „IKT pärandsüsteem“ – IKT-süsteem, mis on jõudnud oma elutsükli lõppu (ealõpp), mis tehnoloogilistel või ärilistel põhjustel ei sobi uuendusteks või parandusteks või mida selle tarnija või kolmandast isikust IKT-teenuste osutaja enam ei toeta, kuid mis on endiselt kasutusel ja toetab finantssektori ettevõtja funktsioone;

4) „võrgu- ja infosüsteemide turvalisus“ – direktiivi (EL) 2022/2555 artikli 6 punktis 2 määratletud võrgu- ja infosüsteemide turvalisus;

5) „IKT-risk“ – mõistlikult tuvastatav asjaolu võrgu- ja infosüsteemide kasutamisel, mis realiseerumise korral võib seada ohtu võrgu- ja infosüsteemide, tehnoloogiast sõltuva vahendi või protsessi, operatsioonide ja protsesside või teenuste osutamise turvalisuse, avaldades negatiivset mõju digitaalsele või füüsilisele keskkonnale;

6) „teabevara“ – materiaalne või mittemateriaalne teabekogu, mida tasub kaitsta;

7) „IKT-vara“ – finantssektori ettevõtja kasutatavates võrgu- ja infosüsteemides sisalduva tark- või riistvara komponent;

8) „IKT intsident“ – finantssektori ettevõtja poolt planeerimata üksiksündmus või omavahel seotud sündmuste jada, mis seab ohtu võrgu- ja infosüsteemide turvalisuse ning mis avaldab negatiivset mõju andmete kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele või finantssektori ettevõtja osutatavatele teenustele;

9) „tegevust või turvalisust mõjutav maksetega seotud intsident“ – artikli 2 lõike 1 punktides a–d osutatud finantssektori ettevõtjate poolt planeerimata üksiksündmus või omavahel seotud sündmuste jada, mis avaldab negatiivset mõju maksete andmete kättesaadavusele, autentsusele, terviklusele või konfidentsiaalsusele või finantssektori ettevõtja osutatud maksetega seotud teenustele, olenemata sellest, kas need sündmused on IKTga seotud;

10) „tõsine IKT intsident“ – IKT intsident, millel on suur negatiivne mõju võrgu- ja infosüsteemidele, mis toetavad finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone;

11) „tegevust või turvalisust mõjutav maksetega seotud tõsine intsident“ – tegevust või turvalisust mõjutav maksetega seotud intsident, mis avaldab suurt negatiivset mõju osutatud maksetega seotud teenustele;

12) „küberoht“ –määruse (EL) 2019/881 artikli 2 punktis 8 määratletud küberoht;

13) „oluline küberoht“ – küberoht, mille tehnilised tunnused näitavad, et selle tulemuseks võib olla tõsine IKT intsident või tegevust või turvalisust mõjutav maksetega seotud tõsine intsident;

14) „küberrünne“ – IKTga seotud pahatahtlik intsident, mille on põhjustanud ohusubjekti katse hävitada, paljastada, muuta, desaktiveerida või varastada vara, saada varale loata juurdepääs või kasutada vara ilma loata;

15) „ohuteadmus“ – teave, mida on agregeeritud, teisendatud, analüüsitud, tõlgendatud või rikastatud, et anda otsuste tegemiseks vajalik kontekst ning tagada asjakohane ja piisav arusaamine IKT intsidendi või küberohu mõju leevendamiseks, sealhulgas küberründe tehnilised üksikasjad, ründe eest vastutavad isikud ning nende töömeetodid ja ajendid;

16) „nõrkus“ – vara, süsteemi, protsessi või kontrolli nõrkus, tundlikkus või viga, mida võidakse ära kasutada;

17) „ohuteabel põhinev läbistustestimine“ – tingimused, mis matkivad taktikat, võtteid ja menetlusi, mida kasutavad tegelikud ohusubjektid, keda tajutakse tegeliku küberohu tekitajatena, ning mis võimaldavad teha finantssektori ettevõtja kriitilise tähtsusega töötavate tarbesüsteemide kontrollitud, kohandatud, teadmuspõhise (punane tiim) testi;

18) „kolmandast isikust tulenev IKT-risk“ – IKT-risk, mis võib finantssektori ettevõtjat ohustada, kui ta kasutab kolmandast isikust IKT-teenuste osutajate või nende alltöövõtjate IKT-teenuseid, sealhulgas tegevuse edasiandmise lepingute kaudu;

19) „kolmandast isikust IKT-teenuste osutaja“ – ettevõtja, kes osutab IKT-teenuseid;

20) „kontsernisisene IKT-teenuste osutaja“ – finantskontserni kuuluv ettevõtja, kes osutab peamiselt IKT-teenuseid samasse kontserni kuuluvatele finantssektori ettevõtjatele või samasse finantsinstitutsioonide kaitseskeemi kuuluvatele finantssektori ettevõtjatele, sealhulgas nende emaettevõtjatele, tütarettevõtjatele, filiaalidele või muudele üksustele, mis on ühises omandis või ühise kontrolli all;

21) „IKT-teenused“ – digi- ja andmeteenused, mida osutatakse pidevalt IKT-süsteemide kaudu ühele või mitmele sise- või väliskasutajale, sealhulgas riistvara teenusena ja riistvarateenused, mis hõlmab tehnilise toe pakkumist riistvara pakkuja tarkvara- või püsivarauuenduste kaudu, välja arvatud tavapärased analoogtelefoniteenused;

22) „kriitilise tähtsusega või oluline funktsioon“ – funktsioon, mille katkestus kahjustaks oluliselt finantssektori ettevõtja finantstulemusi või tema teenuste ja tegevuse usaldusväärsust või jätkuvust, või selle funktsiooni häiritud, vigane või ebaõnnestunud täitmine kahjustaks oluliselt finantssektori ettevõtja tegevusloast tulenevate tingimuste ja kohustuste või tema muude, kohaldatava finantsteenuseid käsitleva õiguse kohaste kohustuste jätkuvat täitmist;

23) „kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja“ – kolmandast isikust IKT-teenuste osutaja, kes määratakse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaks vastavalt artiklile 31;

24) „kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutaja“ – kolmandast isikust IKT-teenuste osutaja, kes on kolmandas riigis asutatud juriidiline isik, kes on sõlminud finantssektori ettevõtjaga IKT-teenuste osutamiseks lepingu;

25) „tütarettevõtja“ – tütarettevõtja direktiivi 2013/34/EL artikli 2 punkti 10 ja artikli 22 tähenduses;

26) „kontsern“ – direktiivi 2013/34/EL artikli 2 punktis 11 määratletud kontsern;

27) „emaettevõtja“ – emaettevõtja direktiivi 2013/34/EL artikli 2 punkti 9 ja artikli 22 tähenduses;

28) „kolmandas riigis asutatud IKT alltöövõtja“ – IKT alltöövõtja, kes on kolmandas riigis asutatud juriidiline isik, kes on sõlminud lepingu kolmandast isikust IKT-teenuste osutajaga või kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajaga;

29) „IKT kontsentratsioonirisk“ – suhe ühe või mitme seotud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaga, mis tekitab nendest teenuseosutajatest teatava sõltuvuse, nii et juhul, kui kõnealused teenuseosutajad ei ole kättesaadavad, muutuvad maksejõuetuks või omavad muid puudusi, võib sattuda ohtu finantssektori ettevõtja suutlikkus täita kriitilise tähtsusega või olulisi funktsioone või tulla toime muud liiki negatiivse mõju, sealhulgas suure kahjuga, või võib sattuda ohtu liidu kui terviku finantsstabiilsus;

30) „juhtorgan“ – direktiivi 2014/65/EL artikli 4 lõike 1 punktis 36, direktiivi 2013/36/EL artikli 3 lõike 1 punktis 7, Euroopa Parlamendi ja nõukogu direktiivi 2009/65/EÜ ([31]) artikli 2 lõike 1 punktis s, määruse (EL) nr 909/2014 artikli 2 lõike 1 punktis 45, määruse (EL) 2016/1011 artikli 3 lõike 1 punktis 20 ning krüptovaraturgude määruse asjakohases sättes määratletud juhtorgan või vastavad isikud, kes tegelikult juhivad üksust või täidavad põhifunktsioone kooskõlas liidu või liikmesriikide asjakohase õigusega;

31) „krediidiasutus“ – Euroopa Parlamendi ja nõukogu määruse (EL) nr 575/2013 ([32]) artikli 4 lõike 1 punktis 1 määratletud krediidiasutus;

32) „asutus, mille suhtes kohaldatakse direktiivi 2013/36/EL kohast erandit“ – direktiivi 2013/36/EL artikli 2 lõike 5 punktides 4–23 osutatud üksused;

33) „investeerimisühing“ – direktiivi 2014/65/EL artikli 4 lõike 1 punktis 1 määratletud investeerimisühing;

34) „väike ja mitteseotud investeerimisühing“ – investeerimisühing, mis vastab Euroopa Parlamendi ja nõukogu määruse (EL) 2019/2033 ([33]) artikli 12 lõikes 1 sätestatud tingimustele;

35) „makseasutus“ – direktiivi (EL) 2015/2366 artikli 4 punktis 4 määratletud makseasutus;

36) „makseasutus, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 kohast erandit“ – makseasutus, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 artikli 32 lõike 1 kohast erandit;

37) „kontoteabe teenuse pakkuja“ – direktiivi (EL) 2015/2366 artikli 33 lõikes 1 osutatud kontoteabe teenuse pakkuja;

38) „e-raha asutus“ – direktiivi 2009/110/EÜ artikli 2 punktis 1 määratletud e-raha asutus;

39) „e-raha asutus, mille suhtes kohaldatakse direktiivi 2009/110/EÜ kohast erandit“ – e-raha asutus, mille suhtes kohaldatakse direktiivi 2009/110/EÜ artikli 9 lõike 1 kohast erandit;

40) „keskne vastaspool“ – määruse (EL) nr 648/2012 artikli 2 punktis 1 määratletud keskne vastaspool;

41) „kauplemisteabehoidla“ – määruse (EL) nr 648/2012 artikli 2 punktis 2 määratletud kauplemisteabehoidla;

42) „väärtpaberite keskdepositoorium“ – määruse (EL) nr 909/2014 artikli 2 lõike 1 punktis 1 määratletud väärtpaberite keskdepositoorium;

43) „kauplemiskoht“ – direktiivi 2014/65/EL artikli 4 lõike 1 punktis 24 määratletud kauplemiskoht;

44) „alternatiivse investeerimisfondi valitseja“ – direktiivi 2011/61/EL artikli 4 lõike 1 punktis b määratletud alternatiivse investeerimisfondi valitseja;

45) „fondivalitseja“ – direktiivi 2009/65/EÜ artikli 2 lõike 1 punktis b määratletud fondivalitseja;

46) „aruandlusteenuse pakkuja“ – aruandlusteenuse pakkuja määruse (EL) nr 600/2014 tähenduses, nagu on osutatud selle artikli 2 lõike 1 punktides 34–36;

47) „kindlustusandja“ – direktiivi 2009/138/EÜ artikli 13 punktis 1 määratletud kindlustusandja;

48) „edasikindlustusandja“ – direktiivi 2009/138/EÜ artikli 13 punktis 4 määratletud edasikindlustusandja;

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

([32]) Euroopa Parlamendi ja nõukogu 26. juuni 2013. aasta määrus (EL) nr 575/2013, mis käsitleb krediidiasutuste suhtes kohaldatavaid usaldatavusnõudeid ja millega muudetakse määrust (EL) nr 648/2012 (ELT L 176, 27.6.2013, lk 1).

([33]) Euroopa Parlamendi ja nõukogu 27. novembri 2019. aasta määrus (EL) 2019/2033, mis käsitleb investeerimisühingute suhtes kohaldatavaid usaldatavusnõudeid ning millega muudetakse määrusi (EL) nr 1093/2010, (EL) nr 575/2013, (EL) nr 600/2014 ja (EL) nr 806/2014 (ELT L 314, 5.12.2019, lk 1).

49) „kindlustusvahendaja“ – Euroopa Parlamendi ja nõukogu direktiivi (EL) 2016/97 ([34]) artikli 2 lõike 1 punktis 3 määratletud kindlustusvahendaja;

50) „kõrvaltegevusena pakutava kindlustuse vahendaja“ – direktiivi (EL) 2016/97 artikli 2 lõike 1 punktis 4 määratletud kõrvaltegevusena pakutava kindlustuse vahendaja;

51) „edasikindlustusvahendaja“ – direktiivi (EL) 2016/97 artikli 2 lõike 1 punktis 5 määratletud edasikindlustusvahendaja;

52) „tööandja kogumispensioni asutus“ – direktiivi (EL) 2016/2341 artikli 6 punktis 1 määratletud tööandja kogumispensioni asutus;

53) „väike tööandja kogumispensioni asutus“ – tööandja kogumispensioni asutus, mis haldab pensioniskeeme, millel on kokku vähem kui 100 liiget;

54) „reitinguagentuur“ – määruse (EÜ) nr 1060/2009 artikli 3 lõike 1 punktis b määratletud reitinguagentuur;

55) „krüptovarateenuse osutaja“ – krüptovaraturgude määruse asjakohases sättes määratletud krüptovarateenuse osutaja;

56) „varapõhiste tokenite emitent“ – krüptovaraturgude määruse asjakohases sättes määratletud varapõhiste tokenite emitent;

57) „kriitilise tähtsusega võrdlusaluse haldur“ – määruse (EL) 2016/1011 artikli 3 lõike 1 punktis 25 määratletud kriitilise tähtsusega võrdlusaluse haldur;

58) „ühisrahastusteenuse osutaja“ – Euroopa Parlamendi ja nõukogu määruse (EL) 2020/1503 ([35]) artikli 2 lõike 1 punktis e määratletud ühisrahastusteenuse osutaja;

59) „väärtpaberistamise register“ – Euroopa Parlamendi ja nõukogu määruse (EL) 2017/2402 ([36]) artikli 2 punktis 23 määratletud väärtpaberistamise register;

60) „mikroettevõtja“ – finantssektori ettevõtja, kes ei ole kauplemiskoht, keskne vastaspool, kauplemisteabehoidla ega väärtpaberite keskdepositoorium, kus töötab vähem kui 10 inimest ning kelle aastakäive ja/või aastabilansi kogumaht ei ületa 2 miljonit eurot;

61) „juhtiv järelevaatamisasutus“ – käesoleva määruse artikli 31 lõike 1 punkti b kohaselt määratud Euroopa järelevalveasutus;

62) „ühiskomitee“ – määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklis 54 osutatud komitee;

63) „väikeettevõtja“ – finantssektori ettevõtja, kus töötab 10 või rohkem inimest, kuid vähem kui 50 inimest ja kelle aastakäive ja/või aastabilansi kogumaht ületab 2 miljonit eurot, kuid ei ületa 10 miljonit eurot;

64) „keskmise suurusega ettevõtja“ – finantssektori ettevõtja, kes ei ole väikeettevõtja ja kus töötab vähem kui 250 inimest ning kelle aastakäive ei ületa 50 miljonit eurot ja/või aastabilanss ei ületa 43 miljonit eurot;

65) „avaliku sektori asutus“ – valitsusüksus või muu avaliku halduse üksus, sealhulgas riikide keskpangad.

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

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

([36]) Euroopa Parlamendi ja nõukogu 12. detsembri 2017. aasta määrus (EL) 2017/2402, millega kehtestatakse väärtpaberistamise üldnormid ning luuakse lihtsa, läbipaistva ja standarditud väärtpaberistamise erinormid ning millega muudetakse direktiive 2009/65/EÜ, 2009/138/EÜ ja 2011/61/EL ning määrusi (EÜ) nr 1060/2009 ja (EL) nr 648/2012 (ELT L 347, 28.12.2017, lk 35).

Artikkel 4

Proportsionaalsuse põhimõte

1. Finantssektori ettevõtjad rakendavad II peatükis sätestatud norme kooskõlas proportsionaalsuse põhimõttega, võttes arvesse oma suurust ja üldist riskiprofiili ning oma teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust.

2. Lisaks kohaldavad finantssektori ettevõtjad III ja IV peatükki ning V peatüki I jagu proportsionaalselt oma suuruse ja üldise riskiprofiiliga ning oma teenuste, tegevuse ja toimingute laadi, ulatuse ja keerukusega, nagu on konkreetselt sätestatud kõnealuste peatükkide asjakohastes normides.

3. Pädevad asutused hindavad proportsionaalsuse põhimõtte kohaldamist finantssektori ettevõtjate poolt, kui nad vaatavad läbi IKT-riski juhtimise raamistiku järjepidevuse, tuginedes aruannetele, mis esitatakse pädevate asutuste taotlusel vastavalt artikli 6 lõikele 5 ja artikli 16 lõikele 2.

II PEATÜKK

IKT-riski juhtimine

I jagu

Artikkel 5

Juhtimine ja organisatsioon

1. Finantssektori ettevõtjatel peab olema sisemine juhtimis- ja kontrolliraamistik, mis tagab IKT-riski tulemusliku ja usaldusväärse juhtimise kooskõlas artikli 6 lõikega 4, et saavutada digitaalse tegevuskerksuse kõrge tase.

2. Finantssektori ettevõtja juhtorgan määrab kindlaks ja kiidab heaks kõigi artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistikuga seotud kokkulepete rakendamise, korraldab selle üle järelevaatamise ja on selle eest vastutav.

Esimese lõigu kohaldamisel juhtorgan

a) vastutab lõplikult finantssektori ettevõtja IKT-riski juhtimise eest;

b) kehtestab põhimõtted, mille eesmärk on tagada igal ajal andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse säilitamise ranged standardid;

c) määrab kõigi IKTga seotud funktsioonide puhul kindlaks selged rollid ja vastutusvaldkonnad ning kehtestab asjakohase juhtimiskorra, et tagada tõhus ja õigeaegne teabevahetus, koostöö ja koordineerimine nende funktsioonide vahel;

d) vastutab üldiselt artikli 6 lõikes 8 osutatud digitaalse tegevuskerksuse strateegia kehtestamise ja heakskiitmise eest, sealhulgas IKT-riski puhul finantssektori ettevõtjale sobiva riskitaluvustaseme kindlaksmääramise eest, nagu on osutatud artikli 6 lõike 8 punktis b;

e) kiidab heaks finantssektori ettevõtja IKT talitluspidevuse põhimõtted ja IKT reageerimis- ja taastekavad, millele on osutatud vastavalt artikli 11 lõigetes 1 ja 3 ja mille võib vastu võtta eriomase korrana, mis on finantssektori ettevõtja üldiste talitluspidevuse põhimõtete ja reageerimis- ja taastekava lahutamatu osa, korraldab nende üle järelevaatamist ja vaatab nende rakendamise perioodiliselt läbi;

f) kiidab heaks ja vaatab perioodiliselt läbi finantssektori ettevõtja IKT siseauditikavad, IKT auditid ja nende olulised muudatused;

g) näeb ette ja vaatab perioodiliselt läbi sobiva eelarve finantssektori ettevõtja digitaalse tegevuskerksuse vajaduste rahuldamiseks, pidades silmas igat liiki ressursse, sealhulgas artikli 13 lõikes 6 osutatud asjakohased IKT-turbe teadlikkuse suurendamise programmid ja digitaalse tegevuskerksuse koolitused ning kõigi töötajate IKT-oskused;

h) kiidab heaks ja vaatab perioodiliselt läbi finantssektori ettevõtja põhimõtted kokkulepete kohta, mis käsitlevad kolmandast isikust IKT-teenuste osutajate osutatavate IKT-teenuste kasutamist;

i) loob organisatsiooni tasandil aruandluskanalid, et olla kõigiti teavitatud järgmisest:

i) kolmandast isikust IKT-teenuste osutajatega sõlmitud kokkulepped, mis käsitlevad IKT-teenuste kasutamist;

ii) kõik asjakohased kavandatud olulised muudatused, mis on seotud kolmandast isikust IKT-teenuste osutajatega;

iii) kõnealuste muudatuste võimalik mõju kriitilise tähtsusega või olulistele funktsioonidele, mille suhtes kohaldatakse kõnealuseid kokkuleppeid, sealhulgas riskianalüüside kokkuvõte, et hinnata nende muudatuste mõju, ning vähemalt tõsised IKT intsidendid ja nende mõju ning reageerimis-, taaste- ja parandusmeetmed.

3. Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, loovad funktsiooni, mille eesmärk on seirata kolmandast isikust IKT-teenuste osutajatega sõlmitud IKT-teenuste kasutamise kokkuleppeid, või annavad kõrgema juhtkonna liikmele vastutuse vaadata seonduva riski ja asjakohaste dokumentide järele.

4. Finantssektori ettevõtja juhtorgani liikmed hoiavad end aktiivselt kursis teadmiste ja oskustega, mis on piisavad selleks, et mõista ja hinnata IKT-riski ning selle mõju finantssektori ettevõtja tegevusele, muu hulgas käies korrapäraselt erikoolitustel, mis vastavad hallatavale IKT-riskile.

II jagu

Artikkel 6

IKT-riski juhtimise raamistik

1. Finantssektori ettevõtjatel on üldise riskide juhtimise süsteemi osana usaldusväärne, laiahaardeline ja hästi dokumenteeritud IKT-riski juhtimise raamistik, mis võimaldab neil käsitleda IKT-riski kiiresti, tõhusalt ja laiahaardeliselt ning tagada kõrgel tasemel digitaalne tegevuskerksus.

2. IKT-riski juhtimise raamistik sisaldab vähemalt neid strateegiaid, põhimõtteid ja menetlusi ning IKT-protokolle ja -vahendeid, mida on vaja, kaitsmaks nõuetekohaselt ja piisavalt kõiki teabevarasid ja IKT-varasid, sealhulgas tarkvara, riistvara ja servereid, ning kaitsmaks kõiki asjaomaseid füüsilisi komponente ja taristuid, nagu ruumid, andmekeskused ja tundlikud määratud alad, et tagada, et kõik teabevarad ja IKT-varad on riskide, sealhulgas kahju ja loata juurdepääsu või kasutamise eest piisavalt kaitstud.

3. Finantssektori ettevõtjad minimeerivad oma IKT-riski juhtimise raamistiku kohaselt IKT-riski mõju, võttes kasutusele asjakohased strateegiad, põhimõtted, menetlused, IKT-protokollid ja -vahendid. Nad esitavad taotluse korral pädevatele asutustele täieliku ja ajakohastatud teabe IKT-riski ja oma IKT-riski juhtimise raamistiku kohta.

4. Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, panevad vastutuse IKT-riski juhtimise ja järelevaatamise eest kontrollifunktsioonile ning tagavad sellise kontrollifunktsiooni asjakohase sõltumatuse taseme, et vältida huvide konflikte. Finantssektori ettevõtjad tagavad, et IKT-riski juhtimise funktsioonid, kontrollifunktsioonid ja siseauditifunktsioonid on sobivalt eraldatud ja sõltumatud vastavalt kolme kaitseliiniga mudelile või sisemisele riskijuhtimis- ja kontrollimudelile.

5. IKT-riski juhtimise raamistik on dokumenteeritud ja see vaadatakse läbi vähemalt kord aastas või mikroettevõtjate puhul perioodiliselt ning tõsiste IKT intsidentide korral, võttes arvesse järelevalvejuhiseid või -järeldusi, mis tulenevad asjaomastest digitaalse tegevuskerksuse testidest või auditiprotsessidest. Seda täiustatakse pidevalt, lähtudes rakendamisel ja seires saadud õppetundidest. Taotluse korral esitatakse pädevale asutusele aruanne IKT-riski juhtimise raamistiku läbivaatamise kohta.

6. Audiitorid teevad finantssektori ettevõtjate, kes ei ole mikroettevõtjad, IKT-riski juhtimise raamistikule regulaarselt siseauditeid kooskõlas finantssektori ettevõtja auditikavaga. Audiitoritel peavad olema piisavad teadmised, oskused ja asjatundlikkus IKT-riski valdkonnas ning asjakohane sõltumatus. IKT-auditite sagedus ja fookus vastab finantssektori ettevõtja IKT-riskile.

7. Tuginedes siseauditi järeldustele, määravad finantssektori ettevõtjad kindlaks edasise ametliku protseduuri, sealhulgas reeglid IKT-auditite kriitilise tähtsusega tulemuste õigeaegse kontrollimise ja parandamise kohta.

8. IKT-riski juhtimise raamistik sisaldab digitaalse tegevuskerksuse strateegiat, milles on kindlaks määratud, kuidas raamistikku rakendatakse. Selleks sisaldab digitaalse tegevuskerksuse strateegia meetodeid IKT-riski käsitlemiseks ja konkreetsete IKT eesmärkide saavutamiseks,

a) selgitades, kuidas toetab IKT-riski juhtimise raamistik finantssektori ettevõtja äristrateegiat ja eesmärke;

b) määrates kooskõlas finantssektori ettevõtja riskivalmidusega kindlaks IKT-riski taluvuse taseme ning analüüsides IKT-katkestuste mõju taluvust;

c) seades selged infoturbe-eesmärgid, sealhulgas peamised tulemusnäitajad ja peamised riskinäitajad;

d) selgitades IKT etalonarhitektuuri ja konkreetsete ärieesmärkide saavutamiseks vajalikke muudatusi;

e) koostades ülevaate mitmesugustest mehhanismidest, mis on võetud kasutusele IKT intsidentide avastamiseks, nende mõju ennetamiseks ja selle eest kaitsmiseks;

f) näidates digitaalse tegevuskerksuse praegust olukorda, võttes aluseks teatatud tõsiste IKT intsidentide arvu ja ennetusmeetmete tulemuslikkuse;

g) tehes digitaalse tegevuskerksuse teste kooskõlas käesoleva määruse IV peatükiga;

h) koostades kommunikatsioonistrateegia selliste IKT intsidentide jaoks, mis tuleb artikli 14 kohaselt avalikustada.

