EES-STOFNANIR

SAMEIGINLEGA EES-NEFNDIN

REGLUGERÐ EVRÓPUÞINGSINS OG RÁÐSINS (ESB) 2022/2554 **2025/EES/15/01**

frá 14. desember 2022

um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (*)

EVRÓPUÞINGIÐ OG RÁÐ EVRÓPUSAMBANDSINS HAFA,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins, einkum 114. gr.,

með hliðsjón af tillögu framkvæmdastjórnar Evrópusambandsins,

eftir að hafa lagt drög að lagagerð fyrir þjóðþingin,

með hliðsjón af áliti Seðlabanka Evrópu ([1]),

með hliðsjón af áliti efnahags- og félagsmálanefndar Evrópusambandsins ([2]),

í samræmi við almenna lagasetningarmeðferð ([3]),

og að teknu tilliti til eftirfarandi:

1) Á stafrænni öld styður upplýsinga- og fjarskiptatækni flókin kerfi sem notuð eru við dagleg störf. Hún heldur hagkerfum okkar gangandi í lykilgeirum, þ.m.t. fjármálageiranum, og eflir starfsemi innri markaðarins. Aukin stafvæðing og samtenging magnar einnig upp upplýsinga- og fjarskiptatækniáhættu og gerir samfélagið í heild sinni og einkum fjármálakerfið berskjaldaðra fyrir netógnum eða röskunum á upplýsinga- og fjarskiptatækni. Þó að útbreidd notkun upplýsinga- og fjarskiptatæknikerfa og mikil stafvæðing og tengjanleiki séu kjarnaþættir í starfsemi aðila á fjármálamarkaði Sambandsins nú á dögum á enn eftir að fjalla betur um stafrænan viðnámsþrótt þeirra og samþætta hann víðari rekstrarumgjörð þeirra.

2) Á síðustu áratugum hefur notkun upplýsinga- og fjarskiptatækni öðlast lykilhlutverk í fjármálaþjónustu, að því marki að hún hefur náð afgerandi mikilvægi í rekstri dæmigerðrar daglegrar starfsemi allra aðila á fjármálamarkaði. Núorðið nær stafvæðing t.d. yfir greiðslur, sem hafa í auknum mæli færst úr notkun á reiðufé og pappír yfir í stafrænar lausnir, sem og stöðustofnun og uppgjör verðbréfa, rafræn viðskipti og algrímsviðskipti, lánveitingar og fjármögnun, jafningjafjármögnun, lánshæfismat, tjónsuppgjör og bakvinnsla. Tryggingafélögin hafa einnig breyst með notkun upplýsinga- og fjarskiptatækni, allt frá tilkomu vátryggingamiðlara sem bjóða þjónustu sína á netinu með

(*) Þessi ESB-gerð birtist í Stjtíð. ESB L 333, 27.12.2022, p. 1. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 40/2025 frá 20. febrúar 2025 um breytingu á IX. viðauka (Fjármálaþjónusta) við EES-samninginn (síður birtingar).

([1]) Stjtíð. ESB C 343, 26.8.2021, bls. 1.

([2]) Stjtíð. ESB C 155, 30.4.2021, bls. 38.

([3]) Afstaða Evrópuþingsins frá 10. nóvember 2022 (hefur enn ekki verið birt í Stjórnartíðindunum) og ákvörðun ráðsins frá 28. nóvember 2022.

vátryggingatækni, til stafrænnar vátryggingaskuldbindingar. Fjármögnun er ekki aðeins orðin meira og minna stafræn í gervöllum geiranum, heldur hefur stafvæðing einnig aukið samtengingu og hæði innan fjármálageirans og við innviði þriðju aðila og þjónustuveitendur.

3) Evrópska kerfisáhætturáðið áréttaði í skýrslu frá 2020, sem fjallar um kerfisbundnar netógnir, hvernig sú mikla samtenging sem nú er fyrir hendi milli aðila á fjármálamarkaði, fjármálamarkaða og innviða fjármálamarkaða, einkum innbyrðis hæði upplýsinga- og fjarskiptatæknikerfa þeirra, gæti skapað kerfislæga veikleika vegna þess að staðbundin netatvik gætu dreifst hratt út frá einhverjum þeirra u.þ.b. 22 000 aðila á fjármálamarkaði í Sambandinu til alls fjármálakerfisins, óháð landfræðilegum mörkum. Alvarleg rof í upplýsinga- og fjarskiptatækni sem eiga sér stað í fjármálageiranum hafa ekki einungis áhrif á hvern aðila á fjármálamarkaði fyrir sig. Þau geta einnig valdið útbreiðslu staðbundinna veikleika í flutningsleiðum fjármagns og haft í för með sér skaðlegar afleiðingar fyrir stöðugleika fjármálakerfis Sambandsins, s.s. að skapa möguleg lausafjáráhlaup og almennt tap á trúnaði og trausti á fjármála-mörkuðum.

4) Undanfarin ár hefur upplýsinga- og fjarskiptatækniáhætta vakið athygli stefnumótenda, eftirlitsaðila og aðila sem annast setningu staðla sem starfa á alþjóðavísu, á vettvangi Sambandsins og á landsvísu, í því skyni að auka stafrænan viðnámsþrótt, setja staðla og samræma vinnu á sviði reglusetningar eða eftirlits. Á alþjóðavettvangi miða Baselnefnd um bankaeftirlit, greiðslu- og markaðsinnviðanefnd, ráðgjafarnefnd um fjármálastöðugleika, stofnun um fjármála-stöðugleika, sem og G7- og G20-hóparnir að því að veita lögbærum yfirvöldum og rekstraraðilum markaða í mismunandi lögsögum úrræði til að efla viðnámsþrótt í fjármálakerfum sínum. Þessi vinna hefur einnig verið knúin áfram af þörfinni á að taka tilhlýðilegt tillit til upplýsinga- og fjarskiptatækniáhættu í tengslum við afar samtengt alþjóðlegt fjármálakerfi og stefna að meira samræmi á milli viðkomandi bestu starfsvenja.

5) Þrátt fyrir markvissar tillögur að stefnumörkun og lagasetningu í Sambandinu og á landsvísu er upplýsinga- og fjarskiptatækniáhætta enn áskorun fyrir rekstrarlegan viðnámsþrótt, afköst og stöðugleika fjármálakerfis Sambandsins. Umbæturnar sem fylgdu í kjölfar fjármálakreppunnar 2008 styrktu fyrst og fremst fjárhagslegan viðnámsþrótt í fjármálageiranum innan Sambandsins og miðuðu að því að standa vörð um samkeppnishæfni og stöðugleika Sambandsins út frá efnahagslegum sjónarmiðum, varfærnissjónarmiðum og háttsemi á markaði. Þótt öryggi í upplýsinga- og fjarskiptatækni og stafrænn viðnámsþróttur séu hluti af rekstraráhættu hefur minna verið lagt upp úr þeim í reglusetningaráætlun eftir fjármálakreppuna og þær hafa eingöngu þróast á nokkrum sviðum í stefnu Sambandsins í fjármálaþjónustu og reglugerðarlandslagi, eða aðeins í nokkrum aðildarríkjum.

6) Í orðsendingu framkvæmdarstjórnarinnar frá 8. mars 2018, sem ber heitið „Aðgerðaáætlun fyrir fjártækni: Til að styrkja samkeppnishæfni og nýsköpun í evrópskum fjármálageira“, undirstrikaði framkvæmdastjórnin að afar mikilvægt væri að auka viðnámsþrótt fjármálageira Sambandsins, þ.m.t. frá rekstrarlegu sjónarmiði til að tryggja tæknilegt öryggi og virkni, til að hann jafni sig fljótt eftir rof og atvik í upplýsinga- og fjarskiptatækni og gera að lokum kleift að veita fjármálaþjónustu með skilvirkum og snurðulausum hætti í öllu Sambandinu, þ.m.t. við erfiðar aðstæður, en viðhalda jafnframt trausti og tiltrú neytenda og markaða.

7) Í apríl 2019 gáfu evrópska eftirlitsstofnunin (Evrópska bankaeftirlitsstofnunin), sem komið var á fót með reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([4]), evrópska eftirlitsstofnunin (Evrópska vátrygginga- og lífeyris-sjóðaeftirlitsstofnunin), sem komið var á fót með reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([5]) og evrópska eftirlitsstofnunin (Evrópska verðbréfamarkaðseftirlitsstofnunin), sem komið var á fót með reglugerð

([4]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska bankaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og niðurfellingu ákvörðunar framkvæmdastjórnarinnar 2009/78/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 12).

([5]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/79/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 48).

Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([6]) (sameiginlega „evrópsku eftirlitsstofnanirnar“) í sameiningu út tækniráðgjöf þar sem þær kalla eftir samræmdri nálgun við upplýsinga- og fjarskiptatækniáhættu í fjármálum og mæla með því að efla stafrænan viðnámsþrótt fjármálaþjónustugeirans á hlutfallslegan hátt með framtaksverkefni Sambandsins sem er sértækt fyrir geirann.

8) Fjármálageiri Sambandsins lýtur sameiginlegum reglum og evrópska fjármálaeftirlitskerfið gildir um hann. Engu að síður hafa ákvæði sem fjalla um stafrænan rekstrarlegan viðnámsþrótt og öryggi í upplýsinga- og fjarskiptatækni ekki enn verið samræmd að fullu eða á einsleitan hátt, þrátt fyrir að stafrænn rekstrarlegur viðnámsþróttur sé afar mikilvægur til að tryggja fjármálastöðugleika og heilleika markaðar á stafrænni öld og ekki síður mikilvægt en t.d. sameiginlegar kröfur um varfærniseftirlit eða háttsemi á markaði. Því ætti að þróa sameiginlegu reglurnar og eftirlitskerfið þannig að það nái einnig yfir stafrænan rekstrarlegan viðnámsþrótt með því að styrkja umboð lögbærra yfirvalda til að gera þeim kleift að hafa eftirlit með stýringu upplýsinga- og fjarskiptatækniáhættu í fjármálageiranum til að vernda heilleika og skilvirkni innri markaðarins og greiða fyrir eðlilegri starfsemi hans.

9) Misræmi í löggjöf og mismunandi innlendar reglur eða aðferðir við eftirlit með tilliti til upplýsinga- og fjarskiptatækniáhættu veldur hömlum á starfsemi innri markaðar fyrir fjármálaþjónustu og hindrar snurðulausa nýtingu staðfesturéttar og þjónustustarfsemi fyrir aðila á fjármálamarkaði sem starfa þvert á landamæri. Samkeppni milli aðila á fjármálamarkaði sem eru af sömu gerð en starfa í ólíkum aðildarríkjum gæti einnig raskast. Þetta á einkum við á sviðum þar sem samræming innan Sambandsins hefur verið mjög takmörkuð, s.s. prófun á stafrænum rekstrarlegum viðnámsþrótti eða ef hún er ekki fyrir hendi, þá vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðja aðila. Misræmi sem stafar af fyrirsjáanlegri þróun á landsvísu gæti leitt til frekari hindrana á starfsemi innri markaðarins, markaðsaðilum og fjármálastöðugleika í óhag.

10) Þar sem aðeins hefur verið fjallað um ákvæði tengd upplýsinga- og fjarskiptatækniáhættu að hluta til á vettvangi Sambandsins eru gloppur eða skörun á mikilvægum sviðum eins og er, s.s. hvað varðar tilkynningar vegna atvika sem tengjast upplýsinga- og fjarskiptatækni og prófanir á stafrænum rekstrarlegum viðnámsþrótti, og misræmi sem stafar af ólíkum landsreglum eða óhagkvæmni, með tilliti til kostnaðar, við beitingu reglna sem skarast. Þetta er sérstaklega skaðlegt fyrir þá sem nota upplýsinga- og fjarskiptatækni mikið, s.s. fjármálageirann, þar sem tæknileg áhætta hefur engin landamæri og fjármálageirinn veitir þjónustu sína vítt og breitt yfir landamæri, innan Sambandsins og utan. Einstaka aðilar á fjármálamarkaði sem starfa þvert á landamæri eða hafa fleiri en eitt starfsleyfi (t.d. getur einn aðili á fjármálamarkaði haft starfsleyfi sem bankaþjónusta, verðbréfafyrirtæki og greiðslustofnun, þar sem hvert starfsleyfi getur verði gefið út af mismunandi lögbærum yfirvöldum í einu eða fleiri aðildarríkjum) standa frammi fyrir rekstrarlegum áskorunum við að takast á við upplýsinga- og fjarskiptatækniáhættu og milda neikvæð áhrif af atvikum í upplýsinga- og fjarskiptatækni á eigin spýtur og á samfelldan og hagkvæman hátt.

11) Þar sem sameiginlegu reglunum hefur ekki fylgt heildarrammi um upplýsinga- og fjarskiptatækni- eða rekstraráhættu er þörf á frekari samræmingu á helstu kröfum um rekstrarlegan viðnámsþrótt allra aðila á fjármálamarkaði. Ef aðilar á fjármálamarkaði þróa færni sína í upplýsinga- og fjarskiptatækni og heildarviðnámsþrótt sinn á grundvelli þessara lykilkrafna í því skyni að standast rekstrartruflanir myndi það efla getu þeirra til að viðhalda stöðugleika og heilleika fjármálamarkaða Sambandsins og stuðla þannig að því að tryggja öfluga vernd fjárfesta og neytenda í Sambandinu. Þar eð með reglugerð þessari er miðað að því að stuðla að snurðulausri starfsemi innri markaðarins ætti hún að byggjast á ákvæðum 114. gr. sáttmálans um starfshætti Evrópusambandsins (SUSE) eins og hann er túlkaður í samræmi við samræmda dómaframkvæmd Evrópudómstólsins (dómstóllinn).

12) Með þessari reglugerð er miðað að því að steypa saman í einn texta og uppfæra kröfur vegna upplýsinga- og fjarskiptatækniáhættu sem hluta af kröfum vegna rekstraráhættu, sem fram að þessu hefur verið fjallað um sérstaklega í ýmsum réttargerðum Sambandsins. Þótt þær gerðir næðu yfir helstu flokka fjárhagslegrar áhættu (t.d. útlánaáhættu, markaðsáhættu, útlánaáhættu mótaðila og lausafjáráhættu, háttsemisáhættu) tóku þær ekki heildstætt á öllum þáttum sem vörðuðu rekstrarlegan viðnámsþrótt þegar þær voru samþykktar. Þegar reglur um rekstraráhættu voru þróaðar frekar í þessum réttargerðum Sambandsins var hefðbundin megindleg nálgun til að takast á við áhættu (þ.e. að setja eiginfjárkröfu til að mæta upplýsinga- og fjarskiptatækniáhættu) oft tekin fram yfir markvissar eigindlegar reglur um

([6]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska verðbréfamarkaðseftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/77/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 84).

getu til að vernda, greina, afmarka, endurreisa og lagfæra í tengslum við atvik sem tengjast upplýsinga- og fjarskiptatækni eða að því er varðar getu til skýrslugjafar og stafrænnar prófunar. Þessar gerðir áttu fyrst og fremst að ná yfir og uppfæra nauðsynlegar reglur um varfærniseftirlit, heilleika markaðar eða háttsemi. Með því að steypa saman og uppfæra ólíkar reglur um upplýsinga- og fjarskiptatækniáhættu ættu öll ákvæði sem fjalla um stafræna áhættu í fjármálageiranum að vera sameinuð á samræmdan hátt í einni lagagerð í fyrsta sinn. Því fyllir þessi reglugerð upp í eyður eða leysir úr ósamræmi í sumum fyrri gerðum, þ.m.t. í tengslum við þau hugtök sem þar eru notuð, og vísar með skýrum hætti til upplýsinga- og fjarskiptatækniáhættu með markvissum reglum um getu til stýringar upplýsinga- og fjarskiptatækniáhættu, skýrslugjöf um atvik, prófun á rekstrarlegum viðnámsþrótti og áhættuvöktun þriðju aðila. Því ætti reglugerðin einnig að auka vitund um upplýsinga- og fjarskiptatækniáhættu og gangast við því að atvik í upplýsinga- og fjarskiptatækni og skortur á rekstrarlegum viðnámsþrótti geti stofnað áreiðanleika aðila á fjármálamarkaði í hættu.

13) Aðilar á fjármálamarkaði ættu að fylgja sömu nálgun og meginreglum þegar þeir takast á við upplýsinga- og fjarskiptatækniáhættu, að teknu tilliti til stærðar þeirra og heildaráhættusniðs og eðlis, umfangs og flækjustigs þjónustu þeirra, starfsemi og reksturs. Samræmi stuðlar að aukinni tiltrú á fjármálakerfið og viðheldur stöðugleika þess, einkum á tímum þegar treyst er mikið á upplýsinga- og fjarskiptatæknikerfi, -vettvanga og -innviði, sem hafa í för með sér aukna stafræna áhættu. Að viðhalda grundvallarnetheilbrigði ætti einnig að forða því að þungar byrðar séu lagðar á hagkerfið með því að lágmarka áhrif og kostnað vegna raskana á upplýsinga- og fjarskiptatækni.

14) Reglugerð stuðlar að því að draga úr flækjustigi í framkvæmd, eykur samleitni í eftirliti og réttarvissu og stuðlar einnig að takmörkun á kostnaði við að fara að reglum, einkum hjá aðilum á fjármálamarkaði sem starfa yfir landamæri, og dregur úr röskun á samkeppni. Að velja reglugerð til að koma á sameiginlegum ramma um stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði hentar því best til að tryggja einsleita og samfellda beitingu allra þátta í stýringu upplýsinga- og fjarskiptatækniáhættu af hálfu fjármálageira Sambandsins.

15) Tilskipun Evrópuþingsins og ráðsins (ESB) 2016/1148 ([7]) var fyrsti þverlægi netöryggisramminn sem var samþykktur á vettvangi Sambandsins og gilti einnig um þrjár tegundir aðila á fjármálamarkaði, nánar tiltekið lánastofnanir, viðskiptavettvanga og miðlæga mótaðila. Þar sem tilskipun (ESB) 2016/1148 setti fram tilhögun tilgreiningar á landsvísu á rekstraraðilum nauðsynlegrar þjónustu hafa þó aðeins tilteknar lánastofnanir, viðskiptavettvangar og miðlægir mótaðilar, sem aðildarríkin hafa tilgreint, verið færð inn á gildissvið hennar í reynd og er þar af leiðandi skylt að fara að þeim kröfum um öryggi upplýsinga- og fjarskiptatækni og tilkynningarskyldu atvika sem þar er mælt fyrir um. Í tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2555 ([8]) eru sett fram samræmd viðmið til að ákvarða hvaða einingar falla undir gildissvið hennar (reglan um stærðartakmörkun) og halda jafnframt þessum þremur tegundum aðila á fjármálamarkaði innan gildissviðs hennar.

16) Þar eð þessi reglugerð eykur samræmingu mismunandi hluta stafræns viðnámsþróttar með því að innleiða kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu og skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni sem eru strangari í samanburði við þær sem mælt er fyrir um í núgildandi lögum Sambandsins um fjármálaþjónustu, telst þessi aukna samræming þó einnig vera aukin í samanburði við kröfurnar sem mælt er fyrir um í tilskipun (ESB) 2022/2555. Af þessum sökum telst þessi reglugerð vera sérlög að því er varðar tilskipun (ESB) 2022/2555. Jafnframt er mikilvægt að viðhalda sterku sambandi milli fjármálageirans og þverlægs netöryggisramma Sambandsins eins og nú er mælt fyrir um í tilskipun (ESB) 2022/2555 til að tryggja samræmi við stefnuáætlanir um netöryggi sem aðildarríkin hafa samþykkt og gera fjármálaeftirlitsaðilum kleift að fá vitneskju um netatvik sem hafa áhrif á aðra geira sem falla undir þá tilskipun.

([7]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2016/1148 frá 6. júlí 2016 varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Sambandinu (Stjtíð. ESB L 194, 19.7.2016, bls. 1).

([8]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2555 frá 14. desember 2022 um ráðstafanir til að ná háu sameiginlegu stigi á sviði netöryggis í öllu Sambandinu, um breytingu á reglugerð (ESB) nr. 910/2014 og tilskipun (ESB) 2018/1972, og um niðurfellingu á tilskipun (ESB) 2016/1148 (NIS 2-tilskipunin) (Stjtíð. ESB L 333, 27.12.2022, bls. 80).

17) Í samræmi við 2. mgr. 4. gr. sáttmálans um Evrópusambandið og með fyrirvara um úrskurðarvald dómstóla ætti þessi reglugerð ekki að hafa áhrif á ábyrgð aðildarríkjanna að því er varðar mikilvæga starfsemi þeirra á sviði almannaöryggis, varna og þjóðaröryggis, t.d. að því er varðar afhendingu upplýsinga sem myndu stríða gegn þjóðaröryggi.

18) Til að auðvelda þekkingarmiðlun á milli geira og byggja á reynslu annarra geira af því að takast á við netógnir ættu aðilar á fjármálamarkaði, sem um getur í tilskipun (ESB) 2022/2555, að vera áfram hluti af „vistkerfi“ þeirrar tilskipunar (t.d. samstarfshópur og viðbragðsteymi vegna váatvika er varða tölvuöryggi. Evrópsku eftirlitsstofnanirnar og lögbær landsyfirvöld ættu að geta tekið þátt í umræðum um stefnumótun og tæknilega vinnu samstarfshópsins samkvæmt þeirri tilskipun og skipst á upplýsingum og átt frekara samstarf við sameiginlega tengiliði sem eru tilnefndir eða komið á fót í samræmi við þá tilskipun. Samkvæmt þessari reglugerð ættu lögbær yfirvöld einnig að hafa samráð við og eiga samstarf við viðbragðsteymi vegna váatvika er varða tölvuöryggi. Lögbær yfirvöld ættu einnig að geta beðið um tækniráðgjöf frá þeim lögbæru yfirvöldum sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555 og komið á samstarfssamningum sem miða að því að tryggja skilvirkar samræmingaraðferðir fyrir skjót viðbrögð.

19) Í ljósi mikilla innri tengsla milli stafræns viðnámsþróttar og raunlægs viðnámsþróttar aðila á fjármálamarkaði er nauðsynlegt að beita samræmdri aðferð að því er varðar viðnámsþrótt mikilvægra rekstrareininga í þessari reglugerð og tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2557 ([9]). Að því gefnu að stýring upplýsinga- og fjarskiptatækniáhættu og skyldur um skýrslugjöf sem falla undir þessa reglugerð taki heildstætt á raunlægum viðnámsþrótti upplýsinga- og fjarskiptatækni, ættu skuldbindingarnar sem mælt er fyrir um í III. og IV. kafla tilskipunar (ESB) 2022/2557 ekki að gilda um aðila á fjármálamarkaði sem falla undir gildissvið þeirrar tilskipunar.

20) Veitendur skýjavinnsluþjónustu eru einn flokkur stafrænna grunnvirkja sem falla undir tilskipun (ESB) 2022/2555. Eftirlitsrammi Sambandsins („eftirlitsrammi“), sem komið er á með þessari reglugerð, gildir um alla mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptaþjónustu, þ.m.t. veitendur skýjavinnsluþjónustu sem veita aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu, og ætti að teljast koma til viðbótar við það eftirlit sem fer fram samkvæmt tilskipun (ESB) 2022/2555. Enn fremur ætti eftirlitsramminn, sem komið er á með þessari reglugerð, að taka til veitenda skýjavinnsluþjónustu þar sem ekki er fyrir hendi þverlægur rammi Sambandsins sem kemur stafrænu eftirlitsyfirvaldi á fót.

21) Til að halda fullri stjórn á upplýsinga- og fjarskiptatækniáhættu þurfa aðilar á fjármálamarkaði að búa yfir yfirgripsmikilli getu til að stuðla að öflugri og skilvirkri stýringu upplýsinga- og fjarskiptatækniáhættu sem og tilteknum kerfum og stefnum til að takast á við öll atvik sem tengjast upplýsinga- og fjarskiptatækni og tilkynna alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Að sama skapi ættu aðilar á fjármálamarkaði að marka stefnur vegna prófunar á upplýsinga- og fjarskiptatæknikerfum, stjórntækjum og ferlum, sem og vegna stýringar á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila. Hækka ætti grunnviðmið stafræns rekstrarlegs viðnámsþróttar fyrir aðila á fjármálamarkaði en gera jafnframt ráð fyrir hlutfallslegri beitingu krafna fyrir tiltekna aðila, einkum örfyrirtæki, sem og aðila á fjármálamarkaði sem falla undir einfaldaðan ramma um stýringu upplýsinga- og fjarskiptatækniáhættu. Til að auðvelda skilvirkt eftirlit með stofnunum um starfstengdan lífeyri sem er hóflegt og tekur á þörfinni á að draga úr stjórnsýsluálagi á lögbær yfirvöld ættu viðeigandi landsbundnar eftirlitsráðstafanir, að því er varðar slíka aðila á fjármálamarkaði, að taka tillit til stærðar þeirra og heildaráhættusniðs og eðlis, umfangs og flækjustigs þjónustu þeirra, starfsemi og reksturs jafnvel þótt farið sé yfir viðeigandi viðmiðunarmörk sem sett eru í 5. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2016/2341 ([10]). Einkum ætti eftirlitsstarfsemi að beinast fyrst og fremst að þörfinni á að taka á alvarlegri áhættu sem tengist stýringu upplýsinga- og fjarskiptatækniáhættu tiltekinnar einingar.