9. Finantssektori ettevõtjad võivad lõikes 8 osutatud digitaalse tegevuskerksuse strateegia kontekstis määrata kontserni või ettevõtja tasandil kindlaks tervikliku mitme IKT-teenuste osutajaga strateegia, millest on näha peamine sõltuvus kolmandast isikust IKT-teenuste osutajatest ja milles on selgitatud kolmandast isikust IKT-teenuste osutajate valiku põhjuseid.

10. Finantssektori ettevõtjad võivad kooskõlas liidu ja liikmesriigi valdkondliku õigusega anda IKT-riski juhtimise nõuete täitmise kontrollimise ülesanded edasi kontsernisisestele või -välistele ettevõtjatele. Sellise edasiandmise korral jääb finantssektori ettevõtja IKT-riski juhtimise nõuete täitmise kontrollimise eest täielikult vastutavaks.

Artikkel 7

IKT-süsteemid, -protokollid ja -vahendid

Selleks et käsitleda ja juhtida IKT-riski, kasutavad ja hoiavad finantssektori ettevõtjad ajakohasena IKT-süsteeme, -protokolle ja -vahendeid, mis:

a) vastavad nende tegevuse elluviimist toetavate operatsioonide ulatusele kooskõlas artiklis 4 osutatud proportsionaalsuse põhimõttega;

b) on usaldusväärsed;

c) on piisavalt võimsad, et töödelda täpselt andmeid, mida on vaja tegevuse elluviimiseks ja teenuste õigeaegseks osutamiseks ning tellimuste, sõnumite või tehingumahtude tipptasemega toimetulekuks vastavalt vajadusele, muu hulgas uue tehnoloogia kasutuselevõtu korral;

d) on tehnoloogiliselt kerksad, et tulla asjakohaselt toime täiendava teabe töötlemise vajadustega vastavalt sellele, mida on vaja halvenenud turutingimuste korral või muus ebasoodsas olukorras.

Artikkel 8

Kindlaksmääramine

1. Artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistiku osana määravad finantssektori ettevõtjad kindlaks, liigitavad ja dokumenteerivad asjakohaselt kõik IKT-põhised ärifunktsioonid, rollid ja vastutusvaldkonnad, neid funktsioone toetavad teabevarad ja IKT-varad ning nende rollid ja sõltuvuse seoses IKT-riskiga. Finantssektori ettevõtjad vaatavad vastavalt vajadusele ja vähemalt kord aastas läbi selle liigituse ja asjakohaste dokumentide asjakohasuse.

2. Finantssektori ettevõtjad teevad jooksvalt kindlaks kõik IKT-riski allikad, eelkõige riski, mis tuleneb muudest finantssektori ettevõtjatest, ning hindavad küberohte ja IKT-nõrkust, mis puudutavad nende IKT-põhiseid ärifunktsioone, teabevarasid ja IKT-varasid. Finantssektori ettevõtjad vaatavad korrapäraselt ja vähemalt kord aastas läbi neid mõjutavad riskistsenaariumid.

3. Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, teevad riskihindamise alati, kui võrgu- ja infosüsteemide taristus, protsessides või menetlustes, mis mõjutavad nende IKT-põhiseid ärifunktsioone, teabevarasid või IKT-varasid, toimub oluline muutus.

4. Finantssektori ettevõtjad teevad kindlaks kõik teabevarad ja IKT-varad, muu hulgas kaugasukohtades, võrguressursid ja riistvara, ning kaardistavad need, mida käsitatakse olevat kriitilise tähtsusega. Nad kaardistavad teabevarade ja IKT-varade konfiguratsiooni ning erinevate teabevarade ja IKT-varade vahelised seosed ja sõltuvuse.

5. Finantssektori ettevõtjad teevad kindlaks ja dokumenteerivad kõik protsessid, mis sõltuvad kolmandast isikust IKT-teenuste osutajatest, ning seosed kolmandast isikust IKT-teenuste osutajatega, kes osutavad teenuseid, mis toetavad kriitilise tähtsusega või olulisi funktsioone.

6. Lõigete 1, 4 ja 5 kohaldamisel säilitavad finantssektori ettevõtjad asjakohaseid inventuuriandmeid ning ajakohastavad neid perioodiliselt ja iga kord, kui toimub lõikes 3 osutatud oluline muutus.

7. Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, teevad korrapäraselt ja vähemalt kord aastas spetsiifilisi IKT-riski hindamisi, milles käsitletakse kõiki IKT pärandsüsteeme, ning igal juhul enne ja pärast tehnoloogia, rakenduste või süsteemide ühendamist.

Artikkel 9

Kaitse ja ennetus

1. Selleks et piisavalt kaitsta IKT-süsteeme ja luua reageerimismeetmed, seiravad ja kontrollivad finantssektori ettevõtjad pidevalt IKT-süsteemide ja -vahendite turvalisust ja toimimist ning minimeerivad IKT-süsteemidele avalduva IKT-riski mõju, võttes kasutusele asjakohased IKT turvalisuse vahendid, põhimõtted ja menetlused.

2. Finantssektori ettevõtjad disainivad ja hangivad IKT turvalisuse põhimõtted, menetlused, protokollid ja vahendid, mille eesmärk on tagada IKT-süsteemide, eeskätt kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide kerksus, toimimispidevus ja kättesaadavus ning säilitada andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse ranged standardid nii nende jõudeoleku, kasutamise kui ka edastamise jaoks, ning rakendavad neid.

3. Lõikes 2 osutatud eesmärkide saavutamiseks kasutavad finantssektori ettevõtjad IKT-lahendusi ja -protsesse, mis on vastavalt artiklile 4 asjakohased. Need IKT-lahendused ja -protsessid:

a) tagavad andmeedastusvahendite turvalisuse;

b) minimeerivad andmelaostuse või -kao riski, loata juurdepääsu võimaluse ja tehnilised puudused, mis võivad takistada äritegevust;

c) hoiavad ära kättesaadavuse puudumise, autentsuse ja tervikluse kahjustamise, konfidentsiaalsusnõuete rikkumise ja andmekao;

d) tagavad, et andmed on kaitstud andmehaldusest tulenevate riskide, sealhulgas halva haldamise, töötlemisega seotud riskide ja inimlike eksimuste eest.

4. Finantssektori ettevõtjad teevad artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistiku osana järgmist:

a) töötavad välja ja dokumenteerivad infoturbe korra, milles määratakse kindlaks reeglid andmete, teabevarade ja IKT-varade (sealhulgas asjakohasel juhul nende klientide andmete, teabevarade ja IKT-varade) kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse kaitsmiseks;

b) kasutavad riskipõhist käsitust, loovad usaldusväärse võrgu- ja taristuhalduse struktuuri, kasutades sobivaid võtteid, meetodeid ja protokolle, mis võivad hõlmata automatiseeritud mehhanismide rakendamist, et isoleerida küberrünnete korral nendest mõjutatud teabevarad;

c) rakendavad põhimõtteid, mille kohaselt antakse füüsiline või loogiline juurdepääs teabevaradele ja IKT-varadele ainult siis, kui seda on vaja õiguspäraste ja heakskiidetud funktsioonide ja toimingute jaoks, ning kehtestavad sel eesmärgil põhimõtted, menetlused ja kontrollid, mis käsitlevad pääsuõigusi ja tagavad nende usaldusväärse juhtimise;

d) rakendavad põhimõtteid ja protokolle tugeva autentimismehhanismi jaoks, lähtudes asjakohastest standarditest ja spetsiaalsetest kontrollisüsteemidest ning krüptovõtmete kaitsmise meetmetest, mille puhul andmed krüptitakse heakskiidetud andmete liigitamise tulemuste ja IKT-riski hindamise protsesside põhjal;

e) rakendavad IKT-muudatuste (sealhulgas tark-, riist- ja püsivara komponentide muudatused, süsteemi- või turvaparameetrid) juhtimise valdkonnas dokumenteeritud põhimõtteid, menetlusi ja kontrolle, mis põhinevad riskihindamisel ja on lahutamatu osa finantssektori ettevõtja üldisest muudatuste juhtimise protsessist, eesmärgiga tagada, et kõik IKT-süsteemide muudatused on kontrollitud viisil registreeritud, testitud, hinnatud, heakskiidetud, rakendatud ja kinnitatud;

f) omavad sobivaid ja laiahaardelisi dokumenteeritud põhimõtteid paikade ja uuenduste jaoks.

Esimese lõigu punkti b kohaldamisel kujundavad finantssektori ettevõtjad võrguühenduste taristu viisil, mis võimaldab need silmapilkselt katkestada või segmentida, et minimeerida ja takistada ülekandumist, eelkõige omavahel seotud finantsprotsesside puhul.

Esimese lõigu punkti e kohaldamisel kiidavad asjaomased juhtimisliinid IKT-muudatuste juhtimise protsessi heaks ja on olemas konkreetsed protokollid.

Artikkel 10

Avastamine

1. Finantssektori ettevõtjatel peavad kooskõlas artikliga 17 olema mehhanismid, mis võimaldavad kohe avastada anomaalset tegevust, sealhulgas IKT-võrgu jõudluse probleeme ja IKT intsidente, ning teha kindlaks võimalikud olulised nõrgad lülid.

Kõiki esimeses lõigus osutatud avastamismehhanisme testitakse korrapäraselt kooskõlas artikliga 25.

2. Lõikes 1 osutatud avastamismehhanism võimaldab mitmetasandilist kontrolli, määrab kindlaks alarmiläved ja -kriteeriumid, mis käivitavad ja algatavad IKT intsidendile reageerimise protsessid, sealhulgas automaatsed häiremehhanismid asjaomastele töötajatele, kes tegelevad IKT intsidentidele reageerimisega.

3. Finantssektori ettevõtjad näevad ette piisavad ressursid ja piisava suutlikkuse, et seirata kasutajate tegevust, IKT anomaaliate esinemist ja IKT intsidente, eriti küberründeid.

4. Aruandlusteenuse pakkujatel peavad lisaks olema olemas süsteemid, mis võimaldavad tulemuslikult kontrollida kauplemisaruannete terviklikkust, märgata andmete väljajäämist ja ilmseid vigu ning nõuda kõnealuste aruannete uuesti esitamist.

Artikkel 11

Reageerimine ja taastamine

1. Finantssektori ettevõtjad määravad artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistiku osana ja artiklis 8 sätestatud kindlaksmääramise nõuete põhjal kindlaks laiahaardelised IKT talitluspidevuse põhimõtted, mille võib vastu võtta eriomase korrana, mis on finantssektori ettevõtja üldiste talitluspidevuse põhimõtete lahutamatu osa.

2. Finantssektori ettevõtjad rakendavad IKT talitluspidevuse põhimõtteid, kasutades spetsiaalseid, asjakohaseid ja dokumenteeritud kokkuleppeid, kavasid, menetlusi ja mehhanisme, mille eesmärk on

a) tagada finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonide jätkumine;

b) reageerida kõigile IKT intsidentidele ja lahendada need kiiresti, asjakohaselt ja tulemuslikult viisil, mis piirab kahju ning prioriseerib tegevuse jätkamist ja taastemeetmeid;

c) aktiveerida viivitamata spetsiaalsed kavad, et võimaldada piiramismeetmeid, -protsesse ja -tehnoloogiaid, mis vastavad igale IKT intsidendi liigile ning hoiavad ära suurema kahju, samuti kohandatud reageerimis- ja taastamismenetlused, mis on kehtestatud kooskõlas artikliga 12;

d) hinnata esialgset mõju, kahjustust ja kahju;

e) näha ette kommunikatsiooni- ja kriisijuhtimismeetmed, millega tagatakse, et ajakohastatud teave edastatakse kooskõlas artikliga 14 kõigile asjaomastele asutusesisestele töötajatele ja välistele sidusrühmadele, ning anda kooskõlas artikliga 19 aru pädevatele asutustele.

3. Finantssektori ettevõtjad rakendavad artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistiku osana seonduvaid IKT reageerimis- ja taastekavasid, mille kohta tehakse muude kui mikroettevõtjate puhul sõltumatu siseaudit.

4. Finantssektori ettevõtjad koostavad sobivad IKT talitluspidevuse kavad ning hoiavad neid jõus ja testivad neid perioodiliselt, eelkõige seoses kriitilise tähtsusega või oluliste funktsioonidega, mis on antud edasi või mille kohta on sõlmitud kolmandast isikust IKT-teenuste osutajatega kokkulepped.

5. Finantssektori ettevõtjad teevad üldiste talitluspidevuse põhimõtete osana talitlusmõju analüüsi, mis käsitleb nende tõsiste tegevushäirete riske. Finantssektori ettevõtjad hindavad talitlusmõju analüüsi käigus tõsiste tegevushäirete võimalikku mõju kvantitatiivsete ja kvalitatiivsete kriteeriumide alusel, kasutades kohasel viisil sisemiste ja väliste andmete ja stsenaariumide analüüsi. Talitlusmõju analüüsis võetakse arvesse tuvastatud ja kaardistatud ärifunktsioonide, tugiprotsesside, kolmandatest isikutest sõltuvuse ja teabevarade kriitilist tähtsust ning nende vastastikust sõltuvust. Finantssektori ettevõtjad tagavad, et IKT-varasid ja IKT-teenuseid kavandatakse ja kasutatakse täielikus kooskõlas talitlusmõju analüüsiga, eelkõige selleks, et asjakohaselt tagada kõigi kriitilise tähtsusega komponentide varu.

6. Finantssektori ettevõtjad teevad oma laiahaardelise IKT-riski juhtimise raames järgmist:

a) testivad kõiki funktsioone toetavate IKT-süsteemide IKT talitluspidevuse kavasid ning IKT reageerimis- ja taastekavasid vähemalt kord aastas ja kriitilise tähtsusega või olulisi funktsioone toetavate IKT-süsteemide oluliste muudatuste korral;

b) testivad kooskõlas artikliga 14 koostatud kriisikommunikatsioonikavasid.

Esimese lõigu punkti a kohaldamisel lisavad finantssektori ettevõtjad, kes ei ole mikroettevõtjad, testimiskavadesse stsenaariumid, mis käsitlevad küberrünnideid ja esmase IKT-taristu ja varuvõimsuse vahelist ümberlülitust, varundamist ja varurajatisi, mida on vaja artiklis 12 sätestatud kohustuste täitmiseks.

Finantssektori ettevõtjad vaatavad oma IKT talitluspidevuse põhimõtted ning IKT reageerimis- ja taastekavad korrapäraselt läbi, võttes arvesse kooskõlas esimese lõiguga tehtud testide tulemusi ja soovitusi, mis tulenevad auditikontrollidest või järelevalvest.

7. Finantssektori ettevõtjatel, kes ei ole mikroettevõtjad, on kriisijuhtimisfunktsioon, mis muu hulgas kehtestab IKT talitluspidevuse kavade või IKT reageerimis- ja taastekavade aktiveerimisel selged menetlused sisemise ja välise kriisikommunikatsiooni juhtimiseks kooskõlas artikliga 14.

8. IKT talitluspidevuse kavade ning IKT reageerimis- ja taastekavade aktiveerimise ajal koguvad finantssektori ettevõtjad andmeid tegevuste kohta enne katkestusi ja nende ajal ning hoiavad need alles kergesti kättesaadavana.

9. Väärtpaberite keskdepositooriumid esitavad pädevatele asutustele IKT talitluspidevuse testide või muude sarnaste testide tulemuste koopiad.

10. Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, teavitavad taotluse korral pädevaid asutusi tõsiste IKT intsidentide tekitatud hinnangulisest aastasest kogukulust ja -kahjust.

11. Euroopa järelevalveasutused koostavad hiljemalt 17. juuliks 2024 kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 16 ühiskomitee kaudu ühised suunised lõikes 10 osutatud aastase kogukulu ja -kahju hindamise kohta.

Artikkel 12

Varunduspõhimõtted ja -menetlused, ennistamise ja taastamise menetlused ja meetodid

1. Selleks et tagada IKT-süsteemide ja andmete ennistamine minimaalse seisuaja, piiratud katkestuse ja kaoga, töötab finantssektori ettevõtja IKT-riski juhtimise raamistiku osana välja ja dokumenteerib

a) varunduspõhimõtted ja -menetlused, milles täpsustatakse varundatavate andmete maht ja minimaalne varundamissagedus, lähtudes teabe kriitilisest tähtsusest või andmete konfidentsiaalsuse tasemest;

b) ennistamise ja taastamise menetlused ja meetodid.

2. Finantssektori ettevõtjad loovad varusüsteemid, mida saab aktiveerida vastavalt varunduspõhimõtetele ja -menetlustele ning ennistamise ja taastamise menetlustele ja meetoditele. Varusüsteemi aktiveerimine ei tohi seada ohtu võrgu- ja infosüsteemide turvalisust ega andmete kättesaadavust, autentsust, terviklust ega konfidentsiaalsust. Varundusmenetlusi ning ennistamise ja taastamise menetlusi ja meetodeid testitakse perioodiliselt.

3. Varundatud andmete ennistamisel oma süsteemide abil kasutavad finantssektori ettevõtjad IKT-süsteeme, mis on oma lähtesüsteemist füüsiliselt ja loogiliselt eraldatud. IKT-süsteemid on turvaliselt kaitstud loata juurdepääsu või IKT laostuse eest ning võimaldavad teenuste õigeaegset ennistamist, kasutades vajaduse korral andmete ja süsteemi varukoopiaid.

Kesksete vastaspoolte puhul võimaldavad sellised kavad taastada katkestuse ajal kõik tehingud, et keskne vastaspool saaks oma tegevust kindlalt jätkata ja viia arveldamine lõpule kavandatud kuupäeval.

Aruandlusteenuse pakkujatel on lisaks piisavad vahendid ning varu- ja ennistamisseadmed, mis võimaldavad neil igal ajal oma teenuseid pakkuda ja nende osutamist jätkata.

4. Finantssektori ettevõtjatel, kes ei ole mikroettevõtjad, on IKT-alane varusuutlikkus koos ärivajaduste rahuldamiseks piisavate ressursside, võimete ja funktsioonidega. Mikroettevõtjad hindavad sellise IKT-alase varusuutlikkuse vajadust oma riskiprofiili alusel.

5. Väärtpaberite keskdepositooriumidel on vähemalt üks varutöötluskoht, millel on ärivajaduste rahuldamiseks piisavad ressursid, võimed, funktsioonid ja personalikorraldus.

Varutöötluskoht:

a) asub peamisest töötluskohast geograafiliselt eemal, et tagada nende erinev riskiprofiil ja vältida, et varutöötluskohta kahjustab peamisele töötluskohale mõju avaldanud sündmus;

b) suudab sarnaselt peamise töötluskohaga tagada kriitilise tähtsusega või oluliste funktsioonide järjepidevuse või sellise teenuste taseme, mida on vaja, et finantssektori ettevõtja täidaks oma kriitilise tähtsusega funktsioone vastavalt taaste-eesmärkidele;

c) on finantssektori ettevõtja töötajatele kohe ligipääsetav, et tagada kriitilise tähtsusega või oluliste funktsioonide jätkumine juhul, kui peamist töötluskohta ei saa enam kasutada.

6. Iga funktsiooni taasteaja ja taastekünnise eesmärkide kindlaksmääramisel võtavad finantssektori ettevõtjad arvesse seda, kas tegemist on kriitilise tähtsusega või olulise funktsiooniga, ning võimalikku üldist mõju turu tõhususele. Selliste ajaliste eesmärkidega tagatakse, et äärmuslike stsenaariumide korral tagatakse teenused kokkulepitud tasemel.

7. IKT intsidendist taastumisel teevad finantssektori ettevõtjad vajalikud kontrollid, sealhulgas mitmekordsed kontrollid ja kooskõlastavad võrdlemised, et tagada kõrgeimal tasemel andmete tervikluse säilimine. Neid kontrolle tehakse ka välistelt sidusrühmadelt saadud andmete rekonstrueerimisel, et tagada kõigi andmete kooskõla eri süsteemides.

Artikkel 13

Õppimine ja areng

1. Finantssektori ettevõtjatel peab olema suutlikkus ja personal, et koguda teavet nõrkuse, küberohtude ja IKT intsidentide, eelkõige küberrünnete kohta, ning analüüsida mõju, mida need võivad avaldada nende digitaalsele tegevuskerksusele.

2. Finantssektori ettevõtjad kehtestavad IKT intsidentide järgsed kontrollid, mida tehakse pärast seda, kui tõsine IKT intsident häirib nende põhitegevust, analüüsides häire põhjuseid ja tehes kindlaks, mida on vaja IKT-operatsioonides või artiklis 11 osutatud IKT talitluspidevuse põhimõtetes muuta.

Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, teavitavad taotluse korral pädevaid asutusi muudatustest, mis tehti pärast esimeses lõigus osutatud IKT intsidentide järgseid kontrolle.

Esimeses lõigus osutatud IKT intsidentide järgse kontrolli käigus tehakse kindlaks, kas järgiti kehtestatud korda ja kas võetud meetmed olid tulemuslikud, sealhulgas seoses järgmisega:

a) turvahoiatustele reageerimise ning IKT intsidentide mõju ja nende tõsiduse kindlakstegemise kiirus;

b) kriminalistika-analüüsi (kui seda peetakse asjakohaseks) kvaliteet ja kiirus;

c) intsidendi eskaleerimise tulemuslikkus finantssektori ettevõtjas;

d) sise- ja välissuhtluse tulemuslikkus.

3. Õppetunnid, mis on saadud artiklite 26 ja 27 kohaselt läbi viidud digitaalse tegevuskerksuse testimise käigus ning reaalses elus toimunud IKT intsidentidest (eelkõige küberründed) ja IKT talitluspidevuse kavade ning IKT reageerimis- ja taastekavade käivitamisega seotud probleemidest, samuti vastaspooltega vahetatud ja järelevalve käigus hinnatud asjakohane teave inkorporeeritakse igatpidi jooksvalt IKT-riski hindamise protsessi. Kõnealuste tulemuste põhjal vaadatakse asjakohaselt läbi artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistiku vastavad osad.

4. Finantssektori ettevõtjad seiravad artikli 6 lõikes 8 sätestatud digitaalse tegevuskerksuse strateegia rakendamise tulemuslikkust. Nad kaardistavad, kuidas on IKT-risk aja jooksul arenenud, analüüsivad IKT intsidentide, eelkõige küberrünnete sagedust, liiki, ulatust ja muutusi ning nende mustreid, et mõista IKT-riski taset eelkõige seoses kriitilise tähtsusega või oluliste funktsioonidega ning parandada finantssektori ettevõtja küberküpsust ja valmisolekut.

5. Kõrgema astme IKT-töötajad esitavad juhtorganile vähemalt kord aastas aruande lõikes 3 osutatud tulemuste kohta ja annavad soovitusi.

6. Finantssektori ettevõtjad töötavad oma personali koolituskavade raames kohustuslike moodulitena välja IKT-turbe teadlikkuse suurendamise programmid ja digitaalse tegevuskerksuse koolituse. Need programmid ja koolitus on suunatud kõigile töötajatele ja kõrgema juhtkonna liikmetele ning nende keerukuse aste on kooskõlas vastavate ametikohtade volitustega. Kohasel juhul kaasavad finantssektori ettevõtjad oma asjakohastesse koolituskavadesse ka kolmandast isikust IKT-teenuste osutajad kooskõlas artikli 30 lõike 2 punktiga i.

7. Finantssektori ettevõtjad, kes ei ole mikroettevõtjad, jälgivad pidevalt tehnoloogia arengut, muu hulgas selleks, et mõista uue tehnoloogia võimalikku mõju IKT turvanõuetele ja digitaalsele tegevuskerksusele. Nad hoiavad end kursis uusimate IKT-riski juhtimise protsessidega, et võidelda tõhusalt praeguste või uute küberrünnevormide vastu.

Artikkel 14

Kommunikatsioon

1. Finantssektori ettevõtjad koostavad artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistiku osana kriisikommunikatsioonikavad, mis võimaldavad teha klientidele ja vastaspooltele ning kohasel määral ka üldsusele vastutustundlikult teatavaks vähemalt tõsiseid IKT intsidente või nõrkust.

2. Finantssektori ettevõtjad rakendavad IKT-riski juhtimise raamistiku osana asutusesiseseid töötajaid ja väliseid sidusrühmi puudutavat kommunikatsioonipoliitikat. Personali kommunikatsioonipoliitikas võetakse arvesse vajadust eristada töötajaid, kes osalevad IKT-riski juhtimises (eelkõige reageerimise ja taaste eest vastutavaid töötajaid), ja töötajaid, keda tuleb teavitada.

3. Vähemalt ühele isikule finantssektori ettevõtjas tehakse ülesandeks rakendada IKT intsidentide kommunikatsioonistrateegiat ning täita sel eesmärgil avalikkuse ja meediaga suhtlemise funktsiooni.