([9]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2557 frá 14. desember 2022 um viðnámsþrótt mikilvægra rekstrareininga og niðurfellingu á tilskipun ráðsins 2008/114/EB (Stjtíð. ESB L 333, 27.12.2022, bls. 164).

([10]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2016/2341 frá 14. desember 2016 um starfsemi og eftirlit með stofnunum sem sjá um starfstengdan lífeyri (Stjtíð. ESB L 354, 23.12.2016, bls. 37).

Lögbær yfirvöld ættu einnig að nota aðferðir sem byggjast á árvekni en eru hóflegar í tengslum við eftirlit með stofnunum um starfstengdan lífeyri sem, í samræmi við 31. gr. tilskipunar (ESB) 2016/2341, útvista verulegum hluta kjarnastarfsemi sinnar, s.s. eignastýringu, tryggingafræðilegum útreikningum, reikningshaldi og gagnastjórnun, til þjónustuveitenda.

22) Viðmiðunarmörk skýrslugjafar um atvik sem tengjast upplýsinga- og fjarskiptatækni og flokkunarfræði atvika eru verulega mismunandi á landsvísu. Þótt ná megi sameiginlegum grundvelli með viðeigandi vinnu sem Netöryggisstofnun Evrópusambandsins, sem komið var á fót með reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881 ([11]), og samstarfshópurinn innti af hendi samkvæmt tilskipun (ESB) 2022/2555 eru mismunandi aðferðir við að setja viðmiðunarmörk og flokka atvik enn fyrir hendi eða geta komið upp hjá hinum aðilunum á fjármálamarkaði. Vegna þessa misræmis eru það margvíslegar kröfur sem aðilar á fjármálamarkaði verða að uppfylla, einkum þegar þær starfa í mörgum aðildarríkjum og þegar þær eru hluti af fjármálasamstæðu. Enn fremur getur slíkt misræmi hugsanlega hindrað frekari samræmingu eða miðstýringu kerfa Sambandsins sem hraða skýrslugjafarferlinu og styðja skjót og snurðulaus upplýsingaskipti á milli lögbærra yfirvalda, sem skiptir sköpum til að takast á við upplýsinga- og fjarskiptatækniáhættu ef til stórfelldra árása kemur sem gætu haft kerfislægar afleiðingar.

23) Til að draga úr stjórnsýslubyrði og hugsanlegri tvöfaldri kvöð um skýrslugjöf fyrir tiltekna aðila á fjármálamarkaði ætti krafa um skýrslugjöf vegna atvika samkvæmt tilskipun Evrópuþingsins og ráðsins (ESB) 2015/2366 ([12]) að falla úr gildi gagnvart greiðsluþjónustuveitendum sem falla innan gildissviðs þessarar reglugerðar. Af þessum sökum ættu lánastofnanir, rafeyrisfyrirtæki, greiðslustofnanir og reikningsupplýsingaþjónustuveitendur, eins og um getur í 1. mgr. 33. gr. þeirrar tilskipunar, að gefa skýrslu samkvæmt þessari reglugerð um öll greiðslutengd rekstrar- og öryggisatvik og áður hefur verið tilkynnt um samkvæmt þeirri tilskipun frá þeim degi sem þessi reglugerð kemur til framkvæmda, án tillits til þess hvort slík atvik tengist upplýsinga- og fjarskiptatækni.

24) Til að gera lögbærum yfirvöldum kleift að uppfylla eftirlitshlutverk sín með því að fá heildaryfirsýn yfir eðli, tíðni, mikilvægi og áhrif atvika sem tengjast upplýsinga- og fjarskiptatækni og bæta upplýsingaskipti milli viðkomandi opinberra yfirvalda, þ.m.t. löggæsluyfirvalda og skilastjórnvalda, ætti þessi reglugerð að mæla fyrir um traust fyrirkomulag fyrir skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni, þar sem viðeigandi kröfur taka á núverandi gloppum í lögum um fjármálaþjónustu og eyða fyrirliggjandi skörun og tvítekningu til að draga úr kostnaði. Nauðsynlegt er að samræma fyrirkomulag um skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni með því að krefjast þess að allir aðilar á fjármálamarkaði gefi lögbærum yfirvöldum skýrslu í gegnum einn einfaldaðan ramma eins og sett er fram í þessari reglugerð. Evrópsku eftirlitsstofnanirnar ættu einnig að hafa vald til að tilgreina nánar viðeigandi þætti fyrir ramma um skýrslugjöf vegna atvika sem tengjast upplýsinga- og fjarskiptatækni, s.s. flokkunarfræði, tímaramma, gagnasöfn, sniðmát og viðeigandi viðmiðunarmörk. Til að tryggja fullt samræmi við tilskipun (ESB) 2022/2555 ætti aðilum á fjármálamarkaði að vera heimilt, að eigin frumkvæði, að tilkynna viðkomandi lögbæru yfirvaldi um verulegar netógnir þegar þær telja að sú netógn varði fjármálakerfið, notendur þjónustu eða viðskiptavini.

25) Kröfur um prófanir á stafrænum rekstrarlegum viðnámsþrótti hafa verið þróaðar í tilteknum fjármálaundirgeirum þar sem settir eru fram aðgerðarammar sem eru ekki alltaf samræmdir að fullu. Þetta leiðir til hugsanlegrar tvöföldunar kostnaðar hjá aðilum á fjármálamarkaði sem starfa yfir landamæri og gerir gagnkvæma viðurkenningu á niðurstöðum úr prófunum á stafrænum rekstrarlegum viðnámsþrótti flókna, sem getur síðan valdið sundrun á innri markaðnum.

([11]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2019/881 frá 17. apríl 2019 um Netöryggisstofnun Evrópusambandsins (ENISA), um netöryggisvottun upplýsinga- og fjarskiptatækni og um niðurfellingu reglugerðar (ESB) nr. 526/2013 (gerð um netöryggi) (Stjtíð. ESB L 151, 7.6.2019, bls. 15).

([12]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2015/2366 frá 25. nóvember 2015 um greiðsluþjónustu á innri markaðnum, um breytingu á tilskipunum 2002/65/EB, 2009/110/EB og 2013/36/ESB og á reglugerð (ESB) nr. 1093/2010 og niðurfellingu á tilskipun 2007/64/EB (Stjtíð. ESB L 337, 23.12.2015, bls. 35).

26) Þegar ekki er krafist prófana á upplýsinga- og fjarskiptatækni munu veikleikar enn fremur ekki greinast, sem gerir aðila á fjármálamarkaði útsetta fyrir upplýsinga- og fjarskiptatækniáhættu og skapar að lokum meiri áhættu fyrir stöðugleika og heilleika fjármálageirans. Án íhlutunar Sambandsins væru prófanir á stafrænum rekstrarlegum viðnámsþrótti áfram ósamræmdar og skortur væri á kerfi til gagnkvæmrar viðurkenningar á niðurstöðum prófana á upplýsinga- og fjarskiptatækni milli ólíkra lögsagnarumdæma. Þar sem ólíklegt er að aðrir fjármálaundirgeirar taki upp prófunarkerfi að einhverju marki myndu þeir að auki missa af mögulegum ávinningi af prófunarramma, hvað varðar afhjúpun veikleika og áhættu í upplýsinga- og fjarskiptatækni, og prófun á varnargetu og rekstrarsamfellu, sem stuðlar að því að auka traust viðskiptavina, birgja og samstarfsaðila. Til að lagfæra þessa skörun, mismun og gloppur er nauðsynlegt að mæla fyrir um reglur um samræmt prófunarfyrirkomulag og greiða þannig fyrir gagnkvæmri viðurkenningu á auknum prófunum fyrir aðila á fjármálamarkaði sem uppfylla viðmiðanirnar sem settar eru fram í þessari reglugerð.

27) Aðilar á fjármálamarkaði eru háðir notkun upplýsinga- og fjarskiptatækniþjónustu sem ræðst að hluta til af þörf þeirra á að aðlagast nýju, samkeppnishæfu og stafrænu hnattrænu hagkerfi, efla skilvirkni viðskipta og mæta eftirspurn neytenda. Eðli og umfang slíks hæðis hefur verið í stöðugri þróun undanfarin ár sem hefur stuðlað að lækkun kostnaðar við miðlun fjármálaþjónustu og auðveldað vöxt og skalanleika rekstrar við útfærslu fjármálastarfsemi um leið og boðið er upp á fjölbreytt úrval upplýsinga- og fjarskiptatæknibúnaðar til að stjórna flóknum innri ferlum.

28) Víðtæk notkun á upplýsinga- og fjarskiptatækniþjónustu kemur fram í flóknu samningsbundnu fyrirkomulagi þar sem aðilar á fjármálamarkaði eiga oft í erfiðleikum með að semja um samningsskilmála sem eru sniðnir að varfærnisviðmiðunum eða öðrum kröfum samkvæmt reglum sem gilda um þá, eða með öðrum hætti við að framfylgja sérstökum réttindum, s.s. aðgangs- eða endurskoðunarréttindum, jafnvel þegar hið síðarnefnda er að finna í samningsbundnu fyrirkomulagi þeirra. Auk þess kveður margt af þessu samningsbundna fyrirkomulagi ekki á um fullnægjandi verndarráðstafanir sem gera kleift að hafa stöðugt eftirlit með ferlum undirverktaka og gera aðilanum á fjármálamarkaði þannig ófært að meta tengda áhættu. Þar sem þriðju aðilar í upplýsinga- og fjarskiptatækniþjónustu veita ólíkum gerðum viðskiptavina oft staðlaða þjónustu er slíkt samningsbundið fyrirkomulag þar að auki ekki alltaf nægilega vel ígrundað fyrir einstakar eða sértækar þarfir aðila á sviði fjármálageirans.

29) Þó að lög Sambandsins um fjármálaþjónustu feli í sér tilteknar almennar reglur um útvistun er eftirlit með umfangi samnings ekki að fullu bundið í lög Sambandsins. Ef skýrir og sérsniðnir Sambandsstaðlar sem gilda um samningsbundið fyrirkomulag við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu eru ekki fyrir hendi er ekki fjallað ítarlega um ytri áhættuþætti vegna upplýsinga- og fjarskiptatækni. Þar af leiðandi er nauðsynlegt að setja fram tilteknar meginreglur til að leiðbeina aðilum á fjármálamarkaði við stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem eru einkar mikilvægar þegar aðilarnir leita til þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til að styðja nauðsynlega eða mikilvæga starfsemi þeirra. Þessum meginreglum ættu fylgja nokkur meginatriði samningsbundins réttar í tengslum við nokkra þætti í framkvæmd og riftun samningsbundins fyrirkomulags með það í huga að veita tilteknar lágmarksverndarráðstafanir til að styrkja getu aðila á fjármálamarkaði til að hafa skilvirkt eftirlit með allri upplýsinga- og fjarskiptatækniáhættu sem stafar af þjónustuveitendum sem eru þriðju aðilar. Þessar meginreglur eru til viðbótar við sérlög sem gilda um útvistun.

30) Augljóst er að í dag er tiltekinn skortur á einsleitni og samleitni í vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila og á því hve mikið er treyst á þriðju aðila í upplýsinga- og fjarskiptatækni. Þrátt fyrir viðleitni til að fjalla um útvistun, s.s. viðmiðunarreglur Evrópsku bankaeftirlitsstofnunarinnar frá 2019 um útvistun og viðmiðunarreglur Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar frá 2021 um útvistun til veitenda skýjaþjónustu, er ekki fjallað nægilega í lögum Sambandsins um hið víðtækara mál að sporna við kerfisáhættu sem kann að stafa af áhættuskuldbindingum fjármálageirans gagnvart takmörkuðum fjölda mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Auk skorts á reglum á vettvangi Sambandsins er skortur á innlendum reglum um umboð og tól sem gera fjármálaeftirlitsaðilum kleift að öðlast góðan skilning á hæði við þriðju aðila í upplýsinga- og fjarskiptatækni og vakta nægilega þá áhættu sem stafar af samþjöppun hæðis við þriðju aðila í upplýsinga- og fjarskiptatækni.

31) Með tilliti til hugsanlegrar kerfisáhættu sem hlýst af aukinni útvistun og samþjöppun þriðju aðila í upplýsinga- og fjarskiptatækni, og með ófullnægjandi landsbundna tilhögun í huga við að veita fjármálaeftirlitsaðilum fullnægjandi verkfæri til að mæla, meta og ráða bót á afleiðingum af upplýsinga- og fjarskiptatækniáhættu sem skapast hjá mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, er mikilvægt að koma á fót viðeigandi eftirlitsramma sem auðveldar stöðuga vöktun á starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og eru mikilvægir fyrir aðila á fjármálamarkaði, um leið og tryggt er að trúnaðar og öryggis annarra viðskiptavina en aðila á fjármálamarkaði sé gætt. Þótt veiting upplýsinga- og fjarskiptatækniþjónustu innan samstæðu feli í sér tiltekna áhættu og ávinning ætti hún ekki sjálfkrafa að teljast áhættuminni en veiting upplýsinga- og fjarskiptatækniþjónustu af hálfu veitenda utan fjármálasamstæðu og ætti því að falla undir sama regluramma. Þegar upplýsinga- og fjarskiptatækniþjónusta er veitt innan sömu fjármálasamstæðu gætu aðilar á fjármálamarkaði þó haft betra eftirlit með veitendum innan samstæðu, sem taka ætti tillit til í heildaráhættumatinu.

32) Þar sem upplýsinga- og fjarskiptatækniáhætta verður sífellt flóknari og háþróaðri eru góðar ráðstafanir til að greina og hindra áhættu í upplýsinga- og fjarskiptatækni að miklu leyti háðar reglulegri miðlun greiningargagna um ógnir og veikleika milli aðila á fjármálamarkaði. Upplýsingamiðlun stuðlar að aukinni vitund um netógnir. Þetta eykur síðan getu aðila á fjármálamarkaði til að koma í veg fyrir að netógnir verði raunveruleg atvik sem tengjast upplýsinga- og fjarskiptatækni og auðveldar þeim að draga úr áhrifum af atvikum sem tengjast upplýsinga- og fjarskiptatækni á skilvirkari hátt og ná sér fyrr á strik. Þegar leiðbeiningar vantar á vettvangi Sambandsins virðast nokkrir þættir hafa hamlað slíkri upplýsingamiðlun, einkum óvissa um samhæfi þeirra við persónuvernd, auðhringavarnir og reglur um bótaábyrgð.

33) Efasemdir um hvaða tegundum upplýsinga heimilt er að deila með öðrum markaðsaðilum eða yfirvöldum sem ekki eru eftirlitsyfirvöld (s.s. Netöryggisstofnun Evrópusambandsins vegna greiningar, eða Löggæslusamvinnustofnun Evrópusambandsins í löggæslutilgangi) leiða þar að auki til þess að gagnlegum upplýsingum er ekki deilt. Umfang og gæði upplýsingaskipta eru því enn takmörkuð og sundurleit og viðkomandi samskipti eru aðallega staðbundin (með landsbundnum framtaksverkefnum) og ekkert samræmt upplýsingaskiptafyrirkomulag innan alls Sambandsins sem miðast við þarfir samþætts fjármálakerfis. Því er mikilvægt að styrkja þessar samskiptaleiðir.

34) Hvetja ætti aðila á fjármálamarkaði til að skiptast á upplýsingum og greiningargögnum um netógnir og nýta í sameiningu þekkingu sína og hagnýta reynslu á stefnumótandi, lausnamiðuðum og rekstrarlegum grundvelli með það fyrir augum að auka getu sína til að meta, vakta, verjast og bregðast við netógnum með fullnægjandi hætti, með því að taka þátt í upplýsingaskiptafyrirkomulagi. Því er nauðsynlegt að koma á fyrirkomulagi á vettvangi Sambandsins um valfrjáls upplýsingaskipti sem, þegar þau eru gerð í áreiðanlegu umhverfi, myndu hjálpa samfélagi aðila á fjármálamarkaði að koma í veg fyrir og bregðast sameiginlega við netógnum með því að takmarka útbreiðslu upplýsinga- og fjarskiptatækniáhættu með hraði og hindra möguleg smitáhrif um fjármálakerfið. Fyrirkomulagið ætti að vera í samræmi við gildandi reglur Sambandsins á sviði samkeppnislaga sem settar eru fram í orðsendingu framkvæmdastjórnarinnar frá 14. janúar 2011 sem ber yfirskriftina „Leiðbeiningar um gildissvið 101. gr. sáttmálans um starfshætti Evrópusambandsins um lárétta samstarfssamninga“, sem og reglur Sambandsins um persónuvernd, einkum reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 ([13]). Það ætti að starfa á grundvelli einnar eða fleiri af þeim lagastoðum sem mælt er fyrir um í 6. gr. þeirrar reglugerðar, s.s. í tengslum við vinnslu persónuupplýsinga sem er nauðsynleg vegna lögmætra hagsmuna sem ábyrgðaraðili eða þriðji aðili gætir, eins og um getur í f-lið 1. mgr. 6. gr. þeirrar reglugerðar, sem og í tengslum við vinnslu persónuupplýsinga sem er nauðsynleg til að uppfylla lagaskyldu sem hvílir á ábyrgðaraðila og er nauðsynleg vegna framkvæmdar verkefnis sem unnið er í þágu almannahagsmuna eða við beitingu opinbers valds sem ábyrgðaraðili fer með, eins og um getur í c- og e-lið 1. mgr. 6. gr. þeirrar reglugerðar.

([13]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) (Stjtíð. ESB L 119, 4.5.2016, bls. 1).

35) Til að viðhalda sem mestum stafrænum rekstrarlegum viðnámsþrótti í öllum fjármálageiranum og fylgja tækniþróun um leið, ætti þessi reglugerð að taka á áhættu sem stafar af öllum tegundum upplýsinga- og fjarskiptatækniþjónustu. Í því skyni ætti að túlka skilgreiningu á upplýsinga- og fjarskiptatækniþjónustu í skilningi þessarar reglugerðar vítt, þannig að hún nái yfir stafræna þjónustu og gagnaþjónustu sem veitt er einum eða fleiri innri eða ytri notendum með upplýsinga- og fjarskiptatæknikerfum á viðvarandi grunni. Sú skilgreining ætti t.d. að ná yfir svokallaða „stafræna þjónustu um internetið (OTT, e. *over the top services*)“, sem fellur innan flokksins rafræn fjarskiptaþjónusta. Einungis ætti að undanskilja hinn takmarkaða flokk hefðbundinnar hliðrænnar símaþjónustu sem fellur undir almennt símakerfi, landlínuþjónustu, hefðbundna símaþjónustu eða fastlínusímaþjónustu.

36) Þrátt fyrir að þessari reglugerð sé ætlað að ná yfir breitt svið ætti beiting reglnanna um stafrænan rekstrarlegan viðnámsþrótt að taka tillit til þess mikla mismunar sem er á aðilum á fjármálamarkaði með tilliti til stærðar þeirra og heildaráhættusniðs. Við dreifingu tilfanga og getu til að innleiða áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni ættu aðilar á fjármálamarkaði almennt að gæta tilhlýðilegs jafnvægis á milli eigin þarfa í tengslum við upplýsinga- og fjarskiptatækni og stærðar sinnar og heildaráhættusniðs, og eðlis, umfangs og flækjustigs þjónustu sinnar, starfsemi og reksturs, á meðan lögbær yfirvöld ættu að halda áfram að meta og endurskoða nálgun við slíka dreifingu.

37) Reikningsupplýsingaþjónustuveitendur, sem um getur í 1. mgr. 33. gr. tilskipunar (ESB) 2015/2366, falla beinlínis undir gildissvið þessarar reglugerðar, að teknu tilliti til sérstaks eðlis starfsemi þeirra og áhættu sem af henni leiðir. Að auki falla rafeyrisfyrirtæki og greiðslustofnanir, sem eru undanþegnar skv. 1. mgr. 9. gr. tilskipunar Evrópuþingsins og ráðsins 2009/110/EB ([14]) og 1. mgr. 32. gr. tilskipunar (ESB) 2015/2366, undir gildissvið þessarar reglugerðar jafnvel þótt þau hafi ekki fengið starfsleyfi í samræmi við tilskipun 2009/110/EB til að gefa út rafeyri, eða hafi ekki fengið starfsleyfi í samræmi við tilskipun (ESB) 2015/2366 til að veita og framkvæma greiðsluþjónustu. Póstgíróstofnanir, sem um getur í 3. lið 5. mgr. 2. gr. tilskipunar Evrópuþingsins og ráðsins 2013/36/ESB ([15]), eru þó undanskildar gildissviði þessarar reglugerðar. Lögbært yfirvald greiðslustofnana sem njóta undanþágu samkvæmt tilskipun (ESB) 2015/2366, rafeyrisfyrirtækja sem njóta undanþágu samkvæmt tilskipun 2009/110/EB og reikningsupplýsingaþjónustuveitenda eins og um getur í 1. mgr. 33. gr. tilskipunar (ESB) 2015/2366 ætti að vera það lögbæra yfirvald sem tilgreint er í samræmi við 22. gr. tilskipunar (ESB) 2015/2366.

38) Þar eð stærri aðilar á fjármálamarkaði kunna að hafa aðgang að meira fjármagni og geta úthlutað fjármunum á skjótan hátt til þróunar eftirlits- og stjórnunarkerfis og uppsetningar á ýmsum aðgerðaáætlunum, ætti aðeins að krefjast þess að aðilar á fjármálamarkaði, sem ekki eru örfyrirtæki í skilningi þessarar reglugerðar, komi á fót flóknari stjórnunarháttum. Slíkir aðilar eru einkum betur í stakk búnir til að koma á fót sérhæfðum starfseiningum til eftirlitsráðstafana með þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu eða til að takast á við krísustjórnun, skipuleggja stýringu upplýsinga- og fjarskiptatækniáhættu samkvæmt líkaninu um þrjár varnarlínur, eða setja upp innri áhættustýringar- og eftirlitslíkan og leggja áhættustýringarramma sinn fyrir innri endurskoðun.

39) Sumir aðilar á fjármálamarkaði njóta undanþága eða falla undir afar lítinn regluramma samkvæmt viðeigandi sérlögum Sambandsins. Til slíkra aðila teljast rekstraraðilar sérhæfðra sjóða sem um getur í 2. mgr. 3. gr. tilskipunar Evrópuþingsins og ráðsins 2011/61/ESB ([16]), vátrygginga- og endurtryggingafélög sem um getur í 4. gr. tilskipunar Evrópuþingsins og ráðsins 2009/138/EB ([17]) og stofnanir um starfstengdan lífeyri sem starfrækja lífeyriskerfi þar sem sjóðfélagar eru ekki fleiri en 15 talsins í heildina litið. Með tilliti til þessara undanþága væri ekki hóflegt að slíkir aðilar

([14]) Tilskipun Evrópuþingsins og ráðsins 2009/110/EB frá 16. september 2009 um stofnun og rekstur rafeyrisfyrirtækja og varfærniseftirlit með þeim, breytingu á tilskipunum 2005/60/EB og 2006/48/EB og um niðurfellingu á tilskipun 2000/46/EB (Stjtíð. ESB L 267, 10.10.2009, bls. 7).

([15]) Tilskipun Evrópuþingsins og ráðsins 2013/36/ESB frá 26. júní 2013 um aðgang að starfsemi lánastofnana og varfærniseftirlit með lánastofnunum, um breytingu á tilskipun 2002/87/EB og um niðurfellingu á tilskipunum 2006/48/EB og 2006/49/EB (Stjtíð. ESB L 176, 27.6.2013, bls. 338).

([16]) Tilskipun Evrópuþingsins og ráðsins 2011/61/ESB frá 8. júní 2011 um rekstraraðila sérhæfðra sjóða og um breytingu á tilskipunum 2003/41/EB og 2009/65/EB og reglugerðum (EB) nr. 1060/2009 og (ESB) nr. 1095/2010 (Stjtíð. ESB L 174, 1.7.2011, bls. 1).