Artikkel 15

IKT-riski juhtimise vahendite, meetodite, protsesside ja põhimõtete edasine ühtlustamine

Euroopa järelevalveasutused töötavad ühiskomitee kaudu ja Euroopa Liidu Küberturvalisuse Ametiga (ENISA) konsulteerides välja ühiste regulatiivsete tehniliste standardite eelnõud, et:

a) täpsustada artikli 9 lõikes 2 osutatud IKT turvalisuse põhimõtetesse, menetlustesse, protokollidesse ja vahenditesse lisatavaid elemente, et tagada võrkude turvalisus, võimaldada piisavaid kaitsemeetmeid sissetungide ja andmete väärkasutamise vastu, säilitada andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus, sealhulgas krüptomeetodeid kasutades, ning tagada andmete täpne ja kiire ning ilma suuremate häirete ja põhjendamatute viivitusteta ülekandmine;

b) töötada välja artikli 9 lõike 4 punktis c osutatud pääsuhalduse õiguste kontrolli täiendavad komponendid ja nendega seotud personalipoliitika, milles määratakse kindlaks pääsuõigused, õiguste andmise ja tühistamise menetlused, IKT-riskiga seotud anomaalse käitumise seire asjakohaste näitajate alusel, sealhulgas võrgu kasutamise mustrite, tundide, IT-tegevuse ja tundmatute seadmete alusel;

c) arendada edasi artikli 10 lõikes 1 sätestatud mehhanisme, mis võimaldavad kõrvalekaldeid kiiresti avastada, ning artikli 10 lõikes 2 sätestatud kriteeriume, mis käivitavad IKT intsidentide tuvastamise ja neile reageerimise protsessid;

d) täpsustada artikli 11 lõikes 1 osutatud IKT talitluspidevuse põhimõtete komponente;

e) täpsustada artikli 11 lõikes 6 osutatud IKT talitluspidevuse kavade testimist tagamaks, et sellisel testimisel võetakse igakülgselt arvesse stsenaariume, mille korral kriitilise tähtsusega või olulise funktsiooni täitmise kvaliteet halveneb vastuvõetamatu tasemeni või funktsiooni täitmine ebaõnnestub, ning võetakse igakülgselt arvesse asjaomase kolmandast isikust IKT-teenuse osutaja maksejõuetuse või muude tõrgete võimalikku mõju ja poliitilisi riske (kui neid on) vastavate teenuseosutajate jurisdiktsioonides;

f) täpsustada artikli 11 lõikes 3 osutatud IKT reageerimis- ja taastekavade komponente;

g) täpsustada artikli 6 lõikes 5 osutatud IKT-riski juhtimise raamistiku läbivaatamist käsitleva aruande sisu ja vormi.

Kõnealuste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust, võttes igati arvesse spetsiifilisi omadusi, mis tulenevad eri finantsteenuste sektorite tegevuse eripärast.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. jaanuariks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

Artikkel 16

Lihtsustatud IKT-riski juhtimise raamistik

1. Käesoleva määruse artikleid 5–15 ei kohaldata järgmiste ettevõtjate suhtes: väikesed ja mitteseotud investeerimisühingud; makseasutused, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 kohast erandit; asutused, mille suhtes kohaldatakse direktiivi 2013/36/EL kohast erandit ja mille suhtes on liikmesriigid otsustanud mitte kohaldada käesoleva määruse artikli 2 lõikes 4 osutatud võimalust; e-raha asutused, mille suhtes kohaldatakse direktiivi 2009/110/EÜ kohast erandit ja väikesed tööandja kogumispensioni asutused.

Ilma et see piiraks esimest lõiku teevad selles nimetatud üksused järgmist:

a) kehtestavad usaldusväärse ja dokumenteeritud IKT-riski juhtimise raamistiku, milles kirjeldatakse üksikasjalikult mehhanisme ja meetmeid, mille eesmärk on IKT-riski kiire, tõhus ja terviklik juhtimine, muu hulgas asjakohaste füüsiliste komponentide ja taristute kaitseks, ning hoiavad seda jõus;

b) seiravad pidevalt kõigi IKT-süsteemide turvalisust ja toimimist;

c) minimeerivad IKT-riski mõju, kasutades selleks usaldusväärseid, vastupidavaid ja ajakohastatud IKT-süsteeme, -protokolle ja -vahendeid, mis on nende tegevuse ja teenuste osutamise toetamiseks asjakohased ning mis kaitsevad piisavalt võrgu- ja infosüsteemides olevate andmete kättesaadavust, autentsust, terviklust ja konfidentsiaalsust;

d) võimaldavad võrgu- ja infosüsteemide IKT-riski ja -anomaaliate allikate kiiret tuvastamist ja avastamist ning IKT intsidentide kiiret käsitlemist;

e) teevad kindlaks peamise sõltuvuse kolmandast isikust IKT-teenuste osutajatest;

f) tagavad kriitilise tähtsusega või oluliste funktsioonide järjepidevuse, kasutades selleks talitluspidevuse kavasid ning reageerimis- ja taastemeetmeid, mis sisaldavad vähemalt varundus- ja ennistamismeetmeid;

g) testivad korrapäraselt punktis f osutatud kavasid ja meetmeid ning punktide a ja c kohaselt rakendatud kontrollide tulemuslikkust;

h) rakendavad punktis g osutatud testidest ja intsidendijärgsest analüüsist tulenevaid asjakohaseid tegevusjäreldusi kohasel määral IKT-riski hindamise protsessis ning kavandavad vajadustest ja IKT-riski profiilist lähtuvalt töötajatele ja juhtkonnale suunatud IKT-turbe teadlikkuse suurendamise programme ning digitaalse tegevuskerksuse koolitust.

2. Lõike 1 teise lõigu punktis a osutatud IKT-riski juhtimise raamistik dokumenteeritakse ning see vaadatakse läbi perioodiliselt ja tõsiste IKT intsidentide puhul kooskõlas järelevalvejuhistega. Seda täiustatakse pidevalt, lähtudes rakendamisel ja seires saadud õppetundidest. Taotluse korral esitatakse pädevale asutusele aruanne IKT-riski juhtimise raamistiku läbivaatamise kohta.

3. Euroopa järelevalveasutused töötavad ühiskomitee kaudu ja ENISAga konsulteerides välja ühiste regulatiivsete tehniliste standardite eelnõud, et:

a) täpsustada lõike 1 teise lõigu punktis a osutatud IKT-riski juhtimise raamistikku lisatavaid elemente;

b) täpsustada elemente seoses lõike 1 teise lõigu punktis c osutatud IKT-riski mõju minimeerimise süsteemide, protokollide ja vahenditega, et tagada võrkude turvalisus, võimaldada piisavaid kaitsemeetmeid sissetungide ja andmete väärkasutamise vastu ning säilitada andmete kättesaadavus, autentsus, terviklus ja konfidentsiaalsus;

c) täpsustada lõike 1 teise lõigu punktis f osutatud IKT talitluspidevuse kavade komponente;

d) täpsustada talitluspidevuse kavade testimise reegleid ja tagada lõike 1 teise lõigu punktis g osutatud kontrollide tulemuslikkus ning tagada, et sellisel testimisel võetakse igakülgselt arvesse stsenaariume, mille korral kriitilise tähtsusega või olulise funktsiooni täitmise kvaliteet halveneb vastuvõetamatu tasemeni või funktsiooni täitmine ebaõnnestub;

e) täpsustada lõikes 2 osutatud IKT-riski juhtimise raamistiku läbivaatamist käsitleva aruande sisu ja vormi.

Kõnealuste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. jaanuariks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

III PEATÜKK

IKT intsidentide haldamine ja liigitamine ning nendest teavitamine

Artikkel 17

IKT intsidentide haldamise protsess

1. Finantssektori ettevõtjad määravad kindlaks, kehtestavad ja rakendavad IKT intsidentide haldamise protsessi nende avastamiseks, haldamiseks ja nendest teatamiseks.

2. Finantssektori ettevõtjad registreerivad kõik IKT intsidendid ja olulised küberohud. Finantssektori ettevõtjad kehtestavad asjakohased menetlused ja protsessid, et tagada IKT intsidentide järjepidev ja integreeritud seire, käsitlemine ja järelmeetmed, et tagada algpõhjuste kindlakstegemine, dokumenteerimine ja nendega tegelemine selliste intsidentide edaspidiseks vältimiseks.

3. Lõikes 1 osutatud IKT intsidentide haldamise protsess hõlmab järgmist:

a) varajase hoiatamise näitajate kehtestamine;

b) menetluste kehtestamine IKT intsidentide tuvastamiseks, jälgimiseks, logimiseks, kategoriseerimiseks ja liigitamiseks vastavalt nende prioriteetsusele ja tõsidusele ning mõjutatud teenuste kriitilisele tähtsusele kooskõlas artikli 18 lõikes 1 sätestatud kriteeriumidega;

c) selliste rollide ja ülesannete määramine, mis tuleb aktiveerida eri liiki IKT intsidentide ja stsenaariumide puhul;

d) kavade koostamine artikli 14 kohaseks töötajate, väliste sidusrühmade ja meedia teavitamiseks ning klientide teavitamiseks sellise asutusesisese intsidentidest teavitamise korra kehtestamine, mis hõlmab IKTga seotud klientide kaebusi, ning kohasel viisil teabe andmiseks vastaspooltena tegutsevatele finantssektori ettevõtjatele;

e) selle tagamine, et vähemalt tõsistest IKT intsidentidest teavitatakse asjaomast kõrgemat juhtkonda, ning vähemalt tõsistest IKT intsidentidest teatatakse juhtorganile, selgitades selliste tõsiste IKT intsidentide mõju, neile reageerimist ja nende tõttu kehtestatud lisakontrolle;

f) IKT intsidentidele reageerimise menetluste kehtestamine, et leevendada mõju ja tagada teenuste õigeaegne taastamine ja turvalisus.

Artikkel 18

IKT intsidentide ja küberohtude liigitamine

1. Finantssektori ettevõtjad liigitavad IKT intsidendid ja määravad nende mõju kindlaks järgmiste kriteeriumide alusel:

a) IKT intsidendist mõjutatud klientide või finantssektori vastaspoolte arv ja/või olulisus ning, kui see on asjakohane, mõjutatud tehingute kogus või arv ning see, kas IKT intsident on kahjustanud mainet;

b) IKT intsidendi kestus, sealhulgas teenuse seisaku aeg;

c) IKT intsidendist mõjutatud geograafilised piirkonnad, eriti kui see mõjutab rohkem kui kahte liikmesriiki;

d) IKT intsidendiga kaasnev andmekadu seoses andmete kättesaadavuse, autentsuse, tervikluse või konfidentsiaalsusega;

e) mõjutatud teenuste, sealhulgas finantssektori ettevõtja tehingute ja toimingute kriitiline tähtsus;

f) IKT intsidendi nii absoluutne kui ka suhteline majanduslik mõju, eeskätt otsene ja kaudne kulu ja kahju.

2. Finantssektori ettevõtjad liigitavad küberohud olulisteks, võttes arvesse ohustatud teenuste kriitilist tähtsust, sealhulgas finantssektori ettevõtja tehinguid ja toiminguid, sihtrühma kuuluvate klientide või finantssektori vastaspoolte arvu ja/või asjakohasust ning ohustatud alade geograafilist paiknemist.

3. Euroopa järelevalveasutused töötavad ühiskomitee kaudu ning EKP ja ENISAga konsulteerides välja ühiste regulatiivsete tehniliste standardite eelnõud, milles täpsustatakse järgmist:

a) lõikes 1 sätestatud kriteeriumid, sealhulgas olulisuse läved selliste tõsiste IKT intsidentide või, kui see on asjakohane, selliste oluliste tegevust või turvalisust mõjutavate maksetega seotud intsidentide kindlaksmääramiseks, mille suhtes kohaldatakse artikli 19 lõikes 1 sätestatud teavitamiskohustust;

b) kriteeriumid, mida pädevad asutused peavad kohaldama, et hinnata tõsiste IKT intsidentide või, kui see on asjakohane, tegevust või turvalisust mõjutavate maksetega seotud intsidentide olulisust teiste liikmesriikide pädevate asutuste jaoks, ning tõsistest IKT intsidentidest või, kui see on asjakohane, tegevust või turvalisust mõjutavate maksetega seotud intsidentidest teavitamise raportite üksikasjad, mida jagatakse teiste pädevate asutustega vastavalt artikli 19 lõigetele 6 ja 7;

c) käesoleva artikli lõikes 2 sätestatud kriteeriumid, sealhulgas kõrged olulisuse läved oluliste küberohtude kindlaksmääramiseks.

4. Käesoleva artikli lõikes 3 osutatud ühiste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse artikli 4 lõikes 2 sätestatud kriteeriume ning rahvusvahelisi standardeid, suuniseid ning ENISA väljatöötatud ja avaldatud spetsifikaate, sealhulgas asjakohasel juhul muude majandussektorite spetsifikaate. Artikli 4 lõikes 2 sätestatud kriteeriumide kohaldamisel kaaluvad Euroopa järelevalveasutused igakülgselt, kas mikroettevõtjatel ning väikestel ja keskmise suurusega ettevõtjatel on vaja kaasata piisavalt ressursse ja suutlikkust IKT intsidentide kiireks haldamiseks.

Euroopa järelevalveasutused esitavad kõnealused ühiste regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. jaanuariks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu lõikes 3 osutatud regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

Artikkel 19

Tõsistest IKT intsidentidest teavitamine ja vabatahtlik teavitamine olulistest küberohtudest

1. Finantssektori ettevõtjad teavitavad tõsistest IKT intsidentidest artiklis 46 osutatud asjaomasele pädevale asutusele kooskõlas käesoleva artikli lõikega 4.

Kui finantssektori ettevõtja üle teevad järelevalvet mitu artiklis 46 osutatud riiklikku pädevat asutust, määravad liikmesriigid ühe pädeva asutuse selliseks asjaomaseks pädevaks asutuseks, kes vastutab käesolevas artiklis sätestatud ülesannete ja kohustuste täitmise eest.

Määruse (EL) nr 1024/2013 artikli 6 lõike 4 kohaselt oluliseks liigitatud krediidiasutused teavitavad tõsistest IKT intsidentidest direktiivi 2013/36/EL artikli 4 kohaselt määratud asjaomasele riiklikule pädevale asutusele, kes edastab selle raporti viivitamata EKP-le.

Esimese lõigu kohaldamisel koostavad finantssektori ettevõtjad pärast kogu asjakohase teabe kogumist ja analüüsimist esialgse teate ja raportid, millele on osutatud käesoleva artikli lõikes 4, kasutades artiklis 20 osutatud vorme, ning esitavad need pädevale asutusele. Kui on tehniliselt võimatu esitada esialgne teade asjakohast vormi kasutades, teatavad finantssektori ettevõtjad sellest pädevale asutusele muul viisil.

Esialgne teade ja raportid, millele on osutatud lõikes 4, sisaldavad kogu teavet, mida pädev asutus vajab, et teha kindlaks tõsise IKT intsidendi tähtsus ja hinnata võimalikku piiriülest mõju.

Ilma et see piiraks finantssektori ettevõtja poolset esimese lõigu kohast asjaomase pädeva asutuse teavitamist, võivad liikmesriigid lisaks otsustada, et mõned või kõik finantssektori ettevõtjad esitavad pädevale asutusele või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt, ka esialgse teate ja kõik raportid, millele on osutatud käesoleva artikli lõikes 4, kasutades artiklis 20 osutatud vorme.

2. Finantssektori ettevõtjad võivad vabatahtlikult teatada asjaomasele pädevale asutusele olulistest küberohtudest, kui nad peavad ohtu finantssüsteemi, teenusekasutajate või klientide jaoks oluliseks. Asjaomane pädev asutus võib esitada selle teabe teistele asjaomastele asutustele, kellele on osutatud lõikes 6.

Määruse (EL) nr 1024/2013 artikli 6 lõike 4 kohaselt oluliseks liigitatud krediidiasutused võivad vabatahtlikult teatada olulistest küberohtudest direktiivi 2013/36/EL artikli 4 kohaselt määratud asjaomasele riiklikule pädevale asutusele, kes edastab teate viivitamata EKP-le.

Liikmesriigid võivad otsustada, et need finantssektori ettevõtjad, kes teatavad vabatahtlikult esimese lõigu kohaselt, võivad kõnealuse teate edastada ka direktiivi (EL) 2022/2555 kohaselt määratud või loodud küberturbe intsidentide lahendamise üksustele.

3. Kui leiab aset tõsine IKT intsident ja see mõjutab klientide finantshuve, teavitavad finantssektori ettevõtjad põhjendamatu viivituseta ja niipea, kui nad sellest teada saavad, oma kliente tõsisest IKT intsidendist ning annavad neile võimalikult kiiresti teada kõigist meetmetest, mis on võetud sellise intsidendi negatiivse mõju leevendamiseks.

Olulise küberohu korral teavitavad finantssektori ettevõtjad kohasel juhul oma kliente, keda see võib mõjutada, kõigist asjakohastest kaitsemeetmetest, mille võtmist viimased võivad kaaluda.

4. Finantssektori ettevõtjad esitavad asjaomasele pädevale asutusele artikli 20 esimese lõigu punkti a alapunkti ii kohaselt kehtestatavateks tähtaegadeks järgmise teabe:

a) esialgse teate;

b) vaheraporti pärast punktis a osutatud esialgset teadet niipea, kui algse intsidendi staatus on oluliselt muutunud või tõsise IKT intsidendi käsitlemine on uue kättesaadava teabe põhjal muutunud, mille järel saadetakse kohasel viisil ajakohastatud teated iga kord, kui on uut teavet, samuti pädeva asutuse konkreetse taotluse korral;

c) lõppraporti, kui algpõhjuste analüüs on lõpule viidud, olenemata sellest, kas leevendusmeetmeid on juba rakendatud või mitte, ja kui hinnangud saab asendada tegelike mõjunäitajatega.

5. Finantssektori ettevõtjad võivad kooskõlas liidu ja liikmesriigi valdkondliku õigusega anda käesoleva artikli kohase teavitamiskohustuse edasi kolmandast isikust teenuseosutajale. Sellise edasiandmise korral jääb finantssektori ettevõtja täielikult vastutavaks intsidentidest teavitamise nõuete täitmise eest.

6. Pärast esialgse teate ja iga lõikes 4 osutatud raporti kättesaamist esitab pädev asutus aegsasti tõsise IKT intsidendi üksikasjad järgmistele adressaatidele, lähtudes nende vastavast pädevusest:

a) EBA-le, ESMA-le või EIOPA-le;

b) EKP-le artikli 2 lõike 1 punktides a, b ja d osutatud finantssektori ettevõtjate puhul;

c) riiklikele pädevatele asutustele, ühtsele kontaktpunktile või küberturbe intsidentide lahendamise üksustele, mis on määratud või loodud direktiivi (EL) 2022/2555 kohaselt;

d) direktiivi 2014/59/EL artiklis 3 osutatud kriisilahendusasutustele ja Ühtsele Kriisilahendusnõukogule seoses Euroopa Parlamendi ja nõukogu määruse (EL) nr 806/2014 ([37]) artikli 7 lõikes 2 osutatud üksustega ning määruse (EL) nr 806/2014 artikli 7 lõike 4 punktis b ja lõikes 5 osutatud üksuste ja kontsernidega, kui sellised üksikasjad on seotud intsidentidega, mis kujutavad endast ohtu kriitiliste funktsioonide tagamisele direktiivi 2014/59/EL artikli 2 lõike 1 punkti 35 tähenduses, ning

e) muudele liikmesriigi õiguse kohastele avaliku sektori asutustele.

7. Pärast teabe saamist vastavalt lõikele 6 hindavad EBA, ESMA või EIOPA ning EKP ENISAga konsulteerides ja koostöös asjaomase pädeva asutusega IKT intsidendi tõsidust teiste liikmesriikide pädevate asutuste jaoks. Pärast hindamist teavitab EBA, ESMA või EIOPA sellest võimalikult kiiresti teiste liikmesriikide asjaomaseid pädevaid asutusi. EKP teavitab Euroopa Keskpankade Süsteemi liikmeid maksesüsteemi jaoks asjakohastest probleemidest. Selle teavituse alusel võtavad pädevad asutused asjakohasel juhul kõik vajalikud meetmed finantssüsteemi stabiilsuse viivitamatuks kaitsmiseks.

([37]) Euroopa Parlamendi ja nõukogu 15. juuli 2014. aasta määrus (EL) nr 806/2014, millega kehtestatakse ühtsed eeskirjad ja ühtne menetlus krediidiasutuste ja teatavate investeerimisühingute kriisilahenduseks ühtse kriisilahenduskorra ja ühtse kriisilahendusfondi raames ning millega muudetakse määrust (EL) nr 1093/2010 (ELT L 225, 30.7.2014, lk 1).

8. ESMA poolt käesoleva artikli lõike 7 kohaselt esitatav teade ei mõjuta pädeva asutuse kohustust edastada kiiresti vastuvõtva liikmesriigi asjaomasele asutusele tõsise IKT intsidendi üksikasjad, kui väärtpaberite keskdepositoorium tegutseb piiriüleselt vastuvõtvas liikmesriigis olulisel määral, kui sellel tõsisel IKT intsidendil on tõenäoliselt tõsised tagajärjed vastuvõtva liikmesriigi finantsturgudele ning kui pädevate asutuste vahel on sõlmitud koostöökokkulepped seoses finantssektori ettevõtjate järelevalvega.

Artikkel 20

Teavitamise sisu ja vormide ühtlustamine

Euroopa järelevalveasutused töötavad ühiskomitee kaudu ENISA ja EKPga konsulteerides välja

a) ühiste regulatiivsete tehniliste standardite eelnõud, et:

   i) määrata kindlaks tõsiseid IKT intsidente käsitlevate raportite sisu, et kajastada artikli 18 lõikes 1 sätestatud kriteeriume ja lisada täiendavaid elemente, näiteks üksikasju, mis võimaldavad kindlaks teha, kas teavitamine on teiste liikmesriikide jaoks oluline ja kas see kujutab endast tegevust või turvalisust mõjutavate maksetega seotud tõsist intsidenti või mitte;

   ii) määrata kindlaks esialgse teate ja kõigi artikli 19 lõikes 4 osutatud raportite esitamise tähtajad;

   iii) kehtestada olulisi küberohtusid käsitleva teate sisu.

   Kõnealuste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust ning seda, et eelkõige käesoleva lõigu punkti a alapunkti ii kohaldamise tagamiseks võivad erinevad tähtajad kajastada kohasel määral finantssektori eripära, ilma et see mõjutaks järjepideva lähenemisviisi säilitamist käesoleva määruse ja direktiivi (EL) 2022/2555 kohaselt IKT intsidentidest teavitamise suhtes. Kui Euroopa järelevalveasutused kalduvad kõrvale kõnealuse direktiivi kontekstis võetud lähenemisviisidest, esitavad nad põhjenduse, kui see on asjakohane;

b) ühiste rakenduslike tehniliste standardite eelnõud, et kehtestada standardvormid, mallid ja menetlused, mida finantssektori ettevõtjad kasutavad tõsisest IKT intsidendist teavitamiseks ning olulisest küberohust teatamiseks.

Euroopa järelevalveasutused esitavad esimese lõigu punktis a osutatud ühiste regulatiivsete tehniliste standardite eelnõud ja esimese lõigu punktis b osutatud ühiste rakenduslike tehniliste standardite eelnõud komisjonile hiljemalt 17. juuliks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimese lõigu punktis a osutatud ühised regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

Komisjonile antakse õigus võtta vastu esimese lõigu punktis b osutatud ühised rakenduslikud tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 15.

Artikkel 21

Tõsistest IKT intsidentidest teavitamise tsentraliseerimine

1. Euroopa järelevalveasutused koostavad ühiskomitee kaudu ning EKP ja ENISAga konsulteerides ühisaruande, milles hinnatakse intsidentidest teavitamise edasise tsentraliseerimise võimalikkust, milleks tuleks luua finantssektori ettevõtjate poolt tõsistest IKT intsidentidest teavitamiseks ühine ELi keskus. Ühisaruandes analüüsitakse, kuidas hõlbustada IKT intsidentidest teavitamist, vähendada sellega seotud kulusid ja toetada temaatilisi analüüse, et suurendada järelevalvealast ühtsust.

2. Lõikes 1 osutatud ühisaruandes käsitletakse vähemalt järgmisi teemasid:

a) ühise ELi keskuse loomise eeltingimused;

b) kasu, takistused ja riskid, sealhulgas tundliku teabe suure kontsentratsiooniga seotud riskid;

c) koostalitlusvõime tagamiseks vajalik suutlikkus seoses muude asjakohaste teavitamissüsteemidega;

d) tegevuse juhtimise elemendid;

e) liikmesuse tingimused;

f) tehniline kord, sealhulgas finantssektori ettevõtjate ja riiklike pädevate asutuste ühisele ELi keskusele juurdepääsu üksikasjad;

g) selliste finantskulude esialgne hinnang, mis kaasnevad ühist ELi keskust toetava tegevusplatvormi loomisega (sealhulgas nõutavad eksperditeadmised).

3. Euroopa järelevalveasutused esitavad lõikes 1 osutatud aruande Euroopa Parlamendile, nõukogule ja komisjonile, hiljemalt 17. jaanuariks 2025.

Artikkel 22

Järelevalveasutuste tagasiside

1. Ilma et see piiraks tehnilist panust, nõuandeid või parandusmeetmeid ning järelmeetmeid, mida võivad asjakohastel juhtudel pakkuda vastavalt liikmesriigi õigusele direktiivi (EL) 2022/2555 kohased küberturbe intsidentide lahendamise üksused, kinnitab pädev asutus esialgse teatise ning iga artikli 19 lõikes 4 osutatud raporti kättesaamisel selle kättesaamist ja võib otstarbekuse korral esitada aegsasti asjakohast ja proportsionaalset tagasisidet või kõrgetasemelisi suuniseid finantssektori ettevõtjale, tehes eelkõige kättesaadavaks asjakohast anonüümitud teavet ja teadmust sarnaste ohtude kohta, ning võib arutada parandusmeetmeid, mida kohaldatakse finantssektori ettevõtja tasandil, ja viise negatiivse mõju minimeerimiseks ja leevendamiseks kogu finantssektorile. Ilma et see piiraks järelevalveasutustelt saadud tagasisidet, jäävad finantssektori ettevõtjad täielikult vastutavaks artikli 19 lõike 1 kohaselt teavitatud IKT intsidentide käsitlemise ja tagajärgede eest.

2. Euroopa järelevalveasutused esitavad ühiskomitee kaudu kord aastas anonüümitud koondaruande tõsiste IKT intsidentide kohta, mille üksikasjad esitavad pädevad asutused kooskõlas artikli 19 lõikega 6, ja milles esitatakse vähemalt tõsiste IKT intsidentide arv, nende laad, mõju finantssektori ettevõtjate või klientide toimingutele, võetud parandusmeetmed ja kantud kulud.

Euroopa järelevalveasutused annavad hoiatusi ja koostavad kvaliteetset statistikat, et toetada IKT-ohtude ja nõrkuse hindamist.

Artikkel 23

Krediidiasutuste, makseasutuste, kontoteabe teenuse pakkujate ja e-raha asutuste tegevust või turvalisust mõjutavate maksetega seotud intsidendid

Käesolevas peatükis sätestatud nõudeid kohaldatakse ka tegevust või turvalisust mõjutavate maksetega seotud intsidentide ning tegevust või turvalisust mõjutavate maksetega seotud tõsiste intsidentide suhtes, kui need puudutavad krediidiasutusi, makseasutusi, kontoteabe teenuse pakkujaid ning e-raha asutusi.

IV PEATÜKK

Digitaalse tegevuskerksuse testimine

Artikkel 24

Digitaalse tegevuskerksuse testimise üldnõuded

1. Et hinnata valmisolekut IKT intsidentide käsitlemiseks, tuvastada nõrgad kohad, puudused ja lüngad digitaalses tegevuskerksuses ning rakendada viivitamata parandusmeetmeid, loovad finantssektori ettevõtjad, välja arvatud mikroettevõtjad, võttes arvesse artikli 4 lõikes 2 sätestatud kriteeriume, artiklis 6 osutatud IKT-riski juhtimise raamistiku lahutamatu osana usaldusväärse ja tervikliku digitaalse tegevuskerksuse testimise programmi, hoiavad seda jõus ja vaatavad selle läbi.

2. Digitaalse tegevuskerksuse testimise programm hõlmab mitmesuguseid hindamisi, teste, meetodeid, tavasid ja vahendeid, mida kohaldatakse kooskõlas artiklitega 25 ja 26.

3. Käesoleva artikli lõikes 1 osutatud digitaalse tegevuskerksuse programmi testimisel järgivad finantssektori ettevõtjad, välja arvatud mikroettevõtjad, riskipõhist lähenemisviisi, arvestades artikli 4 lõikes 2 sätestatud kriteeriume, võttes igakülgselt arvesse IKT-riski muutuvat laadi, spetsiifilisi riske, millele asjaomane finantssektori ettevõtja on või võib olla avatud, teabevarade ja osutatud teenuste kriitilist tähtsust, aga ka kõiki muid tegureid, mida finantssektori ettevõtja peab asjakohaseks.

4. Finantssektori ettevõtjad, välja arvatud mikroettevõtjad, tagavad, et teste teevad sõltumatud isikud, kes on ettevõtja sisesed või välised. Kui teste teeb ettevõtja sisetestija, eraldab finantssektori ettevõtja piisavad vahendid ja tagab huvide konflikti vältimise testi kavandamis- ja läbiviimisetapis.

5. Finantssektori ettevõtjad, välja arvatud mikroettevõtjad, kehtestavad menetlused ja põhimõtted, et prioriseerida, liigitada ja kõrvaldada kõik testide käigus ilmnenud probleemid, ning kehtestavad sisemised valideerimismeetodid, et teha kindlaks, kas kõik tuvastatud nõrgad kohad, puudused või lüngad on täielikult kõrvaldatud.

6. Finantssektori ettevõtjad, välja arvatud mikroettevõtjad, tagavad, et kõigi kriitilise tähtsusega IKT-süsteemide ja -rakenduste suhtes viiakse läbi asjakohased testid vähemalt kord aastas.

Artikkel 25

IKT-vahendite ja -süsteemide testimine

1. Artiklis 24 osutatud digitaalse tegevuskerksuse testimise programmiga nähakse kooskõlas artikli 4 lõikes 2 sätestatud kriteeriumitega ette asjakohased testid, näiteks nõrkuse hindamised ja skaneerimised, avatud lähtekoodiga tarkvara analüüsid, võrguturvalisuse hindamised, lünkade analüüsid, füüsilise turvalisuse läbivaatamised, küsimustikud ja skaneerimistarkvara lahendused, võimaluse korral lähtekoodi ülevaatus, stsenaariumipõhised testid, ühilduvuse testimine ja jõudlustestid ning läbiv- ja läbistustestimine.

2. Väärtpaberite keskdepositooriumid ja kesksed vastaspooled viivad nõrkuse hindamise läbi enne uute või olemasolevate rakenduste ja taristukomponentide ning finantssektori ettevõtja kriitilise tähtsusega või olulisi funktsioone toetavate uute või olemasolevate IKT-teenuste esmakordset või uuesti kasutusele võttu.

3. Mikroettevõtjad teevad lõikes 1 osutatud testid, kombineerides riskipõhise lähenemisviisi IKT testimise strateegilise planeerimisega, võttes igakülgselt arvesse vajadust säilitada tasakaalustatud lähenemisviis ühelt poolt ressursside ulatuse ja käesolevas artiklis sätestatud IKT testimisele eraldatava aja ning teiselt poolt kiireloomulisuse, riski liigi, teabevarade ja osutatavate teenuste kriitilise tähtsuse ning muu asjakohase teguri vahel, sealhulgas finantssektori ettevõtja võime võtta kalkuleeritud riske.

Artikkel 26

IKT-vahendite, -süsteemide ja -protsesside süvatestimine, mis tugineb ohuteabel põhinevale läbistustestimisele

1. Finantssektori ettevõtjad, kes on kindlaks määratud vastavalt käesoleva artikli lõike 8 kolmandale lõigule, välja arvatud artikli 16 lõike 1 esimeses lõigus osutatud üksused ja mikroettevõtjad, viivad vähemalt iga kolme aasta järel läbi süvatestimise, kasutades selleks ohuteabel põhinevat läbistustestimist. Lähtudes finantssektori ettevõtja riskiprofiilist ja võttes arvesse tegevusolukorda, võib pädev asutus vajaduse korral nõuda finantssektori ettevõtjalt selle sageduse vähendamist või suurendamist.

2. Iga ohuteabel põhinev läbistustest hõlmab finantssektori ettevõtja mitmeid või kõiki kriitilise tähtsusega või olulisi funktsioone ning seda tehakse selliseid funktsioone toetavates toimivates süsteemides.

Finantssektori ettevõtjad teevad kindlaks kõik asjassepuutuvad IKT-süsteemid, -protsessid ja -tehnoloogiad, mis toetavad kriitilise tähtsusega või olulisi funktsioone ja IKT-teenuseid, sealhulgas sellised, mis toetavad kriitilise tähtsusega või olulisi funktsioone, mis on edasi antud kolmandast isikust IKT-teenuste osutajatele või nendelt alltöövõtulepingu alusel ostetud.

Finantssektori ettevõtjad hindavad, milliseid kriitilise tähtsusega või olulisi funktsioone tuleb ohuteabel põhineva läbistustestimisega hõlmata. Selle hindamise tulemusega määratakse kindlaks ohuteabel põhineva läbistustestimise täpne kohaldamisala ja pädevad asutused kinnitavad selle.

3. Kui kolmandast isikust IKT-teenuste osutajad on kaasatud ohuteabel põhinevasse läbistustestimisse, võtab finantssektori ettevõtja vajalikud meetmed ja kaitseabinõud, et tagada selliste kolmandast isikust IKT-teenuste osutajate osalemine, ning ta jääb alati täielikult vastutavaks käesoleva määruse järgimise tagamise eest.

4. Ilma et see mõjutaks lõike 2 esimest ja teist lõiku ning kui võib põhjendatult eeldada, et kolmandast isikust IKT-teenuste pakkuja osalemine ohuteabel põhinevas läbistustestimises, millele on osutatud lõikes 3, avaldab negatiivset mõju kolmandast isikust IKT-teenuste osutaja poolt selliste klientide, kes on käesoleva määruse kohaldamisalast välja jäävad üksused, osutatud teenuste kvaliteedile või turvalisusele või selliste teenustega seotud andmete konfidentsiaalsusele, võivad finantssektori ettevõtja ja kolmandast isikust IKT-teenuste osutaja kirjalikult kokku leppida, et kolmandast isikust IKT-teenuste osutaja sõlmib otse lepingu välistestijaga, eesmärgiga teha finantssektori ühe määratud ettevõtja juhtimisel ühine ohuteabel põhinev läbistustestimine, mis hõlmab mitut finantssektori ettevõtjat (ühine testimine), kellele kolmandast isikust IKT-teenuste osutaja IKT-teenuseid osutab.

Ühine testimine hõlmab asjakohast hulka IKT-teenuseid, mis toetavad finantssektori ettevõtjate poolt asjaomaselt kolmandast isikust IKT-teenuste osutajalt lepingu alusel ostetud kriitilise tähtsusega või olulisi funktsioone. Ühist testimist käsitatakse ohuteabel põhineva läbistustestimisena, mille teevad ühises testimises osalevad finantssektori ettevõtjad.

Ühistes testimistes osalevate finantssektori ettevõtjate arvu kohandatakse sobivalt, võttes arvesse asjaomaste teenuste keerukust ja liike.

5. Finantssektori ettevõtjad rakendavad koostöös kolmandast isikust IKT-teenuste osutajate ja muude asjaomaste isikutega, sealhulgas testijatega, kuid mitte pädevate asutustega, tõhusat riskijuhtimiskontrolli, et leevendada riske, mis tulenevad võimalikust mõjust andmetele, vara kahjustamisest ja kriitilise tähtsusega või oluliste funktsioonide, teenuste või toimingute häiretest finantssektori ettevõtjas endas, selle vastaspooltes või finantssektoris.

6. Testimise lõpus, pärast aruannetes ja paranduskavades kokkuleppimist, esitavad finantssektori ettevõtja ja asjakohasel juhul välistestijad lõike 9 või 10 kohaselt määratud asutusele oma järelduste kokkuvõtte, paranduskavad ning dokumendid, milles näidatakse, et ohuteabel põhinev läbistustestimine on tehtud vastavalt nõuetele.

7. Asutus esitab finantssektori ettevõtjale tõendi, milles kinnitatakse, et test viidi läbi vastavalt nõuetele, nagu on näidatud dokumentides, eesmärgiga võimaldada ohuteabel põhinevate läbistustestide vastastikust tunnustamist pädevate asutuste poolt. Finantssektori ettevõtja teavitab asjaomast pädevat asutust tõendist, asjakohaste järelduste kokkuvõttest ja paranduskavadest.

Ilma et see piiraks sellist tõendamist, vastutavad finantssektori ettevõtjad alati täielikult lõikes 4 osutatud testide mõju eest.

8. Finantssektori ettevõtjad sõlmivad ohuteabel põhineva läbistustestimise tegemiseks testijatega lepingu vastavalt artiklile 27. Kui finantsettevõtjad kasutavad ohuteabel põhineva läbistustestimise tegemiseks sisetestijaid, sõlmivad nad iga kolmanda testi puhul lepingu välistestijaga.

Krediidiasutused, kes on määruse (EL) nr 1024/2013 artikli 6 lõike 4 kohaselt liigitatud oluliseks, kasutavad kooskõlas artikli 27 lõike 1 punktidega a–e üksnes välistestijaid.

Pädevad asutused määravad kindlaks finantssektori ettevõtjad, kellelt nõutakse ohuteabel põhineva läbistustestimise tegemist, võttes arvesse artikli 4 lõikes 2 sätestatud kriteeriume, hinnates järgmisi asjaolusid:

a) mõjuga seotud tegurid, eelkõige mil määral mõjutavad finantssektori ettevõtja osutatavad teenused ja tema tegevus finantssektorit;

b) võimalikud finantsstabiilsusega seotud probleemid, sealhulgas finantssektori ettevõtja süsteemne olulisus riigi või liidu tasandil, vastavalt kohaldatavusele;

c) konkreetne IKT-riski profiil, finantssektori ettevõtja IKT küpsus või hõlmatud tehnoloogilised omadused.

9. Liikmesriigid võivad määrata finantssektoris ühe avaliku sektori asutuse, kes vastutab riiklikul tasandil ohuteabel põhineva läbistustestimisega seotud küsimuste eest finantssektoris, ning annavad talle kõik selleks vajalikud volitused ja ülesanded.

10. Käesoleva artikli lõike 9 kohase määramise puudumisel ja ilma et see piiraks õigust määrata kindlaks finantssektori ettevõtjad, kes teevad ohuteabel põhinevat läbistustestimist, võib pädev asutus delegeerida mõne või kõigi käesolevas artiklis ja artiklis 27 osutatud ülesannete täitmise mõnele teisele finantssektori riiklikule asutusele.

11. Euroopa järelevalveasutused töötavad kokkuleppel EKPga välja ühiste regulatiivsete tehniliste standardite eelnõud kooskõlas TIBER-EU raamistikuga, et täpsustada järgmist:

a) lõike 8 teise lõigu kohaldamisel kasutatud kriteeriumid;

b) sisetestijate kasutamist reguleerivad nõuded ja standardid;

c) nõuded, mis käsitlevad järgmist:

   i) lõikes 2 osutatud ohuteabel põhineva läbistustestimise kohaldamisala;

   ii) testimismetoodika ja meetodid, mida tuleb igas konkreetses testimisprotsessi etapis järgida;

   iii) testimise tulemused, lõpetamise ja parandamise etapid;

d) milline peab järelevalvealane ja muu asjaomane koostöö olema ohuteabel põhineva läbistustestimise ja selle testimise vastastikuse tunnustamise hõlbustamise korral finantssektori ettevõtjate puhul, kes tegutsevad rohkem kui ühes liikmesriigis, et võimaldada piisavat järelevalvealast kaasatust ja paindlikku rakendamist, et võtta arvesse finantssektori allsektorite või kohalike finantsturgude eripära.

Kõnealuste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused igakülgselt arvesse spetsiifilisi omadusi, mis tulenevad eri finantsteenuste sektorite tegevuse eripärast.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. juuliks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

Artikkel 27

Testijatele esitatavad nõuded ohuteabel põhineva läbistustestimise tegemiseks

1. Finantssektori ettevõtjad kasutavad ohuteabel põhinevaks läbistustestimiseks üksnes testijaid, kes:

a) on kõige sobivamad ja parima mainega;

b) omavad tehnilist ja organisatsioonilist suutlikkust ning tõendavad, et neil on eriteadmised ohuteadmuse, läbistustestimise ja punase tiimi testimise alal;

c) on sertifitseeritud liikmesriigi akrediteerimisasutuse poolt või järgivad ametlikke tegevusjuhendeid või eetikaraamistikke;

d) esitavad sõltumatu kinnituse või auditiaruande ohuteabel põhineva läbistustestimisega seotud riskide usaldusväärse juhtimise kohta, sealhulgas finantssektori ettevõtja konfidentsiaalse teabe nõuetekohase kaitse kohta ja õiguskaitsevahendite kohta finantssektori ettevõtja äririskide puhul;

e) on nõuetekohaselt ja täielikult kaetud asjakohase ametialase vastutuskindlustusega, sealhulgas väärkäitumise ja hooletuse riskide vastu.

2. Sisetestijate kasutamisel peavad finantssektori ettevõtjad tagama, et lisaks lõike 1 nõuetele täidetakse kõik järgmised tingimused:

a) kasutamise on heaks kiitnud asjaomane pädev asutus või artikli 26 lõigete 9 ja 10 kohaselt määratud üks avaliku sektori asutus;

b) asjaomane pädev asutus on teinud kindlaks, et finantssektori ettevõtjal on piisavalt asjakohaseid vahendeid ja ta on taganud huvide konflikti vältimise testi kavandamis- ja läbiviimisetapis, ning

c) ohuteadmuse pakkuja on finantssektori ettevõtja väline.

3. Finantssektori ettevõtjad tagavad, et välistestijatega sõlmitud lepingud eeldavad ohuteabel põhineva läbistustestimise tulemuste usaldusväärset haldamist ning et nende igasugune töötlemine, sealhulgas genereerimine, säilitamine, koondamine, koostamine, aru andmine, edastamine või hävitamine, ei tekita finantssektori ettevõtjale riske.

V PEATÜKK

Kolmandast isikust tuleneva IKT-riski juhtimine

I jagu

Kolmandast isikust tuleneva IKT-riski usaldusväärse juhtimise peamised põhimõtted

Artikkel 28

Üldpõhimõtted

1. Finantssektori ettevõtjad juhivad kolmandast isikust tulenevat IKT-riski oma artikli 6 lõikes 1 osutatud IKT-riski juhtimise raamistikus IKT-riski lahutamatu osana ja kooskõlas järgmiste põhimõtetega:

a) finantssektori ettevõtjad, kellel on lepingud IKT-teenuste kasutamiseks oma äritegevuses, jäävad alati täielikult vastutavaks kõigi kohustuste järgimise ja täitmise eest, mis tulenevad käesolevast määrusest ja kohaldatavast finantsteenuseid käsitlevast õigusest;

b) finantssektori ettevõtjad juhivad kolmandast isikust tulenevat IKT-riski proportsionaalsuse põhimõtet järgides, võttes arvesse järgmist:

i) IKTga seotud sõltuvuse laad, ulatus, keerukus ja tähtsus;

ii) riskid, mis tulenevad IKT-teenuste kasutamise lepingust, mis on sõlmitud kolmandast isikust IKT-teenuste osutajatega, võttes arvesse vastava teenuse, protsessi või funktsiooni kriitilist tähtsust või olulisust ning võimalikku mõju finantsteenuste ja -tegevuse järjepidevusele ja kättesaadavusele nii individuaalsel kui ka kontserni tasandil.

2. Finantssektori ettevõtjad, välja arvatud artikli 16 lõike 1 esimeses lõigus osutatud üksused ja mikroettevõtjad, võtavad IKT-riski juhtimise raamistiku osana vastu ja vaatavad korrapäraselt läbi kolmandast isikust tulenevat IKT-riski käsitleva strateegia, võttes arvesse artikli 6 lõikes 9 osutatud mitme teenuseosutajaga strateegiat, kui see on asjakohane. Kolmandast isikust tulenevat IKT-riski käsitlev strateegia hõlmab kolmandast isikust IKT-teenuste osutajate pakutavate, kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise põhimõtteid ning seda kohaldatakse individuaalselt või kohasel juhul allkonsolideeritud ja konsolideeritud alusel. Juhtorgan vaatab finantssektori ettevõtja üldise riskiprofiili ning äriteenuste ulatuse ja keerukuse hindamise alusel regulaarselt läbi riskid, mis on tuvastatud seoses kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist käsitlevate lepingutega seoses.

3. IKT-riski juhtimise raamistiku osana peavad ja ajakohastavad finantssektori ettevõtjad ettevõtja tasandil ning allkonsolideeritud ja konsolideeritud tasandil seoses kõigi lepingutega teaberegistrit kolmandast isikust IKT-teenuste osutajate osutatud IKT-teenuste kasutamise kohta.

Esimeses lõigus osutatud lepingud dokumenteeritakse asjakohaselt, eristades kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid käsitlevaid lepinguid muudest lepingutest.

Finantssektori ettevõtjad esitavad pädevatele asutustele vähemalt kord aastas teabe IKT-teenuste kasutamist käsitlevate uute lepingute arvu, kolmandast isikust IKT-teenuste osutajate kategooriate, lepingute liigi ning pakutavate teenuste ja funktsioonide kohta.

Finantssektori ettevõtjad teevad taotluse korral pädevale asutusele kättesaadavaks kogu teaberegistri või vastavalt taotlusele selle teatavad osad koos teabega, mida peetakse finantssektori ettevõtja tõhusa järelevalve seisukohast vajalikuks.

Finantssektori ettevõtjad teavitavad pädevat asutust aegsasti kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist käsitlevatest igasugustest kavandatud lepingutest ning sellest, kui funktsioon on muutunud kriitiliseks või oluliseks.

4. Enne IKT-teenuste kasutamist käsitlevate lepingute sõlmimist teevad finantssektori ettevõtjad järgmist:

a) hindavad, kas leping hõlmab kriitilise tähtsusega või olulist funktsiooni toetavate IKT-teenuste kasutamist;

b) hindavad, kas lepingu sõlmimise järelevalvealased tingimused on täidetud;

c) teevad kindlaks ja hindavad kõiki lepinguga seotud asjakohaseid riske, sealhulgas võimalust, et sellised lepingud võivad suurendada IKT kontsentratsiooniriski, nagu on osutatud artiklis 29;

d) võtavad kõik hoolsusmeetmed võimalike kolmandast isikust IKT-teenuste osutajate suhtes ning tagavad kogu valiku- ja hindamisprotsessi jooksul, et kolmandast isikust IKT-teenuste osutaja oleks sobiv;

e) tuvastavad ja hindavad huvide konflikte, mida leping võib põhjustada.

5. Finantssektori ettevõtjad võivad sõlmida lepinguid ainult selliste kolmandast isikust IKT-teenuste osutajatega, kes vastavad asjakohastele infoturbestandarditele. Kui kõnealused lepingud käsitlevad kriitilise tähtsusega või olulisi funktsioone, võtavad finantssektori ettevõtjad enne lepingu sõlmimist igakülgselt arvesse seda, kas kolmandast isikust IKT-teenuste osutajad kasutavad kõige ajakohasemaid ja parima kvaliteediga infoturbestandardeid.

6. Rakendades kolmandast isikust IKT-teenuste osutaja suhtes pääsu-, kontrolli- ja auditeerimisõigusi, määravad finantssektori ettevõtjad eelnevalt riskipõhise lähenemisviisi alusel kindlaks auditite ja kontrollide sageduse ning ka auditeeritavad valdkonnad, järgides üldtunnustatud auditeerimisstandardeid kooskõlas järelevalvejuhistega selliste auditeerimisstandardite kasutamise ja inkorporeerimise kohta.

Kui kolmandast isikust IKT-teenuste osutajatega sõlmitud IKT-teenuste kasutamise lepingud on tehniliselt väga keerukad, kontrollib finantssektori ettevõtja, kas audiitoritel (siseaudiitorid või välisaudiitorid või audiitorite rühm) on piisavad oskused ja teadmised asjaomaste auditite ja hindamiste tõhusaks läbiviimiseks.

7. Finantssektori ettevõtjad tagavad, et IKT-teenuste kasutamise lepingud võidakse lõpetada mis tahes järgmisel asjaolul:

a) kolmandast isikust IKT-teenuste osutaja rikub oluliselt kohaldatavaid õigusakte või lepingutingimusi;

b) kolmandast isikust tuleneva IKT-riski seire käigus on tuvastatud asjaolud, mis võivad muuta lepingutega reguleeritud funktsioonide täitmist, sealhulgas olulised muutused, mis mõjutavad kolmandast isikust IKT-teenuste osutaja töökorraldust või olukorda;

c) kolmandast isikust IKT-teenuste osutaja puhul on tõendatud nõrgad kohad, mis on seotud tema üldise IKT-riski juhtimisega, ja eelkõige puudused, mis puudutavad seda, kuidas ta tagab andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse isiku- või muude tundlike või isikustamata andmete puhul;

d) kui pädev asutus ei saa asjaomase lepingu tingimuste või sellega seotud olude tõttu enam finantssektori ettevõtja üle tõhusat järelevalvet teha.

8. Kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste jaoks kehtestavad finantssektori ettevõtjad väljumisstrateegiad. Väljumisstrateegiates võetakse arvesse riske, mis võivad tekkida kolmandast isikust IKT-teenuste osutajate tasandil, eelkõige nende võimalik maksejõuetuks muutumine, osutatavate IKT-teenuste kvaliteedi halvenemine, IKT-teenuste sobimatust või ebaõnnestunud osutamisest tingitud äritegevuse häired või mis tahes oluline risk, mis tekib seoses vastava IKT-teenuse asjakohase ja pideva rakendamisega või kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingute lõpetamise korral ükskõik millises lõikes 7 loetletud olukorras.

Finantssektori ettevõtjad tagavad, et neil on võimalik loobuda lepingutest,

a) häirimata oma äritegevust;

b) takistamata õigusnormide järgimist;

c) kahjustamata klientidele osutatavate teenuste järjepidevust ja kvaliteeti.

Väljumiskavad on põhjalikud, dokumenteeritud ja kooskõlas artikli 4 lõikes 2 sätestatud kriteeriumidega piisavalt testitud ja neid vaadatakse perioodiliselt läbi.

Finantssektori ettevõtjad määravad kindlaks alternatiivsed lahendused ja töötavad välja üleminekukavad, mis võimaldavad neil võtta ära lepingupõhised IKT-teenused ja asjaomased andmed kolmandast isikust IKT-teenuste osutajalt ning kanda need turvaliselt ja terviklikult üle alternatiivsetele teenuseosutajatele või inkorporeerida need uuesti ettevõttesiseselt.

Finantssektori ettevõtjad on kehtestanud asjakohased erandolukorra meetmed, et säilitada talitluspidevus kõigi esimeses lõigus osutatud asjaolude korral.

9. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja rakenduslike tehniliste standardite eelnõud, et kehtestada lõikes 3 osutatud teaberegistri standardvormid, hõlmates teavet, mis on ühine IKT-teenuste kasutamist käsitlevate kõigi lepingute puhul. Euroopa järelevalveasutused esitavad kõnealused rakenduslike tehniliste standardite eelnõud komisjonile hiljemalt 17. jaanuariks 2024.

Komisjonile antakse õigus võtta vastu esimeses lõigus osutatud rakenduslikud tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 15.

10. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja regulatiivsete tehniliste standardite eelnõud, et täpsustada lõikes 2 osutatud põhimõtete üksikasjalik sisu seoses lepingutega, mis käsitlevad kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid, mida osutavad kolmandast isikust IKT-teenuste osutajad.

Kõnealuste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust. Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. jaanuariks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

Artikkel 29

IKT kontsentratsiooniriski esialgne hindamine ettevõtjate tasandil

1. Artikli 28 lõike 4 punktis c osutatud riskide kindlakstegemisel ja hindamisel võtavad finantssektori ettevõtjad arvesse ka seda, kas kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenustega seotud lepingu kavandatav sõlmimine tooks kaasa mõne järgmise asjaolu:

a) lepingu sõlmimine kolmandast isikust IKT-teenuste osutajaga, keda ei saa hõlpsasti asendada, või

b) mitu kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste osutamist käsitlevat lepingut sama kolmandast isikust IKT-teenuste osutajaga või omavahel tihedalt seotud kolmandast isikust IKT-teenuste osutajatega.