([17]) Tilskipun Evrópuþingsins og ráðsins 2009/138/EB frá 25. nóvember 2009 um stofnun og rekstur fyrirtækja á sviði vátrygginga og endurtrygginga (Gjaldþolsáætlun II) (Stjtíð. ESB L 335, 17.12.2009, bls. 1).

á fjármálamarkaði féllu innan gildissviðs þessarar reglugerðar. Í þessari reglugerð er að auki viðurkenndir sérstakir eiginleikar tryggingamiðlunarmarkaðarins sem leiðir til þess að vátryggingamiðlarar, endurtryggingamiðlarar og vátryggingamiðlarar í hliðarstarfsemi, sem teljast örfyrirtæki eða lítil eða meðalstór fyrirtæki, ættu ekki að falla undir þessa reglugerð.

40) Þar eð einingarnar sem um getur í 4.–23. lið 5. mgr. 2. gr. tilskipunar 2013/36/ESB eru undanskildar gildissviði þeirrar tilskipunar ættu aðildarríki af þeim sökum að geta valið að undanskilja slíkar einingar sem staðsettar eru innan yfirráðasvæðis þeirra frá beitingu þessarar reglugerðar.

41) Til að aðlaga þessa reglugerð að gildissviði tilskipunar Evrópuþingsins og ráðsins 2014/65/ESB ([18]) er einnig rétt að undanskilja frá gildissviði þessarar reglugerðar einstaklinga og lögaðila sem um getur í 2. og 3. gr. þeirrar tilskipunar sem heimilt er að veita fjárfestingarþjónustu án þess að þurfa starfsleyfi samkvæmt tilskipun 2014/65/ESB. Ákvæði 2. gr. tilskipunar 2014/65/ESB útiloka þó einnig frá gildissviði þeirrar tilskipunar aðila sem teljast vera aðilar á fjármálamarkaði að því er þessa reglugerð varðar, s.s. verðbréfamiðstöðvar, sjóði um sameiginlega fjárfestingu eða vátrygginga- og endurtryggingafélög. Undanþága aðila og eininga sem um getur í 2. og 3. gr. þeirrar tilskipunar frá gildissviði þessarar reglugerðar ætti ekki að ná yfir þessar verðbréfamiðstöðvar, sjóði um sameiginlega fjárfestingu eða vátrygginga- og endurtryggingafélög.

42) Samkvæmt sérlögum Sambandsins falla sumir aðilar á fjármálamarkaði undir vægari kröfur eða undanþágur af ástæðum sem varða stærð þeirra eða þá þjónustu sem þeir veita. Þessi flokkur aðila á fjármálamarkaði nær yfir lítil og ótengd verðbréfafyrirtæki, litlar stofnanir um starfstengdan lífeyri sem hlutaðeigandi aðildarríki getur undanskilið frá gildissviði tilskipunar (ESB) 2016/2341 að uppfylltum þeim skilyrðum sem mælt er fyrir um í 5. gr. þeirrar tilskipunar og starfrækja lífeyriskerfi þar sem sjóðfélagar eru ekki fleiri en 100 í heild, sem og stofnanir sem eru undanþegnar samkvæmt tilskipun 2013/36/ESB. Í samræmi við meðalhófsregluna og til að viðhalda anda sérlaga Sambandsins þykir því einnig rétt að þessir aðilar á fjármálamarkaði falli undir einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni samkvæmt þessari reglugerð. Tæknilegir eftirlitsstaðlar sem evrópsku eftirlitsstofnanirnar skulu þróa ættu ekki að breyta því meðalhófi sem einkennir áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem tekur til þessara aðila á fjármálamarkaði. Í samræmi við meðalhófsregluna þykir enn fremur rétt að greiðslustofnanir, sem um getur í 1. mgr. 32. gr. tilskipunar (ESB) 2015/2366, og rafeyrisstofnanir, sem um getur í 9. gr. tilskipunar 2009/110/EB, sem eru undanþegnar í samræmi við landslög sem lögleiða þessar réttargerðir Sambandsins, falli einnig undir einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni samkvæmt þessari reglugerð en greiðslustofnanir og rafeyrisfyrirtæki, sem hafa ekki verið undanskilin í samræmi við landslög sem lögleiða sérlög Sambandsins, ættu að fara að almenna rammanum sem mælt er fyrir um í þessari reglugerð.

43) Að sama skapi ætti ekki að gera kröfu um að aðilar á fjármálamarkaði sem teljast vera örfyrirtæki eða falla undir einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni samkvæmt þessari reglugerð komi á fót hlutverki til að vakta ráðstafanir sem gerðar eru við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu um notkun á upplýsinga- og fjarskiptatækniþjónustu; eða tilnefni aðila að framkvæmdastjórn til að bera ábyrgð á umsjón með tengdri áhættu og viðeigandi gögnum; feli eftirlitseiningu ábyrgð á stýringu og umsjón með upplýsinga- og fjarskiptatækniáhættu og tryggi viðeigandi sjálfstæði slíkra eftirlitseininga til að forðast hagsmunaárekstra; skjalfesti og geri úttekt á áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni a.m.k. einu sinni á ári; láti áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni reglulega gangast undir innri úttekt; framkvæmi ítarlegt mat eftir meiri háttar breytingar á grunnvirkjum og ferlum net- og upplýsingakerfa sinna; geri reglulegar áhættugreiningar á fornkerfum í upplýsinga- og fjarskiptatækni; láti framkvæmd viðbragðs- og endurreisnaráætlana á sviði upplýsinga- og fjarskiptatækni lúta sjálfstæðum innri úttektum; hafi krísustjórnunarteymi til að auka prófanir á áætlunum um rekstrarsamfellu og viðbragðs- og endurreisnaráætlunum til greiningar á sviðsmyndum við flutning milli aðalkerfis upplýsinga- og fjarskiptatækni og varakerfis; tilkynni lögbærum yfirvöldum, ef þau óska eftir því, um áætlaðan samantekinn árlegan kostnað og tap af alvarlegum atvikum sem tengjast upplýsinga- og fjarskiptatækni til að viðhalda

([18]) Tilskipun Evrópuþingsins og ráðsins 2014/65/ESB frá 15. maí 2014 um markaði fyrir fjármálagerninga og um breytingu á tilskipun 2002/92/EB og tilskipun 2011/61/ESB (Stjtíð. ESB L 173, 12.6.2014, bls. 349).

varakerfum í upplýsinga- og fjarskiptatækni; tilkynni lögbærum landsyfirvöldum um breytingar sem gerðar eru í kjölfar athugana á atvikum sem tengjast upplýsinga- og fjarskiptatækni; vakti stöðugt viðeigandi tækniþróun til að koma á fót alhliða prófunaráætlun um stafrænan rekstrarlegan viðnámsþrótt sem óaðskiljanlegum hluta áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem kveðið er á um í þessari reglugerð eða taki upp og endurskoði reglulega stefnuáætlun um upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila. Auk þess ætti örfyrirtækjum aðeins að vera skylt að meta þörfina á að viðhalda varaupplýsinga- og fjarskiptatæknikerfum á grundvelli áhættusniðs. Örfyrirtæki ættu að njóta góðs af sveigjanlegra fyrirkomulagi að því er varðar prófunaráætlanir um stafrænan rekstrarlegan viðnámsþrótt. Við mat á tegund og tíðni prófana sem á að framkvæma ættu þau að gæta þess vandlega að ná jafnvægi milli markmiðsins um að viðhalda sem mestum stafrænum rekstrarlegum viðnámsþrótti, tiltækra tilfanga og heildaráhættusniðs. Örfyrirtæki og aðilar á fjármálamarkaði sem falla undir einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni samkvæmt þessari reglugerð ættu að vera undanþegin kröfunni um að framkvæma auknar prófanir á upplýsinga- og fjarskiptatæknibúnaði, -kerfum og -ferlum sem grundvallast á ógnamiðuðum innbrotsprófunum (TLPT) þar sem aðeins aðilum á fjármálamarkaði sem uppfylla viðmiðanirnar sem settar eru fram í þessari reglugerð ætti að vera skylt að gera slíkar prófanir. Í ljósi takmarkaðrar getu örfyrirtækja ætti þeim að vera mögulegt að semja við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu um að framselja rétt aðilans til aðgangs, eftirlits og úttektar til óháðs þriðja aðila sem tilnefndur skal af viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, að því tilskildu að aðilinn á fjármálamarkaði geti hvenær sem er óskað eftir öllum viðeigandi upplýsingum og fullvissu um frammistöðu þjónustuveitanda upplýsinga- og fjarskiptatækni frá viðkomandi óháðum þriðja aðila.

44) Þar sem einungis ætti að skylda þá aðila á fjármálamarkaði sem tilgreindir eru að því er varðar auknar stafrænar prófanir á viðnámsþrótti til að gera ógnamiðaðar innbrotsprófanir ættu stjórnsýsluferlar og fjárhagslegur kostnaður sem leiðir af framkvæmd slíkra prófana að falla á lítinn hluta aðila á fjármálamarkaði.

45) Til að tryggja fullt samræmi og heildarsamkvæmni milli viðskiptaáætlana aðila á fjármálamarkaði annars vegar og framkvæmd stýringar upplýsinga- og fjarskiptatækniáhættu hins vegar ætti að skylda stjórn og/eða framkvæmdastjórn viðkomandi aðila til að gegna virku lykilhlutverki við stýringu og aðlögun áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni og heildarstefnuáætlunar um stafrænan rekstrarlegan viðnámsþrótt. Sú nálgun sem stjórn og/eða framkvæmdastjórn þurfa að beita ætti ekki aðeins að beinast að leiðum til að tryggja viðnámsþrótt upplýsinga- og fjarskiptatæknikerfa, heldur ætti hún einnig að ná yfir fólk og ferla með stefnum sem leggja rækt við, í hverju fyrirtæki fyrir sig og hjá öllu starfsfólki, sterka vitund um netöryggi og skuldbindingu um að fylgja ströngu netheilbrigði á öllum stigum. Endanleg ábyrgð stjórnar og/eða framkvæmdastjórnar aðila á fjármálamarkaði á stýringu upplýsinga- og fjarskiptatækniáhættu ætti að vera grundvallarmeginregla þeirrar heildstæðu nálgunar og endurspeglast í áframhaldandi þátttöku stjórnar og/eða framkvæmdastjórnar í eftirliti með stýringu upplýsinga- og fjarskiptatækniáhættu.

46) Þar að auki helst meginreglan um fulla og endanlega ábyrgð stjórnar og/eða framkvæmdastjórnar á stýringu upplýsinga- og fjarskiptatækniáhættu aðilans á fjármálamarkaði í hendur við þörfina á að tryggja fjárhæð fjárfestinga sem tengjast upplýsinga- og fjarskiptatækni og heildarfjárhagsáætlun fyrir viðkomandi aðila sem myndi gera honum kleift að ná auknum stafrænum rekstrarlegum viðnámsþrótti.

47) Þessi reglugerð, sem sækir innblástur í viðeigandi alþjóðlegar, innlendar og geirasértækar bestu starfsvenjur, viðmiðunarreglur, tilmæli og aðferðir við stýringu netáhættu, stuðlar að meginreglum sem greiða fyrir heildarskipulagi í stýringu upplýsinga- og fjarskiptatækniáhættu. Af þessum sökum ætti aðilum á fjármálamarkaði að vera frjálst að nota áhættustýringarlíkön fyrir upplýsinga- og fjarskiptatækni sem eru sett fram með ólíkum hætti, svo lengi sem helsta geta sem aðilar á fjármálamarkaði búa yfir tekur til hinna ýmsu starfseininga í stýringu upplýsinga- og fjarskiptatækniáhættu (auðkenningar, verndunar og forvarna, greiningar, viðbragða og endurreisnar, náms og þróunar og samskipta) sem sett eru fram í þessari reglugerð.

48) Til að halda í við breytingar á landslagi netógna ættu aðilar á fjármálamarkaði að viðhalda uppfærðum upplýsinga- og fjarskiptakerfum sem eru áreiðanleg og hentug, ekki eingöngu til að tryggja vinnslu á nauðsynlegum gögnum fyrir þjónustu þeirra heldur einnig til að tryggja fullnægjandi tæknilegan viðnámsþrótt svo þau geti uppfyllt nægilega vel þarfir á viðbótarvinnslu vegna erfiðra markaðsaðstæðna eða annarra óhagstæðra aðstæðna.

49) Skilvirkar áætlanir um rekstrarsamfellu og endurreisn eru nauðsynlegar til að gera aðilum á fjármálamarkaði kleift að bregðast skjótt og vel við atvikum sem tengjast upplýsinga- og fjarskiptatækni, einkum netárásum, með því að takmarka tjón og setja í forgang að hefja aftur starfsemi og endurreisnaraðgerðir í samræmi við stefnu um öryggisafritun. Slík endurupptaka starfsemi ætti þó ekki að stefna heilleika og öryggi net- og upplýsingakerfa eða tiltækileika, ósvikni, réttleika eða leynd gagna í hættu á neinn hátt.

50) Þótt þessi reglugerð heimili aðilum á fjármálamarkaði að ákvarða markmið um endurreisnartíma sinn og endamark endurheimtar á sveigjanlegan hátt og setja slík markmið að teknu fullu tilliti til eðlis og mikilvægis viðkomandi starfsemi og sértækra viðskiptaþarfa ætti hún samt sem áður að krefjast þess að þeir framkvæmi mat á mögulegum heildaráhrifum á skilvirkni markaðar við ákvörðun slíkra markmiða.

51) Þeir sem standa að netárásum sækjast gjarnan eftir fjárhagslegum ávinningi beint frá uppsprettunni sem gerir aðila á fjármálamarkaði útsetta fyrir verulegum afleiðingum. Til að hindra að upplýsinga- og fjarskiptatæknikerfi tapi heilleika eða verði óaðgengileg og forðast þannig öryggisbresti við meðferð upplýsinga og skemmdir á efnislegum grunnvirkjum upplýsinga- og fjarskiptatækni ætti að bæta verulega og einfalda skýrslugjöf aðila á fjármálamarkaði um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Samræma ætti skýrslugjöf vegna atvika sem tengjast upplýsinga- og fjarskiptatækni með því að gera þá kröfu að allir aðilar á fjármálamarkaði gefi skýrslur beint til viðkomandi lögbærra yfirvalda. Ef aðili á fjármálamarkaði lýtur eftirliti fleiri en eins lögbærs landsyfirvalds ættu aðildarríkin að tilnefna eitt lögbært yfirvald sem viðtakanda slíkrar skýrslugjafar. Lánastofnanir sem flokkast sem mikilvægar í samræmi við 4. mgr. 6. gr. reglugerðar ráðsins (ESB) nr. 1024/2013 ([19]) ættu að leggja slíka skýrslugjöf fyrir lögbær landsyfirvöld sem ættu í kjölfarið að senda skýrsluna til Seðlabanka Evrópu.

52) Bein skýrslugjöf ætti að gera fjármálaeftirlitsaðilum kleift að fá tafarlaust aðgang að upplýsingum um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Fjármálaeftirlitsaðilar ættu síðan að miðla upplýsingum um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni til opinberra yfirvalda sem ekki tengjast fjármálageiranum (s.s. lögbærra yfirvalda og sameiginlegra tengiliða samkvæmt tilskipun (ESB) 2022/2555, landsbundinna persónuverndaryfirvalda og löggæsluyfirvalda vegna alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni sem varða hegningarlög) til að auka vitund slíkra yfirvalda um slík atvik og greiða fyrir tafarlausri aðstoð sem aðilum á fjármálamarkaði kann að vera veitt, eins og við á, ef um er að ræða viðbragðsteymi vegna váatvika er varða tölvuöryggi. Aðildarríki ættu auk þess að geta ákvarðað að aðilar á fjármálamarkaði eigi sjálfir að veita opinberum yfirvöldum utan fjármálaþjónustusviðs slíkar upplýsingar. Þetta upplýsingaflæði ætti að gera aðilum á fjármálamarkaði kleift að njóta skjóts ávinnings af hvers kyns viðeigandi tæknilegum upplýsingum, ráðgjöf um úrræði og eftirfylgni frá slíkum yfirvöldum í kjölfarið. Deila ætti upplýsingum um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni með gagnkvæmum hætti: fjármálaeftirlitsaðilar ættu að veita umræddum aðila á fjármálamarkaði alla nauðsynlega endurgjöf eða leiðsögn en evrópsku eftirlitsstofnanirnar ættu að deila nafnlausum gögnum um netógnir og veikleika í tengslum við atvik, til að stuðla að víðtækari sameiginlegum vörnum.

53) Þótt gera ætti kröfu um að allir aðilar á fjármálamarkaði geri skýrslu vegna atvika er ekki búist við að sú krafa hafi sömu áhrif á þá alla. Aðlaga ætti viðeigandi mikilvægismörk, sem og tímamörk fyrir skýrslugjöf, á tilhlýðilegan hátt í tengslum við framseldar gerðir sem byggjast á tæknilegu eftirlitsstöðlunum sem evrópsku eftirlitsstofnanirnar skulu þróa, með það í huga að ná aðeins yfir alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Auk þess ætti að taka tillit til sérstakra eiginleika aðilans á fjármálamarkaði við setningu tímamarka fyrir kröfur um gagnaskil.

54) Í þessari reglugerð ætti að skylda lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki til að tilkynna um öll greiðslutengd rekstrar- eða öryggisatvik sem áður hefur verið tilkynnt um samkvæmt tilskipun (ESB) 2015/2366, án tillits til eðlis upplýsinga- og fjarskiptatækniatviksins.

([19]) Reglugerð ráðsins (ESB) nr. 1024/2013 frá 15. október 2013 um að fela Seðlabanka Evrópu sérstök verkefni að því er varðar stefnur sem snerta varfærniseftirlit með lánastofnunum (Stjtíð. ESB L 287, 29.10.2013, bls. 63).

55) Evrópsku eftirlitsstofnanirnar ættu að fá það hlutverk að meta hagkvæmni og skilyrði fyrir hugsanlegri miðstýringu atvikaskýrslna sem tengjast upplýsinga- og fjarskiptatækni á vettvangi Sambandsins. Slík miðstýring gæti falist í sameiginlegri ESB-miðstöð vegna tilkynninga um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem annaðhvort tekur beint á móti viðeigandi tilkynningum og tilkynnir lögbærum landsyfirvöldum sjálfvirkt eða gerir einungis viðeigandi tilkynningar, sem lögbær landsyfirvöld hafa sent, miðlægar og gegnir þannig samræmingarhlutverki. Fela ætti evrópsku eftirlitsstofnununum, í samráði við Seðlabanka Evrópu og Netöryggisstofnun Evrópusambandsins, að undirbúa sameiginlega skýrslu þar sem könnuð er hagkvæmni þess að koma á fót sameiginlegri ESB-miðstöð.

56) Til að skapa sem mestan stafrænan rekstrarlegan viðnámsþrótt og í samræmi við bæði viðeigandi alþjóðlega staðla (t.d. grundvallarþætti G7 fyrir ógnamiðaðar innbrotsprófanir) og þess ramma sem er beitt í Sambandinu, s.s. TIBER-EU, ættu aðilar á fjármálamarkaði að prófa upplýsinga- og fjarskiptatæknikerfi sín reglulega og starfsfólk sem starfar í tengslum við upplýsinga- og fjarskiptatækni með tilliti til skilvirkni forvarnargetu, getu til að greina hana, bregðast við og endurreisa, afhjúpa og takast á við hugsanlega veikleika í upplýsinga- og fjarskiptatækni. Til að endurspegla þann mismun sem er þvert á og innan mismunandi fjármálaundirgeira að því er varðar viðbúnaðarstig aðila á fjármálamarkaði á sviði netöryggis ættu prófanir að fela í sér margs konar búnað og aðgerðir, allt frá mati á grunnkröfum (t.d. mat og skönnun á veikleikum, greiningu með opnum hugbúnaði, netöryggismati, greiningu á eyðum, úttektum á raunlægu öryggi, spurningalistum og skönnunarhugbúnaðarlausnum, úttektum á frumkóða ef mögulegt er, sviðsmyndatengdum prófunum, samhæfisprófunum, prófunum á frammistöðu eða prófunum enda á milli) til aukinna prófana með ógnamiðaðri innbrotsprófun. Einungis ætti að krefjast slíkra aukinna prófana af aðilum á fjármálamarkaði sem eru nægilega þroskaðar með tilliti til upplýsinga- og fjarskiptatækni til að geta gert þær með góðu móti. Þannig ætti prófun á stafrænum rekstrarlegum viðnámsþrótti sem krafist er með þessari reglugerð að vera strangari fyrir þá aðila á fjármálamarkaði sem uppfylla viðmiðanirnar sem settar eru fram í þessari reglugerð (t.d. stórar, kerfislegar og upplýsinga- og fjarskiptatæknilega þroskaðar lánastofnanir, kauphallir, verðbréfamiðstöðvar og miðlægir mótaðilar) en fyrir aðra aðila á fjármálamarkaði. Á sama tíma ættu prófanir á stafrænum rekstrarlegum viðnámsþrótti með ógnamiðaðri innbrotsprófun að hafa meira vægi fyrir aðila á fjármálamarkaði sem starfa innan undirgeira kjarnafjármálaþjónustu og gegna kerfislægu hlutverki (t.d. við greiðslur, bankaþjónustu, greiðslujöfnun og uppgjör) og skipta minna máli fyrir aðra undirgeira (t.d. eignastýringaraðila og lánshæfismatsfyrirtæki).

57) Aðilar á fjármálamarkaði sem taka þátt í starfsemi sem nær yfir landamæri og nýta sér staðfesturétt eða þjónustustarfsemi innan Sambandsins ættu að hlíta einum kröfum um auknar prófanir (þ.e. ógnamiðaða innbrotsprófun) í heimaaðildarríki sínu, sem ættu að taka til grunnvirkja upplýsinga- og fjarskiptatækni í öllum lögsögum þar sem fjármálasamstæðan sem starfar yfir landamæri hefur starfsemi innan Sambandsins, og gera slíkum fjármálasamstæðum sem starfa yfir landamæri þannig kleift að stofna til tengds kostnaðar fyrir upplýsinga- og fjarskiptatækniprófanir í aðeins einni lögsögu.

58) Til að nýta sér þá sérþekkingu sem tiltekin lögbær yfirvöld hafa þegar aflað sér, einkum að því er varðar framkvæmd á TIBER-EU-rammanum, ætti þessi reglugerð að gera aðildarríkjum kleift að tilnefna eitt opinbert yfirvald sem ábyrgðaraðila í fjármálageiranum, á landsvísu, í öllum málum sem tengjast ógnamiðaðri innbrotsprófun eða lögbær yfirvöld, til að úthluta öðru lögbæru landsyfirvaldi á sviði fjármálaþjónustu verkefnum sem tengjast ógnamiðaðri innbrotsprófun, þegar slík tilnefning er ekki fyrir hendi.

59) Þar sem þess er ekki krafist í þessari reglugerð að aðilar á fjármálamarkaði taki til allra nauðsynlegra eða mikilvægra þátta í stakri ógnamiðaðri innbrotsprófun ætti aðilum á fjármálamarkaði að vera frjálst að ákveða hvaða og hversu margir nauðsynlegir eða mikilvægir þættir ættu að falla undir gildissvið slíkrar prófunar.

60) Aðeins ætti að leyfa samsettar prófanir í skilningi þessarar reglugerðar, sem fela í sér þátttöku nokkurra aðila á fjármálamarkaði í ógnamiðaði innbrotsprófun og sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu getur gert samning um beint við utanaðkomandi prófanda, ef búast má við að gæði eða öryggi þjónustunnar sem viðkomandi þriðji aðili veitir viðskiptamönnum, sem eru einingar utan gildissviðs þessarar reglugerðar, eða trúnaður um gögn sem tengjast slíkri þjónustu, verði fyrir neikvæðum áhrifum. Samsettar prófanir ættu einnig að falla undir verndarráðstafanir (af hálfu eins tilnefnds aðila á fjármálamarkaði, kvörðun á fjölda aðila sem taka þátt) til að tryggja strangar prófanir fyrir hlutaðeigandi aðila á fjármálamarkaði sem uppfylla markmið ógnamiðaðra innbrotsprófana samkvæmt þessari reglugerð.