Finantssektori ettevõtjad kaaluvad alternatiivsete lahenduste, näiteks erinevate kolmandast isikust IKT-teenuste osutajate kasutamise eeliseid ja kulusid, võttes arvesse seda, kas ja kuidas kavandatud lahendused vastavad nende digitaalse kerksuse strateegias kindlaks määratud ärivajadustele ja -eesmärkidele.

2. Kui kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist käsitlev leping hõlmab võimalust, et kolmandast isikust IKT-teenuste osutaja tellib kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid omakorda mõnelt muult kolmandast isikust IKT-teenuste osutajalt, kaaluvad finantssektori ettevõtjad kasu ja riske, mis võivad tekkida seoses tegevuse sellise võimaliku edasiandmisega, eriti juhul, kui IKT alltöövõtja on asutatud kolmandas riigis.

Kui lepingud puudutavad kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid, võtavad finantssektori ettevõtjad igakülgselt arvesse maksejõuetusõiguse sätteid, mida kohaldataks kolmandast isikust IKT-teenuste osutaja pankroti korral, ning ka takistusi, mis võivad tekkida seoses finantssektori ettevõtja andmete kiire taastamisega.

Kui kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist käsitlevad lepingud sõlmitakse kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajaga, võtavad finantssektori ettevõtjad lisaks esimeses ja teises lõigus osutatud kaalutlustele arvesse ka liidu andmekaitsenormide järgimist ning õiguse tulemuslikku jõustamist kõnealuses kolmandas riigis.

Kui kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamist käsitlevad lepingud sisaldavad sätteid alltöövõtu kohta, hindavad finantssektori ettevõtjad, kas ja kuidas pikad või keerukad alltöövõtuahelad võivad mõjutada nende võimet täielikult seirata lepingupõhiseid funktsioone ja pädeva asutuse suutlikkust teha selles osas finantssektori ettevõtja üle tulemuslikku järelevalvet.

Artikkel 30

Peamised lepingusätted

1. Finantssektori ettevõtja ja kolmandast isikust IKT-teenuste osutaja õigused ja kohustused jaotatakse selgelt ja sedastatakse kirjalikult. Täisleping sisaldab teenustaseme kokkuleppeid ja see dokumenteeritakse ühes kirjalikus dokumendis, mis on pooltele kättesaadav paberil, või dokumendina, mis on mõnes muus allalaaditavas, vastupidavas ja kättesaadavas vormingus.

2. IKT-teenuste kasutamist käsitlevad lepingud sisaldavad vähemalt järgmisi elemente:

a) kolmandast isikust IKT-teenuste osutaja kõigi funktsioonide ja IKT-teenuste selge ja täielik kirjeldus, märkides ära, kas kriitilise tähtsusega või olulist funktsiooni toetava IKT-teenuse või selle oluliste osade edasiandmine on lubatud, ja kui on, siis sellise alltöövõtu suhtes kohaldatavad tingimused;

b) asukohad, täpsemalt piirkonnad ja riigid, kus täidetakse või pakutakse lepingupõhiseid või alltöövõtu korras osutatavaid funktsioone ja IKT-teenuseid ning kus andmeid töödeldakse, sealhulgas andmete säilitamise asukoht, ning nõue, et kolmandast isikust IKT-teenuste osutaja teavitaks finantssektori ettevõtjat ette, kui ta kavatseb sellist asukohta muuta;

c) sätted andmete kohta, sealhulgas isikuandmete kaitse kättesaadavus, autentsus, terviklus ja konfidentsiaalsus;

d) sätted, mis käsitlevad ligipääsu finantssektori ettevõtja poolt töödeldavatele kergesti kättesaadavas vormis isikuandmetele ja isikustamata andmetele, samuti nende taastamist ja tagastamist kolmandast isikust IKT-teenuste osutaja maksejõuetuse, kriisilahenduse või äritegevuse lõpetamise korral või lepingute lõpetamise korral;

e) teenustaseme kirjeldused, sealhulgas nende muutmised ja läbivaatamised;

f) kolmandast isikust IKT-teenuste osutaja kohustus osutada finantssektori ettevõtjale abi ilma lisakuludeta või eelnevalt kindlaksmääratud hinnaga, kui leiab aset finantssektori ettevõtjale osutatava IKT-teenusega seotud IKT intsident;

g) kolmandast isikust IKT-teenuste osutaja kohustus teha täielikku koostööd finantssektori ettevõtja pädevate asutuste ja kriisilahendusasutustega, sealhulgas nimetatud asutuste määratud isikutega;

h) lepingu lõpetamise õigused ja sellega seotud minimaalne lepingu lõpetamisest etteteatamise aeg, vastavalt pädevate asutuste ja kriisilahendusasutuste ootustele;

i) kolmandast isikust IKT-teenuste osutajate osalemise tingimused finantssektori ettevõtjate IKT-turbe teadlikkuse suurendamise programmides ja digitaalse tegevuskerksuse koolitusel kooskõlas artikli 13 lõikega 6.

3. Kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste kasutamise lepingud sisaldavad lisaks lõikes 2 osutatud elementidele vähemalt järgmist:

a) täielikud teenustasemete kirjeldused, sealhulgas nende muutmised ja läbivaatamised koos täpsete kvantitatiivsete ja kvalitatiivsete tulemuseesmärkidega kokkulepitud teenustasemete piires, et finantssektori ettevõtja saaks teha tõhusat seiret IKT-teenuste üle ja võtta põhjendamatu viivituseta asjakohaseid parandusmeetmeid, kui kokkulepitud teenustasemeid ei saavutata;

b) kolmandast isikust IKT-teenuste osutaja poolsete teadete esitamise tähtajad ja aruandluskohustus finantssektori ettevõtja ees, hõlmates teavitamist kõigist muutustest, mis võivad oluliselt mõjutada kolmandast isikust IKT-teenuste osutaja suutlikkust tulemuslikult osutada kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid kooskõlas kokkulepitud teenustasemetega;

c) kolmandast isikust IKT-teenuste osutajale esitatavad nõuded rakendada ja testida ettevõtte talitluspidevuse plaane ning kehtestada IKT-turvameetmed, -vahendid ja -põhimõtted, mis tagavad piisaval tasemel, et finantssektori ettevõtja osutab teenuseid turvaliselt kooskõlas oma õigusraamistikuga;

d) kolmandast isikust IKT-teenuste osutaja kohustus osaleda finantssektori ettevõtja ohuteabel põhinevas läbistustestimises ja teha selle raames täielikku koostööd, nagu on osutatud artiklites 26 ja 27;

e) õigus pidevalt seirata kolmandast isikust IKT-teenuste osutaja tegevust, mis hõlmab järgmist:

i) finantssektori ettevõtja või määratud kolmanda isiku ning pädeva asutuse piiramatud pääsu-, kontrolli- ja auditeerimisõigused ning õigus teha kohapeal koopiaid asjaomastest dokumentidest, kui need on kolmandast isikust IKT-teenuste osutaja toimingute seisukohast kriitilise tähtsusega; nende õiguste tegelikku kasutamist ei takista ega piira muud lepingud ega rakenduspõhimõtted;

ii) õigus leppida kokku alternatiivsed usaldusväärsuse tasemed, kui teiste klientide õigused on mõjutatud;

iii) kolmandast isikust IKT-teenuste osutaja kohustus teha pädevate asutuste, juhtiva järelevaatamisasutuse, finantssektori ettevõtja või määratud kolmanda isiku tehtavate kohapealsete kontrollide ja auditite ajal täielikku koostööd ning

iv) kohustus esitada selliste kontrollide ja auditite ulatuse, järgitavate menetluste korra ja sageduse üksikasjad;

f) väljumisstrateegiad, eelkõige piisava kohustusliku üleminekuperioodi kehtestamine,

i) mille jooksul kolmandast isikust IKT-teenuste osutaja jätkab vastavate funktsioonide täitmist või IKT-teenuste osutamist, et vähendada häirete riski finantssektori ettevõtjas või tagada selle tõhus lahendamine ja restruktureerimine;

ii) mis võimaldab finantssektori ettevõtjal migreerida teisele kolmandast isikust IKT-teenuste osutajale või hakata kasutama ettevõtja siseseid lahendusi, mis on kooskõlas osutatud teenuse keerukusega.

Erandina punktist e võivad kolmandast isikust IKT-teenuste osutaja ja finantssektori ettevõtja, kes on mikroettevõtja, kokku leppida, et finantssektori ettevõtja pääsu-, kontrolli- ja auditeerimisõigused võib delegeerida kolmandast isikust IKT-teenuste osutaja määratud sõltumatule kolmandale isikule ning et finantssektori ettevõtja saab asjaomaselt kolmandalt isikult igal ajal nõuda kolmandast isikust IKT-teenuste osutaja tegevuse kohta teavet ja kinnitust.

4. Lepingute üle läbi rääkides kaaluvad finantssektori ettevõtjad ja kolmandast isikust IKT-teenuste osutajad, kas kasutada konkreetsete teenuste jaoks avaliku sektori asutuste välja töötatud lepingu tüüptingimusi.

5. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja regulatiivsete tehniliste standardite eelnõud, et täpsustada lõike 2 punktis a osutatud elemente, mida finantssektori ettevõtja peab kindlaks määrama ja hindama alltöövõtulepingute sõlmimisel kriitilise tähtsusega või olulisi funktsioone toetavate IKT-teenuste jaoks.

Kõnealuste regulatiivsete tehniliste standardite eelnõude väljatöötamisel võtavad Euroopa järelevalveasutused arvesse finantssektori ettevõtja suurust ja üldist riskiprofiili ning tema teenuste, tegevuse ja toimingute laadi, ulatust ja keerukust.

Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. juuliks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu esimeses lõigus osutatud regulatiivsed tehnilised standardid kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

II jagu

Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevaatamisraamistik

Artikkel 31

Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate määramine

1. Euroopa järelevalveasutused teevad ühiskomitee kaudu ja artikli 32 lõike 1 kohaselt loodud järelevalvefoorumi soovitusel järgmist:

a) määravad finantssektori ettevõtjate jaoks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad pärast hindamist, milles võetakse arvesse lõikes 2 sätestatud kriteeriume;

b) määravad igale kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale juhtivaks järelevaatamisasutuseks Euroopa järelevalveasutuse, kes on vastavalt määrusele (EL) nr 1093/2010, (EL) nr 1094/2010 või (EL) nr 1095/2010 vastutav finantssektori ettevõtjate eest, kellele ühiselt kuulub suurim osa kõigi selliste finantssektori ettevõtjate varade koguväärtusest, kes kasutavad asjaomase kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja teenuseid, lähtudes nende finantssektori ettevõtjate individuaalsete bilansside summast.

2. Lõike 1 punktis a osutatud määramine põhineb kõigil järgmistel kriteeriumidel, mis on seotud kolmandast isikust IKT-teenuste osutaja osutatavate IKT-teenustega:

a) süsteemne mõju finantsteenuste pakkumise stabiilsusele, järjepidevusele või kvaliteedile juhul, kui asjaomast kolmandast isikust IKT-teenuste osutajat tabaks laiaulatuslik teenuste osutamise katkemine, võttes arvesse nende finantssektori ettevõtjate arvu ja nende finantssektori ettevõtjate varade koguväärtust, kellele asjaomane kolmandast isikust IKT-teenuste osutaja teenuseid osutab;

b) asjaomasest kolmandast isikust IKT-teenuste osutajast sõltuvate finantssektori ettevõtjate süsteemne olemus või olulisus, mida hinnatakse järgmiste parameetrite alusel:

   i) nende globaalsete süsteemselt oluliste ettevõtjate või muude süsteemselt oluliste ettevõtjate arv, kes sõltuvad asjaomasest kolmandast isikust IKT-teenuste osutajast;

   ii) punktis i osutatud globaalsete süsteemselt oluliste ettevõtjate või muude süsteemselt oluliste ettevõtjate ja muude finantssektori ettevõtjate vastastikune sõltuvus, sealhulgas olukorrad, kus globaalsed või muud süsteemselt olulised ettevõtjad osutavad finantstaristu teenuseid teistele finantssektori ettevõtjatele;

c) finantssektori ettevõtjate tuginemine teenustele, mida osutab asjaomane kolmandast isikust IKT-teenuste osutaja seoses finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonidega, mis lõpuks hõlmavad sama kolmandast isikust IKT-teenuste osutajat, olenemata sellest, kas finantssektori ettevõtjad sõltuvad nendest teenustest otseselt või kaudselt alltöövõtulepingute kaudu;

d) kolmandast isikust IKT-teenuste osutaja asendatavus, võttes arvesse järgmisi parameetreid:

   i) tõeliste alternatiivide (isegi osaliselt) puudumine, mis on tingitud konkreetsel turul tegutsevate kolmandast isikust IKT-teenuste osutajate vähesusest või asjaomase kolmandast isikust IKT-teenuste osutaja turuosast või tegevuse tehnilisest keerukusest (sealhulgas seoses patenditud tehnoloogiaga) või kolmandast isikust IKT-teenuste osutaja organisatsiooni või tegevuse eripärast;

   ii) raskused seoses asjaomaste andmete ja töökoormuse osalise või täieliku migreerimisega asjaomaselt kolmandast isikust IKT-teenuste osutajalt teisele kolmandast isikust IKT-teenuste osutajale, mis on tingitud kas märkimisväärsetest rahalistest kuludest, ajakulust või muudest ressurssidest, mida migratsioon võib hõlmata, või suurenenud IKT-riskist või muudest operatsiooniriskidest, millega finantssektori ettevõtja võib sellise migratsiooni tõttu kokku puutuda;

3. Kui kolmandast isikust IKT-teenuste osutaja kuulub kontserni, hinnatakse lõikes 2 osutatud kriteeriume nendest IKT-teenustest lähtuvalt, mida osutab kontsern tervikuna.

4. Kontserni kuuluvad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad määravad ühe juriidilise isiku koordineerimiskeskuseks, et tagada piisav esindatus ja teabevahetus juhtiva järelevaatamisasutusega.

5. Juhtiv järelevaatamisasutus teavitab kolmandast isikust IKT-teenuste osutajat hindamise tulemusest, millele järgneb lõike 1 punktis a osutatud määramine. Kuue nädala jooksul alates teavitamise kuupäevast võib kolmandast isikust IKT-teenuste osutaja esitada juhtivale järelevaatamisasutusele hindamiseks põhjendatud avalduse koos asjakohase teabega. Juhtiv järelevaatamisasutus vaatab põhjendatud avalduse läbi ja võib nõuda lisateabe esitamist 30 kalendripäeva jooksul avalduse saamisest.

Pärast kolmandast isikust IKT-teenuste osutaja kriitilise tähtsusega teenuseosutajaks määramist teatavad Euroopa järelevalveasutused ühiskomitee kaudu kolmandast isikust IKT-teenuste osutajale sellisest määramisest ja kuupäevast, millest alates tema üle tegelikult järelevaatamist tehakse. See alguskuupäev ei tohi olla hilisem kui üks kuu pärast teatamist. Kolmandast isikust IKT-teenuste osutaja teavitab finantssektori ettevõtjaid, kellele nad teenuseid osutavad, oma kriitilise tähtsusega teenuseosutajaks määramisest.

6. Komisjonil on õigus võtta kooskõlas artikliga 57 käesoleva määruse täiendamiseks vastu delegeeritud õigusakt, milles täpsustatakse veelgi käesoleva artikli lõikes 2 osutatud kriteeriume hiljemalt 17. juuliks 2024.

7. Lõike 1 punktis a osutatud määramist ei kasutata enne, kui komisjon on võtnud kooskõlas lõikega 6 vastu delegeeritud õigusakti.

8. Lõike 1 punktis a osutatud määramist ei kohaldata järgmise suhtes:

i) finantssektori ettevõtjad, kes osutavad IKT-teenuseid teistele finantssektori ettevõtjatele;

ii) kolmandast isikust IKT-teenuste osutajad, kelle suhtes kohaldatakse järelevaatamisraamistikke, mis on kehtestatud Euroopa Liidu toimimise lepingu artikli 127 lõikes 2 osutatud ülesannete täitmise toetamiseks;

iii) kontsernisisesed IKT-teenuste osutajad;

iv) kolmandast isikust IKT-teenuste osutajad, kes osutavad IKT-teenuseid üksnes ühes liikmesriigis ainult selles liikmesriigis tegutsevatele finantssektori ettevõtjatele.

9. Euroopa järelevalveasutused koostavad, avaldavad ja ajakohastavad igal aastal ühiskomitee kaudu liidu tasandil kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate loetelu.

10. Lõike 1 punkti a kohaldamisel edastavad pädevad asutused igal aastal artikli 28 lõike 3 kolmandas lõigus osutatud koondaruanded artikli 32 kohaselt loodud järelevaatamisfoorumile. Järelevaatamisfoorum hindab finantssektori ettevõtjate sõltuvust kolmandast isikust IKT-teenuste osutajatest pädevatelt asutustelt saadud teabe põhjal.

11. Kolmandast isikust IKT-teenuste osutajad, kes ei ole kantud lõikes 9 osutatud loetellu, võivad taotleda kriitilise tähtsusega ettevõtjaks määramist vastavalt lõike 1 punktile a.

Esimese lõigu kohaldamisel esitab kolmandast isikust IKT-teenuste osutaja põhjendatud taotluse EBA-le, ESMA-le või EIOPA-le, kes otsustab ühiskomitee kaudu, kas määrata see kolmandast isikust IKT-teenuste osutaja kriitilise tähtsusega ettevõtjaks vastavalt lõike 1 punktile a.

Teises lõigus osutatud otsus võetakse vastu ja sellest teatatakse kolmandast isikust IKT-teenuste osutajale kuue kuu jooksul alates taotluse saamisest.

12. Finantssektori ettevõtjad kasutavad sellise kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutaja teenuseid, mis on lõike 1 punkti a kohaselt määratud kriitilise tähtsusega ettevõtjaks, üksnes juhul, kui kõnealune ettevõtja on asutanud liidus tütarettevõtja 12 kuu jooksul pärast määramist.

13. Lõikes 12 osutatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja teavitab juhtivat järelevaatamisasutust kõigist muudatustest liidus asutatud tütarettevõtja juhtimisstruktuuris.

Artikkel 32

Järelevaatamisraamistiku struktuur

1. Ühiskomitee asutab kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikli 57 lõikega 1 allkomiteena järelevaatamisfoorumi, et toetada ühiskomitee ja artikli 31 lõike 1 punktis b osutatud juhtiva järelevaatamisasutuse tööd, mis on seotud kolmandast isikust tuleneva IKT-riskiga finantssektoris. Järelevaatamisfoorum valmistab ette ühiskomitee kõnealuse valdkonna ühisseisukohtade ja -aktide eelnõud.

Järelevaatamisfoorum arutab korrapäraselt IKT-riski ja nõrkusega seotud muutusi ning edendab kolmandast isikust tuleneva IKT-riski järjepidevat seiret liidu tasandil.

2. Järelevaatamisfoorum hindab igal aastal ühiselt kõigi kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevaatamise tulemusi ja leide ning edendab koordineerimismeetmeid, et suurendada finantssektori ettevõtjate digitaalset tegevuskerksust, edendada IKT kontsentratsiooniriski käsitlemise parimaid tavasid ja uurida riskide valdkonnaülest ülekandumist leevendavaid tegureid.

3. Järelevaatamisfoorum esitab kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate põhjalikud võrdlusalused, mille ühiskomitee võtab vastu Euroopa järelevalveasutuste ühiste seisukohtadena kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikli 56 lõikega 1.

4. Järelevaatamisfoorumisse kuuluvad:

a) Euroopa järelevalveasutuste eesistujad;

b) igast liikmesriigist üks kõrgetasemeline esindaja artiklis 46 osutatud asjaomase pädeva asutuse praeguste töötajate hulgast;

c) vaatlejatena kõigi Euroopa järelevalveasutuste tegevdirektorid ning üks komisjoni, Euroopa Süsteemsete Riskide Nõukogu, EKP ja ENISA esindaja;

d) asjakohasel juhul vaatlejana artiklis 46 osutatud pädeva asutuse üks täiendav esindaja igast liikmesriigist;

e) asjakohasel juhul vaatlejana nende direktiivi (EL) 2022/2555 kohaselt määratud või asutatud pädevate asutuste üks esindaja, kes vastutavad nimetatud direktiivi kohaldamisalasse jääva elutähtsa või olulise üksuse järelevalve eest.

Järelevaatamisfoorum võib kohasel juhul küsida nõu lõike 6 kohaselt ametisse nimetatud sõltumatutelt ekspertidelt.

5. Iga liikmesriik määrab asjaomase pädeva asutuse, kelle töötaja on lõike 4 esimese lõigu punktis b osutatud kõrgetasemeline esindaja, ja teavitab sellest juhtivat järelevaatamisasutust.

Euroopa järelevalveasutused avaldavad oma veebisaidil liikmesriikide asjaomase pädeva asutuse praeguste töötajate hulgast määratud kõrgetasemeliste esindajate nimekirja.

6. Lõike 4 teises lõigus osutatud sõltumatud eksperdid nimetab järelevaatamisfoorum ametisse ekspertide seast, kes valitakse avalikus ja läbipaistvas kandideerimismenetluses.

Sõltumatud eksperdid nimetatakse ametisse, arvestades nende eksperditeadmisi finantsstabiilsuse, digitaalse tegevuskerksuse ja IKT turvalisuse alal. Nad täidavad oma ülesandeid sõltumatult ja objektiivselt üksnes liidu kui terviku huvides ning ei küsi ega võta vastu juhiseid liidu institutsioonidelt ega asutustelt, liikmesriikide valitsustelt ega muudelt avaliku või erasektori asutustelt.

7. Euroopa järelevalveasutused annavad kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artikliga 16 hiljemalt 17. juuliks 2024 välja käesoleva jao kohaldamise suunised, milles käsitletakse Euroopa järelevalveasutuste ja pädevate asutuste vahelist koostööd ning mis hõlmavad pädevate asutuste ja Euroopa järelevalveasutuste vahel ülesannete jaotamise ja täitmise üksikasjalikke protseduure ja tingimusi ning teabevahetuse üksikasju, mida pädevad asutused vajavad, et tagada artikli 35 lõike 1 punkti d kohaselt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele esitatud soovituste järgimine.

8. Käesolevas jaos sätestatud nõuded ei piira direktiivi (EL) 2022/2555 ega pilvteenuste osutajate suhtes kohaldatavate muude liidu järelevaatamisnormide kohaldamist.

9. Euroopa järelevalveasutused esitavad igal aastal ühiskomitee kaudu ja järelevaatamisfoorumi eeltöö põhjal Euroopa Parlamendile, nõukogule ja komisjonile aruande käesoleva jao kohaldamise kohta.

Artikkel 33

Juhtiva järelevaatamisasutuse ülesanded

1. Artikli 31 lõike 1 punkti b kohaselt määratud juhtiv järelevaatamisasutus korraldab järelevaataamise määratud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle ning on kõigi järelevaatamisega seotud küsimuste puhul nende kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate peamine kontaktpunkt.

2. Lõike 1 kohaldamisel hindab juhtiv järelevaatamisasutus, kas kõik kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad on kehtestanud põhjalikud, usaldusväärsed ja tulemuslikud reeglid, protsessid, mehhanismid ja korra, et juhtida IKT-riski, mida ta võib tekitada finantssektori ettevõtjatele.

Esimeses lõigus osutatud hindamisel keskendutakse peamiselt IKT-teenustele, mida osutab kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonide toetamiseks. Kui see on vajalik kõigi asjakohaste riskide käsitlemiseks, hõlmab kõnealune hindamine ka muid kui kriitilise tähtsusega või olulisi funktsioone toetavaid IKT-teenuseid.

3. Lõikes 2 osutatud hindamine hõlmab järgmist:

a) IKT-nõuded, et tagada eelkõige selliste teenuste turvalisus, kättesaadavus, järjepidevus, skaleeritavus ja kvaliteet, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja osutab finantssektori ettevõtjatele, samuti suutlikkus säilitada igal ajal andmete kättesaadavuse, autentsuse, tervikluse ja konfidentsiaalsuse ranged standardid;

b) füüsiline julgeolek, mis aitab tagada IKT turvalisust, sealhulgas ruumide, rajatiste ja andmekeskuste turvalisus;

c) riskijuhtimisprotsessid, sealhulgas IKT-riski juhtimise põhimõtted, IKT talitluspidevuse põhimõtted ning IKT reageerimis- ja taastekavad;

d) juhtimiskord, sealhulgas organisatsiooniline struktuur, millel on selged, läbipaistvad ja järjepidevad vastutusliinid, ning IKT-riski tõhusalt juhtida võimaldavad vastutusreeglid;

e) tõsiste IKT intsidentide tuvastamine, seire ja neist finantssektori ettevõtjatele kiire teatamine ning selliste intsidentide, eelkõige küberrünnete käsitlemine ja lahendamine;

f) andmete ja rakenduste porditavuse ja koostalitlusvõime mehhanismid, mis tagavad, et finantssektori ettevõtjad saavad lõpetamisõigust tulemuslikult kasutada;

g) IKT-süsteemide, -taristu ja -kontrollide testimine;

h) IKT-auditid;

i) selliste asjakohaste riiklike ja rahvusvaheliste standardite kasutamine, mida kohaldatakse IKT-teenuste osutamisel finantssektori ettevõtjatele.

4. Lõikes 2 osutatud hindamise alusel ja artikli 34 lõikes 1 osutatud ühise järelevaatamisvõrgustikuga koostöös võtab juhtiv järelevaatamisasutus vastu selge, üksikasjaliku ja põhjendatud individuaalse järelevaatamiskava, milles kirjeldatakse iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja jaoks kavandatud iga-aastase järelevaatamise eesmärke ja peamisi järelevaatamismeetmeid. See kava edastatakse igal aastal kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale.

Enne järelevaatamiskava vastuvõtmist edastab juhtiv järelevaatamisasutus järelevaatamiskava projekti kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale.