61) Til að nýta innri tilföng sem eru tiltæk hjá fyrirtækjum ætti þessi reglugerð að heimila notkun á innri prófunaraðilum til að gera ógnamiðaðar innbrotsprófanir, að því tilskildu að fyrir liggi samþykki eftirlitsyfirvalda, að ekki verði hagsmunaárekstrar, að reglubundið sé skipt um innri og ytri prófendur (fyrir þriðju hverja prófun) og að jafnframt sé gerð krafa um að veitandi ógnargreiningargagna í ógnamiðuðu innbrotsprófuninni sé ávallt utanaðkomandi aðilanum á fjármálamarkaði. Viðkomandi aðili á fjármálamarkaði ætti að bera fulla ábyrgð á framkvæmd ógnamiðaðrar innbrotsprófunar. Staðfestingar yfirvalda ættu einungis að vera vegna gagnkvæmrar viðurkenningar og ættu ekki að útiloka framhaldsaðgerðir sem nauðsynlegar eru til að takast á við þá upplýsinga- og fjarskiptatækniáhættu sem aðilinn á fjármálamarkaði stendur frammi fyrir, né heldur ætti að líta á þær sem samþykki eftirlitsyfirvalds fyrir stýringu upplýsinga- og fjarskiptatækniáhættu aðila á fjármálamarkaði og getu til að draga úr áhættu.

62) Til að tryggja trausta vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila í fjármálageiranum er nauðsynlegt að mæla fyrir um meginreglur sem leiðbeina aðilum á fjármálamarkaði við vöktun áhættu sem myndast í tengslum við starfsemi sem er útvistað til þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, einkum vegna þjónustu í upplýsinga- og fjarskiptatækni sem styður við nauðsynlega eða mikilvæga starfsemi, sem og almennt með tilliti til hæðis við þriðju aðila í upplýsinga- og fjarskiptatækni.

63) Til að leysa flækjustig margs konar upplýsinga- og fjarskiptatækniáhættu, að teknu tilliti til fjölda og fjölbreytni veitenda tæknilausna sem gera kleift að veita snurðulausa fjármálaþjónustu, ætti þessi reglugerð að ná til margvíslegra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. veitenda skýjavinnsluþjónustu, hugbúnaðar, gagnagreiningarþjónustu og veitenda gagnaversþjónustu. Þar sem aðilar á fjármálamarkaði ættu að greina og stýra öllum tegundum áhættu á skilvirkan og samfelldan hátt, þ.m.t. með tilliti til þjónustu í upplýsinga- og fjarskiptatækni sem fjármálasamstæða kaupir, ætti einnig að skýra að fyrirtæki sem eru hluti fjármálasamstæðu og veita upplýsinga- og fjarskiptatækniþjónustu fyrst og fremst til móðurfyrirtækja sinna eða dótturfélaga eða útibúa móðurfyrirtækja, og aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu til annarra aðila á fjármálamarkaði ættu einnig að teljast til þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu samkvæmt þessari reglugerð. Að lokum, í ljósi þess að greiðsluþjónustumarkaðurinn er að verða sífellt háðari flóknum tæknilausnum og að teknu tilliti til nýrra tegunda greiðsluþjónustu og greiðslutengdra lausna, ætti einnig að líta á þátttakendur í vistkerfi greiðsluþjónustu, sem veita greiðsluþjónustustarfsemi eða starfrækja greiðsluinnviði, sem þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu samkvæmt þessari reglugerð, að undanskildum seðlabönkum sem reka greiðslu- eða verðbréfauppgjörskerfi og opinberum yfirvöldum sem veita þjónustu sem tengist upplýsinga- og fjarskiptatækni í tengslum við að uppfylla hlutverk ríkisins.

64) Aðili á fjármálamarkaði ætti ætíð að bera fulla ábyrgð á því að uppfylla skyldur sínar sem settar eru fram í þessari reglugerð. Aðilar á fjármálamarkaði ættu að beita hlutfallslegri nálgun við vöktun áhættu sem stafar af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, með því að taka tilhlýðilegt tillit til eðlis, umfangs, flækjustigs og mikilvægis hæðis þeirra í tengslum við upplýsinga- og fjarskiptatækni, mikilvægis þjónustu, ferla eða starfsemi sem fellur undir samningsbundið fyrirkomulag og að lokum á grundvelli ítarlegs mats á hvers kyns mögulegum áhrifum á samfellu og gæði fjármálaþjónustu á einstaklings- og samstæðustigi, eftir því sem við á.

65) Framkvæmd slíks eftirlits ætti að fylgja skipulegri nálgun gagnvart upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem er formfest með samþykkt stjórnar og/eða framkvæmdastjórnar aðilans á fjármálamarkaði á sérstakri stefnuáætlun um upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem á rætur að rekja til sífelldrar skimunar á öllu hæði við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Til að auka eftirlitsvitund um hæði við þriðju aðila í upplýsinga- og fjarskiptatækni og með það fyrir augum að styðja enn frekar við starfið í tengslum við eftirlitsrammann sem komið er á fót með þessari reglugerð, ætti að skylda alla aðila á fjármálamarkaði til að halda skrá yfir upplýsingar um allt samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem þriðju aðilar veita. Fjármálaeftirlitsaðilar ættu að geta óskað eftir tæmandi skrá eða beðið um tiltekna hluta hennar og þannig aflað nauðsynlegra upplýsinga til að öðlast víðtækari skilning á hæði aðila á fjármálamarkaði við upplýsinga- og fjarskiptatækni.

66) Ítarleg greining áður en samningur er gerður ætti að renna stoðum undir og vera undanfari þess að gengið sé formlega frá samningsbundnu fyrirkomulagi, einkum með því að beina sjónum að þáttum á borð við hversu nauðsynleg eða mikilvæg sú þjónusta er sem fyrirhugaður upplýsinga- og fjarskiptatæknisamningur styður, nauðsynlegu samþykki eftirlitsyfirvalda eða öðrum skilyrðum, hugsanlegri samþjöppunaráhættu sem því kann að fylgja, sem og að beita áreiðanleikakönnunum við val og mat á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og við mat á hugsanlegum hagsmunaárekstrum. Að því er varðar samningsbundið fyrirkomulag sem tengist nauðsynlegri eða mikilvægri starfsemi ættu aðilar á fjármálamarkaði að taka tillit til notkunar þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu samkvæmt nýjustu og ströngustu stöðlum um upplýsingaöryggi. Riftun samningsbundins fyrirkomulags gæti a.m.k. leitt af ýmsum aðstæðum sem sýna annmarka hjá þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu, einkum ef um er að ræða veruleg brot á lögum eða samningsskilmálum, aðstæðum sem leiða í

ljós hugsanlegar breytingar á framkvæmd starfsþátta sem kveðið er á um í samningsbundnu fyrirkomulagi, vísbendingum um veikleika þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í heildaráhættustýringu sinni á sviði upplýsinga- og fjarskiptatækni, eða aðstæðum sem gefa til kynna vangetu viðkomandi lögbærs yfirvalds til að hafa skilvirkt eftirlit með aðila á fjármálamarkaði.

67) Til að bregðast við kerfislægum áhrifum samþjöppunaráhættu þriðja aðila á sviði upplýsinga- og fjarskiptatækni stuðlar þessi reglugerð að jafnvægi með því að nálgast slíka samþjöppunaráhættu á sveigjanlegan og stigskiptan hátt þar eð álagning hvers kyns ósveigjanlegra hámarka eða strangra takmarkana gæti hindrað viðskipti og heft samningsfrelsi. Aðilar á fjármálamarkaði ættu að gera ítarlegt mat á fyrirhuguðu samningsbundnu fyrirkomulagi til að greina líkurnar á að slík áhætta komi fram, þ.m.t. með ítarlegri greiningu á fyrirkomulagi undirverktakastarfsemi, einkum þegar það er gert við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi. Á þessu stigi og með það fyrir augum að finna viðeigandi jafnvægi milli mikilvægis þess að vernda samningsfrelsi og þess að tryggja fjármálastöðugleika, er ekki talið viðeigandi að setja reglur um ströng hámörk og takmarkanir á áhættuskuldbindingum þriðja aðila í upplýsinga- og fjarskiptatækni. Í tengslum við eftirlitsrammann ætti aðaleftirlitsaðili sem tilnefndur er samkvæmt þessari reglugerð, að því er varðar mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, að huga sérstaklega að því að skilja umfang víxltengsla, greina sérstök tilvik þar sem líklegt er að mikil samþjöppun mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu í Sambandinu valdi þrýstingi á stöðugleika og heilleika fjármálakerfis Sambandsins og halda áfram viðræðum við mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu þegar sú sértæka áhætta greinist.

68) Til að meta og vakta reglulega getu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til að veita aðila á fjármálamarkaði þjónustu á öruggan hátt, án skaðlegra áhrifa á stafrænan rekstrarlegan viðnámsþrótt aðilans, ætti að samræma nokkra lykilþætti samninga við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Slík samræming ætti að taka til lágmarksatriða sem skipta sköpum til að auðvelda fulla vöktun aðila á fjármálamarkaði á þeirri áhættu sem stafa kann af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, í ljósi þess að viðkomandi aðili á fjármálamarkaði þarf að tryggja stafrænan viðnámsþrótt sinn vegna þess að hann er verulega háður stöðugleika, virkni, tiltækileika og öryggi móttekinnar upplýsinga- og fjarskiptatækniþjónustu.

69) Þegar samið er að nýju um samningsbundið fyrirkomulag til að leita samræmingar við kröfur þessarar reglugerðar ættu aðilar á fjármálamarkaði og þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu að tryggja að samningurinn nái yfir helstu samningsákvæði sem kveðið er á um í þessari reglugerð.

70) Skilgreiningin á „nauðsynlegri eða mikilvægri starfsemi“ sem kveðið er á um í þessari reglugerð tekur til „nauðsynlegrar starfsemi“ eins og hún er skilgreind í 35. lið 1. mgr. 2. gr. tilskipunar Evrópuþingsins og ráðsins 2014/59/ESB ([20]). Til samræmis við það er starfsemi sem telst mikilvæg samkvæmt tilskipun 2014/59/ESB hluti af skilgreiningunni á nauðsynlegri starfsemi í skilningi þessarar reglugerðar.

71) Án tillits til þess hversu nauðsynleg eða mikilvæg sú starfsemi er sem upplýsinga- og fjarskiptatækniþjónusta styður ætti samningsbundið fyrirkomulag einkum að kveða á um nákvæmar lýsingar á starfsemi og þjónustu, staðsetningum þar sem slík starfsemi er veitt og unnið er með gögn, sem og upplýsingar um lýsingar á þjónustustigum. Aðrir mikilvægir þættir sem gera aðila á fjármálamarkaði kleift að vakta upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila eru: samningsákvæði sem tilgreina hvernig þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu tryggir aðgengi, tiltækileika, réttleika, öryggi og vernd persónuupplýsinga, ákvæði sem mæla fyrir um viðeigandi tryggingu fyrir því að unnt sé að fá aðgang að, endurreisa og skila gögnum ef um er að ræða ógjaldfærni, skilameðferð eða slit á starfsemi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, sem og ákvæði sem skylda þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að veita aðstoð ef um er að ræða atvik í upplýsinga- og fjarskiptatækni í tengslum við veitta þjónustu, án viðbótarkostnaðar eða á fyrirframákveðnu verði; ákvæði um skyldu þriðja aðila sem

([20]) Tilskipun Evrópuþingsins og ráðsins 2014/59/ESB frá 15. maí 2014 sem kemur á ramma um endurreisn og skilameðferð lánastofnana og verðbréfafyrirtækja og um breytingu á tilskipun ráðsins 82/891/EBE, og tilskipunum 2001/24/EB, 2002/47/EB, 2004/25/EB, 2005/56/EB, 2007/36/EB, 2011/35/ESB, 2012/30/ESB og 2013/36/ESB og reglugerðum Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 og (ESB) nr. 648/2012 (Stjtíð. ESB L 173, 12.6.2014, bls. 190).

veitir upplýsinga- og fjarskiptatækniþjónustu til að hafa fullt samstarf við lögbær yfirvöld og skilastjórnvöld aðila á fjármálamarkaði; og ákvæði um uppsagnarrétt og tengdan lágmarkstilkynningarfrest vegna slita á samningsbundnu fyrirkomulagi í samræmi við væntingar lögbærra yfirvalda og skilastjórnvalda.

72) Til viðbótar við slík samningsákvæði og með það fyrir augum að tryggja að aðilar á fjármálamarkaði hafi áfram fullt eftirlit með allri þróun á vettvangi þriðja aðila sem gæti skaðað öryggi þeirra í upplýsinga- og fjarskiptatækni ættu samningar um veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi einnig að kveða á um eftirfarandi: fulla lýsingu á heildarþjónustustigi, með nákvæmum megindlegum og eigindlegum frammistöðumarkmiðum, til að gera kleift að grípa til viðeigandi aðgerða til úrbóta án ástæðulausrar tafar þegar samþykktu þjónustustigi er ekki náð; viðkomandi uppsagnarfrest og tilkynningaskyldu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu komi til þróunar sem kann að hafa veruleg áhrif á getu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til að veita skilvirka upplýsinga- og fjarskiptatækniþjónustu; kröfu um að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu framkvæmi og prófi viðbragðsáætlanir fyrir fyrirtæki og hafi til staðar öryggisráðstafanir, -búnað og -stefnur sem gera kleift að veita örugga þjónustu og taki fullan þátt í ógnamiðuðum innbrotsprófunum sem aðili á fjármálamarkaði annast.

73) Í samningum um veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfþætti ættu einnig að vera ákvæði sem veita aðila á fjármálamarkaði eða tilnefndum þriðja aðila rétt til aðgangs, skoðunar og úttektar og rétt til að taka afrit en slíkt skiptir sköpum fyrir stöðuga vöktun aðila á fjármálamarkaði á frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, ásamt fullri samvinnu þjónustuveitandans meðan á eftirliti stendur. Að sama skapi ætti lögbært yfirvald aðila á fjármálamarkaði að hafa heimild, á grundvelli tilkynninga, til að skoða og gera úttekt á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, með fyrirvara um vernd trúnaðarupplýsinga.

74) Slíkt samningsbundið fyrirkomulag ætti einnig að kveða á um sérstakar útgönguáætlanir, einkum og sér í lagi til að gera kleift að hafa lögboðin umbreytingartímabil þar sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu ættu að halda áfram að veita viðeigandi þjónustu með það fyrir augum að draga úr hættu á röskunum fyrir aðila á fjármálamarkaði eða gera þeim síðarnefndu kleift að skipta yfir í notkun á öðrum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu á skilvirkan hátt eða breyta að öðrum kosti yfir í innri lausnir, í samræmi við flækjustig veittrar upplýsinga- og fjarskiptatækniþjónustu. Enn fremur ættu aðilar á fjármálamarkaði sem falla innan gildissviðs tilskipunar 2014/59/ESB að tryggja að viðeigandi samningar um upplýsinga- og fjarskiptatækniþjónustu séu traustir og að fullu framfylgjanlegir komi til skilameðferðar hjá þessum aðilum. Þessir aðilar á fjármálamarkaði ættu því, í samræmi við væntingar skilastjórnvalda, að tryggja að viðkomandi samningar um upplýsinga- og fjarskiptatækniþjónustu standist þó að viðkomandi aðili fari í skilameðferð. Svo framarlega sem þessar aðilar á fjármálamarkaði uppfylla áfram greiðsluskuldbindingar sínar ættu þeir m.a. að tryggja að í viðkomandi samningum um upplýsinga- og fjarskiptatækniþjónustu séu ákvæði um að endurskipulagning eða skilameðferð hafi ekki í för með sér slit, tímabundna sviptingu og breytingu.

75) Enn fremur gæti valfrjáls notkun á föstum samningsákvæðum, sem opinber yfirvöld eða stofnanir Sambandsins þróa, einkum notkun samningsákvæða sem framkvæmdastjórnin þróar fyrir skýjavinnsluþjónustu, veitt aðilum á fjármálamarkaði og þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu frekara öryggi með því að auka réttarvissu þeirra varðandi notkun skýjavinnsluþjónustu í fjármálageiranum í fullu samræmi við þær kröfur og væntingar sem settar eru fram í lögum Sambandsins um fjármálaþjónustu. Þróun fastra samningsákvæða byggist á ráðstöfunum sem þegar voru fyrirhugaðar í aðgerðaáætlun fyrir fjártækni frá 2018 þar sem tilkynnt var um áform framkvæmdastjórnarinnar að hvetja til og greiða fyrir þróun fastra samningsákvæða við útvistun aðila á fjármálamarkaði á skýjavinnsluþjónustu á grundvelli viðleitni hagsmunaaðila skýjavinnsluþjónustu þvert á atvinnugreinar sem framkvæmdastjórnin hefur greitt fyrir með þátttöku fjármálageirans.

76) Í því skyni að efla samleitni og skilvirkni í tengslum við eftirlitsaðferðir þegar tekist er á við upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila í fjármálageiranum, sem og að styrkja stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði sem reiða sig á mikilvæga þriðju aðila til að veita upplýsinga- og fjarskiptatækniþjónustu sem styður veitingu fjármálaþjónustu og stuðla þannig að því að viðhalda stöðugleika fjármálakerfis Sambandsins og heilleika innri markaðarins fyrir fjármálaþjónustu, ættu mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu að falla undir eftirlitsramma Sambandsins. Þótt uppsetning eftirlitsrammans sé réttlætt með því aukna vægi sem felst í því að grípa til aðgerða á vettvangi Sambandsins og í krafti innbyggðs hlutverks og sérkenna við

notkun upplýsinga- og fjarskiptatækniþjónustu við veitingu fjármálaþjónustu, ætti um leið að hafa í huga að þessi lausn virðist einungis henta í tengslum við þessa reglugerð sem fjallar sérstaklega um stafrænan rekstrarlegan viðnámsþrótt í fjármálageiranum. Hins vegar ætti ekki að líta á slíkan eftirlitsramma sem nýja fyrirmynd að eftirliti Sambandsins á öðrum sviðum fjármálaþjónustu og -starfsemi.

77) Eftirlitsramminn ætti aðeins gilda um mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Því ætti að koma á tilnefningarfyrirkomulagi til að taka tillit til umfangs og eðlis þess að fjármálageirinn reiðir sig á slíka þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Þetta fyrirkomulag ætti að fela í sér megindlegar og eigindlegar viðmiðanir til að ákvarða mikilvægisbreytur sem grundvöll þess að fella þá undir eftirlitsrammann. Til að tryggja nákvæmni þessa mats og án tillits til fyrirtækjaskipulags þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu ættu slíkar viðmiðanir, ef um er að ræða þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem er hluti stærri hóps, að taka tillit til alls samstæðuskipulags þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Annars vegar ættu mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu, sem eru ekki sjálfkrafa tilnefndir vegna beitingar þessara viðmiðana, að hafa kost á að velja eftirlitsrammann að eigin frumkvæði, hins vegar ættu þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem falla nú þegar undir eftirlitsráðstöfunarramma sem styðja framkvæmd verkefna seðlabankakerfis Evrópu eins og um getur í 2. mgr. 127. gr. sáttmálans um starfshætti Evrópusambandsins að vera undanþegnir.

78) Á sama hátt ættu aðilar á fjármálamarkaði sem veita öðrum slíkum aðilum upplýsinga- og fjarskiptatækniþjónustu en tilheyra jafnframt flokki þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu samkvæmt þessari reglugerð, einnig að vera undanþegnir eftirlitsrammanum þar sem þeir falla nú þegar undir eftirlitsráðstafanir sem komið er á fót með viðeigandi lögum Sambandsins um fjármálaþjónustu. Í tengslum við eftirlitsstarfsemi sína ættu lögbær yfirvöld eftir atvikum að taka tillit til þeirrar upplýsinga- og fjarskiptatækniáhættu sem steðjar að aðilum á fjármálamarkaði vegna aðila á fjármálamarkaði sem veita upplýsinga- og fjarskiptatækniþjónustu. Vegna núverandi fyrirkomulags áhættueftirlitskerfis á samstæðustigi ætti sömuleiðis að innleiða sömu undanþágu fyrir þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og veita aðallega aðilum innan samstæðu þeirra þjónustu. Þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu eingöngu í einu aðildarríki til aðila á fjármálamarkaði sem starfa einungis í því aðildarríki ættu einnig að vera undanþegnir tilnefningarfyrirkomulagi vegna takmarkaðrar starfsemi og skorts á áhrifum yfir landamæri.

79) Sú stafræna umbreyting sem orðið hefur á fjármálaþjónustu hefur leitt til fordæmalausrar notkunar á upplýsinga- og fjarskiptatækniþjónustu. Þar sem ógerlegt er orðið að veita fjármálaþjónustu án skýjavinnsluþjónustu, hugbúnaðarlausna og gagnatengdrar þjónustu er fjármálaumhverfi Sambandsins orðið órjúfanlega háð tiltekinni upplýsinga- og fjarskiptatækniþjónustu sem veitendur upplýsinga- og fjarskiptatækniþjónustu veita. Sumir þessara veitenda, frumkvöðlar í þróun og beitingu á tækni sem byggist á upplýsinga- og fjarskiptatækni, gegna mikilvægu hlutverki við veitingu fjármálaþjónustu eða eru orðnir hluti af virðiskeðju fjármálaþjónustu. Þeir hafa því orðið nauðsynlegir fyrir stöðugleika og heilleika fjármálakerfis Sambandsins. Þessi víðtæka notkun þjónustu sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veita, ásamt vixltengslum upplýsingakerfa ýmissa rekstraraðila markaða, skapar beina og mögulega alvarlega áhættu fyrir fjármálaþjónustukerfi Sambandsins og fyrir samfellu í veitingu fjármálaþjónustu ef raskanir á rekstri eða alvarleg netatvik myndu hafa áhrif á mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Netatvik eru einstök að því leyti að þau geta margfaldast og breiðst um allt fjármálakerfið umtalsvert hraðar en aðrar tegundir áhættu sem fylgst er með í fjármálageiranum og geta dreifst yfir geira og landfræðileg mörk. Þau geta þróast yfir í kerfislæga krísu þar sem traust á fjármálakerfinu rofnar vegna röskunar á starfsemi sem styður við raunhagkerfið eða vegna verulegs fjárhagslegs taps sem nær stigi sem fjármálakerfið þolir ekki eða krefst þess að gripið sé til ráðstafana til að bregðast við þungum áföllum. Til að koma í veg fyrir að þessar sviðsmyndir eigi sér stað og stofni þar með fjármálastöðugleika og heilleika Sambandsins í hættu er nauðsynlegt að stuðla að samleitni eftirlitsaðferða að því er varðar upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, einkum með nýjum reglum sem gera Sambandinu kleift að hafa eftirlit með mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu.

80) Eftirlitsramminn veltur að miklu leyti á umfangi samstarfs milli aðaleftirlitsaðila og mikilvægs þriðja aðila sem veitir aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu sem hefur áhrif á veitingu fjármálaþjónustu. Árangursríkt eftirlit byggist m.a. á getu aðaleftirlitsaðila til að framkvæma vöktunarverkefni og skoðanir með skilvirkum hætti, til að meta reglur, stjórntæki og ferla sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu nota, sem og að meta möguleg uppsöfnuð áhrif af starfsemi þeirra á fjármálastöðugleika og heilleika fjármálakerfisins. Samtímis er mikilvægt að mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu fylgi tilmælum aðaleftirlitsaðila og bregðist við áhyggjum hans. Þar sem skortur á samstarfi af hálfu mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem hefur áhrif á veitingu fjármálaþjónustu, s.s. með því að neita að veita aðgang að athafnasvæðum sínum eða leggja fram upplýsingar, myndi á endanum svipta aðaleftirlitsaðila mikilvægustu verkfærum sínum við að meta upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila og gæti haft neikvæð áhrif á fjármálastöðugleika og heilleika fjármálakerfisins, er nauðsynlegt að kveða einnig á um samsvarandi fyrirkomulag um viðurlög.