Pärast järelevaatamiskava projekti kättesaamist võib kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esitada 15 kalendripäeva jooksul põhjendatud avalduse, milles tõendatakse eeldatavat mõju klientidele, kes on käesoleva määruse kohaldamisalast välja jäävad üksused, ning sõnastatakse lahendused riskide maandamiseks, kui see on asjakohane.

5. Kui lõikes 4 osutatud iga-aastased järelevaatamiskavad on vastu võetud ja neist on teatatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele, võivad pädevad asutused võtta meetmeid seoses kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega üksnes kokkuleppel juhtiva järelevaatamisasutusega.

Artikkel 34

Tegevuse koordineerimine juhtivate järelevaatamisasutuste vahel

1. Selleks et tagada järjepidev lähenemisviis järelevaatamistegevusele ning võimaldada koordineeritud üldiste järelevaatamisstrateegiate ning sidusate tegevuspõhiste lähenemisviiside ja töömeetodite kasutamist, loovad kolm artikli 31 lõike 1 punkti b kohaselt määratud juhtivat järelevaatamisasutust ühise järelevaatamisvõrgustiku, et koordineerida omavahel tegevust ettevalmistavates etappides ja järelevaatamistoimingute tegemist kõigi kolme järelevaatamisasutuse järelevaatamise all olevate kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate üle ning artikli 42 kohaselt vajalikku tegevust.

2. Lõike 1 kohaldamisel koostavad juhtivad järelevaatamisasutused ühise järelevaatamisprotokolli, milles täpsustatakse üksikasjalik kord, mida tuleb järgida igapäevasel koordineerimisel ning kiire teabevahetuse ja reageerimise tagamisel. Protokoll vaadatakse korrapäraselt läbi, et võtta arvesse tegevusega seotud vajadusi, eelkõige praktilise järelevaatamiskorra muutumist.

3. Juhtivad järelevaatamisasutused võivad vajaduse korral paluda EKP-l ja ENISA-l anda tehnilist nõu, jagada praktilisi kogemusi või ühineda ühise järelevaatamisvõrgustiku konkreetsete koordineerimiskoosolekutega.

Artikkel 35

Juhtiva järelevaatamisasutuse volitused

1. Käesolevas jaos sätestatud ülesannete täitmiseks on juhtival järelevaatamisasutusel seoses kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaga järgmised volitused:

a) nõuda vastavalt artiklile 37 kogu asjakohast teavet ja dokumentatsiooni;

b) viia läbi üldisi uurimisi ja kontrolle kooskõlas kas artikliga 38 või artikliga 39;

c) nõuda pärast järelevalvetoimingute lõpuleviimist aruandeid, milles täpsustatakse meetmed või parandusmeetmed, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad on võtnud seoses käesoleva lõike punktis d osutatud soovitustega;

d) anda soovitusi artikli 33 lõikes 3 osutatud valdkondades, eelkõige seoses järgmisega:

   i) konkreetsete IKT turva- ja kvaliteedinõuete või -protsesside kasutamine, eelkõige seoses paikade, uuenduste, krüpteerimise ja muude turvameetmete kasutuselevõtuga, mida juhtiv järelevaatamisasutus peab vajalikuks, et tagada finantssektori ettevõtjatele osutatavate IKT-teenuste turvalisus;

   ii) selliste tingimuste kasutamine (sealhulgas tehniline rakendamine), mille alusel kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad osutavad teenuseid finantssektori ettevõtjatele, mida juhtiv järelevaatamisasutus peab oluliseks, et hoida ära nõrkade lülide tekitamist või nende võimendamist või et minimeerida võimalikku süsteemset mõju kogu liidu finantssektoris IKT kontsentratsiooniriski korral;

   iii) mis tahes kavandatud alltöövõtt, kui juhtiv järelevaatamisasutus leiab, et tegevuse täiendav edasiandmine, sealhulgas alltöövõtulepingud, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad kavatsevad sõlmida kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutajatega või IKT alltöövõtjaga, võib põhjustada riske finantssektori ettevõtja teenuste osutamisel või ohustada finantsstabiilsust, lähtudes artiklite 37 ja 38 kohaselt kogutud teabe läbivaatamisest;

   iv) täiendavate alltöövõtulepingute sõlmimisest hoidumine, kui on täidetud järgmised kumulatiivsed tingimused:

      — kavandatav alltöövõtja on kolmandas riigis asutatud kolmandast isikust IKT-teenuste osutaja või IKT alltöövõtja;

      — alltöövõtt on seotud finantssektori ettevõtja kriitilise tähtsusega või oluliste funktsioonidega ning

— juhtiv järelevaaatamisasutus leiab, et sellise alltöövõtu kasutamine kujutab endast selget ja tõsist ohtu liidu finantsstabiilsusele või finantssektori ettevõtjatele, sealhulgas finantssektori ettevõtjate suutlikkusele täita järelevalvenõudeid.

Käesoleva punkti alapunkti iv kohaldamisel edastavad kolmandast isikust IKT-teenuste osutajad, kasutades artikli 41 lõike 1 punktis b osutatud vormi, juhtivale järelevaatamisasutusele alltöövõttu käsitleva teabe.

2. Käesolevas artiklis osutatud volituste kasutamisel teeb juhtiv järelevaatamisasutus järgmist:

a) tagab korrapärase koordineerimise ühise järelevaatamisvõrgustiku raames ja püüab kohasel viisil eelkõige jõuda järjepideva lähenemisviisini seoses kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järele vaatamisega;

b) võtab täielikult arvesse direktiiviga (EL) 2022/2555 kehtestatud raamistikku ning konsulteerib vajaduse korral nimetatud direktiivi kohaselt määratud või asutatud pädevate asutustega, et vältida selliste tehniliste ja korralduslike meetmete tarbetut dubleerimist, mida võidakse kõnealuse direktiivi kohaselt kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes kohaldada;

c) püüab nii palju kui võimalik minimeerida selliste teenuste katkemise riski, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad osutavad klientidele, kes on käesoleva määruse kohaldamisalast välja jäävad üksused.

3. Juhtiv järelevaatamisasutus konsulteerib enne lõikes 1 osutatud volituste kasutamist järelevaatamisfoorumiga.

Enne lõike 1 punkti d kohaste soovituste esitamist annab juhtiv järelevaatamisasutus kolmandast isikust IKT-teenuste osutajale võimaluse esitada 30 kalendripäeva jooksul asjakohast teavet, millega tõendatakse eeldatavat mõju klientidele, kes on käesoleva määruse kohaldamisalast välja jäävad üksused, ning sõnastatakse lahendused riskide maandamiseks, kui see on asjakohane.

4. Juhtiv järelevaatamisasutus teavitab ühist järelevaatamisvõrgustikku lõike 1 punktides a ja b osutatud volituste kasutamise tulemustest. Juhtiv järelevaatamisasutus edastab lõike 1 punktis c osutatud aruanded põhjendamatu viivituseta ühisele järelevaatamisvõrgustikule ja asjaomase kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja IKT-teenuseid kasutavate finantssektori ettevõtjate pädevatele asutustele.

5. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad teevad heas usus koostööd juhtiva järelevaatamisasutusega ja abistavad teda tema ülesannete täitmisel.

6. Kui lõike 1 punktide a, b ja c kohaste volituste kasutamiseks nõutavad meetmed on täielikult või osaliselt täitmata ja pärast vähemalt 30 kalendripäeva möödumist alates kuupäevast, mil kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja sai vastava meetme kohta teate, võtab juhtiv järelevaatamisasutus vastu otsuse, millega määratakse sunniraha, et sundida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajat kõnealuseid meetmeid täitma.

7. Lõikes 6 osutatud sunniraha määratakse iga päeva kohta kuni meetmete täitmise saavutamiseni ja mitte kauemaks kui kuueks kuuks pärast kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja teavitamist sunniraha määramise otsusest.

8. Sunniraha summa, mis arvutatakse alates sunniraha määramise otsuses kindlaks määratud kuupäevast, on kuni 1 % kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja eelmise majandusaasta ülemaailmsest keskmisest päevakäibest. Sunniraha summa kindlaksmääramisel võtab juhtiv järelevaatamisasutus seoses lõikes 6 osutatud meetmete täitmatajätmisega arvesse järgmisi kriteeriume:

a) täitmatajätmise raskusaste ja kestus;

b) kas täitmatajätmine pandi toime tahtlikult või hooletuse tõttu;

c) kolmandast isikust IKT-teenuste osutaja koostöö ulatus juhtiva järelevaatamisasutusega.

Esimese lõigu kohaldamisel konsulteerib juhtiv järelevaatamisasutus järjepideva lähenemisviisi tagamiseks ühise järelevaatamisvõrgustikuga.

9. Sunniraha on haldusõiguslik sunnivahend ja täitmisele pööratav. Täitmist reguleerivad selles liikmesriigis kehtivad tsiviilmenetluse normid, mille territooriumil kontrollid aset leiavad ja kus on juurdepääs. Kaebused, mis on seotud täitmise normide eiramisega, kuuluvad asjaomase liikmesriigi kohtute pädevusse. Sunniraha summad kantakse Euroopa Liidu üldeelarvesse.

10. Juhtiv järelevaatamisasutus avalikustab kõik sunniraha määramise juhud, välja arvatud juhul, kui selline avalikustamine ohustaks tõsiselt finantsturge või tekitaks asjaomastele isikutele ebaproportsionaalset kahju.

11. Enne lõike 6 alusel sunniraha määramist annab juhtiv järelevaatamisasutus selle kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esindajatele, kelle suhtes on algatatud menetlus, võimaluse esitada järelduste kohta oma seisukoht, ning teeb oma otsused üksnes nende järelduste põhjal, mille kohta kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajal, kelle suhtes on algatatud menetlus, on olnud võimalus oma seisukoht esitada.

Menetluse käigus tagatakse täielikult uurimisaluste isikute õigus kaitsele. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajal, kelle suhtes on algatatud menetlus, on õigus tutvuda toimikuga tingimusel, et võetakse arvesse teiste isikute õigustatud huvi kaitsta oma ärisaladusi. Toimikuga tutvumise õigus ei hõlma konfidentsiaalset teavet ega juhtiva järelevaatamisasutuse asutusesiseseks kasutuseks ette nähtud ettevalmistavaid dokumente.

Artikkel 36

Juhtiva järelevaatamisasutuse volituste kasutamine väljaspool liitu

1. Kui järelevaatamise eesmärke ei ole võimalik saavutada suheldes artikli 31 lõike 12 kohaselt asutatud tütarettevõtjaga või tehes järelevaatamist liidus asuvates ruumides, võib juhtiv järelevaatamisasutus kasutada kolmandas riigis asuvates ruumides, mis on kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja omandis või mida ta mis tahes viisil kasutab liidu finantssektori ettevõtjatele teenuste osutamiseks, kõnealuse IKT-teenuste osutaja äritegevuse, funktsioonide või teenuste, sealhulgas haldus-, äri- või tegevbüroode, ruumide, maa, hoonete või muu varaga seoses järgnevates sätetes osutatud volitusi:

a) artikli 35 lõike 1 punkt a ning

b) artikli 35 lõike 1 punkt b kooskõlas artikli 38 lõike 2 punktidega a, b ja d ning artikli 39 lõikega 1 ja lõike 2 punktiga a.

Esimeses lõigus osutatud volitusi võib kasutada, kui on täidetud kõik järgnevad tingimused:

i) juhtiva järelevaatamisasutuse hinnangul on vajalik kontrolli tegemine kolmandas riigis, et tal oleks võimalik täielikult ja tõhusalt täita oma käesolevast määrusest tulenevaid ülesandeid;

ii) kolmandas riigis tehtav kontroll on otseselt seotud IKT-teenuste osutamisega liidu finantssektori ettevõtjatele;

iii) asjaomane kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja nõustub kontrolli tegemisega kolmandas riigis ning

iv) juhtiv järelevaatamisasutus on asjaomase kolmanda riigi asjakohast asutust ametlikult teavitanud ja viimane ei ole kontrolli suhtes vastuväiteid esitanud.

2. Ilma et see piiraks liidu institutsioonide ja liikmesriikide vastavat pädevust, sõlmib EBA, ESMA või EIOPA lõike 1 kohaldamisel kolmanda riigi asjakohase asutusega halduskoostöö kokkulepped, et juhtiv järelevaatamisasutus ja tema määratud töörühm saaksid asjaomases kolmandas riigis sujuvalt kontrolle teha. Kõnealused koostöökokkulepped ei loo liidu ega selle liikmesriikide jaoks õiguslikke kohustusi ega takista liikmesriike ja nende pädevaid asutusi sõlmimast kahe- või mitmepoolseid kokkuleppeid kõnealuste kolmandate riikide ja nende asjakohaste asutustega.

Nendes koostöökokkulepetes määratakse kindlaks vähemalt järgmised elemendid:

a) käesoleva määruse kohase järelevaatamistegevuse koordineerimise kord ja asjaomase kolmanda riigi asjakohase asutuse tehtav analoogne kolmandast isikust tuleneva IKT-riski seire finantssektoris, sealhulgas asjakohase asutuse nõusoleku edastamise üksikasjad, millega lubatakse juhtival järelevaatamisasutusel ja tema määratud töörühmal korraldada asjakohase asutuse jurisdiktsiooni alla kuuluval territooriumil üldisi uurimisi ja kohapealseid kontrolle, millele on osutatud lõike 1 esimeses lõigus;

b) asjakohase teabe edastamise kord EBA, ESMA või EIOPA ning asjaomase kolmanda riigi asjakohase asutuse vahel, eelkõige seoses teabega, mida juhtiv järelevaatamisasutus võib artikli 37 kohaselt nõuda;

c) mehhanismid, mille abil asjaomase kolmanda riigi asjakohane asutus teavitab viivitamata EBAd, ESMAd või EIOPAd juhtumitest, mille puhul kolmandas riigis asutatud ja artikli 31 lõike 1 punkti a kohaselt kriitilise tähtsusega ettevõtjaks määratud kolmandast isikust IKT-teenuste osutaja on rikkunud nõudeid, mida ta on kohustatud asjaomase kolmanda riigi kohaldatava õiguse kohaselt järgima kui ta osutab teenuseid kõnealuses kolmandas riigis asutatud finantsasutustele, ning kohaldatud õiguskaitsevahenditest ja karistustest;

d) asjaomase kolmanda riigi finantsasutuste kolmandast isikust tuleneva IKT-riski seiret käsitlevate regulatiivsete või järelevalvealaste suundumuste kohta ajakohastatud teabe korrapärane edastamine;

e) üksikasjad, mis võimaldavad vajaduse korral ühe asjaomase kolmanda riigi asutuse esindaja osalemist juhtiva järelevaatamisasutuse ja määratud rühma tehtavates kontrollides.

3. Kui juhtiv järelevaatamisasutus ei saa teha lõigetes 1 ja 2 osutatud järelevaatamist väljaspool liitu, teeb juhtiv järelevaatamisasutus järgmist:

a) kasutab oma artikli 35 kohaseid volitusi kõigi talle kättesaadavate faktide ja dokumentide alusel;

b) dokumenteerib ja selgitab kõiki tagajärgi, mis tulenevad asjaolust, et ta ei saanud teha järelevaatamist käesolevas artiklis osutatud viisil.

Käesoleva lõike punktis b osutatud võimalikke tagajärgi võetakse arvesse juhtiva järelevaatamisasutuse soovitustes, mis esitatakse artikli 35 lõike 1 punkti d kohaselt.

Artikkel 37

Teabenõue

1. Juhtiv järelevaatamisasutus võib lihtteabenõude või otsusega nõuda, et kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad esitaksid kogu teabe, mida on juhtival järelevaatamisasutusel vaja käesolevast määrusest tulenevate ülesannete täitmiseks, sealhulgas kõik asjakohased äri- või tegevusdokumendid, lepingud, strateegiad, dokumentatsioon, IKT turvalisuse auditiaruanded ja IKT intsidentide aruanded, samuti kogu teabe, mis on seotud isikutega, kellele kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja on funktsioonid või tegevuse edasi andnud.

2. Kui juhtiv järelevaatamisasutus saadab lõike 1 kohase lihtteabenõude, peab ta:

a) viitama nõude õigusliku alusena käesolevale artiklile;

b) nimetama teabenõude eesmärgi;

c) täpsustama, millise teabe esitamist nõutakse;

d) määrama tähtaja, mille jooksul teave tuleb esitada;

e) teavitama kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esindajat, kellelt teavet taotletakse, et teabe andmine ei ole kohustuslik, kuid et teabenõude alusel vabatahtlikult esitatav teave ei tohi olla ebaõige ega eksitav.

3. Kui juhtiv järelevaatamisasutus nõuab otsuse alusel teabe esitamist vastavalt lõikele 1, peab ta:

a) viitama nõude õigusliku alusena käesolevale artiklile;

b) nimetama teabenõude eesmärgi;

c) täpsustama, millise teabe esitamist nõutakse;

d) määrama tähtaja, mille jooksul teave tuleb esitada;

e) märkima artikli 35 lõikes 6 ette nähtud sunniraha, mida kohaldatakse, kui nõutav teave esitatakse mittetäielikult või kui teavet ei esitata käesoleva lõike punktis d osutatud tähtaja jooksul;

f) viitama õigusele kaevata otsus edasi Euroopa järelevalveasutuse apellatsiooninõukogule ja õigusele vaidlustada otsus Euroopa Liidu Kohtus (edaspidi „Euroopa Kohus“) vastavalt määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitele 60 ja 61.

4. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate esindajad esitavad nõutud teabe. Nõuetekohaselt volitatud juristid võivad teavet esitada oma klientide nimel. Kui esitatud teave on ebatäielik, ebaõige või eksitav, jääb täielikult vastutavaks kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja.

5. Juhtiv järelevaatamisasutus edastab teabeesitamise otsuse koopia viivitamata nende finantssektori ettevõtjate pädevatele asutustele, kes kasutavad asjaomaste kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate teenuseid, ning ühisele järelevaatamisvõrgustikule.

Artikkel 38

Üldised uurimised

1. Käesolevast määrusest tulenevate ülesannete täitmiseks võib juhtiv järelevaatamisasutus, keda abistab artikli 40 lõikes 1 osutatud ühine kontrollirühm, korraldada kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate suhtes uurimisi, kui see on vajalik.

2. Juhtival järelevaatamisasutusel on volitus:

a) kontrollida dokumente, andmeid, protseduure ja muid tema ülesannete täitmisega seonduvaid materjale, sõltumata nende säilitamiseks kasutatud andmekandjast;

b) teha või saada nendest dokumentidest, andmetest, dokumenteeritud protseduuridest ja mis tahes muudest materjalidest tõendatud koopiaid või väljavõtteid;

c) kutsuda kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esindajaid välja ja paluda neil anda suulisi või kirjalikke selgitusi uurimise sisu ja eesmärgiga seotud asjaolude või dokumentide kohta ning dokumenteerida vastuseid;

d) küsitleda teisi küsitlemisega nõustuvaid füüsilisi või juriidilisi isikuid, et koguda teavet uurimise sisu kohta;

e) nõuda andmeid telefonikõnede ja andmeedastuse kohta.

3. Juhtiva järelevaatamisasutuse poolt lõikes 1 osutatud uurimiseks volitatud ametnikud ja muud isikud teostavad oma õigusi, esitades kirjaliku volituse, milles on täpsustatud uurimise sisu ja eesmärk.

Nimetatud volitusse märgitakse ka artikli 35 lõikes 6 sätestatud sunniraha, mida kohaldatakse juhul, kui nõutud dokumente, andmeid, teavet dokumenteeritud protseduuride kohta ja muid materjale või vastuseid kolmandast isikust IKT-teenuste osutaja esindajatele esitatud küsimustele ei esitata või kui need esitatakse mittetäielikult.

4. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate esindajad peavad alluma juhtiva järelevaatamisasutuse otsuse alusel algatatud uurimisele. Otsuses märgitakse uurimise sisu ja eesmärk, artikli 35 lõikes 6 sätestatud sunniraha, määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 kohased õiguskaitsevahendid ja samuti õigus otsuse läbivaatamisele Euroopa Kohtus.

5. Aegsasti enne uurimise algust teavitab juhtiv järelevaatamisasutus selle kolmandast isikust kriitilise tähtsusega IKT-teenuste osutaja IKT-teenuseid kasutavate finantssektori ettevõtjate pädevaid asutusi uurimisest ja volitatud isikutest.

Juhtiv järelevaatamisasutus edastab ühisele järelevalvevõrgustikule kogu esimese lõigu kohaselt edastatud teabe.

Artikkel 39

Kontroll

1. Käesolevast määrusest tulenevate ülesannete täitmiseks võib juhtiv järelevaatamisasutus, keda abistavad artikli 40 lõikes 1 osutatud ühised kontrollirühmad, siseneda kolmandast isikust IKT-teenuste osutajate äriruumidesse ja valdustesse, näiteks peakontoritesse, tegevuskeskustesse ja varuruumidesse, ning teha kõik vajalikud kohapealsed kontrollid, aga teha ka kaugkontrolle.

Esimeses lõigus osutatud volituste kasutamisel konsulteerib juhtiv järelevaatamisasutus ühise järelevaatamisvõrgustikuga.

2. Juhtiva järelevaatamisasutuse poolt kohapealse kontrolli tegemiseks volitatud ametnikel ja teistel isikutel on õigus:

a) siseneda sellistesse äriruumidesse ja valdustesse ning

b) pitseerida selliseid äriruume, raamatupidamis- ja muid dokumente selliseks ajavahemikuks ja sellises ulatuses, mida on kontrolli tegemiseks vaja.

Juhtiva järelevaatamisasutuse volitatud ametnikud ja teised isikud kasutavad oma õigusi, esitades kirjaliku volituse, milles täpsustatakse kontrolli sisu ja eesmärk ning artikli 35 lõikes 6 sätestatud sunniraha, mida kohaldatakse juhul, kui asjaomaste kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate esindajad ei nõustu kontrolliga.

3. Aegsasti enne kontrolli teavitab juhtiv järelevaatamisasutus nende finantssektori ettevõtjate pädevaid asutusi, kes kasutavad selle kolmandast isikust IKT-teenuste osutaja teenuseid.

4. Kontrollid hõlmavad kõiki asjakohaseid IKT-süsteeme,-võrke,-seadmeid, -teavet ja -andmeid, mida kasutatakse IKT-teenuste osutamisel finantssektori ettevõtjatele või mis aitavad sellele kaasa.

5. Enne kavandatud kohapealset kontrolli teavitab juhtiv järelevaatamisasutus mõistliku aja jooksul kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaid, välja arvatud juhul, kui selline teatamine ei ole võimalik häda- või kriisiolukorra tõttu või kui see viiks olukorrani, kus kontroll või audit ei oleks enam tulemuslik.

6. Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja peab alluma juhtiva järelevaatamisasutuse otsuse alusel korraldatud kohapealsele kontrollile. Otsuses määratakse kindlaks kontrolli sisu ja eesmärk ning kontrolli alustamise kuupäev ning selles märgitakse artikli 35 lõikes 6 sätestatud sunniraha ja määrustega (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 tagatud õiguskaitsevahendid, samuti õigus otsuse läbivaatamisele Euroopa Kohtus.

7. Kui juhtiva järelevaatamisasutuse volitatud ametnikud ja muud isikud leiavad, et kriitilise tähtsusega kolmandast isikust IKT-teenuse osutaja ei nõustu käesoleva artikli kohaselt otsusega ette nähtud kontrolliga, teavitab juhtiv järelevaatamisasutus kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajat sellise vastuseisu tagajärgedest, sealhulgas asjaomaste finantssektori ettevõtjate pädevate asutuste võimalusest nõuda finantssektori ettevõtjatelt selliste lepingute lõpetamist, mis on sõlmitud kõnealuse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaga.

Artikkel 40

Pidev järelevaatamine

1. Eelkõige üldist laadi uurimiste või kontrollide läbiviimisel abistab juhtivat järelevaatamisasutust järelevaatamise käigus ühine kontrollirühm, mis on moodustatud iga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja jaoks.

2. Lõikes 1 osutatud ühine kontrollirühm koosneb järgmiste asutuste töötajatest:

a) Euroopa järelevalveasutused;

b) sellised asjaomased pädevad asutused, kes teevad järelevalvet nende finantssektori ettevõtjate üle, kellele kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja osutab IKT-teenuseid;

c) artikli 32 lõike 4 punktis e osutatud riiklik pädev asutus, vabatahtlikkuse alusel;

d) üks pädev asutus liikmesriigist, kus kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja on asutatud, vabatahtlikkuse alusel.

Ühise kontrollirühma liikmetel peavad olema IKT- ja operatsiooniriskialased teadmised. Ühine kontrollirühm töötab juhtiva järelevaatamiseasutuse määratud töötaja (edaspidi „juhtiv järelevaatamiskoordinaator“) koordineerimisel.

3. Kolme kuu jooksul pärast uurimise või kontrolli lõpetamist võtab juhtiv järelevaatamisasutus pärast järelevaatamisfoorumiga konsulteerimist vastu soovitused, mis esitatakse vastavalt artiklis 35 osutatud volitustele kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale.

4. Lõikes 3 osutatud soovitused edastatakse viivitamata kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajale ja nendele finantssektori ettevõtjate pädevatele asutustele, kellele ta IKT-teenuseid osutab.

Järelevaatamise käigus võib juhtiv järelevaatamisasutus võtta arvesse asjakohaseid kolmandate isikute sertifikaate ning kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja kättesaadavaks tehtud sise- või välisauditi aruandeid.