81) Í ljósi þessa ætti ekki að stofna þörf aðaleftirlitsaðila á að leggja á févíti til að þvinga mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, til að uppfylla þær skuldbindingar um gagnsæi og aðgang sem settar eru fram í þessari reglugerð, í hættu vegna erfiðleika sem upp koma við að framfylgja þessum févítum í tengslum við mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðju löndum. Til að tryggja að hægt sé að framfylgja slíkum viðurlögum og hægt sé að koma hratt á ferlum sem halda uppi rétti mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til varna í tengslum við tilnefningarfyrirkomulagið og útgáfu tilmæla, ætti að krefjast þess að þessir mikilvægu þriðju aðilar sem veita aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu sem hefur áhrif á veitingu fjármálaþjónustu, hafi fullnægjandi viðskiptanærveru í Sambandinu. Vegna eðlis eftirlitsins og þar sem sambærilegt fyrirkomulag er ekki fyrir hendi í öðrum lögsögum eru engar aðrar viðeigandi aðferðir sem tryggja þetta markmið með skilvirkri samvinnu við fjármálaeftirlit í þriðju löndum í tengslum við vöktun á áhrifum af stafrænni rekstrarlegri áhættu af völdum kerfislægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og uppfylla skilyrði til að teljast mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðju löndum. Til að halda áfram að veita aðilum á fjármálamarkaði í Sambandinu upplýsinga- og fjarskiptatækniþjónustu ætti þriðji aðili með staðfestu í þriðja landi sem hefur verið tilnefndur sem mikilvægur í samræmi við þessa reglugerð því, innan 12 mánaða frá slíkri tilnefningu, að gera allar nauðsynlegar ráðstafanir til að tryggja stöðu hans sem lögaðila í Sambandinu með því að koma á fót dótturfélagi, eins og það er skilgreint í réttarreglum Sambandsins, þ.e. í tilskipun Evrópuþingsins og ráðsins 2013/34/ESB ([21]).

82) Krafan um að setja á stofn dótturfélag í Sambandinu ætti ekki að koma í veg fyrir að mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu veiti upplýsinga- og fjarskiptatækniþjónustu og tengdan tæknilegan stuðning frá starfsstöðvum og grunnvirkjum utan Sambandsins. Með þessari reglugerð er ekki lögð á skylda til staðbindingar gagna þar eð hún krefst þess ekki að geymsla eða vinnsla gagna fari fram í Sambandinu.

83) Mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu ættu að geta veitt upplýsinga- og fjarskiptaþjónustu hvaðan sem er í heiminum, ekki endilega eða aðeins frá athafnasvæðum í Sambandinu. Eftirlitsstarfsemi ætti fyrst að fara fram á athafnasvæði sem staðsett er í Sambandinu og með samskiptum við einingar sem staðsettar eru í Sambandinu, þ.m.t. dótturfélög sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafa komið á fót samkvæmt þessari reglugerð. Slíkar aðgerðir innan Sambandsins gætu þó verið ófullnægjandi til að gera aðaleftirlitsaðila kleift að sinna skyldum sínum að fullu og á skilvirkan hátt samkvæmt þessari reglugerð. Aðaleftirlitsaðili ætti því einnig að geta beitt viðeigandi eftirlitsheimildum í þriðju löndum. Með því að beita þessum valdheimildum í þriðju löndum ætti aðaleftirlitsaðili að geta kannað starfsstöð þar sem upplýsinga- og fjarskiptatækniþjónusta eða tæknileg stoðþjónusta er í raun veitt eða stjórnað af mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og það ætti að veita aðaleftirlitsaðila víðtækan og rekstrarlegan skilning á stýringu upplýsinga- og fjarskiptatækniáhættu hjá mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Möguleiki aðaleftirlitsaðilans sem stofnunar í Sambandinu á að beita heimildum utan yfirráðasvæðis Sambandsins ætti að afmarkast af viðeigandi skilyrðum, einkum samþykki viðkomandi mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Að sama skapi ætti að upplýsa viðeigandi yfirvöld í þriðja landi um að starfsemi aðaleftirlitsaðila fari fram á yfirráðasvæði þeirra og þeir ekki að hafa andmælt því. Til að tryggja skilvirka framkvæmd og með fyrirvara um viðeigandi valdheimildir stofnana Sambandsins og aðildarríkjanna þarf þó einnig að festa slíkar valdheimildir að fullu í sessi með gerð fyrirkomulags samvinnu á sviði stjórnsýslu við viðeigandi

([21]) Tilskipun Evrópuþingsins og ráðsins 2013/34/ESB frá 26. júní 2013 um árleg reikningsskil, samstæðureikningsskil og tilheyrandi skýrslur tiltekinna tegunda fyrirtækja, um breytingu á tilskipun Evrópuþingsins og ráðsins 2006/43/EB og niðurfellingu tilskipana ráðsins 78/660/EBE og 83/349/EBE (Stjtíð. ESB L 182, 29.6.2013, bls. 19).

yfirvöld í því þriðja landi sem um er að ræða. Þessi reglugerð ætti því að gera Evrópsku eftirlitsstofnununum kleift að taka upp fyrirkomulag til samvinnu á sviði stjórnsýslu við viðeigandi yfirvöld þriðju landa sem ætti ekki með öðrum hætti að skapa lagaskyldur að því er varðar Sambandið og aðildarríki þess.

84) Til að auðvelda samskipti við aðaleftirlitsaðila og tryggja fullnægjandi fyrirsvar ættu mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru hluti af samstæðu að tilnefna einn lögaðila sem samræmingaraðila.

85) Eftirlitsramminn ætti ekki að hafa áhrif á valdheimildir aðildarríkja til að annast eigið eftirlit eða vöktunarverkefni að því er varðar þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem ekki eru tilnefndir sem mikilvægir samkvæmt þessari reglugerð en teljast mikilvægir á landsvísu.

86) Til að ýta undir marglaga stofnanauppbyggingu á sviði fjármálaþjónustu ætti sameiginleg nefnd evrópsku eftirlitsstofnananna að halda áfram að tryggja heildarsamræmingu þvert á atvinnugreinar í tengslum við öll málefni sem varða upplýsinga- og fjarskiptatækniáhættu í samræmi við verkefni hennar varðandi netöryggi. Hún ætti að njóta stuðnings nýrrar undirnefndar („eftirlitsvettvangurinn“) sem vinnur undirbúningsvinnu bæði fyrir einstakar ákvarðanir sem beint er til mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og fyrir útgáfu sameiginlegra tilmæla, einkum í tengslum við setningu viðmiðana fyrir eftirlitsáætlanir fyrir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og tilgreiningu bestu starfsvenja til að takast á við samþjöppunaráhættu í upplýsinga- og fjarskiptatækni.

87) Til að tryggja að viðeigandi og skilvirkt eftirlit sé haft með mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu á vettvangi Sambandsins er í þessari reglugerð kveðið á um að heimilt sé að tilnefna hverja sem er af evrópsku eftirlitsstofnununum þremur sem aðaleftirlitsaðila. Úthlutun hvers og eins mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til einnar af hinum þremur evrópsku eftirlitsstofnunum ætti að byggjast á mati á því hvort meirihluti aðila á fjármálamarkaði starfar innan þess fjármálageira sem sú evrópska eftirlitsstofnun ber ábyrgð á. Þessi nálgun ætti að leiða til jafnvægis í skiptingu verkefna og ábyrgðar í tengslum við eftirlitsstarfsemi milli evrópsku eftirlitsstofnananna þriggja og ætti að nýta sem best þann mannauð og tæknilega sérþekkingu sem tiltæk er í sérhverri hinna þriggja evrópsku eftirlitsstofnana.

88) Aðaleftirlitsaðilar ættu að fá mikilvægar heimildir til að framkvæma rannsóknir, framkvæma skoðanir á vettvangi og utan hans á athafnasvæðum og stöðum hjá mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og afla tæmandi og uppfærðra upplýsinga. Þessar valdheimildir ættu að gera aðaleftirlitsaðila kleift að öðlast raunverulega innsýn í tegund, umfang og áhrif þeirrar upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem steðjar að aðilum á fjármálamarkaði og að lokum fjármálakerfi Sambandsins. Forsenda þess að evrópsku eftirlitsstofnanirnar geti skilið og tekist á við kerfislega þætti upplýsinga- og fjarskiptatækniáhættu í fjármálum er að þær fái hlutverk aðaleftirlitsaðila. Áhrif mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu á fjármálageira Sambandsins og hugsanleg álitamál af völdum samþjöppunaráhættu í upplýsinga- og fjarskiptatækni kalla á sameiginlega aðferð á vettvangi Sambandsins. Samhliða framkvæmd á mörgum úttektum og aðgangsréttindum sem fjöldi lögbærra yfirvalda framkvæma hvert fyrir sig, þar sem lítil eða engin samræming er þeirra á milli, myndi koma í veg fyrir að fjármálaeftirlitið fengi tæmandi og heildstætt yfirlit yfir upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila í Sambandinu, en skapa um leið óþarfa endurtekningu, byrði og flækjustig fyrir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu ef þeir féllu undir fjölda eftirlits- og eftirlitsbeiðna.

89) Vegna verulegra áhrifa þess að teljast vera mikilvægur aðili ætti þessi reglugerð að tryggja að réttindi mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu séu virt við framkvæmd eftirlitsrammans. Áður en slíkir veitendur eru tilnefndir sem mikilvægir ættu þeir t.d. að hafa rétt til að leggja fyrir aðaleftirlitsaðila rökstudda yfirlýsingu sem felur í sér allar viðeigandi upplýsingar að því er varðar matið sem tengist tilnefningu þeirra. Þar sem aðaleftirlitsaðili ætti að hafa valdheimild til að leggja fram tilmæli um mál sem varða upplýsinga- og fjarskiptatækniáhættu og viðeigandi úrræði þar að lútandi, sem fela í sér vald til að andmæla tilteknu samningsbundnu fyrirkomulagi sem hefur að lokum áhrif á stöðugleika aðilans á fjármálamarkaði eða fjármálakerfisins, ættu mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu einnig að fá tækifæri til að gefa útskýringar á tilætluðum áhrifum af lausnunum sem gert er ráð fyrir í tilmælunum á viðskiptavini sem eru einingar utan gildissviðs þessarar reglugerðar og setja fram lausnir til að draga úr áhættu, áður en gengið er frá þessum tilmælum. Mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru ósammála tilmælunum ættu að leggja fram rökstudda

skýringu á því að þeir ætli ekki að fylgja tilmælunum. Ef slík rökstudd skýring er ekki lögð fram eða ef hún telst ófullnægjandi ætti aðaleftirlitsaðilinn að gefa út opinbera tilkynningu þar sem lýst er í stuttu máli hvernig ekki er farið að tilskildum ákvæðum.

90) Lögbær yfirvöld ættu að hafa það verkefni að sannreyna í verulegum mæli að farið sé að tilmælum sem aðaleftirlitsaðili gefur út í starfsemi sinni að því er varðar varfærniseftirlit með aðilum á fjármálamarkaði. Lögbær yfirvöld ættu að geta krafist þess að aðilar á fjármálamarkaði geri viðbótarráðstafanir til að taka á þeirri áhættu sem tilgreind eru í tilmælum aðaleftirlitsaðilans og ættu, þegar þar að kemur, að gefa út tilkynningar þess efnis. Ef aðaleftirlitsaðili beinir tilmælum til mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem falla undir eftirlit samkvæmt tilskipun (ESB) 2022/2555 ættu lögbær yfirvöld, að eigin frumkvæði og áður en þau samþykkja viðbótarráðstafanir, að hafa samráð við lögbær yfirvöld samkvæmt þeirri tilskipun til að stuðla að samræmdri nálgun í samskiptum við mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

91) Framkvæmd eftirlitsins ætti að byggjast á þremur meginreglum um rekstur sem miða að því að tryggja: a) náið samstarf milli evrópsku eftirlitsstofnananna í hlutverki sínu sem aðaleftirlitsaðilar í gegnum sameiginlegt eftirlitskerfi (e. *JON*), b) samræmi við rammann sem komið er á með tilskipun (ESB) 2022/2555 (með valkvæðu samráði aðila samkvæmt þeirri tilskipun til að forðast tvítekningu ráðstafana sem beinast að mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu) og c) að kostgæfni sé sýnd við að lágmarka hugsanlega hættu á röskun á þjónustu sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veita viðskiptavinum sem eru einingar utan gildissviðs þessarar reglugerðar.

92) Eftirlitsramminn ætti ekki að koma í stað, eða á nokkurn hátt eða að neinum hluta vera staðgengill, kröfunnar um að aðilar á fjármálamarkaði stýri sjálfar þeirri áhættu sem fylgir notkun þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. skuldbindingar þeirra til að viðhalda stöðugu eftirliti með samningsbundnu fyrirkomulagi sem gert er við mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Að sama skapi ætti eftirlitsramminn ekki að hafa áhrif á fulla ábyrgð aðila á fjármálamarkaði á því að fara að og uppfylla allar lagalegar skuldbindingar sem mælt er fyrir um í þessari reglugerð og viðeigandi lögum um fjármálaþjónustu.

93) Til að koma í veg fyrir tvíverknað og skörun ættu lögbær yfirvöld að forðast að gera hvers kyns ráðstafanir á eigin spýtur sem miða að því að vakta áhættu mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og í því sambandi ættu þau að treysta á viðeigandi mat aðaleftirlitsaðila. Í öllum tilvikum ætti aðaleftirlitsaðili að samræma og samþykkja hvers kyns ráðstafanir fyrir fram í tengslum við framkvæmd verkefna innan eftirlitsrammans.

94) Til að stuðla að samleitni á alþjóðavettvangi að því er varðar notkun bestu starfsvenja við endurskoðun og eftirlit með stafrænni áhættustýringu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu ætti að hvetja evrópsku eftirlitsstofnanirnar til að koma á samstarfssamningum við viðeigandi eftirlitsyfirvöld og yfirvöld sem setja reglugerðir í þriðju löndum.

95) Til að nýta sérstaka hæfni, tæknilega kunnáttu og sérþekkingu starfsfólks sem sérhæfir sig í rekstrar- og upplýsinga- og fjarskiptatækniáhættu innan lögbærra yfirvalda, evrópsku eftirlitsstofnananna þriggja og að eigin vali lögbærra yfirvalda samkvæmt tilskipun (ESB) 2022/2555 ætti aðaleftirlitsaðili að nýta sér landsbundna eftirlitsgetu og þekkingu og koma á fót sérstökum rannsóknarteymum fyrir hvern mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptaþjónustu og samnýta þverfagleg teymi til að styðja við undirbúning og framkvæmd eftirlitsstarfsemi, þ.m.t. almennar rannsóknir og eftirlit með mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, sem og alla mikilvæga eftirfylgni með henni.

96) Þar eð kostnaður sem hlýst af eftirlitsverkefnum yrði að fullu fjármagnaður með gjöldum sem lögð eru á mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu er samt sem áður líklegt að evrópsku eftirlitsstofnanirnar verði fyrir kostnaði vegna framkvæmdar á sérnota upplýsinga- og fjarskiptatæknikerfum sem styðja við eftirlitið sem fyrir er áður en eftirlitsramminn tekur gildi, þar sem þróa þyrfti sérstök upplýsinga- og fjarskiptatæknikerfi og taka þau í notkun fyrirfram. Í þessari reglugerð er því kveðið á um blandað fjármögnunarlíkan þar sem eftirlitsramminn yrði sem slíkur fjármagnaður að fullu en þróun evrópsku eftirlitsstofnananna á upplýsinga- og fjarskiptatæknikerfum yrði fjármögnuð með framlagi frá Sambandinu og lögbærum landsyfirvöldum.

97) Lögbær yfirvöld ættu að hafa allar tilskildar valdheimildir til eftirlits, rannsóknar og viðurlaga til að tryggja að þau geti sinnt skyldustörfum sínum sem skyldi samkvæmt þessari reglugerð. Þau ættu að jafnaði að birta tilkynningar um þau stjórnsýsluviðurlög sem þau beita. Þar sem hægt er að koma á fót aðilum á fjármálamarkaði og þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu í ólíkum aðildarríkjum og undir eftirliti mismunandi lögbærra yfirvalda ætti að auðvelda beitingu þessarar reglugerðar með nánu samstarfi milli viðkomandi lögbærra yfirvalda annars vegar, þ.m.t. Seðlabanka Evrópu með tilliti til sértækra verkefna sem honum eru falin með reglugerð ráðsins (ESB) nr. 1024/2013, og samráði við evrópsku eftirlitsstofnanirnar með gagnkvæmum upplýsingaskiptum og aðstoð í tengslum við viðkomandi eftirlitsstarfsemi hins vegar.

98) Til að magngreina enn frekar og skilgreina viðmiðanirnar fyrir tilnefningu á mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og samræma eftirlitsgjöld ætti að fela framkvæmdastjórninni vald til að samþykkja gerðir í samræmi við 290. gr. sáttmálans um starfshætti Evrópusambandsins sem viðbót við þessa reglugerð með því að tilgreina nánar þau kerfislægu áhrif sem bilun eða röskun á rekstri þriðja aðila sem veita upplýsinga- og fjarskiptatækniþjónustu gæti haft á þá aðila á fjármálamarkaði sem hann veitir upplýsinga- og fjarskiptatækniþjónustu, fjölda kerfislega mikilvægra stofnana á alþjóðavísu eða aðrar kerfislega mikilvægar stofnanir sem reiða sig á viðkomandi þjónustuveitanda upplýsinga- og fjarskiptatækni, fjölda þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem starfa á tilteknum markaði, kostnað við að flytja gögn og vinnuálag í upplýsinga- og fjarskiptatækni til annarra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem og upphæð eftirlitsgjalda og með hvaða hætti eigi að greiða þau. Einkar mikilvægt er að framkvæmdastjórnin hafi viðeigandi samráð meðan á undirbúningsvinnu hennar stendur, þ.m.t. við sérfræðinga, og að þetta samráð fari fram í samræmi við meginreglurnar sem mælt er fyrir um í samstarfssamningnum milli stofnana um betri lagasetningu frá 13. apríl 2016 ([22]). Einkum, í því skyni að tryggja jafna þátttöku við undirbúning framseldra gerða, ættu Evrópuþingið og ráðið að fá öll skjöl á sama tíma og sérfræðingar aðildarríkjanna og ættu sérfræðingar þeirra að hafa kerfisbundinn aðgang að fundum sérfræðingahópa framkvæmdastjórnarinnar sem vinna að undirbúningi framseldra gerða.

99) Tæknilegir eftirlitsstaðlar ættu að tryggja samræmda samhæfingu krafnanna sem mælt er fyrir um í þessari reglugerð. Í hlutverkum sínum sem aðilar með afar sérhæfða kunnáttu ættu evrópsku eftirlitsstofnanirnar að semja drög að tæknilegum eftirlitsstöðlum sem fela ekki í sér stefnuákvarðanir, til að leggja fyrir framkvæmdastjórnina. Þróa ætti tæknilega eftirlitsstaðla á sviði stýringar upplýsinga- og fjarskiptatækniáhættu, tilkynninga um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni, prófana, sem og með tilliti til lykilkrafna um trausta vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila. Framkvæmdastjórnin og evrópsku eftirlitsstofnanirnar ættu að tryggja að allir aðilar á fjármálamarkaði geti beitt þessum stöðlum og kröfum á þann hátt sem er í réttu hlutfalli við stærð þeirra og heildaráhættusnið og samræmist eðli, umfangi og flækjustigi þjónustu þeirra, starfsemi og rekstri. Framkvæmdastjórnin ætti að hafa vald til að samþykkja þessa tæknilegu eftirlitsstaðla með framseldum gerðum skv. 290. gr. sáttmálans um starfshætti Evrópusambandsins og í samræmi við 10. til 14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010.

100) Til að auðvelda samanburð á tilkynningum um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og meiri háttar greiðslutengd rekstrar- eða öryggisatvik, sem og til að tryggja gagnsæi að því er varðar samningsbundið fyrirkomulag um notkun á upplýsinga- og fjarskiptatækniþjónustu sem veitt er af þriðju aðilum í upplýsinga- og fjarskiptatækniþjónustu, ættu evrópsku eftirlitsstofnanirnar að semja drög að tæknilegum framkvæmdarstöðlum um að koma á stöðluðum sniðmátum, eyðublöðum og verklagsreglum fyrir aðila á fjármálamarkaði til að tilkynna um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og alvarleg greiðslutengd rekstrar- eða öryggisatvik, sem og stöðluð sniðmát fyrir upplýsingaskrána. Við þróun þessara staðla ættu evrópsku eftirlitsstofnanirnar að taka tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði og eðlis, umfangs og flækjustigs þjónustu hans, starfsemi og reksturs. Framkvæmdastjórnin ætti að hafa vald til að samþykkja þessa tæknilegu framkvæmdarstaðla með framkvæmdargerðum skv. 291. gr. sáttmálans um starfshætti Evrópusambandsins og í samræmi við 15. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010.

([22]) Stjtíð. ESB L 123, 12.5.2016, bls. 1.

101) Þar eð frekari kröfur hafa þegar verið tilgreindar með framseldum gerðum og framkvæmdargerðum sem byggjast á tæknilegum eftirlits- og framkvæmdarstöðlum í reglugerðum Evrópuþingsins og ráðsins (EB) nr. 1060/2009 ([23]), (ESB) nr. 648/2012 ([24]), (ESB) nr. 600/2014 ([25]) og (ESB) nr. 909/2014 ([26]) þykir rétt að veita evrópsku eftirlitsstofnununum, annaðhvort hverri um sig eða sameiginlega fyrir milligöngu sameiginlegu nefndarinnar, umboð til að leggja fyrir framkvæmdastjórnina tæknilega eftirlits- og framkvæmdarstaðla til samþykktar á framseldum gerðum og framkvæmdargerðum sem yfirfæra og uppfæra gildandi reglur um stýringu upplýsinga- og fjarskiptatækniáhættu.

102) Þar eð þessi reglugerð, ásamt tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2556 ([27]), felur í sér samsteypu ákvæða um stýringu upplýsinga- og fjarskiptatækniáhættu úr mörgum reglugerðum og tilskipunum Sambandsins um fjármálaþjónustu, þ.m.t. reglugerðir (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014 og (ESB) nr. 909/2014 og reglugerð Evrópuþingsins og ráðsins (ESB) 2016/1011 ([28]), ætti að breyta þessum reglugerðum til að tryggja fullt samræmi, til að skýra nánar að mælt sé fyrir um viðeigandi ákvæði tengd upplýsinga- og fjarskiptatækniáhættu í þessari reglugerð.

103) Af þessum sökum ætti að þrengja gildissvið viðeigandi greina sem tengjast rekstraráhættu, sem valdheimildir sem mælt er fyrir um í reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 höfðu falið umboð til að samþykkja framseldar gerðir og framkvæmdargerðir, með það fyrir augum að yfirfæra í reglugerðina öll þau ákvæði sem taka til þátta stafræns rekstrarlegs viðnámsþróttar sem er hluti þessara reglugerða í dag.

104) Taka ætti tilhlýðilegt tillit til mögulegrar kerfisáhættu sem tengist notkun á grunnvirkjum upplýsinga- og fjarskiptatækni sem gera greiðslukerfum kleift að reka og veita greiðsluvinnslustarfsemi á vettvangi Sambandsins með samræmdum reglum um stafrænan viðnámsþrótt. Í því skyni ætti framkvæmdastjórnin að meta hratt þörfina á endurskoðun á gildissviði þessarar reglugerðar, um leið og slík endurskoðun er löguð að niðurstöðu þeirrar ítarlegu endurskoðunar sem gert er ráð fyrir samkvæmt tilskipun (ESB) 2015/2366. Fjölmargar stórfelldar árásir undanfarna áratugi sýna að greiðslukerfi hafa orðið útsett fyrir netógnum. Greiðslukerfi og greiðsluvinnslustarfsemi liggja til grundvallar greiðsluþjónustukeðjunnar og sýna sterkar samtengingar við fjármálakerfið í heild og hafa öðlast afgerandi þýðingu fyrir starfsemi fjármálamarkaða Sambandsins. Netárásir á slík kerfi geta valdið alvarlegri röskun á rekstri og haft beinar afleiðingar á mikilvæga efnahagslega starfsemi, svo sem greiðsluþjónustu, og óbein áhrif á tengda efnahagslega ferla. Þar til samræmdu fyrirkomulagi og eftirliti með rekstraraðilum greiðslukerfa og vinnslueininga er komið á fót á vettvangi Sambandsins geta aðildarríki, með það í huga að beita svipuðum markaðsvenjum, sótt innblástur í kröfurnar um stafrænan rekstrarlegan viðnámsþrótt, sem mælt er fyrir um í þessari reglugerð, þegar þau beita reglum á rekstraraðila greiðslukerfa og vinnslueininga sem eru undir eftirliti í þeirra eigin lögsögu.

([23]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 1060/2009 frá 16. september 2009 um lánshæfismatsfyrirtæki (Stjtíð. ESB L 302, 17.11.2009, bls. 1).

([24]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 648/2012 frá 4. júlí 2012 um OTC-afleiður, miðlæga mótaðila og afleiðuviðskiptaskrár (Stjtíð. ESB L 201, 27.7.2012, bls. 1).

([25]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 600/2014 frá 15. maí 2014 um markaði fyrir fjármálagerninga og um breytingu á reglugerð ráðsins (ESB) nr. 648/2012 (Stjtíð. ESB L 173, 12.6.2014, bls. 84).

([26]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 909/2014 frá 23. júlí 2014 um bætt verðbréfauppgjör í Evrópusambandinu og um verðbréfamiðstöðvar og um breytingu á tilskipunum 98/26/EB og 2014/65/ESB og reglugerð (ESB) nr. 236/2012 (Stjtíð. ESB L 257, 28.8.2014, bls. 1).

([27]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2556 frá 14. desember 2022 um breytingu á tilskipunum 2009/65/EB, 2009/138/EB, 2011/61/ESB, 2013/36/ESB, 2014/59/ESB, 2014/65/ESB, (ESB) 2015/2366 og (ESB) 2016/2341 að því er varðar stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann (Stjtíð. ESB L 333, 27.12.2022, bls. 153).

([28]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/1011 frá 8. júní 2016 um vísitölur sem notaðar eru sem viðmiðanir í fjármálagerningum og fjárhagslegum samningum eða til að mæla árangur fjárfestingarsjóða og um breytingu á tilskipunum 2008/48/EB og 2014/17/ESB og reglugerð (ESB) nr. 596/2014 (Stjtíð. ESB L 171, 29.6.2016, bls.1).

105) Þar eð aðildarríkin geta ekki fyllilega náð markmiði þessarar reglugerðar, þ.e. að skapa sem mestan stafrænan rekstrarlegan viðnámsþrótt hjá eftirlitsskyldum aðilum á fjármálamarkaði, þar sem hún krefst samræmingar á nokkrum mismunandi reglum í lögum Sambandsins og landslögum, og því verður betur náð á vettvangi Sambandsins, vegna umfangs þess og áhrifa, er Sambandinu heimilt að samþykkja ráðstafanir í samræmi við nálægðarregluna eins og kveðið er á um í 5. gr. sáttmálans um Evrópusambandið. Í samræmi við meðalhófsregluna, eins og hún er sett fram í þeirri grein, er ekki gengið lengra en nauðsyn krefur í þessari reglugerð til að ná því markmiði.

106) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([29]) og skilaði hún áliti 10. maí 2021 ([30]).

SAMÞYKKT REGLUGERÐ ÞESSA:

I. KAFLI

Almenn ákvæði

1. gr.

Efni

1. Til að skapa sem mestan almennan stafrænan rekstrarlegan viðnámsþrótt er í þessari reglugerð mælt fyrir um samræmdar kröfur varðandi öryggi net- og upplýsingakerfa, sem styðja við viðskiptaferla aðila á fjármálamarkaði, sem hér segir:

a) kröfur sem eiga við um aðila á fjármálamarkaði í tengslum við:

   i. áhættustýringu á sviði upplýsinga- og fjarskiptatækni,

   ii. skýrslugjöf um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og tilkynningar til lögbærra yfirvalda, að eigin frumkvæði, um verulegar netógnir,

   iii. skýrslugjöf aðila á fjármálamarkaði, sem um getur í a- til d-lið 1. mgr. 2. gr., um alvarleg greiðslutengd rekstrar- eða öryggisatvik til lögbærra yfirvalda,

   iv. prófanir á stafrænum rekstrarlegum viðnámsþrótti,

   v. miðlun upplýsinga og greiningargagna í tengslum við netógnir og veikleika,

   vi. ráðstafanir til traustrar stýringar á upplýsinga- og fjarskiptatækniáhættu vegna þriðja aðila,

b) kröfur í tengslum við samningsbundið fyrirkomulag sem gert er milli þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og aðila á fjármálamarkaði,

c) reglur um stofnun og framkvæmd eftirlitsrammans fyrir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu þegar þeir veita aðilum á fjármálamarkaði þjónustu,

d) reglur um samstarf milli lögbærra yfirvalda og reglur um eftirlit og framfylgd af hálfu lögbærra yfirvalda í tengslum við öll málefni sem falla undir þessa reglugerð.

2. Að því er varðar aðila á fjármálamarkaði sem eru tilgreindir sem nauðsynlegar eða mikilvægar rekstrareiningar samkvæmt landslögum sem lögleiða 3. gr. tilskipunar (ESB) 2022/2555 skal þessi reglugerð teljast sérlög Sambandsins að því er varðar 4. gr. þeirrar tilskipunar.

3. Þessi reglugerð er með fyrirvara um ábyrgð aðildarríkja að því er varðar nauðsynlega starfsemi ríkja varðandi almannaöryggi, landvarnir og þjóðaröryggi í samræmi við lög Sambandsins.

([29]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2018/1725 frá 23. október 2018 um vernd einstaklinga í tengslum við vinnslu meginstofnana, stofnana, skrifstofa og fagstofnana Sambandsins á persónuupplýsingum og um frjálsa miðlun slíkra upplýsinga og um niðurfellingu reglugerðar (EB) nr. 45/2001 og ákvörðunar nr. 1247/2002/EB (Stjtíð. ESB L 295, 21.11.2018, bls. 39).

([30]) Stjtíð. ESB C 229, 15.6.2021, bls. 16.

2. gr.

Gildissvið

1. Með fyrirvara um 3. og 4. mgr. gildir þessi reglugerð um eftirfarandi einingar:

a) lánastofnanir,

b) greiðslustofnanir, þ.m.t. greiðslustofnanir sem eru undanþegnar samkvæmt tilskipun (ESB) 2015/2366,

c) reikningsupplýsingaþjónustuveitendur,

d) rafeyrisfyrirtæki, þ.m.t. rafeyrisfyrirtæki sem eru undanþegin samkvæmt tilskipun 2009/110/EB,

e) verðbréfafyrirtæki,

f) þjónustuveitendur sýndareigna með starfsleyfi samkvæmt reglugerð Evrópuþingsins og ráðsins um markaði með sýndareignir og um breytingu á reglugerðum (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipunum 2013/36/ESB og (ESB) 2019/1937 („reglugerð um markaði með sýndareignir“) og útgefendur eignatengdra tóka,

g) verðbréfamiðstöðvar,

h) miðlæga mótaðila,

i) viðskiptavettvanga,

j) viðskiptaskrár,

k) rekstraraðila sérhæfðra sjóða,

l) rekstrarfélög,

m) veitendur gagnaskýrsluþjónustu,

n) vátrygginga- og endurtryggingafélög,

o) vátryggingamiðlara, endurtryggingamiðlara og vátryggingamiðlara í hliðarstarfsemi,

p) stofnanir um starfstengdan lífeyri,

q) lánshæfismatsfyrirtæki,

r) stjórnendur mjög mikilvægra viðmiðana,

s) þjónustuveitendur hópfjármögnunar,

t) verðbréfunarskrár,

u) þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

2. Að því er varðar þessa reglugerð skulu einingar sem um getur í a- til t-lið 1. mgr. sameiginlega nefndar „aðilar á fjármálamarkaði“.

3. Þessi reglugerð gildir ekki um:

a) rekstraraðila sérhæfðra sjóða eins og um getur í 2. mgr. 3. gr. tilskipunar 2011/61/ESB,

b) vátrygginga- og endurtryggingafélög eins og um getur í 4. gr. tilskipunar 2009/138/EB,

c) stofnanir um starfstengdan lífeyri sem starfrækja lífeyriskerfi þar sem sjóðfélagar eru samtals ekki fleiri en 15,

d) einstaklinga eða lögaðila sem njóta undanþágu skv. 2. og 3. gr. tilskipunar 2014/65/ESB,

e) vátryggingamiðlara, endurtryggingamiðlara og vátryggingamiðlara í hliðarstarfsemi sem eru örfyrirtæki eða lítil eða meðalstór fyrirtæki,

f) póstgíróstofnanir eins og um getur í 3. lið 5. mgr. 2. gr. tilskipunar 2013/36/ESB.

4. Aðildarríkjunum er heimilt að undanskilja aðila sem um getur í 4.–23. lið 5. mgr. 2. gr. tilskipunar 2013/36/ESB og eru staðsettir innan yfirráðasvæða þeirra frá gildissviði þessarar reglugerðar. Ef aðildarríki nýtir sér slíkan kost skal það tilkynna framkvæmdastjórninni um það, sem og um allar síðari breytingar sem því tengjast. Framkvæmdastjórnin skal gera upplýsingarnar aðgengilegar öllum á vefsetri sínu eða annars staðar þar sem þær eru auðaðgengilegar.

3. gr.

Skilgreiningar

Í þessari reglugerð er merking eftirfarandi hugtaka sem hér segir:

1) „stafrænn rekstrarlegur viðnámsþróttur“: geta aðila á fjármálamarkaði til að byggja upp, viðhalda og endurmeta heilleika og áreiðanleika í rekstri með því að tryggja, hvort heldur beint, eða óbeint, með notkun upplýsinga- og fjarskiptatækniþjónustu þriðju aðila, alla þá getu sem tengist upplýsinga- og fjarskiptatækni sem þarf til að tryggja öryggi net- og upplýsingakerfa sem aðili á fjármálamarkaði notar og sem styður samfellda veitingu fjármálaþjónustu og gæði hennar, þ.m.t. meðan röskun varir,

2) „net- og upplýsingakerfi“: net- og upplýsingakerfi eins og skilgreint er í 1. lið 6. gr. tilskipunar (ESB) 2022/2555,

3) „fornkerfi í upplýsinga- og fjarskiptatækni“: upplýsinga- og fjarskiptatæknikerfi sem er orðið úrelt (úr sér gengið), sem, af tæknilegum eða viðskiptalegum ástæðum, ekki er fýsilegt að uppfæra eða lagfæra, eða þjónustuaðili eða þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu styður ekki lengur, en er enn í notkun og styður starfsemi aðila á fjármálamarkaði,

4) „öryggi net- og upplýsingakerfa“: öryggi net- og upplýsingakerfa eins og skilgreint er í 2. lið 6. gr. tilskipunar (ESB) 2022/2555,

5) „upplýsinga- og fjarskiptatækniáhætta“: hvers kyns aðstæður, í tengslum við notkun á net- og upplýsingakerfum, sem eru nokkuð greinanlegar og sem geta, ef þær eru til staðar, stofnað öryggi net- og upplýsingakerfa, hvers kyns tækniháðs búnaðar eða ferla, starfrækslu og ferla eða veitingu þjónustu í hættu með því að hafa skaðleg áhrif á stafrænt eða efnislegt umhverfi,

6) „upplýsingaeign“: safn upplýsinga, annaðhvort efnislegra eða óefnislegra, sem vert er að vernda,

7) „upplýsinga- og fjarskiptatæknieign“: hugbúnaðar- eða vélbúnaðareign í net- og upplýsingakerfum sem aðili á fjármálamarkaði notar,

8) „atvik sem tengist upplýsinga- og fjarskiptatækni“: stakur atburður, eða röð tengdra atburða, ófyrirséður af aðila á fjármálamarkaði sem stofnar öryggi net- og upplýsingakerfa í hættu og hafa neikvæð áhrif á tiltækileika, ósvikni, réttleika eða leynd gagna, eða á þá þjónustu sem viðkomandi aðili á fjármálamarkaði veitir,

9) „greiðslutengt rekstrar- eða öryggisatvik“: stakur atburður, eða röð tengdra atburða, ófyrirséður af þeim aðilum á fjármálamarkaði er um getur í a- til d-lið 1. mgr. 2. gr., hvort sem þeir tengjast upplýsinga- og fjarskiptatækni eða ekki, sem hefur neikvæð áhrif á tiltækileika, ósvikni, réttleika eða leynd greiðslutengdra gagna eða á greiðslutengda þjónustu sem viðkomandi aðili á fjármálamarkaði veitir,

10) „alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni“: atvik sem tengist upplýsinga- og fjarskiptatækni og hefur mikil neikvæð áhrif á net- og upplýsingakerfi sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði,

11) „alvarlegt greiðslutengt rekstrar- eða öryggisatvik“: greiðslutengt rekstrar- eða öryggisatvik sem hefur mikil neikvæð áhrif á veitta greiðslutengda þjónustu,

12) „netógn“: netógn eins og skilgreind er í 8. lið 2. gr. reglugerðar (ESB) 2019/881,

13) „veruleg netógn“: netógn sem hefur tæknilega eiginleika sem benda til þess að hún gæti haft í för með sér alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni eða alvarlegt greiðslutengt rekstrar- eða öryggisatvik,

14) „netárás“: illskeytt atvik sem tengist upplýsinga- og fjarskiptatækni sem stafar af tilraun hvers kyns ógnvalds til að eyða, afhjúpa, breyta, gera óvirkt, stela eða fá óheimilan aðgang að eða nota eign í heimildarleysi,

15) „ógnagreiningargögn“: upplýsingar sem hefur verið safnað saman, umbreytt, greindar, túlkaðar eða auðgaðar til að veita nauðsynlegt samhengi fyrir ákvarðanatöku og auðvelda viðeigandi og fullnægjandi skilning til að draga úr áhrifum af atviki sem tengist upplýsinga- og fjarskiptatækni eða netógn, þ.m.t. tæknilegum upplýsingum um netárás, þá sem bera ábyrgð á árásinni og aðferðir þeirra og hvatir,

16) „veikleiki“: veila, næmleiki eða galli eignar, kerfis, ferlis eða stjórntækja sem hægt er að nýta,

17) „ógnamiðuð innbrotsprófun“: rammi sem líkir eftir úrræðum, aðferðum og verklagi raunverulegra ógnvalda sem raunveruleg netógn er talin stafa af, sem skilar stýrðri, sérsniðinni og greiningargagnamiðaðri prófun (rautt teymi) á nauðsynlegum framleiðslukerfum aðila á fjármálamarkaði í rauntíma,

18) „upplýsinga- og fjarskiptatækniáhætta vegna þriðja aðila“: upplýsinga- og fjarskiptatækniáhætta sem getur skapast fyrir aðila á fjármálamarkaði í tengslum við notkun hans á upplýsinga- og fjarskiptatækniþjónustu sem veitt er af þriðja aðila eða undirverktökum þeirra síðarnefndu, þ.m.t. með útvistunarsamningum,

19) „þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu“: fyrirtæki sem veitir upplýsinga- og fjarskiptatækniþjónustu,

20) „þjónustuveitandi upplýsinga- og fjarskiptatækni innan samstæðu“: fyrirtæki sem er hluti fjármálasamstæðu og aðallega veitir aðilum á fjármálamarkaði innan sömu samstæðu eða aðilum sem tilheyra sömu stofnanaverndarkerfum, einkum móðurfyrirtækjum þeirra, dótturfélögum, útibúum eða öðrum einingum sem eru í sameiginlegri eigu eða undir sameiginlegum yfirráðum, upplýsinga- og fjarskiptatækniþjónustu,

21) „upplýsinga- og fjarskiptatækniþjónusta“: stafræn þjónusta og gagnaþjónusta sem veitt er, fyrir milligöngu upplýsinga- og fjarskiptatæknikerfa, einum eða fleiri innri eða ytri notendum á áframhaldandi grundvelli, þ.m.t. vélbúnaður sem þjónusta og vélbúnaðarþjónusta sem felur í sér að veitandi vélbúnaðarþjónustunnar veitir tækniaðstoð með hugbúnaði eða fastbúnaðaruppfærslum (*e. firmware update*), að undanskilinni hefðbundinni hliðrænni símaþjónustu,

22) „nauðsynleg eða mikilvæg starfsemi“: starfsemi þar sem röskun myndi rýra fjárhagslega afkomu aðila á fjármálamarkaði verulega eða traustleika eða samfellu þjónustu hennar og starfsemi eða að aflögð, gölluð eða misheppnuð framkvæmd starfseminnar myndi rýra verulega getu aðila á fjármálamarkaði til að uppfylla áfram skilyrði og skyldur sem fylgja starfsleyfi hans eða aðrar skyldur hans samkvæmt gildandi lögum um fjármálaþjónustu,

23) „mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu“: þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sem er tilnefndur sem mikilvægur í samræmi við 31. gr.,

24) „þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi“: þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sem er lögaðili með staðfestu í þriðja landi og hefur gert samning við aðila á fjármálamarkaði um veitingu upplýsinga- og fjarskiptatækniþjónustu,

25) „dótturfélag“: dótturfélag í skilningi 10. liðar 2.gr. og 22. gr. tilskipunar 2013/34/ESB,

26) „samstæða“: samstæða eins og skilgreind er í 11. lið 2. gr. tilskipunar 2013/34/ESB,

27) „móðurfyrirtæki“: móðurfyrirtæki í skilningi 9. liðar 2. gr. og 22. gr. tilskipunar 2013/34/ESB,

28) „undirverktaki í upplýsinga- og fjarskiptatækni með staðfestu í þriðja landi“: undirverktaki í upplýsinga- og fjarskiptatækni sem er lögaðili með staðfestu í þriðja landi og hefur gert samningsbundið fyrirkomulag annaðhvort við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi,

29) „samþjöppunaráhætta í upplýsinga- og fjarskiptatækni“: berskjöldun gagnvart einstökum eða mörgum tengdum mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem veldur því að aðili á fjármálamarkaði verður svo háður slíkum veitendum að óaðgengileiki, bilun eða annars konar brestur hjá slíkum veitanda gæti hugsanlega dregið úr getu aðila á fjármálamarkaði til að sinna nauðsynlegri eða mikilvægri starfsemi eða valdið honum annars konar skaðlegum áhrifum, þ.m.t. miklu tapi, eða stofnað fjármálastöðugleika Sambandsins í heild í hættu,

30) „stjórn og/eða framkvæmdastjórn“: stjórn og/eða framkvæmdastjórn (e. *management body*) [áður þýtt stjórn] eins og skilgreint er í 36. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB, 7. lið 1. mgr. 3. gr. tilskipunar 2013/36/ESB, s-lið 1. mgr. 2. gr. tilskipunar Evrópuþingsins og ráðsins 2009/65/EB ([31]), 45. lið 1. mgr. 2. gr. reglugerðar (ESB) nr. 909/2014, 20. lið 1. mgr. 3. gr. reglugerðar (ESB) 2016/1011 og í viðeigandi ákvæði reglugerðarinnar um markaði með sýndareignir, eða jafngildir aðilar sem reka einingunа í reynd eða gegna lykilhlutverki í samræmi við viðeigandi landslög Sambandsins eða landslög,

31) „lánastofnun“: lánastofnun eins og hún er skilgreind í 1. lið 1. mgr. 4. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 575/2013 ([32]),

32) „stofnun sem er undanþegin samkvæmt tilskipun 2013/36/ESB“: aðili eins og um getur í 4.–23. lið 5. mgr. 2. gr. tilskipunar 2013/36/ESB,

33) „verðbréfafyrirtæki“: verðbréfafyrirtæki eins og skilgreint er í 1. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB,

34) „lítið og ótengt verðbréfafyrirtæki“: verðbréfafyrirtæki sem uppfyllir skilyrðin sem mælt er fyrir um í 1. mgr. 12. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2019/2033 ([33]),

35) „greiðslustofnun“: greiðslustofnun eins og skilgreint er í 4. lið 4. gr. tilskipunar (ESB) nr. 2015/2366,

36) „greiðslustofnun sem er undanþegin samkvæmt tilskipun (ESB) 2015/2366“: greiðslustofnun sem er undanþegin skv. 1. mgr. 32. gr. tilskipunar (ESB) 2015/2366,

37) „reikningsupplýsingaþjónustuveitandi“: reikningsupplýsingaþjónustuveitandi eins og um getur í 1. mgr. 33. gr. tilskipunar (ESB) 2015/2366,

38) „rafeyrisfyrirtæki: rafeyrisfyrirtæki eins og skilgreint er í 1. lið 2. gr. tilskipunar Evrópuþingsins og ráðsins 2009/110/EB,

39) „rafeyrisfyrirtæki sem er undanþegið samkvæmt tilskipun 2009/110/EB“: rafeyrisfyrirtæki sem nýtur undanþágu eins og um getur í 1. mgr. 9. gr. í tilskipun 2009/110/EB,

40) „miðlægur mótaðili“: miðlægur mótaðili eins og skilgreindur er í 1. lið 2. gr. reglugerðar (ESB) nr. 648/2012,

41) „viðskiptaskrá“: viðskiptaskrá eins og skilgreind er í 2. lið 2. gr. reglugerðar (ESB) nr. 648/2012,

42) „verðbréfamiðstöð“: verðbréfamiðstöð eins og skilgreind er í 1. lið 1. mgr. 2. gr. reglugerðar (ESB) nr. 909/2014,

43) „viðskiptavettvangur“: viðskiptavettvangur eins og skilgreindur er í 24. lið 1. mgr. 4. gr. tilskipunar 2014/65/ESB,

44) „rekstraraðili sérhæfða sjóða“: rekstraraðili eins og skilgreindur er í b-lið 1. mgr. 4. gr. tilskipunar 2011/61/ ESB,

45) „rekstrarfélag“: rekstrarfélag eins og skilgreint er í b-lið 1. mgr. 2. gr. tilskipunar 2009/65/EB,

46) „veitandi gagnaskýrsluþjónustu“: veitandi gagnaskýrsluþjónustu í skilningi reglugerðar (ESB) nr. 600/2014, eins og um getur í 34.-36. lið 1. mgr. 2. gr. hennar,

47) „vátryggingafélag“: vátryggingafélag eins og skilgreint er í 1. lið 13. gr. tilskipunar 2009/138/EB,

48) „endurtryggingafélag“: endurtryggingafélag eins og skilgreint er í 4. lið 13. gr. tilskipunar 2009/138/EB,

([31]) Tilskipun Evrópuþingsins og ráðsins 2009/65/EB frá 13. júlí 2009 um samræmingu á lögum og stjórnsýslufyrirmælum að því er varðar verðbréfasjóði (UCITS) (Stjtíð. ESB L 302, 17.11.2009, bls. 32).

([32]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 575/2013 frá 26. júní 2013 um varfærniskröfur að því er varðar lánastofnanir og um breytingu á reglugerð (ESB) nr. 648/2012 (Stjtíð. ESB L 176, 27.6.2013, bls. 1).

([33]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2019/2033 frá 27. nóvember 2019 um varfærniskröfur fyrir verðbréfafyrirtæki og breytingu á reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 575/2013, (ESB) nr. 600/2014 og (ESB) nr. 806/2014 (Stjtíð. ESB L 314, 5.12.2019, bls. 1).

49) „vátryggingamiðlari“: vátryggingamiðlari eins og skilgreindur er í 3. lið 1. mgr. 2. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) nr. 2016/97 ([34]),

50) „vátryggingamiðlari í hliðarstarfsemi“: vátryggingamiðlari í hliðarstarfsemi eins og skilgreindur er í 4. lið 1. mgr. 2. gr. tilskipunar (ESB) 2016/97,

51) „endurtryggingamiðlari“: endurtryggingamiðlari eins og skilgreindur er í 5. lið 1. mgr. 2. gr. tilskipunar (ESB) 2016/97,

52) „stofnun um starfstengdan lífeyri“: stofnun um starfstengdan lífeyri eins og skilgreind er í 1. lið 6. gr. tilskipunar (ESB) 2016/2341,

53) „lítil stofnun um starfstengdan lífeyri“: stofnun um starfstengdan lífeyri sem starfrækir lífeyriskerfi þar sem sjóðfélagar eru samanlagt innan við 100,

54) „lánshæfismatsfyrirtæki“: lánshæfismatsfyrirtæki eins og skilgreint er í b-lið 1. mgr. 3. gr. reglugerðar (EB) nr. 1060/2009,

55) „þjónustuveitandi sýndareigna“: þjónustuveitandi sýndareigna eins og skilgreindur er í viðeigandi ákvæði reglugerðarinnar um markaði með sýndareignir,

56) „útgefandi tóka sem vísa í eignir“: útgefandi eignatengdra tóka eins og skilgreint er í viðeigandi ákvæði reglugerðarinnar um markaði með sýndareignir,

57) „stjórnandi mjög mikilvægra viðmiðana“: stjórnandi mjög mikilvægra viðmiðana eins og skilgreindur er í 25. lið 1. mgr. 3. gr. reglugerðar (ESB) 2016/1011,

58) „þjónustuveitandi hópfjármögnunar“: þjónustuveitandi hópfjármögnunar eins og skilgreindur er í e-lið 1. mgr. 2. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2020/1503 ([35]),

59) „verðbréfunarskrá“: verðbréfunarskrá eins og skilgreind er í 23. lið 2. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2017/2402 ([36]),

60) „örfyrirtæki“: aðili á fjármálamarkaði, annar en viðskiptavettvangur, miðlægur mótaðili, viðskiptaskrá eða verðbréfamiðstöð, sem hefur færri en tíu starfsmenn og þar sem ársvelta og/eða niðurstöðutala efnahagsreiknings fer ekki yfir 2 milljónir evra,

61) „aðaleftirlitsaðili“: sú evrópska eftirlitsstofnun sem tilnefnd er í samræmi við b-lið 1. mgr. 31. gr. þessarar reglugerðar,

62) „sameiginleg nefnd“: nefndin sem um getur í 54. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010,

63) „lítið fyrirtæki“: aðili á fjármálamarkaði sem hefur 10 starfsmenn eða fleiri en færri en 50 starfsmenn og þar sem ársvelta og/eða niðurstöðutala efnahagsreiknings fer yfir 2 milljónir evra en ekki yfir 10 milljónir evra,

64) „meðalstórt fyrirtæki“: aðili á fjármálamarkaði sem er ekki lítið fyrirtæki og hefur færri en 250 starfsmenn og þar sem ársvelta fer ekki yfir 50 milljónir evra og/eða efnahagsreikningur fer ekki yfir 43 milljónir evra á ári,

65) „opinbert yfirvald“: ríkisstjórn eða annar opinber stjórnsýsluaðili, þ.m.t. seðlabankar aðildarríkjanna.