Artikkel 41

Järelevaatamist võimaldavate tingimuste ühtlustamine

1. Euroopa järelevalveasutused töötavad ühiskomitee kaudu välja regulatiivsete tehniliste standardite eelnõud, et täpsustada järgmist:

a) teave, mille kolmandast isikust IKT-teenuste osutaja peab esitama taotluses, kui ta soovib artikli 31 lõike 11 kohaselt taotleda vabatahtlikku kriitilise tähtsusega ettevõtjaks määramist;

b) sellise teabe sisu, struktuur ja vorm, mille kolmandast isikust IKT-teenuste osutajad peavad artikli 35 lõike 1 kohaselt esitama või avalikustama või mida nad peavad aruannetes käsitlema, sealhulgas alltöövõtulepinguid käsitleva teabe esitamise vorm;

c) kriteeriumid, mille alusel määratakse kindlaks ühise kontrollirühma koosseis, tagades Euroopa järelevalveasutuste ja asjaomaste pädevate asutuste töötajate tasakaalustatud osalemise, nimetatakse ametisse kontrollirühma liikmed, määratakse kindlaks ülesanded ja töökorraldus;

d) pädevate asutuste üksikasjalik hinnang meetmetele, mida kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad on võtnud artikli 42 lõike 3 kohaste juhtiva järelevaatamisasutuse soovituste alusel.

2. Euroopa järelevalveasutused esitavad kõnealused regulatiivsete tehniliste standardite eelnõud komisjonile hiljemalt 17. juuliks 2024.

Komisjonile antakse õigus käesolevat määrust täiendada, võttes vastu lõikes 1 osutatud regulatiivsed tehnilised standardid vastavalt menetlusele, mis on sätestatud kooskõlas määruste (EL) nr 1093/2010, (EL) nr 1094/2010 ja (EL) nr 1095/2010 artiklitega 10–14.

Artikkel 42

Pädevate asutuste järelmeetmed

1. 60 kalendripäeva jooksul pärast juhtiva järelevaatamisasutuse poolt artikli 35 lõike 1 punkti d kohaselt antud soovituste kättesaamist teatavad kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad juhtivale järelevaatamisasutusele kas oma kavatsusest neid soovitusi järgida või esitavad põhjendatud selgituse selle kohta, miks nad neid soovitusi ei järgi. Juhtiv järelevaatamisasutus edastab selle teabe viivitamata asjaomaste finantssektori ettevõtjate pädevatele asutustele.

2. Juhtiv järelevaatamisasutus avalikustab juhud, mil kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja ei teavita juhtivat järelevaatamisasutust kooskõlas lõikega 1 või kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja esitatud selgitust ei peeta piisavaks. Avaldatud teabes avalikustatakse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja identiteet ning teave nõuete täitmata jätmise liigi ja laadi kohta. Selline teave piirdub sellega, mis on üldsuse teadlikkuse tagamiseks asjakohane ja proportsionaalne, välja arvatud juhul, kui selline avaldamine põhjustaks asjaomastele isikutele ebaproportsionaalset kahju või ohustaks tõsiselt finantsturgude nõuetekohast toimimist ja terviklikkust või liidu finantssüsteemi kui terviku või selle osa stabiilsust.

Juhtiv järelevaatamisasutus teavitab kolmandast isikust IKT-teenuste osutajat kõnealusest avalikustamisest.

3. Pädevad asutused teavitavad asjaomaseid finantssektori ettevõtjaid kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele esitatud soovitustes kindlaks tehtud riskidest kooskõlas artikli 35 lõike 1 punktiga d.

Kolmandast isikust tuleneva IKT-riski juhtimisel võtavad finantssektori ettevõtjad arvesse esimeses lõigus osutatud riske.

4. Kui pädev asutus leiab, et finantssektori ettevõtja ei võta kolmandast isikust tuleneva IKT-riski juhtimise raames arvesse soovitustes kindlaks tehtud konkreetseid riske või ei käsitle neid piisavalt, teavitab ta finantssektori ettevõtjat võimalusest teha 60 kalendripäeva jooksul teatise saamisest otsus vastavalt lõikele 6, kui puuduvad asjakohased lepingud, mille eesmärk on selliseid riske käsitleda.

5. Pärast artikli 35 lõike 1 punktis c osutatud teadete saamist ja enne käesoleva artikli lõikes 6 osutatud otsuse tegemist võivad pädevad asutused vabatahtlikult konsulteerida direktiivi (EL) 2022/2555 kohaselt määratud või asutatud pädevate asutustega, kes vastutavad nimetatud direktiivi kohaldamisalasse jääva sellise elutähtsa või olulise üksuse järelevalve eest, mis on määratud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaks.

6. Pädevad asutused võivad viimase abinõuna pärast käesoleva artikli lõigetes 4 ja 5 sätestatud teavitamist ja kohasel juhul konsulteerimist teha kooskõlas artikliga 50 otsuse selle kohta, et finantssektori ettevõtjad peataksid ajutiselt osaliselt või täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja pakutava teenuse kasutamise või kasutuselevõtu, kuni kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatele suunatud soovitustes nimetatud riskid on kõrvaldatud. Vajaduse korral võivad nad nõuda, et finantssektori ettevõtjad lõpetaksid osaliselt või täielikult kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega sõlmitud lepingud.

7. Kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja keeldub soovitustega nõustumast, rakendades juhtiva järelevaatamisasutuse soovitatud lähenemisviisist erinevat lähenemisviisi, ja selline erinev lähenemisviis võib negatiivselt mõjutada paljusid finantssektori ettevõtjaid või olulist osa finantssektorist ning pädevate asutuste antud individuaalsete hoiatuste tulemusel ei ole kasutusele võetud finantsstabiilsusele avalduvat võimalikku riski leevendavaid järjepidevaid lähenemisviise, võib juhtiv järelevaatamisasutus pärast järelevalvefoorumiga konsulteerimist esitada pädevatele asutustele kohasel viisil mittesiduvaid ja mitteavalikke arvamusi, et edendada järjepidevaid ja ühtseid järelevalvealaseid järelmeetmeid.

8. Pärast artikli 35 lõike 1 punktis c osutatud aruannete saamist võtavad pädevad asutused käesoleva artikli lõikes 6 osutatud otsuste tegemisel arvesse kriitilise tähtsusega kolmandast isikust IKT-teenuste osutaja poolt käsitlemata riski liiki ja ulatust ning nõuete täitmata jätmise tõsidust, võttes arvesse järgmisi kriteeriume:

a) nõuete täitmata jätmise raskusaste ja kestus;

b) kas nõuete täitmata jätmine on paljastanud tõsiseid nõrku kohti kolmandast isikust IKT-teenuste osutaja menetlustes, juhtimissüsteemides, riskijuhtimises ja sisekontrollis;

c) kas nõuete täitmata jätmine hõlbustas finantskuritegu, põhjustas selle või on muul viisil sellega seostatav;

d) kas nõuete täitmata jätmine pandi toime tahtlikult või hooletuse tõttu;

e) kas lepingute peatamine või lõpetamine ohustab finantssektori ettevõtja äritegevuse järjepidevust, olenemata finantssektori ettevõtja jõupingutustest vältida häireid oma teenuste pakkumisel;

f) asjakohasel juhul nende direktiivi (EL) 2022/2555 kohaselt. määratud või asutatud pädevate asutuste arvamus, kes vastutavad nimetatud direktiivi kohaldamisalasse jääva sellise elutähtsa või olulise üksuse järelevalve eest, mis on määratud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajaks, on taotletud vabatahtlikkuse alusel kooskõlas käesoleva artikli lõikega 5.

Pädevad asutused annavad finantssektori ettevõtjatele vajaliku aja, et nad saaksid kohandada kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatega sõlmitud lepinguid, et vältida negatiivset mõju nende digitaalsele tegevuskerksusele ning võimaldada neil rakendada artiklis 28 osutatud väljumisstrateegiaid ja üleminekukavasid.

9. Käesoleva artikli lõikes 6 osutatud otsusest teatatakse artikli 32 lõike 4 punktides a, b ja c osutatud järelevaatamisfoorumi liikmetele ja ühisele järelevaatamisvõrgustikule.

Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad, keda lõikes 6 sätestatud otsused mõjutavad, teevad mõjutatud finantssektori ettevõtjatega täielikku koostööd, eelkõige seoses nende lepingute peatamise või lõpetamisega.

10. Kui kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajad ei ole juhtiva järelevaatamisasutuse soovitusi osaliselt või täielikult heaks kiitnud, teavitavad pädevad asutused juhtivat järelevaatamisasutust korrapäraselt finantssektori ettevõtjatega seotud järelevalveülesannete täitmisel kasutatud lähenemisviisidest ja meetmetest ning finantssektori ettevõtjate sõlmitud lepingutest.

11. Juhtiv järelevaatamisasutus võib taotluse korral anda esitatud soovituste kohta täiendavaid selgitusi, et suunata pädevaid asutusi järelmeetmete võtmisel.

Artikkel 43

Järelevaatamistasud

1. Juhtiv järelevaatamisasutus võtab kooskõlas käesoleva artikli lõikes 2 osutatud delegeeritud õigusaktiga kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajatelt tasu, mis katab täielikult käesoleva määruse kohaste järelevaatamisülesannete täitmisel tekkivad juhtiva järelevaatamisasutuse kulud, muu hulgas hüvitatakse kõik sellised kulud, mis võivad tekkida seoses artiklis 40 osutatud ühise kontrollirühma tööga ning otsese järelevaatamise alla kuuluvates küsimustes artikli 32 lõike 4 teises lõigus osutatud sõltumatute ekspertide nõuannetega seotud kulud.

Kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajalt võetav tasu katab kõik käesolevas jaos ette nähtud ülesannete täitmisega seotud kulud ja on proportsionaalne tema käibega.

2. Komisjonil on õigus võtta kooskõlas artikliga 57 vastu delegeeritud õigusakt käesoleva määruse täiendamiseks ning määrata kindlaks tasude suuruse ja nende maksmise viisi hiljemalt 17. juuliks 2024.

Artikkel 44

Rahvusvaheline koostöö

1. Ilma et see piiraks artikli 36 rakendamist, võivad EBA, ESMA ja EIOPA kooskõlas vastavalt määruste (EL) nr 1093/2010, (EL) nr 1095/2010 ja (EL) nr 1094/2010 artiklile 33 sõlmida halduskokkuleppeid kolmandate riikide reguleerivate ja järelevalveasutustega, et edendada rahvusvahelist koostööd seoses kolmandast isikust tuleneva IKT-riskiga eri finantssektorites ning eelkõige töötada välja IKT-riski juhtimise ja kontrolli, leevendusmeetmete ja intsidentidele reageerimise parimad tavad.

2. Euroopa järelevalveasutused esitavad ühiskomitee kaudu iga viie aasta järel Euroopa Parlamendile, nõukogule ja komisjonile ühise konfidentsiaalse aruande, milles võetakse kokku lõikes 1 osutatud kolmandate riikide ametiasutustega peetud asjakohaste arutelude tulemused, keskendudes kolmandast isikust tuleneva IKT-riski muutusele ja mõjule, mida see avaldab finantsstabiilsusele, turu usaldusväärsusele, investorite kaitsele ja siseturu toimimisele.

VI PEATÜKK

Teabe jagamise kokkulepped

Artikkel 45

Küberohte käsitleva teabe ja teadmuse jagamise kokkulepped

1. Finantssektori ettevõtjad võivad omavahel vahetada küberohte käsitlevat teavet ja teadmust, sealhulgas ohunäitajaid, taktikat, võtteid ja menetlusi, küberturbehoiatusi ja konfigureerimisvahendeid, kui sellise teabe ja teadmuse jagamine:

a) aitab suurendada finantssektori ettevõtjate digitaalset tegevuskerksust ning eelkõige suurendab küberohtudest teadlikkust, piirab või takistab küberohtude levikut, toetab kaitsevõimeid, ohu avastamise meetodeid, leevendusstrateegiaid või reageerimis- ja taastamisetappe;

b) toimub finantssektori ettevõtjate jaoks usaldusväärses kogukonnas;

c) toimub selliste teabejagamise kokkulepete alusel, mis kaitsevad jagatava teabe potentsiaalselt tundlikku laadi ning mille suhtes kohaldatakse tegevusreegleid, austades täielikult ärisaladuse ja isikuandmete kaitse põhimõtteid kooskõlas määrusega (EL) 2016/679 ning konkurentsipoliitika suuniseid.

2. Lõike 1 punkti c kohaldamisel määratakse teabe jagamise kokkulepetes kindlaks osalemistingimused ning kohasel juhul esitatakse üksikasjad avaliku sektori asutuste osalemise ja ulatuse kohta, milles neid võib teabe jagamise kokkulepetesse kaasata, kolmandast isikust IKT-teenuste osutajate kaasamise kohta ning tegevusaspektide, sealhulgas spetsiaalsete IT-platvormide kasutamise kohta.

3. Finantssektori ettevõtjad teavitavad pädevaid asutusi oma osalemisest lõikes 1 osutatud teabevahetuse kokkulepetes pärast oma liikmesuse kinnitamist, või kui see on asjakohane, oma liikmesuse lõpetamisest pärast nende jõustumist.

VII PEATÜKK

Pädevad asutused

Artikkel 46

Pädevad asutused

Ilma et see piiraks käesoleva määruse V peatüki II jaos osutatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate järelevaatamisraamistikku käsitlevate sätete kohaldamist, tagavad käesoleva määruse järgimise kooskõlas vastavates õigusaktides sätestatud volitustega järgmised pädevad asutused:

a) krediidiasutuste ja nende asutuste puhul, mille suhtes kohaldatakse direktiivi 2013/36/EL kohast erandit, kõnealuse direktiivi artikli 4 kohaselt määratud pädev asutus ning määruse (EL) nr 1024/2013 artikli 6 lõike 4 kohaselt oluliseks liigitatud krediidiasutuste puhul EKP vastavalt kõnealuse määrusega antud volitustele ja ülesannetele;

b) makseasutuste puhul, sealhulgas nende makseasutuste puhul, mille suhtes kohaldatakse direktiivi (EL) 2015/2366 kohast erandit, e-raha asutuste puhul, sealhulgas nende puhul, mille suhtes kohaldatakse direktiivi 2009/110/EÜ kohast erandit, ning direktiivi (EL) 2015/2366 artikli 33 lõikes 1 osutatud kontoteabe teenuse pakkujate puhul direktiivi (EL) 2015/2366 artikli 22 kohaselt määratud pädev asutus;

c) investeerimisühingute puhul Euroopa Parlamendi ja nõukogu direktiivi (EL) 2019/2034 artikli 4 kohaselt määratud pädev asutus ([38]);

d) krüptovarateenuse osutajate, kes on tegevusloa saanud krüptovaraturgude määruse alusel, ja varapõhiste tokenite emitentide puhul kõnealuse määruse asjakohase sätte kohaselt määratud pädev asutus;

e) väärtpaberite keskdepositooriumide puhul määruse (EL) nr 909/2014 artikli 11 kohaselt määratud pädev asutus;

f) kesksete vastaspoolte puhul määruse (EL) nr 648/2012 artikli 22 kohaselt määratud pädev asutus;

g) kauplemiskohtade ja aruandlusteenuse pakkujate puhul direktiivi 2014/65/EL artikli 67 kohaselt määratud pädev asutus ja määruse (EL) nr 600/2014 artikli 2 lõike 1 punktis 18 määratletud pädev asutus;

h) kauplemisteabehoidlate puhul määruse (EL) nr 648/2012 artikli 22 kohaselt määratud pädev asutus;

i) alternatiivsete investeerimisfondide valitsejate puhul direktiivi 2011/61/EL artikli 44 kohaselt määratud pädev asutus;

j) fondivalitsejate puhul direktiivi 2009/65/EÜ artikli 97 kohaselt määratud pädev asutus;

k) kindlustus- ja edasikindlustusandjate puhul direktiivi 2009/138/EÜ artikli 30 kohaselt määratud pädev asutus;

l) kindlustus- ja edasikindlustusvahendajate ja kõrvaltegevusena pakutava kindlustuse vahendajate puhul direktiivi (EL) 2016/97 artikli 12 kohaselt määratud pädev asutus;

m) tööandja kogumispensioni asutuste puhul direktiivi (EL) 2016/2341 artikli 47 kohaselt määratud pädev asutus;

n) reitinguagentuuride puhul määruse (EÜ) nr 1060/2009 artikli 21 kohaselt määratud pädev asutus;

o) kriitilise tähtsusega võrdlusaluste haldurite puhul määruse (EL) 2016/1011 artiklite 40 ja 41 kohaselt määratud pädev asutus;

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

p) ühisrahastusteenuse osutajate puhul määruse (EL) 2020/1503 artikli 29 kohaselt määratud pädev asutus;

q) väärtpaberistamise registrite puhul määruse (EL) 2017/2402 artikli 10 ja artikli 14 lõike 1 kohaselt määratud pädev asutus.

Artikkel 47

Koostöö direktiiviga (EL) 2022/2555 loodud struktuuride ja asutustega

1. Koostöö edendamiseks ja järelevalvealase teabevahetuse võimaldamiseks käesoleva määruse kohaselt määratud pädevate asutuste ning direktiivi (EL) 2022/2555 artikli 14 alusel loodud koostöörühma vahel võivad Euroopa järelevalveasutused ja pädevad asutused osaleda koostöörühma tegevuses nendes küsimustes, mis on seotud nendepoolse järelevalvega finantssektori ettevõtjate üle. Euroopa järelevalveasutused ja pädevad asutused võivad taotleda koostöörühma töös osalemist küsimustes, mis on seotud direktiivi (EL) 2022/2555 kohaldamisalasse jäävate elutähtsate või oluliste üksustega, mis on samuti käesoleva määruse artikli 31 kohaselt määratud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajateks.

2. Kohasel juhul võivad pädevad asutused konsulteerida ja jagada teavet direktiivi (EL) 2022/2555 kohaselt määratud või loodud ühtsete kontaktpunktide ja küberturbe intsidentide lahendamise üksustega.

3. Kohasel juhul võivad pädevad asutused küsida asjakohast tehnilist nõu ja abi direktiivi (EL) 2022/2555 kohaselt määratud või asutatud pädevatelt asutustelt ning sõlmida koostöökokkuleppeid, mille eesmärk on tagada tõhusad ja kiirelt reageerivad koordineerimismehhanismid.

4. Käesoleva artikli lõikes 3 osutatud kokkulepetes võib muu hulgas kindlaks määrata järelevalve ja järelevaatamise koordineerimise menetlused seoses direktiivi (EL) 2022/2555 kohaldamisalasse jäävate elutähtsate või oluliste üksustega, kes on käesoleva määruse artikli 31 kohaselt määratud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajateks, sealhulgas uurimiste ja kohapealsete kontrollide läbiviimiseks kooskõlas liikmesriigi õigusega, samuti käesoleva määruse kohaldamisalasse jäävate pädevate asutuste ja nimetatud direktiivi kohaselt määratud või asutatud asutuste vahel teabevahetuse toimumise viisi, mis hõlmab juurdepääsu nende asutuste nõutud teabele.

Artikkel 48

Asutustevaheline koostöö

1. Pädevad asutused teevad omavahel ja kui see on kohaldatav, juhtiva järelevaatamisasutusega tihedat koostööd.

2. Pädevad asutused ja juhtiv järelevaatamisasutus vahetavad aegsasti vastastikku kogu asjakohast teavet kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate kohta, mida neil on vaja oma vastavate käesolevast määrusest tulenevate ülesannete täitmiseks, eelkõige seoses juhtiva järelevaatamisasutuse järelevaatamisülesannete raames kindlaks tehtud riskide, lähenemisviiside ja võetud meetmetega.

Artikkel 49

Finantssektoriteülesed simulatsioonid, teabevahetus ja koostöö

1. Et suurendada teadlikkust olukorrast ning teha kindlaks sektoritele ühine kübernõrkus ja ühised küberriskid, võivad Euroopa järelevalveasutused ühiskomitee kaudu ning koostöös pädevate asutuste, direktiivi 2014/59/EL artiklis 3 osutatud kriisilahendusasutuste, EKP, Ühtse Kriisilahendusnõukogu (määruse (EL) nr 806/2014 kohaldamisalasse jäävate ettevõtjatega seotud teabe osas), Euroopa Süsteemsete Riskide Nõukogu ja kohasel viisil ENISAga luua mehhanisme, mis võimaldavad jagada finantssektorite vahel tõhusaid tavasid.

Nad võivad välja töötada kriisijuhtimis- ja erandolukorra simulatsioone, mis hõlmavad küberrünnete stsenaariume, et töötada välja sidekanalid ja võimaldada järk-järgult tõhusat koordineeritud reageerimist liidu tasandil IKTga seotud olulise piiriülese intsidendi või seonduva ohu korral, millel on süsteemne mõju liidu finantssektorile tervikuna.

Nende simulatsioonide käigus võib kohasel määral testida ka finantssektori sõltuvust muudest majandussektoritest.

2. Pädevad asutused, Euroopa järelevalveasutused ja EKP teevad omavahel tihedat koostööd ja vahetavad teavet, et täita oma artiklite 47–54 kohaseid ülesandeid. Nad kooskõlastavad tihedalt oma järelevalvetegevust, et teha kindlaks käesoleva määruse rikkumised ja võtta parandusmeetmeid, töötada välja ja edendada parimaid tavasid, hõlbustada koostööd, edendada tõlgendamise ühtsust ning anda lahkhelide korral jurisdiktsiooniüleseid hinnanguid.

Artikkel 50

Halduskaristused ja parandusmeetmed

1. Pädevatel asutustel on kõik käesoleva määruse kohaste ülesannete täitmiseks vajalikud järelevalve-, uurimis- ja karistuste määramise volitused.

2. Lõike 1 kohased volitused peavad hõlmama vähemalt järgmisi volitusi:

a) tutvuda kõigi dokumentidega või mis tahes vormis muude andmetega, mis pädeva asutuse arvates võiksid olla tema ülesannete täitmiseks olulised, ja saada või teha nende dokumentide koopiaid;

b) teha kohapeal kontrolle või uurimisi, mis hõlmavad muu hulgas järgmist, kuid ei piirdu sellega:

   i) kutsuda finantssektori ettevõtjate esindajaid välja ja paluda neil anda suulisi või kirjalikke selgitusi uurimise sisu ja eesmärgiga seotud asjaolude või dokumentide kohta ning salvestada vastuseid;

   ii) küsitleda teisi küsitlemisega nõustuvaid füüsilisi või juriidilisi isikuid, et koguda teavet uurimise sisu kohta;

c) nõuda käesoleva määruse nõuete rikkumise korral parandus- ja ennetusmeetmete võtmist.

3. Ilma et see piiraks liikmesriikide õigust määrata kriminaalkaristusi kooskõlas artikliga 52, kehtestavad liikmesriigid õigusnormid, milles sätestatakse asjakohased halduskaristused ja parandusmeetmed käesoleva määruse rikkumise puhuks, ning tagavad nende tulemusliku rakendamise.

Sellised karistused ja meetmed peavad olema tulemuslikud, proportsionaalsed ja hoiatavad.

4. Liikmesriigid annavad pädevatele asutustele õiguse kohaldada käesoleva määruse rikkumise korral vähemalt järgmisi halduskaristusi või parandusmeetmeid:

a) teha ettekirjutus, et füüsiline või juriidiline isik lõpetaks käesolevat määrust rikkuva tegevuse ja hoiduks selle tegevuse kordamisest;

b) nõuda sellise tegevuse või tava ajutist või alalist peatamist, mis pädeva asutuse arvates on vastuolus käesoleva määruse sätetega, ning hoida ära sellise tegevuse või tava kordumine;

c) võtta mis tahes liiki meetmeid, sealhulgas rahalisi meetmeid, tagamaks, et finantssektori ettevõtjad jätkavad õigusnormide järgimist;

d) nõuda liikmesriigi õigusega lubatud ulatuses sideoperaatorite valduses olevaid andmeliiklusandmeid, kui on piisav alus kahtlustada käesoleva määruse nõuete rikkumist ja kui sellised andmed võivad olla olulised käesoleva määruse rikkumiste uurimisel, ning

e) väljastada avalikke teadaandeid, mis sisaldavad füüsilise või juriidilise isiku identiteeti ja rikkumise laadi.

5. Kui lõike 2 punkti c ja lõike 4 sätteid kohaldatakse juriidiliste isikute suhtes, annavad liikmesriigid pädevatele asutustele õiguse kohaldada halduskaristusi ja parandusmeetmeid vastavalt liikmesriigi õiguses sätestatud tingimustele juhtorgani liikmete ja teiste isikute suhtes, kes vastutavad liikmesriigi õiguse alusel asjaomase rikkumise eest.

6. Liikmesriigid tagavad, et iga otsus, millega määratakse lõikes 2 punktis c sätestatud halduskaristused või parandusmeetmed, on nõuetekohaselt põhjendatud ja et selle võib edasi kaevata.

Artikkel 51

Halduskaristuste ja parandusmeetmete määramise õiguse kasutamine

1. Vajaduse korral kasutavad pädevad asutused oma volitusi artiklis 50 osutatud halduskaristuste ja parandusmeetmete määramisel kooskõlas oma riigi õigusraamistikuga kas

a) otse;

b) koostöös teiste ametiasutustega;

c) omal vastutusel, delegeerides küsimuse teistele ametiasutustele, või

d) suunates küsimuse pädevatele õigusasutustele.

2. Kui pädevad asutused määravad kindlaks artikli 50 kohase halduskaristuse või parandusmeetme liiki ja ulatust, võtavad nad seejuures arvesse, mil määral on rikkumine tahtlik või tuleneb hooletusest, ja kõiki muid asjakohaseid asjaolusid, sealhulgas kohasel juhul järgmist:

a) rikkumise olulisus, raskusaste ja kestus;

b) rikkumise toime pannud füüsilise või juriidilise isiku vastutuse ulatus;

c) vastutava füüsilise või juriidilise isiku finantsseisundi tugevus;

d) vastutava füüsilise või juriidilise isiku saadud kasu või välditud kahju suurus, kui seda on võimalik kindlaks määrata;

e) kolmandate isikute kahju, mis tulenes rikkumisest, kui seda on võimalik kindlaks määrata;

f) vastutava füüsilise või juriidilise isiku ja pädeva asutuse koostöö tase, ilma et see piiraks vajadust tagada kõnealuse füüsilise või juriidilise isiku saadud kasumi tagastamine või välditud kahjumi sissenõudmine;

g) vastutava füüsilise või juriidilise isiku varasemad rikkumised.