([34]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2016/97 frá 20. janúar 2016 um dreifingu vátrygginga (Stjtíð. ESB L 26, 2.2.2016, bls. 19).

([35]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2020/1503 frá 7. október 2020 um evrópska þjónustuveitendur hópfjármögnunar fyrir fyrirtæki, og um breytingu á reglugerð (ESB) 2017/1129 og tilskipun (ESB) 2019/1937 (Stjtíð. ESB L 347, 20.10.2020, bls. 1).

([36]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2017/2402 frá 12. desember 2017 um almennan ramma fyrir verðbréfun og gerð sértæks ramma fyrir einfalda, gagnsæja og staðlaða verðbréfun, og um breytingu á tilskipunum 2009/65/EB, 2009/138/EB og 2011/61/ESB og reglugerðum (EB) nr. 1060/2009 og (ESB) nr. 648/2012 (Stjtíð. ESB L 347, 28.12.2017, bls. 35).

4. gr.

Meðalhófsreglan

1. Aðilar á fjármálamarkaði skulu innleiða reglurnar sem mælt er fyrir um í II. kafla í samræmi við meðalhófsregluna, að teknu tilliti til stærðar þeirra og heildaráhættusniðs og eðlis, umfangs og flækjustigs þjónustu þeirra, starfsemi og reksturs.

2. Að auki skal beiting aðila á fjármálamarkaði á III. og IV. kafla og I. þætti V. kafla vera í réttu hlutfalli við stærð þeirra og heildaráhættusnið og eðli, umfang og flækjustig þjónustu þeirra, starfsemi og reksturs, eins og sérstaklega er kveðið á um í viðeigandi reglum þessara kafla.

3. Lögbær yfirvöld skulu taka beitingu aðila á fjármálamarkaði á meðalhófsreglunni til athugunar við endurskoðun á samkvæmni áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni á grundvelli þeirra skýrslna sem lagðar eru fram að beiðni lögbærra yfirvalda skv. 5. mgr. 6. gr. og 2. mgr. 16. gr.

II. KAFLI

Stýring upplýsinga- og fjarskiptatækniáhættu

I. þáttur

5. gr.

Stjórnunarhættir og skipulag

1. Aðilar á fjármálamarkaði skulu hafa innri stjórnunar- og eftirlitsramma sem tryggir skilvirka og varfærna stýringu upplýsinga- og fjarskiptatækniáhættu, í samræmi við 4. mgr. 6. gr., til að skapa sem mestan stafrænan rekstrarlegan viðnámsþrótt.

2. Stjórn og/eða framkvæmdastjórn aðila á fjármálamarkaði skal skilgreina, samþykkja, hafa umsjón með og bera ábyrgð á framkvæmd allra ráðstafana sem tengjast áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr.

Að því er varðar fyrstu undirgrein skal stjórn og/eða framkvæmdastjórn:

a) bera endanlega ábyrgð á stýringu upplýsinga- og fjarskiptatækniáhættu aðila á fjármálamarkaði,

b) koma á stefnum sem miða að því að tryggja að strangar kröfur séu gerðar um tiltækileika, ósvikni, réttleika og leynd gagna,

c) fastsetja skýr hlutverk og ábyrgðarsvið fyrir alla starfsemi sem tengist upplýsinga- og fjarskiptatækni og koma á fót viðeigandi stjórnunarháttum til að tryggja skilvirk og tímanleg samskipti, samstarf og samræmingu milli þessara starfssviða,

d) bera heildarábyrgð á að setja og samþykkja stefnuáætlun um stafrænan rekstrarlegan viðnámsþrótt eins og um getur í 8. mgr. 6. gr., þ.m.t. að ákvarða viðeigandi áhættuþolmörk upplýsinga- og fjarskiptatækniáhættu viðkomandi aðila á fjármálamarkaði, eins og um getur í b-lið 8. mgr. 6. gr.,

e) samþykkja, hafa umsjón með og endurskoða reglulega framkvæmd stefnu aðilans á fjármálamarkaði um rekstrarsamfellu og viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni, sem um getur, eftir því sem við á, í 1. og 3. mgr. 11. gr. sem hægt er að samþykkja sem sértæka stefnu sem myndar órjúfanlegan þátt af heildarstefnu aðilans á fjármálamarkaði um rekstrarsamfellu og viðbragðs- og endurreisnaráætlunar hans,

f) samþykkja og skoða reglulega áætlanir aðilans á fjármálamarkaði um innri úttektir á upplýsinga- og fjarskiptatækni, upplýsinga- og fjarskiptatækniúttektir og breytingar á þeim,

g) úthluta og endurskoða reglulega viðeigandi fjárveitingar til að uppfylla þarfir aðilans á fjármálamarkaði fyrir stafrænan rekstrarlegan viðnámsþrótt að því er varðar allar tegundir tilfanga, þ.m.t. viðeigandi áætlanir um öryggisvitund í upplýsinga- og fjarskiptatækni og þjálfun í stafrænum rekstrarlegum viðnámsþrótti, sem um getur í 6. mgr. 13. gr., og færni í upplýsinga- og fjarskiptatækni fyrir allt starfsfólk,

h) samþykkja og endurskoða reglulega stefnu aðilans á fjármálamarkaði um tilhögun varðandi notkun upplýsinga- og fjarskiptatækniþjónustu sem þriðju aðilar veita,

i) koma á leiðum til skýrslugjafar innan fyrirtækisins svo að hægt sé að upplýsa stjórnina á viðeigandi hátt um eftirfarandi:

i. tilhögun sem samið er um við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu um notkun á upplýsinga- og fjarskiptatækniþjónustu,

ii. hvers kyns viðeigandi fyrirhugaðar efnislegar breytingar hvað varðar þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu,

iii. hugsanleg áhrif slíkra breytinga á nauðsynlega eða mikilvæga starfsemi sem fellur undir þessa tilhögun, þ.m.t. samantekt áhættugreiningar til að meta áhrif þessara breytinga, og a.m.k. alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og áhrif þeirra, sem og ráðstafanir til viðbragðs, endurreisnar og úrbóta.

3. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu koma á fót hlutverki til að fylgjast með ráðstöfunum sem samið er um við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu um notkun á upplýsinga- og fjarskiptatækniþjónustu, eða tilnefna fulltrúa í framkvæmdastjórn sem ábyrgan fyrir eftirliti með tengdri áhættu og viðeigandi skjölun.

4. Þeir sem sitja í stjórn og/eða framkvæmdastjórn aðila á fjármálamarkaði skulu á virkan hátt viðhalda þeirri þekkingu og færni sinni sem þarf til að skilja og meta upplýsinga- og fjarskiptatækniáhættu og áhrif hennar á starfsemi aðilans á fjármálamarkaði, þ.m.t. með því að sækja reglulega sérstaka þjálfun, í samræmi við þá upplýsinga- og fjarskiptatækniáhættu sem er stýrt.

II. þáttur

6. gr.

Áhættustýringarrammi í upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu hafa traustan, yfirgripsmikinn og vel skjalfestan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem hluta af heildaráhættustýringarkerfi sínu, sem gerir þeim kleift að bregðast við upplýsinga- og fjarskiptatækniáhættu á skjótan, skilvirkan og heildstæðan hátt og tryggja hátt stig stafræns rekstrarlegs viðnámsþróttar.

2. Áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni skal a.m.k. ná yfir stefnuáætlanir, stefnur og verklagsreglur, samskiptareglur (e. *protocols*) og búnað í upplýsinga- og fjarskiptatækni sem eru nauðsynleg til að vernda á tilhlýðilegan og fullnægjandi hátt allar upplýsingaeignir og upplýsinga- og fjarskiptatækneignir, þ.m.t. hugbúnað, vélbúnað, tölvuþjóna (e. *servers*), sem og til að vernda alla viðeigandi raunlæga þætti og innviði, s.s. athafnasvæði, gagnaver og viðkvæm, tilgreind svæði, til að tryggja að allar upplýsingaeignir og upplýsinga- og fjarskiptatækneignir séu nægilega verndaðar fyrir áhættu, þ.m.t. tjóni og óheimilum aðgangi eða notkun.

3. Aðilar á fjármálamarkaði skulu lágmarka áhrif upplýsinga- og fjarskiptatækniáhættu í samræmi við áhættustýringarramma sinn fyrir upplýsinga- og fjarskiptatækni með því að taka upp viðeigandi áætlanir, stefnur, verklagsreglur, samskiptareglur og búnað. Þær skulu veita lögbærum yfirvöldum fullnægjandi og uppfærðar upplýsingar um upplýsinga- og fjarskiptatækniáhættu og áhættustýringarrammann, samkvæmt beiðni.

4. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu fela eftirlitseiningu ábyrgð á stýringu og umsjón upplýsinga- og fjarskiptatækniáhættu og tryggja viðeigandi sjálfstæði slíkrar eftirlitseiningar til að forðast hagsmunaárekstra. Aðilar á fjármálamarkaði skulu tryggja viðeigandi aðgreiningu og sjálfstæði áhættustýringareininga, eftirlitseininga og innri endurskoðunar, samkvæmt líkaninu um þrjár varnarlínur eða líkani um innri áhættustýringu- og eftirlit.

5. Áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni skal skjalfestur og endurskoðaður a.m.k. einu sinni á ári, eða reglulega ef um er að ræða örfyrirtæki, sem og þegar alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eiga sér stað, og í kjölfar eftirlitsfyrirmæla eða niðurstaðna sem leiða af viðeigandi prófunum eða úttektarferlum á stafrænum rekstrarlegum viðnámsþrótti. Stöðugar endurbætur skulu gerðar á honum á grundvelli fengins lærdóms af framkvæmd og vöktun. Leggja skal skýrslu um endurskoðun á áhættustýringarramma í upplýsinga- og fjarskiptatækni fyrir lögbært yfirvald, sé þess óskað.

6. Áhættustýringarrammi aðila á fjármálamarkaði, annarra en örfyrirtækja, vegna upplýsinga- og fjarskiptatækni skal reglulega sæta innri úttekt endurskoðenda í samræmi við úttektaráætlun aðilans á fjármálamarkaði. Þessir endurskoðendur skulu búa yfir nægilegri þekkingu, hæfni og sérþekkingu varðandi upplýsinga- og fjarskiptatækniáhættu, sem og viðeigandi sjálfstæði. Tíðni og áhersla endurskoðana á sviði upplýsinga- og fjarskiptatækni skal vera í réttu hlutfalli við upplýsinga- og fjarskiptatækniáhættu aðila á fjármálamarkaði.

7. Á grundvelli niðurstaðna innri úttektar skulu aðilar á fjármálamarkaði koma á formlegu eftirfylgniferli, þ.m.t. reglum um tímanlega sannprófun og úrbætur á nauðsynlegum niðurstöðum úttekta á upplýsinga- og fjarskiptatækni.

8. Áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni skal innihalda stefnuáætlun um stafrænan rekstrarlegan viðnámsþrótt þar sem fram kemur hvernig ramminn skal innleiddur. Í því skyni skal áætlun um stafrænan rekstrarlegan viðnámsþrótt ná yfir aðferðir til að bregðast við upplýsinga- og fjarskiptatækniáhættu og ná sértækum markmiðum í upplýsinga- og fjarskiptatækni með því að:

a) skýra hvernig áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni styður við viðskiptaáætlun og -markmið aðilans á fjármálamarkaði,

b) ákvarða ásættanleg áhættuþolmörk upplýsinga- og fjarskiptatækniáhættu, í samræmi við áhættuvilja aðilans á fjármálamarkaði, og greina þolmörk fyrir raskanir á upplýsinga- og fjarskiptatækni,

c) setja fram skýr markmið um upplýsingaöryggi, þ.m.t. lykilárangursmælikvarða og lykiláhættumælistikur,

d) útskýra viðmið fyrir upplýsinga- og fjarskiptatæknihögun og hvers kyns breytingar sem þarf til að ná tilteknum viðskiptamarkmiðum,

e) gera grein fyrir mismunandi leiðum sem komið hefur verið á til að bera kennsl á atvik sem tengjast upplýsinga- og fjarskiptatækni, koma í veg fyrir áhrif af þeirra völdum og verjast þeim,

f) sýna fram á núverandi stöðu stafræns rekstrarlegs viðnámsþróttar á grundvelli fjölda tilkynntra alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni og skilvirkni forvarnarráðstafana,

g) innleiða prófanir á stafrænum rekstrarlegum viðnámsþrótti í samræmi við IV. kafla þessarar reglugerðar,

h) útlista samskiptaáætlun þegar um er að ræða atvik sem tengjast upplýsinga- og fjarskiptatækni sem eru tilkynningaskyld í samræmi við 14. gr.

9. Aðilar á fjármálamarkaði geta, í tengslum við áætlunina um stafrænan rekstrarlegan viðnámsþrótt sem um getur í 8. mgr., skilgreint heildræna fjölbreytileikastefnu m.t.t. seljenda í upplýsinga- og fjarskiptatækni, á samstæðustigi eða einingarstigi, þar sem fram kemur hvar þeir eru háðastir þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og rök færð fyrir þeirri blöndu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem notaðir eru.

10. Aðila á fjármálamarkaði er heimilt, í samræmi við lög Sambandsins og landsbundin sérlög, að útvista þeim verkefnum að sannreyna hlítni við kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu til fyrirtækja innan eða utan samstæðu. Komi til slíkrar útvistunar ber aðilinn á fjármálamarkaði áfram fulla ábyrgð á sannprófuninni á hlítni við kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu.

7. gr.

Upplýsinga- og fjarskiptatæknikerfi, samskiptareglur og búnaður

Til að takast á við og stýra upplýsinga- og fjarskiptatækniáhættu skulu aðilar á fjármálamarkaði nota og halda uppfærðum upplýsinga- og fjarskiptatæknikerfum, samskiptareglum og búnaði sem eru:

a) viðeigandi fyrir umfang aðgerða sem styðja rekstur á starfsemi þeirra, í samræmi við meðalhófsregluna eins og um getur í 4. gr.,

b) áreiðanleg,

c) búin nægilegri getu til að vinna rétt úr gögnum sem nauðsynleg eru til að sinna starfsemi og veita tímanlega þjónustu og til að ráða við álagstoppa beiðna, skeyta eða færslumagni, eftir því sem þörf krefur, þ.m.t. þegar ný tækni er innleidd,

d) með nægilega mikla tæknilega viðnámsgetu til að takast á fullnægjandi hátt á við auknar þarfir við vinnslu upplýsinga eins og krafist er við erfiðar markaðsaðstæður eða aðrar óhagstæðar aðstæður.

8. gr.

Auðkenning

1. Sem hluti af áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr. skulu aðilar á fjármálamarkaði greina, flokka og skjalfesta á viðunandi hátt alla starfsþætti, hlutverk og ábyrgðarsvið sem upplýsinga- og fjarskiptatækni styður við, upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir sem styðja við þessa starfsþætti og hlutverk þeirra og hæði í tengslum við upplýsinga- og fjarskiptatækniáhættu. Aðilar á fjármálamarkaði skulu endurskoða eftir þörfum og a.m.k. árlega hvort flokkunin og hvers kyns viðeigandi gögn séu fullnægjandi.

2. Aðilar á fjármálamarkaði skulu með viðvarandi hætti bera kennsl á allar uppsprettur upplýsinga- og fjarskiptatækniáhættu, einkum áhættu gagnvart og vegna annarra aðila á fjármálamarkaði, og meta netógnir og upplýsinga- og fjarskiptatækniveikleika sem varða upplýsinga- og fjarskiptatæknistudda starfsemi þeirra, upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir. Aðilar á fjármálamarkaði skulu reglulega, og a.m.k. árlega, endurmeta þær áhættusviðsmyndir sem hafa áhrif á þá.

3. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu gera áhættumat á öllum stórfelldum breytingum á innviðum net- og upplýsingakerfa, í ferlum eða verklagsreglum sem hafa áhrif á upplýsinga- og fjarskiptatæknistudda starfsemi þeirra, upplýsingaeignir eða upplýsinga- og fjarskiptatæknieignir.

4. Aðilar á fjármálamarkaði skulu tilgreina allar upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir, þ.m.t. þær sem eru staðsettar á fjartengdum starfsstöðvum, netbúnað og vélbúnað, og skulu kortleggja þau sem teljast mikilvæg. Þeir skulu kortleggja samskipan upplýsingaeignanna og upplýsinga- og fjarskiptatæknieignanna og tengsl og innbyrðis hæði milli mismunandi upplýsingaeigna og upplýsinga- og fjarskiptatæknieigna.

5. Aðilar á fjármálamarkaði skulu greina og skjalfesta öll ferli sem eru háð þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og greina samtengingar við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

6. Að því er varðar 1., 4. og 5. mgr. skulu aðilar á fjármálamarkaði halda viðeigandi skrár og uppfæra þær reglulega og í hvert sinn sem stórfelldar breytingar, eins og um getur í 3. mgr., eiga sér stað.

7. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu reglulega og a.m.k. árlega gera sérstakt áhættumat í tengslum við upplýsinga- og fjarskiptatækni á öllum fornkerfum í upplýsinga- og fjarskiptatækni og í öllum tilvikum fyrir og eftir tengingu tækni, hugbúnaðar eða kerfa.

9. gr.

Verndun og forvarnir

1. Til að vernda upplýsinga- og fjarskiptatæknikerfi með fullnægjandi hætti og skipuleggja viðbragðsráðstafanir skulu aðilar á fjármálamarkaði stöðugt vakta og hafa eftirlit með öryggi og virkni upplýsinga- og fjarskiptatæknikerfa og -búnaðar og lágmarka áhrif upplýsinga- og fjarskiptatækniáhættu á upplýsinga- og fjarskiptatæknikerfi með því að innleiða viðeigandi öryggisbúnað, stefnur og verklagsreglur.

2. Aðilar á fjármálamarkaði skulu hanna, afla og innleiða öryggisstefnur, verklagsreglur, samskiptareglur og búnað fyrir upplýsinga- og fjarskiptatækni, sem miða að því að tryggja viðnámsþrótt, samfellu og aðgengileika upplýsinga- og fjarskiptatæknikerfa, einkum þeirra sem styðja við nauðsynlega eða mikilvæga starfsemi, og viðhalda ströngum kröfum um tiltækileika, ósvikni, réttleika eða leynd gagna, hvort sem þau eru í geymslu, notkun eða flutningi.

3. Til að ná þeim markmiðum sem um getur í 2. mgr. skulu aðilar á fjármálamarkaði nota viðeigandi upplýsinga- og fjarskiptatæknilausnir og -ferli í samræmi við 4. gr. Þessar upplýsinga- og fjarskiptatæknilausnir og -ferli skulu:

a) tryggja öryggi gagnaflutningsleiða,

b) lágmarka hættu á spillingu eða tapi á gögnum, óheimilum aðgangi og tæknilegum annmörkum sem geta hindrað starfsemi,

c) koma í veg fyrir skerðingu á tiltækileika, ósvikni og réttleika, brot á leynd og tap á gögnum,

d) tryggja að gögn séu varin fyrir áhættu sem stafar af gagnastjórnun, þ.m.t. ófullnægjandi umsýslu, áhættu í tengslum við vinnslu og mannlegum mistökum.

4. Aðilar á fjármálamarkaði skulu, sem hluti af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr.:

a) þróa og skjalfesta stefnu um upplýsingaöryggi þar sem skilgreindar eru reglur til að vernda tiltækileika, ósvikni, réttleika og leynd gagna, upplýsingaeigna og upplýsinga- og fjarskiptatæknieigna, þ.m.t. í eigu viðskiptavina þeirra, eftir atvikum,

b) koma á traustum net- og innviðastjórnunarháttum með áhættumiðaðri nálgun, með því að nota viðeigandi tækni, aðferðir og samskiptareglur sem geta falið í sér að koma á sjálfvirkum kerfum til að einangra upplýsingaeignir sem verða fyrir áhrifum, komi til netárása,

c) framfylgja stefnum sem takmarka raunlægan eða röklegan aðgang að upplýsingaeignum og upplýsinga- og fjarskiptatæknieignum við eingöngu það sem nauðsynlegt er fyrir lögmæta og samþykkta starfsemi og aðgerðir og koma í því skyni á stefnum, verklagsreglum og stýringum sem taka á aðgangsrétti og tryggja trausta aðgangsstjórnun,

d) innleiða stefnur og samskiptareglur fyrir traust sannvottunarferli, sem byggjast á viðeigandi stöðlum og sérhæfðum stjórnkerfum, og verndarráðstafanir fyrir dulkóðunarlykla þannig að gögn séu dulkóðuð á grundvelli niðurstaðna samþykkts gagnaflokkunar- og matferlis að því er varðar upplýsinga- og fjarskiptatækniáhættu,

e) innleiða skjalfestar stefnur, verklagsreglur og stýringar vegna breytingastjórnunar í upplýsinga- og fjarskiptatækni, þ.m.t. breytingar á hugbúnaði, vélbúnaði, fastbúnaðarhlutum (*e. firmware components*), kerfum eða öryggisstillingum sem byggjast á áhættumatsaðferð og eru óaðskiljanlegur hluti af heildarferli aðila á fjármálamarkaði við breytingastjórnun, til að tryggja að allar breytingar á upplýsinga- og fjarskiptatæknikerfum séu skráðar, prófaðar, metnar, samþykktar, innleiddar og sannprófaðar á stýrðan hátt,

f) hafa viðeigandi og ítarlega skjalfestar stefnur um bætur og uppfærslur.

Að því er varðar b-lið fyrstu undirgreinar skulu aðilar á fjármálamarkaði hanna innviði fyrir nettengingar með þeim hætti að hægt sé að rjúfa þær samstundis eða aðgreina til að lágmarka og koma í veg fyrir smitáhrif, einkum að því er varðar samtengda fjármálaferla.

Að því er varðar e-lið fyrstu undirgreinar skal breytingastjórnunarferli í upplýsinga- og fjarskiptatækni samþykkt af viðeigandi stjórnunarstigum og fylgja sértækum samskiptareglur.

10. gr.

Greining

1. Aðilar á fjármálamarkaði skulu hafa til staðar leiðir til að greina óvenjulegar athafnir án tafar í samræmi við 17. gr., þ.m.t. vandamál sem varða afköst upplýsinga- og fjarskiptatækninets og atvik sem tengjast upplýsinga- og fjarskiptatækni og til að greina hugsanlegan veigamikinn stakan bilanapunkt (e. *material single point of failure*).

Prófa skal reglulega allar greiningarleiðir sem um getur í fyrstu undirgrein í samræmi við 25. gr.

2. Greiningarleiðirnar sem um getur í 1. mgr. skulu leyfa marglaga stýringu, skilgreina viðvörunarmörk og viðmiðanir til að virkja og hefja viðbragðsferli við atvikum sem tengjast upplýsinga- og fjarskiptatækni, þ.m.t. sjálfvirk viðvörunarkerfi fyrir viðeigandi starfsfólk sem ber ábyrgð á viðbrögðum við atvikum sem tengjast upplýsinga- og fjarskiptatækni.

3. Aðilar á fjármálamarkaði skulu verja nægum tilföngum og getu til að fylgjast með athöfnum notenda, frávikum í upplýsinga- og fjarskiptatækni og atvikum sem tengjast henni, einkum netárásum.

4. Veitendur gagnaskýrsluþjónustu skulu auk þess hafa kerfi sem geta á skilvirkan hátt greint heilleika viðskiptaskýrslna, hvort upplýsingar vanti og augljósar villur og farið fram á að skýrslurnar séu endursendar.

11. gr.