Artikkel 52

Kriminaalkaristused

1. Liikmesriigid võivad otsustada mitte kehtestada halduskaristusi või parandusmeetmeid käsitlevaid õigusnorme selliste rikkumiste suhtes, mille suhtes kohaldatakse nende riiklikus õiguses kriminaalkaristusi.

2. Kui liikmesriigid on otsustanud kehtestada kriminaalkaristused käesoleva määruse rikkumise eest, tagavad nad asjakohaste abinõude kasutuselevõtu, nii et pädevatel asutustel oleksid kõik vajalikud volitused suhelda oma jurisdiktsiooni piires kohtute, prokuratuuri või kriminaalõigusasutustega, et saada konkreetset teavet käesolevas määruses osutatud rikkumiste asjus algatatud kriminaaluurimiste või -menetluste kohta, ning anda sama teavet teistele pädevatele asutustele ja EBA-le, ESMA-le või EIOPA-le, et täita käesoleva määruse kohast koostöökohustust.

Artikkel 53

Teatamiskohustus

Liikmesriigid teavitavad komisjoni, ESMAt, EBAt ja EIOPAt oma õigus- ja haldusnormidest, millega võetakse üle käesolev peatükk, sealhulgas asjaomastest kriminaalõiguse sätetest hiljemalt 17. jaanuariks 2025. Liikmesriigid teatavad komisjonile, ESMA-le, EBA-le ja EIOPA-le kõigist nende õigusnormide hilisematest muudatustest ilma põhjendamatu viivituseta.

Artikkel 54

Halduskaristuste avaldamine

1. Pädevad asutused avaldavad oma ametlikel veebisaitidel põhjendamatu viivituseta kõik halduskaristuse määramise otsused, mida ei ole edasi kaevatud pärast seda, kui karistuse saanud isikut on otsusest teavitatud.

2. Lõike 1 kohasel karistuste avaldamisel tuleb avaldada teave rikkumise liigi ja laadi kohta, vastutavad isikud ning määratud karistused.

3. Kui pädev asutus leiab pärast juhtumipõhist hindamist, et juriidilise isiku identiteedi või füüsilise isiku identiteedi ja isikuandmete avaldamine oleks ebaproportsionaalne, hõlmates isikuandmete kaitsega seotud riske, ohustaks finantsturgude stabiilsust või käimasolevat kriminaaluurimist või põhjustaks asjaomasele isikule ebaproportsionaalselt suurt kahju, niivõrd kui seda on võimalik kindlaks teha, võtab ta halduskaristuse määramise otsuse suhtes vastu ühe järgmistest võimalustest:

a) lükata otsuse avaldamine edasi seni, kuni kõik mitteavaldamise põhjused langevad ära;

b) avaldada see anonüümselt kooskõlas liikmesriigi õigusega või

c) hoiduda selle avaldamisest, kui punktides a ja b sätestatud võimalusi peetakse kas ebapiisavaks, et tagada ohu puudumine finantsturgude stabiilsusele, või kui selline avaldamine ei oleks proportsionaalne karistuse määramisel rakendatud leebema kohtlemisega.

4. Kui halduskaristuse määramise otsus otsustatakse avaldada kooskõlas lõike 3 punktiga b anonüümselt, võib asjaomaste andmete avaldamise edasi lükata.

5. Kui pädev asutus avaldab halduskaristuse määramise otsuse, mis on asjaomastele kohtuasutustele edasi kaevatud, lisavad pädevad asutused ühtlasi viivitamata oma ametlikule veebisaidile selle teabe ja hiljem kogu täiendava teabe sellise edasikaebamise tulemuste kohta. Samuti avaldatakse kohtuotsus, millega tühistatakse halduskaristuse määramise otsus.

6. Pädevad asutused tagavad, et lõigete 1–4 kohaselt avaldatud andmed jäävad nende ametlikule veebisaidile üksnes käesoleva artikli rakendamiseks vajalikuks ajaks. See ajavahemik ei tohi olla pikem kui viis aastat pärast avaldamist.

Artikkel 55

Ametisaladus

1. Käesoleva määruse kohaselt saadud, vahetatud või edastatud konfidentsiaalse teabe suhtes kehtib lõikes 2 sätestatud ametisaladuse hoidmise kohustus.

2. Ametisaladuse hoidmise kohustus kehtib kõigile isikutele, kes töötavad või on töötanud käesoleva määruse alusel pädeva asutuse heaks või mõne ametiasutuse või turul tegutseva ettevõtja või füüsilise või juriidilise isiku heaks, kellele need pädevad asutused on volitusi delegeerinud, sealhulgas pädevate asutuste lepingulised audiitorid ja eksperdid.

3. Ametisaladuse alla kuuluvat teavet, sealhulgas teabevahetust käesoleva direktiivi kohaldamisalasse jäävate pädevate asutuste ja direktiivi (EL) 2022/2555 kohaselt määratud või asutatud pädevate asutuste vahel, ei avaldata ühelegi teisele isikule ega asutusele, välja arvatud juhul, kui see on ette nähtud liidu või liikmesriigi õigusega.

4. Kogu käesoleva määruse kohaselt pädevate asutuste vahel vahetatavat teavet, mis puudutab äri- või tegevustingimusi ja muid majanduslikke või isiklikke küsimusi, peetakse konfidentsiaalseks ja selle suhtes kohaldatakse ametisaladuse nõudeid, välja arvatud juhul, kui pädev asutus märgib teavet edastades, et seda võib avaldada, või kui avalikustamine on vajalik tulenevalt kohtumenetlusest.

Artikkel 56

Andmekaitse

1. Euroopa järelevalveasutustel ja pädevatel asutustel on lubatud töödelda isikuandmeid üksnes juhul, kui see on vajalik nende käesolevast määrusest tulenevate kohustuste täitmiseks, eelkõige seoses uurimise, kontrolli, teabe taotlemise, teavitamise, avaldamise, analüüsimise, kontrollimise, hindamise ja järelevaatamiskavade koostamisega. Isikuandmeid töödeldakse kooskõlas määrusega (EL) 2016/679 või määrusega (EL) 2018/1725, olenevalt sellest, kumb on kohaldatav.

2. Kui muudes valdkondlikes õigusaktides ei ole sätestatud teisiti, säilitatakse lõikes 1 osutatud isikuandmeid kuni kohaldatavate järelevalvekohustuste täitmiseni, ent mitte kauem kui 15 aastat, välja arvatud poolelioleva kohtumenetluse korral, mis nõuab selliste andmete pikemaajalisemat säilitamist.

VIII PEATÜKK

Delegeeritud õigusaktid

Artikkel 57

Delegeeritud volituste rakendamine

1. Komisjonile antakse õigus võtta vastu delegeeritud õigusakte käesolevas artiklis sätestatud tingimustel.

2. Artikli 31 lõikes 6 ja artikli 43 lõikes 2 osutatud õigus võtta vastu delegeeritud õigusakte antakse komisjonile viieks aastaks alates 17. jaanuarist 2024. Komisjon esitab delegeeritud volituste kohta aruande hiljemalt üheksa kuud enne viieaastase tähtaja möödumist. Volituste delegeerimist pikendatakse automaatselt samaks ajavahemikuks, välja arvatud juhul, kui Euroopa Parlament või nõukogu esitab selle suhtes vastuväite hiljemalt kolm kuud enne iga ajavahemiku lõppemist.

3. Euroopa Parlament ja nõukogu võivad artikli 31 lõikes 6 ja artikli 43 lõikes 2 osutatud volituste delegeerimise igal ajal tagasi võtta. Tagasivõtmise otsusega lõpetatakse otsuses nimetatud volituste delegeerimine. Otsus jõustub järgmisel päeval pärast selle avaldamist *Euroopa Liidu Teatajas* või otsuses nimetatud hilisemal kuupäeval. See ei mõjuta juba jõustunud delegeeritud õigusaktide kehtivust.

4. Enne delegeeritud õigusakti vastuvõtmist konsulteerib komisjon vastavalt 13. aprilli 2016. aasta institutsioonidevahelises parema õigusloome kokkuleppes sätestatud põhimõtetele iga liikmesriigi määratud ekspertidega.

5. Niipea kui komisjon on delegeeritud õigusakti vastu võtnud, teavitab ta sellest samal ajal Euroopa Parlamenti ja nõukogu.

6. Artikli 31 lõike 6 ja artikli 43 lõike 2 alusel vastu võetud delegeeritud õigusakt jõustub üksnes juhul, kui Euroopa Parlament ega nõukogu ei ole kolme kuu jooksul pärast Euroopa Parlamendi ja nõukogu teavitamist õigusaktist esitanud selle suhtes vastuväidet või kui Euroopa Parlament ja nõukogu on enne selle tähtaja möödumist komisjonile teatanud, et nad ei esita vastuväidet. Euroopa Parlamendi või nõukogu algatusel pikendatakse seda tähtaega kolme kuu võrra.

IX PEATÜKK

Ülemineku- ja lõppsätted

I jagu

Artikkel 58

Läbivaatamisklausel

1. Komisjon teeb hiljemalt 17. jaanuariks 2028 ning pärast kohasel viisil Euroopa järelevalveasutuste ja Euroopa Süsteemsete Riskide Nõukoguga konsulteerimist läbivaatamise ning esitab Euroopa Parlamendile ja nõukogule aruande, millele lisatakse seadusandlik ettepanek, kui see on asjakohane. Läbivaatamine hõlmab vähemalt järgmist:

a) artikli 31 lõikes 2 sätestatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajateks määramise kriteeriumid;

b) artiklis 19 osutatud olulistest küberohtudest teavitamise vabatahtlikkus;

c) artikli 31 lõikes 12 osutatud kord ja artikli 35 lõike 1 punkti d alapunkti iv esimeses taandes sätestatud juhtiva järelevaatamisasutuse volitused, et hinnata nende sätete tõhusust kolmandas riigis asutatud kriitilise tähtsusega kolmandast isikust IKT-teenuste osutajate tõhusa järelevaatamise tagamisel ning vajadust asutada liidus tütarettevõtja.

Käesoleva punkti esimese lõigu kohaldamisel hõlmab läbivaatamine artikli 31 lõikes 12 osutatud korra analüüsi, sealhulgas liidu finantssektori ettevõtjate juurdepääsu tingimusi kolmandatest riikidest pärit teenustele ja teenuste kättesaadavust liidu turul, ning selles võetakse arvesse käesoleva määrusega hõlmatud teenuste turgude edasist arengut, finantssektori ettevõtjate ja finantsjärelevalveasutuste praktilisi kogemusi vastavalt kõnealuse korra kohaldamise ja järelevalvega seoses ning kõiki rahvusvahelisel tasandil toimuvaid asjakohaseid regulatiivseid ja järelevalvealaseid suundumusi;

d) käesoleva määruse kohaldamisalasse nende artikli 2 lõike 3 punktis e osutatud finantssektori ettevõtjate lisamise asjakohasus, kes kasutavad automatiseeritud müügisüsteeme, võttes arvesse selliste süsteemide kasutamisega seotud tulevasi turusuundumusi;

e) ühise järelevaatamisvõrgustiku toimimine ja tõhusus järelevaatamisraamistiku raames toimuva järelevaatamise järjepidevuse ja teabevahetuse tõhususe toetamisel.

2. Direktiivi (EL) 2015/2366 läbivaatamise raames hindab komisjon maksesüsteemide ja maksete töötlemise toimingute küberkerksuse suurendamise vajadust ning seda, kas käesoleva määruse kohaldamisala laiendamine maksesüsteemide käitajatele ja makseid töötlevatele ettevõtjatele on asjakohane. Seda hinnangut arvesse võttes esitab komisjon direktiivi (EL) 2015/2366 läbivaatamise osana Euroopa Parlamendile ja nõukogule aruande hiljemalt 17. juuliks 2023.

Kõnealuse läbivaatamisaruande põhjal ja pärast konsulteerimist Euroopa järelevalveasutustega, EKP ja Euroopa Süsteemsete Riskide Nõukoguga võib komisjon asjakohasel juhul ja osana seadusandlikust ettepanekust, mille ta võib direktiivi (EL) 2015/2366 artikli 108 teise lõigu kohaselt vastu võtta, esitada ettepaneku, millega tagatakse, et kõigi maksesüsteemide käitajate ja makseid töötlevate ettevõtjate suhtes kohaldatakse asjakohast järelevaatamist, võttes samal ajal arvesse olemasolevat keskpangapoolset järelevaatamist.

3. Komisjon teeb hiljemalt 17. jaanuariks 2026 ning pärast Euroopa järelevalveasutuste ja Euroopa audiitorite järelevalveasutuste komiteega konsulteerimist läbivaatamise ning esitab Euroopa Parlamendile ja nõukogule aruande, millele lisatakse asjakohasel juhul seadusandlik ettepanek, vandeaudiitorite ja audiitorühingute digitaalse tegevuskerksuse rangemate nõuete asjakohasuse kohta, lisades vannutatud audiitorid ja audiitorühingud käesoleva määruse kohaldamisalasse või muutes Euroopa Parlamendi ja nõukogu direktiivi 2006/43/EÜ ([39]).

II jagu

Muudatused

Artikkel 59

Määruse (EÜ) nr 1060/2009 muutmine

Määrust (EÜ) nr 1060/2009 muudetakse järgmiselt.

1) I lisa A jao punkti 4 esimene lõik asendatakse järgmisega:

„Reitinguagentuuril on usaldusväärne haldus- ja raamatupidamiskord, sisekontrollimehhanism, tõhusad riskianalüüsi menetlused ning tõhus kontrolli- ja kaitsekord IKT-süsteemide haldamiseks kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554 (*).“

(*) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).“

2) III lisa punkt 12 asendatakse järgmisega:

„12. Reitinguagentuur rikub artikli 6 lõiget 2 koostoimes I lisa A jao punktiga 4, kui tal ei ole usaldusväärset haldus- või raamatupidamiskorda, sisekontrollimehhanismi, tõhusaid riskianalüüsi menetlusi ning tõhusat kontrolli- ja kaitsekorda IKT-süsteemide haldamiseks kooskõlas määrusega (EL) 2022/2554, või kui ta ei rakenda ega hoia jõus kõnealuses punktis nõutud otsuste tegemise menetlusi või organisatsioonilist struktuuri.“

Artikkel 60

Määruse (EL) nr 648/2012 muutmine

Määrust (EL) nr 648/2012 muudetakse järgmiselt.

1) Artiklit 26 muudetakse järgmiselt:

a) lõige 3 asendatakse järgmisega:

„3. Keskse vastaspoole organisatsiooniline struktuur peab olema selline, millega tagatakse, et teenuseid osutatakse ja tegevusi sooritatakse järjepidevalt ja korrektselt. Ta kasutab asjakohaseid ja proportsionaalseid süsteeme, ressursse ja protseduure, sealhulgas IKT-süsteeme, mida hallatakse kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554 (*).

(*) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).“;

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

b) lõige 6 jäetakse välja.

2) Artiklit 34 muudetakse järgmiselt:

a) lõige 1 asendatakse järgmisega:

„1. Keskne vastaspool kehtestab asjakohased talitluspidevuse põhimõtted ja avariitaastekava, mis hõlmab vastavalt määrusele (EL) 2022/2554 koostatud ja rakendatavaid IKT talitluspidevuse põhimõtteid ning IKT reageerimis- ja taastekavasid, ning rakendab ja hoiab need jõus, et tagada keskse vastaspoole funktsioonide säilitamine, tema tegevuse kiire taastamine ja kohustuste täitmine.“;

b) lõike 3 esimene lõik asendatakse järgmisega:

„3. Selleks et tagada käesoleva artikli ühetaoline kohaldamine, töötab Väärtpaberiturujärelevalve pärast EKPSi liikmetega konsulteerimist välja regulatiivsete tehniliste standardite eelnõud, milles täpsustatakse talitluspidevuse põhimõtete ja avariitaastekava (välja arvatud IKT talitluspidevuse põhimõtted ja avariitaastekavad) minimaalne sisu ning neile esitatavad nõuded.“

3) Artikli 56 lõike 3 esimene lõik asendatakse järgmisega:

„3. Selleks et tagada käesoleva artikli ühetaoline kohaldamine, töötab Väärtpaberiturujärelevalve välja regulatiivsete tehniliste standardite eelnõud, milles täpsustatakse lõikes 1 osutatud registreerimistaotluse üksikasju, välja arvatud IKT-riski juhtimisega seotud nõuded.“

4) Artikli 79 lõiked 1 ja 2 asendatakse järgmisega:

„1. Kauplemisteabehoidla teeb kindlaks operatsiooniriski allikad ja töötab nende minimeerimiseks välja asjakohased süsteemid, kontrollid ja protseduurid, sealhulgas kooskõlas määrusega (EL) 2022/2554 hallatavad IKT-süsteemid.

2. Kauplemisteabehoidla kehtestab asjakohased talitluspidevuse põhimõtted ja avariitaastekava (sealhulgas kooskõlas määrusega (EL) 2022/2554 koostatud IKT talitluspidevuse põhimõtted ning IKT reageerimis- ja taastekavad) ning rakendab ja hoiab neid jõus, et tagada kauplemisteabehoidla funktsioonide säilimine, tema tegevuse kiire taastamine ja kohustuste täitmine.“

5) Artikli 80 lõige 1 jäetakse välja.

6) I lisa II jagu muudetakse järgmiselt:

a) punktid a ja b asendatakse järgmisega:

„a) kauplemisteabehoidla rikub artikli 79 lõiget 1, kui ta ei tee kindlaks operatsiooniriski allikaid ega tööta nende minimeerimiseks välja asjakohaseid süsteeme, kontrolle ega protseduure, sealhulgas kooskõlas määrusega (EL) 2022/2554 hallatavaid IKT-süsteeme;

b) kauplemisteabehoidla rikub artikli 79 lõiget 2, kui ta ei kehtesta kooskõlas määrusega (EL) 2022/2554 asjakohaseid talitluspidevuse põhimõtteid ja avariitaastekava ning ei rakenda ega hoia neid jõus, et tagada kauplemisteabehoidla funktsioonide säilimine, tema tegevuse kiire taastamine ja kohustuste täitmine;“;

b) punkt c jäetakse välja.

7) III lisa muudetakse järgmiselt:

a) II jagu muudetakse järgmiselt:

i) punkt c asendatakse järgmisega:

„c) teise taseme keskne vastaspool rikub artikli 26 lõiget 3, kui ta ei hoia jõus ega rakenda sellist organisatsioonilist struktuuri, millega tagatakse, et teenuseid osutatakse ja tegevusi sooritatakse järjepidevalt ja korrektselt, või kui ta ei kasuta asjakohaseid ja proportsionaalseid süsteeme, ressursse ja protseduure, sealhulgas kooskõlas määrusega (EL) 2022/2554 hallatavaid IKT-süsteeme;“;

ii) punkt f jäetakse välja;

b) III jao punkt a asendatakse järgmisega:

„a) teise taseme keskne vastaspool rikub artikli 34 lõiget 1, kui ta ei kehtesta kooskõlas määrusega (EL) 2022/2554 asjakohaseid talitluspidevuse põhimõtteid ja avariitaastekava, ning ei rakenda ega hoia neid jõus, et tagada keskse vastaspoole funktsioonide säilitamine, tema tegevuse kiire taastamine ja kohustuste täitmine, võimaldades vähemalt taastada katkestuse korral kõik tehingud, et keskne vastaspool saaks jätkata toimimist kindlalt ja viia arveldamise lõpule kavandatud kuupäeval;“.

Artikkel 61

Määruse (EL) nr 909/2014 muutmine

Määruse (EL) nr 909/2014 artiklit 45 muudetakse järgmiselt:

1) lõige 1 asendatakse järgmisega:

„1. Keskdepositoorium tuvastab operatsiooniriski nii sisemised kui ka välised allikad ning minimeerib nende mõju asjakohaste IT-vahendite, -protsesside ja -põhimõtete rakendamise kaudu, mis on kehtestatud ja mida hallatakse kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554 (*), ning kõigi muud liiki operatsiooniriskide seisukohast asjakohaste vahendite, kontrollide ja menetluste kaudu, sealhulgas kõigi tema korraldatavate väärtpaberiarveldussüsteemide puhul.

_____

(*) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).“;

2) lõige 2 jäetakse välja;

3) lõiked 3 ja 4 asendatakse järgmisega:

„3. Keskdepositoorium kehtestab osutatavate teenuste ja iga korraldatava väärtpaberiarveldussüsteemi jaoks sobivad talitluspidevuse põhimõtted ja avariitaaste kava (sealhulgas kooskõlas määrusega (EL) 2022/2554 koostatud IKT talitluspidevuse põhimõtted ning IKT reageerimis- ja taastekavad) ning rakendab ja hoiab neid jõus, et tagada teenuste jätkuv osutamine, tegevuse kiire taastamine ja keskdepositooriumi kohustuste täitmine sündmuste korral, mille puhul on märkimisväärne tegevuse katkemise oht.

4. Lõikes 3 osutatud kava võimaldab katkestuse korral taastada kõik tehingud ja liikmete positsioonid, et võimaldada keskdepositooriumi liikmetel jätkata kindlalt tegevust ja viia arveldus lõpule kavandatud kuupäeval, sealhulgas tagades, et kriitilise tähtsusega IT-süsteemid saaksid katkestuse korral kiiresti uuesti tööle hakata, nagu on sätestatud määruse (EL) 2022/2554artikli 12 lõigetes 5 ja 7.“;

4) lõige 6 asendatakse järgmisega:

„6. Keskdepositoorium tuvastab, jälgib ja juhib riske, mille võivad tema tegevusele kaasa tuua tema korraldatavate väärtpaberiarveldussüsteemide peamised liikmed, samuti teenuste pakkujad ning muud keskdepositooriumid või muud turuinfrastruktuurid. Pädeva asutuse ja asjaomaste asutuste taotluse korral esitab ta neile teabe tuvastatud riskide kohta. Samuti teavitab ta pädevat asutust ja asjaomaseid asutusi viivitamata kõigist tegevusega seotud intsidentidest (välja arvatud IKT-riskiga seotud intsidendid), mis tulenesid kõnealustest riskidest.“;

5) lõike 7 esimene lõik asendatakse järgmisega:

„7. Euroopa Väärtpaberiturujärelevalve töötab tihedas koostöös EKPSi liikmetega välja regulatiivsete tehniliste standardite eelnõud, et täpsustada lõigetes 1 ja 6 osutatud operatsiooniriske (välja arvatud IKT-risk), kõnealuste riskide testimise, kõrvaldamise või minimeerimise meetodeid, sealhulgas lõigetes 3 ja 4 osutatud talitluspidevuse põhimõtteid ja avariitaastekava ning nende hindamise meetodeid.“

Artikkel 62

Määruse (EL) nr 600/2014 muutmine

Määrust (EL) nr 600/2014 muudetakse järgmiselt.

1) Artiklit 27g muudetakse järgmiselt:

a) lõige 4 asendatakse järgmisega:

„4. Tunnustatud kauplemisteabearuandluse avalikustaja peab täitma Euroopa Parlamendi ja nõukogu määruses (EL) 2022/2554 (*) sätestatud võrgu- ja infosüsteemide turvalisuse nõudeid.

(*) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).“;

b) lõike 8 punkt c asendatakse järgmisega:

„c) lõigetes 3 ja 5 sätestatud konkreetsed organisatsioonilised nõuded.“

2) Artiklit 27h muudetakse järgmiselt:

a) lõige 5 asendatakse järgmisega:

„5. Kauplemiskoondteabe pakkuja peab täitma määruses (EL) 2022/2554 sätestatud võrgu- ja infosüsteemide turvalisuse nõudeid.“;

b) lõike 8 punkt e asendatakse järgmisega:

„e) lõikes 4 sätestatud konkreetsed organisatsioonilised nõuded.“

3) Artiklit 27i muudetakse järgmiselt:

a) lõige 3 asendatakse järgmisega:

„3. Tunnustatud aruandlussüsteemi pakkuja peab täitma määruses (EL) 2022/2554 sätestatud võrgu- ja infosüsteemide turvalisuse nõudeid.“;

b) lõike 5 punkt b asendatakse järgmisega:

„b) lõigetes 2 ja 4 sätestatud konkreetsed organisatsioonilised nõuded.“

Artikkel 63

Määruse (EL) 2016/1011 muutmine

Määruse (EL) 2016/1011 artiklisse 6 lisatakse järgmine lõige:

„6. „Kriitilise tähtsusega võrdlusaluste puhul peab halduril olema usaldusväärne haldus- ja arvestuskord, sisekontrollimehhanism, tõhusad riskianalüüsi menetlused ning tõhus kontrolli- ja kaitsekord IKT-süsteemide haldamiseks kooskõlas Euroopa Parlamendi ja nõukogu määrusega (EL) 2022/2554 (*).

(*) Euroopa Parlamendi ja nõukogu 14. detsembri 2022. aasta määrus (EL) 2022/2554, mis käsitleb finantssektori digitaalset tegevuskerksust ning millega muudetakse määrusi (EÜ) nr 1060/2009, (EL) nr 648/2012, (EL) nr 600/2014, (EL) nr 909/2014 ja (EL) 2016/1011 (ELT L 333, 27.12.2022, lk 1).“

Artikkel 64

Jõustumine ja kohaldamine

Käesolev määrus jõustub kahekümnendal päeval pärast selle avaldamist *Euroopa Liidu Teatajas*.

Seda kohaldatakse alates 17. jaanuarist 2025.

Käesolev määrus on tervikuna siduv ja vahetult kohaldatav kõikides liikmesriikides.

Strasbourg, 14. detsember 2022

Euroopa Parlamendi nimel	*Nõukogu nimel*
president	*eesistuja*
R. METSOLA	M. BEK