Viðbrögð og endurreisn

1. Sem hluta af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr. 6. gr., og á grundvelli greiningarkrafnanna sem settar eru fram í 8. gr. skulu aðilar á fjármálamarkaði setja fram heildstæða stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem hægt er að samþykkja sem sértæka stefnu sem myndar órjúfanlegan þátt af heildarstefnu aðilans á fjármálamarkaði um rekstrarsamfellu.

2. Aðilar á fjármálamarkaði skulu innleiða stefnuna um rekstrarsamfellu í upplýsinga- og fjarskiptatækni með sérhæfðum, viðeigandi og skjalfestum ráðstöfunum, áætlunum, verklagsreglum og fyrirkomulagi sem miða að því að:

a) tryggja samfellu í nauðsynlegri eða mikilvægri starfsemi aðila á fjármálamarkaði,

b) bregðast skjótt, á viðeigandi og skilvirkan hátt við öllum atvikum sem tengjast upplýsinga- og fjarskiptatækni og vinna úr þeim með þeim hætti að takmarka skaða og setja í forgang að hefja aftur starfsemi og endurreisnaraðgerðir,

c) virkja án tafar sérhæfðar áætlanir sem gera kleift að beita afmörkunarráðstöfunum, ferlum og tækniþekkingu sem henta sérhverri tegund atviks í upplýsinga- og fjarskiptatækni og koma í veg fyrir frekari skaða, sem og sérsniðið verklag um viðbragð og endurreisn sem komið er á í samræmi við 12. gr.,

d) leggja frummat á áhrif, skaða og tap,

e) setja fram aðgerðir varðandi samskipti og krísustjórnun sem tryggja að uppfærðar upplýsingar séu sendar öllu viðeigandi starfsfólki og ytri hagsmunaaðilum í samræmi við 14. gr. og gefa lögbærum yfirvöldum skýrslu í samræmi við 19. gr.

3. Sem hluta af áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr. skulu aðilar á fjármálamarkaði innleiða viðeigandi viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni sem, ef um aðra aðila á fjármálamarkaði en örfyrirtæki er að ræða, lúta úttektum frá óháðri innri endurskoðun.

4. Aðilar á fjármálamarkaði skulu koma á, viðhalda og prófa reglulega viðeigandi áætlanir um rekstrarsamfellu í upplýsinga- og fjarskiptatækni, einkum með tilliti til nauðsynlegrar eða mikilvægrar starfsemi sem er útvistað til eða framkvæmd samkvæmt samningi við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

5. Sem hluta af heildarstefnunni um rekstrarsamfellu skulu aðilar á fjármálamarkaði gera rekstraráhrifagreiningu m.t.t. útsetningar fyrir meiriháttar rekstrarröskunum. Með rekstraráhrifagreiningunni skulu aðilar á fjármálamarkaði leggja mat á möguleg áhrif meiriháttar rekstrarraskana með megindlegum og eigindlegum viðmiðum og nota til þess innri og ytri gögn og sviðsmyndagreiningar, eins og við á. Í rekstraráhrifagreiningunni skal taka tillit til mikilvægis skilgreindrar og kortlagðrar viðskiptastarfsemi, stuðningsferla, hæðis við þriðju aðila og upplýsingaeignir og innbyrðis tengsl þeirra. Aðilar á fjármálamarkaði skulu tryggja að upplýsinga- og fjarskiptatæknieignir og -þjónusta séu hannaðar og notaðar í fullu samræmi við rekstraráhrifagreininguna, einkum að því er varðar að tryggja viðnámsþol allra nauðsynlegra eininga.

6. Aðilar á fjármálamarkaði skulu, sem hluti af alhliða stýringu sinni á upplýsinga- og fjarskiptatækniáhættu:

a) prófa áætlanir um rekstrarsamfellu í upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlanir í tengslum við upplýsinga- og fjarskiptatæknikerfi sem styðja alla starfsemi a.m.k. árlega, sem og ef gerðar eru verulegar breytingar á upplýsinga- og fjarskiptatæknikerfum sem styðja við nauðsynlega eða mikilvæga starfsemi,

b) prófa krísusamskiptaáætlanir sem eru gerðar í samræmi við 14. gr.

Að því er varðar a-lið fyrstu undirgreinar skulu aðilar á fjármálamarkaði, aðrir en örfyrirtæki, hafa sem hluta af prófunaráætlunum sínum sviðsmyndir netárása og flutnings vinnslu frá aðalinnviði upplýsinga- og fjarskiptatækni yfir á varainnvið, öryggisafrit og varakerfi sem nauðsynleg eru til að uppfylla skuldbindingarnar sem settar eru fram í 12. gr.

Aðilar á fjármálamarkaði skulu reglulega endurskoða stefnu sína um rekstrarsamfellu í upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni, að teknu tilliti til niðurstaðna prófana sem gerðar eru í samræmi við fyrstu undirgrein og tilmæla í kjölfar úttekta endurskoðenda eða eftirlitsyfirvalds.

7. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu hafa krísustjórnunarteymi sem, ef áætlun þeirra um rekstrarsamfellu í upplýsinga- og fjarskiptatækni eða viðbragðs- og endurreisnaráætlanir eru virkjaðar, skal m.a. setja fram skýrar verklagsreglur til að stjórna krísusamskiptum innan og utan fyrirtækis í samræmi við 14. gr.

8. Aðilar á fjármálamarkaði skulu halda aðgengilegar skrár yfir aðgerðir fyrir og meðan á atburði sem veldur röskun stendur þegar áætlanir þeirra um rekstrarsamfellu og viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni eru virkjaðar.

9. Verðbréfamiðstöðvar skulu láta lögbærum yfirvöldum í té afrit af niðurstöðum prófana á rekstrarsamfellu upplýsinga- og fjarskiptatækni eða samsvarandi æfinga.

10. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu gefa lögbærum yfirvöldum skýrslu, að beiðni þeirra, um mat á samanlögðum árlegum kostnaði og tapi af völdum alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni.

11. Í samræmi við 16. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010, skulu evrópsku eftirlitsstofnanirnar, fyrir milligöngu sameiginlegu nefndarinnar, eigi síðar en 17. júlí 2024 semja sameiginlegar viðmiðunarreglur um mat á samanlögðum árlegum kostnaði og tapi sem um getur í 10. mgr.

12. gr.

Stefnur og verklag við öryggisafritun, verklag og aðferðir við endurheimt og endurreisn

1. Til að tryggja endurheimt upplýsinga- og fjarskiptatæknikerfa og gagna með lágmarks niðritíma, takmarkaðri röskun og tapi, sem hluta af áhættustýringarramma þeirra í upplýsinga- og fjarskiptatækni, skulu aðilar á fjármálamarkaði útfæra og skjalfesta:

a) stefnur og verklag um öryggisafritun sem tilgreina umfang gagnanna sem falla undir öryggisafritun og lágmarkstíðni öryggisafritunar sem byggist á mikilvægi upplýsinga eða trúnaðarstigi gagna,

b) verklag og aðferðir við endurheimt og endurreisn.

2. Aðilar á fjármálamarkaði skulu setja upp öryggisafritunarkerfi sem hægt er að virkja í samræmi við stefnur og verklag við öryggisafritun, sem og verklag og aðferðir við endurheimt og endurreisn. Virkjun öryggisafritunarkerfa skal ekki stefna öryggi net- og upplýsingakerfa eða tiltækileika, ósvikni, réttleika eða leynd gagna í hættu á neinn hátt. Reglulega skal prófa verklag við öryggisafritun og verklag og aðferðir við endurheimt og endurreisn.

3. Við endurheimt öryggisafritunargagna með eigin kerfum skulu aðilar á fjármálamarkaði nota upplýsinga- og fjarskiptatæknikerfi sem eru einangruð frá frumupplýsinga- og fjarskiptatæknikerfinu á raunlægan og röklegan hátt. Upplýsinga- og fjarskiptatæknikerfin skulu vera tryggilega varin fyrir óheimilum aðgangi eða spillingu í upplýsinga- og fjarskiptatækni og gera kleift að endurreisa þjónustu tímanlega með nýtingu öryggisafrita gagna og kerfa eins og til þarf.

Að því er varðar miðlæga mótaðila skulu endurreisnaráætlanirnar gera kleift að endurheimta allar færslur frá þeim tíma sem röskun átti sér stað til að miðlægi mótaðilinn geti haldið starfsemi áfram af öryggi og lokið uppgjöri á áætluðum degi.

Veitandi gagnaskýrsluþjónustu skal auk þess hafa yfir að ráða nægum tilföngum og öryggisafritunar- og endurheimtarkerfi til að geta ávallt boðið og viðhaldið þjónustu sinni.

4. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu viðhalda umframgetu í upplýsinga- og fjarskiptatækni með tilföngum, getu og starfsþáttum sem eru fullnægjandi til að tryggja viðskiptaþarfir. Örfyrirtæki skulu leggja mat á þörfina á að viðhalda varaupplýsinga- og fjarskiptatæknikerfum með hliðsjón af áhættusniði sínu.

5. Verðbréfamiðstöðvar skulu hafa a.m.k. einn viðbótarvinnslustað sem hefur yfir að ráða fullnægjandi tilföngum, getu, starfsþáttum og starfsmannafyrirkomulagi til að tryggja viðskiptaþarfir.

Viðbótarvinnslustaðurinn skal vera:

a) staðsettur í landfræðilegri fjarlægð frá aðalvinnslustað til að tryggja að hann hafi annað áhættusnið og til að koma í veg fyrir að hann verði fyrir áhrifum af atburði sem hefur haft áhrif á aðalvinnslustaðinn,

b) fær um að tryggja samfellu í nauðsynlegri eða mikilvægri starfsemi á sama hátt og á aðalvinnslustaðnum eða veitt nauðsynlegt þjónustustig til að tryggja að aðili á fjármálamarkaði sinni mikilvægri starfsemi sinni innan markmiða um endurreisn,

c) tafarlaust aðgengilegur starfsfólki viðkomandi aðila á fjármálamarkaði til að tryggja samfellu í nauðsynlegri eða mikilvægri starfsemi ef aðalvinnslustaður verður óaðgengilegur.

6. Við ákvörðun á markmiðum um endurreisnartíma og endamark endurheimtar fyrir hvern starfsþátt skulu aðilar á fjármálamarkaði taka tillit til þess hvort hann teljist nauðsynleg eða mikilvæg starfsemi og mögulegra heildaráhrifa á skilvirkni markaðarins. Slík tímamarkmið skulu tryggja að við óvenjulegar aðstæður sé samþykktu þjónustustigi náð.

7. Við endurreisn eftir atvik sem tengist upplýsinga- og fjarskiptatækni skulu aðilar á fjármálamarkaði framkvæma nauðsynlegar athuganir, þ.m.t. margþátta athuganir og afstemmingar, til að tryggja áfram hæsta stig heilleika gagna. Einnig skal framkvæma þessar athuganir þegar gögn frá ytri hagsmunaaðilum eru endurgerð til að tryggja að öll gögn séu í samræmi milli kerfa.

13. gr.

Lærdómur og þróun

1. Aðilar á fjármálamarkaði skulu hafa yfir að ráða getu og starfsfólki til að safna upplýsingum um veikleika og netógnir, atvik sem tengjast upplýsinga- og fjarskiptatækni, einkum netárásir, og greina líkleg áhrif þeirra á stafrænan rekstrarlegan viðnámsþrótt.

2. Aðilar á fjármálamarkaði skulu koma á greiningarferli fyrir atvik sem tengjast upplýsinga- og fjarskiptatækni í kjölfar þess að alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni raskar kjarnastarfsemi þeirra, greina orsakir raskana og bera kennsl á nauðsynlegar úrbætur á upplýsinga- og fjarskiptatæknirekstrinum eða innan stefnunnar um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem um getur í 11. gr.

Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu, sé þess óskað, tilkynna lögbærum yfirvöldum um breytingar sem gerðar eru í kjölfar greiningar á atvikum sem tengjast upplýsinga- og fjarskiptatækni, eins og um getur í fyrstu undirgrein.

Við greiningu í kjölfar atviks sem tengist upplýsinga- og fjarskiptatækni sem um getur í fyrstu undirgrein skal ákvarðað hvort farið hafi verið að settum verklagsreglum og þær aðgerðir sem gripið var til hafi verið skilvirkar, þ.m.t. í tengslum við eftirfarandi:

a) hversu skjótt brugðist var við öryggisviðvörunum og metin áhrif af atvikum sem tengjast upplýsinga- og fjarskiptatækni og alvarleiki þeirra,

b) gæði og hraða á framkvæmd réttarfræðilegrar greiningar, eftir því sem við á,

c) skilvirkni stigmögnunar viðbragða við atviki innan viðkomandi aðila á fjármálamarkaði,

d) skilvirkni í innri og ytri samskiptum.

3. Sá lærdómur sem dreginn er af prófun á stafrænum rekstrarlegum viðnámsþrótti sem framkvæmd er í samræmi við 26. og 27. gr. og af raungerðum atvikum sem tengjast fjarskipta- og upplýsingatækni, einkum netárásum, ásamt áskorunum sem blasað hafa við þegar komið hefur til virkjunar áætlana um rekstrarsamfellu í upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlana í upplýsinga- og fjarskiptatækni, ásamt viðeigandi upplýsingum sem skipst er á við mótaðila og metnar eru við úttektir eftirlitsyfirvalda, skal jafnóðum felldur inn í matsferli upplýsinga- og fjarskiptatækniáhættu. Þessar niðurstöður skulu mynda grundvöll fyrir viðeigandi endurskoðun á viðkomandi þáttum í áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr.

4. Aðilar á fjármálamarkaði skulu vakta skilvirkni í framkvæmd stefnuáætlunar um stafrænan rekstrarlegan viðnámsþrótt sinn sem sett er fram í 8. mgr. 6. gr. Þeir skulu kortleggja þróun upplýsinga- og fjarskiptatækniáhættu til lengri tíma, greina tíðni, tegundir, umfang og þróun atvika sem tengjast upplýsinga- og fjarskiptatækni, einkum netárásir og mynstur þeirra, með það í huga að skilja hve útsettir þeir eru fyrir upplýsinga- og fjarskiptatækniáhættu, einkum í tengslum við nauðsynlega eða mikilvæga starfsemi, og efla stafrænan þroska og viðbúnað viðkomandi aðila á fjármálamarkaði.

5. Háttsett starfsfólk á sviði upplýsinga- og fjarskiptatækni skal gefa stjórn og/eða framkvæmdastjórn skýrslu a.m.k. árlega um niðurstöðurnar sem um getur í 3. mgr. og leggja fram ráðleggingar.

6. Aðilar á fjármálamarkaði skulu þróa áætlanir um öryggisvitund í upplýsinga- og fjarskiptatækni og þjálfun í stafrænum rekstrarlegum viðnámsþrótti sem skyldubundinn hluta af þjálfunaráætlunum sínum fyrir starfsfólk. Þessar áætlanir og þjálfun skulu gilda um allt starfsfólk og yfirstjórnendur og hafa flækjustig sem samsvarar verkefnum þeirra. Aðilar á fjármálamarkaði skulu, eftir því sem við á, einnig fella þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu inn í viðeigandi þjálfunaráætlun sína í samræmi við i-lið 2. mgr. 30. gr.

7. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu vakta viðeigandi tæknilega framþróun með viðvarandi hætti, einnig með það í huga að skilja hugsanleg áhrif af nýtingu slíkrar nýrrar tækni á öryggiskröfur fyrir upplýsinga- og fjarskiptatækni og stafrænan rekstrarlegan viðnámsþrótt. Þær skulu halda í við nýjustu áhættustýringaraðferðir í upplýsinga- og fjarskiptatækni til að berjast með skilvirkum hætti gegn yfirstandandi eða nýjum tegundum netárása.

14. gr.

Samskipti

1. Aðilar á fjármálamarkaði skulu, sem hluti af áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr., hafa krísusamskiptaáætlanir sem gera kleift að upplýsa viðskiptavini og mótaðila, sem og almenning, á ábyrgan hátt um a.m.k. alvarleg atvik eða veikleika sem tengjast upplýsinga- og fjarskiptatækni, eins og við á.

2. Aðilar á fjármálamarkaði skulu, sem hluta af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, innleiða samskiptastefnur fyrir starfsfólk og ytri hagsmunaaðila. Í samskiptastefnum fyrir starfsfólk skal taka tillit til þarfarinnar á að gera greinarmun á starfsfólki sem tekur þátt að stýra upplýsinga- og fjarskiptatækniáhættu, einkum því starfsfólki sem ber ábyrgð á viðbrögðum og endurreisn og starfsfólki sem þarf að fá upplýsingar.

3. Að minnsta kosti einum einstaklingi innan aðilans á fjármálamarkaði skal falið að innleiða samskiptaáætlun vegna atvika sem tengjast upplýsinga- og fjarskiptatækni og sinna því hlutverki að upplýsa almenning og fjölmiðla í þeim tilgangi.

15. gr.

Frekari samhæfing búnaðar, aðferða, ferla og stefna til stýringar á upplýsinga- og fjarskiptatækniáhættu

Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og í samráði við Netöryggisstofnun Evrópusambandsins, semja sameiginleg drög að tæknilegum eftirlitsstöðlum til að:

a) tilgreina frekari þætti sem skulu koma fram í öryggisstefnum, verklagsreglum, samskiptareglum og búnaði í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr., með það í huga að tryggja öryggi netkerfa, gera fullnægjandi verndarráðstafanir gegn innbrotum og gagnamisnotkun, viðhalda tiltækileika, ósvikni, réttleika eða leynd gagna, þ.m.t. dulkóðunaraðferðir, og tryggja nákvæma og skjótar gagnasendingar án verulegra raskana og ótilhlýðilegra tafa,

b) útfæra fleiri þætti í eftirliti með aðgangsstjórnunarréttindum sem um getur í c-lið 4. mgr. 9. gr. og tengdri mannauðsstefnu þar sem tilgreindar eru aðgangsheimildir, verklagsreglur um veitingu og afturköllun heimilda, eftirlit með óeðlilegri hegðun í tengslum við upplýsinga- og fjarskiptatækniáhættu með viðeigandi vísum, þ.m.t. fyrir netnotkunarmynstur, notkunartíma, upplýsingatækniathafnir og óþekkt tæki,

c) útfæra frekar leiðirnar sem tilgreindar eru í 1. mgr. 10. gr. og gera kleift að greina fljótt óvenjulegar athafnir og viðmiðanirnar sem settar eru fram í 2. mgr. 10. gr. til virkjunar greiningar- og viðbragðsferla vegna atvika í tengslum við upplýsinga- og fjarskiptatækni,

d) tilgreina nánar þá þætti stefnunnar um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 11. gr.,

e) tilgreina nánar prófanir á áætlunum um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem um getur í 6. mgr. 11. gr. til að tryggja að slík prófun taki tilhlýðilegt tillit til sviðsmynda þar sem gæði veitingar nauðsynlegrar eða mikilvægrar starfsemi minnka niður að óviðunandi marki eða bregðast og taka tilhlýðilegt tillit til hugsanlegra áhrifa af ógjaldfærni eða öðrum misbrestum viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og, ef við á, stjórnmálaáhættu í lögsögu viðkomandi veitenda,

f) tilgreina nánar þá þætti í viðbragðs- og endurreisnaráætlunum í upplýsinga- og fjarskiptatækni sem um getur í 3. mgr. 11. gr.,

g) tilgreina nánar innihald og snið skýrslunnar um endurskoðun á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 5. mgr. 6. gr.

Við gerð þessara draga að tæknilegum eftirlitsstöðlum skulu evrópsku eftirlitsstofnanirnar taka tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði, sem og eðlis, umfangs og flækjustigs þjónustu hans, starfsemi og reksturs, að teknu tilhlýðilegu tilliti til hvers kyns sérkenna sem stafa af sérstöku eðli starfseminnar þvert á ólíka fjármálaþjónustugeira.

Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. janúar 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í fyrstu málsgrein í samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

16. gr.

Einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni

1. Ákvæði 5.–15. gr. þessarar reglugerðar gilda ekki um lítil og ótengd verðbréfafyrirtæki, greiðslustofnanir sem eru undanþegnar samkvæmt tilskipun (ESB) 2015/2366, stofnanir sem eru undanþegnar samkvæmt tilskipun 2013/36/ESB og aðildarríkin hafa ákveðið að beita ekki valkostinum á, sem um getur í 4. mgr. 2. gr. þessarar reglugerðar, rafeyrisfyrirtæki sem eru undanþegin samkvæmt tilskipun 2009/110/EB og litlar stofnanir um starfstengdan lífeyri.

Með fyrirvara um fyrstu undirgrein skulu þeir aðilar sem taldir eru upp í fyrstu undirgrein:

a) koma á og viðhalda traustum og skjalfestum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem lýsir ítarlega fyrirkomulagi og ráðstöfunum sem miða að skjótvirkri, skilvirkri og alhliða stýringu upplýsinga- og fjarskiptatækniáhættu, þ.m.t. til að vernda viðeigandi raunlæga þætti og innviði,

b) fylgjast stöðugt með öryggi og virkni allra upplýsinga- og fjarskiptatæknikerfa,

c) lágmarka áhrif upplýsinga- og fjarskiptatækniáhættu með því að nota traust, öflug og uppfærð upplýsinga- og fjarskiptakerfi, samskiptareglur og búnað sem eru viðeigandi til að styðja afkastagetu starfsemi þeirra og veitingu þjónustu og vernda með fullnægjandi hætti tiltækileika, ósvikni, réttleika eða leynd gagna í net- og upplýsingakerfum,

d) gera kleift að bera án tafar kennsl á og greina uppruna upplýsinga- og fjarskiptatækniáhættu og -frávika í net- og upplýsingakerfum og bregðast skjótt við atvikum sem tengjast upplýsinga- og fjarskiptatækni,

e) greina áhrifamesta hæði gagnvart þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,

f) tryggja samfellu í nauðsynlegri eða mikilvægri starfsemi með áætlunum um rekstrarsamfellu og viðbragðs- og endurreisnarráðstöfunum sem taka a.m.k. til ráðstafana til öryggisafritunar og endurheimtar,

g) prófa reglulega áætlanir og ráðstafanir sem um getur í f-lið, sem og skilvirkni þeirra stýringa sem innleiddar eru í samræmi við a- og c-lið,

h) innleiða, eins og við á, viðeigandi niðurstöður varðandi rekstur, sem koma út úr prófununum sem um getur í g-lið og atvikagreiningu, inn í matsferli á upplýsinga- og fjarskiptatækniáhættu og útfæra öryggisvitundaráætlanir fyrir upplýsinga- og fjarskiptatækni og þjálfun í stafrænum rekstrarlegum viðnámsþrótti fyrir starfsfólk og stjórnendur í samræmi við þarfir og áhættusnið upplýsinga- og fjarskiptatækni.

2. Áhættustýringarramminn fyrir upplýsinga- og fjarskiptatækni sem um getur í a-lið annarrar undirgreinar 1. mgr. skal skjalfestur og yfirfarinn reglulega og í kjölfar alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni, í samræmi við eftirlitsfyrirmæli. Stöðugar endurbætur skulu gerðar á honum á grundvelli fengins lærdóms af framkvæmd og vöktun. Leggja skal skýrslu um endurskoðun á áhættustýringarramma í upplýsinga- og fjarskiptatækni fyrir lögbært yfirvald, sé þess óskað.

3. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og í samráði við Netöryggisstofnun Evrópusambandsins, semja sameiginleg drög að tæknilegum eftirlitsstöðlum til að:

a) tilgreina nánar þá þætti sem skulu vera innan rammans um áhættustýringu í upplýsinga- og fjarskiptatækni og um getur í a-lið annarrar undirgreinar 1. mgr.,

b) tilgreina nánar þá þætti í tengslum við kerfi, samskiptareglur og búnað til að lágmarka áhrif af upplýsinga- og fjarskiptatækniáhættu, sem um getur í c-lið annarrar undirgreinar 1. mgr., með það að markmiði að tryggja öryggi neta, gera fullnægjandi verndarráðstafanir gegn innbrotum og gagnamisnotkun og varðveita tiltækileika, ósvikni, réttleika eða leynd gagna,

c) tilgreina nánar þá þætti í áætluninni um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem um getur í f-lið annarrar undirgreinar 1. mgr.,

d) tilgreina nánar reglur um prófanir á áætlunum um rekstrarsamfellu og tryggja skilvirkni stýringa sem um getur í g-lið annarrar undirgreinar 1. mgr. og tryggja að slík prófun taki tilhlýðilegt tillit til sviðsmynda þar sem gæði í veitingu nauðsynlegrar eða mikilvægrar starfsemi minnka niður að óviðunandi marki eða bregðast,

e) tilgreina nánar efni og snið skýrslunnar um yfirferð á ramma um áhættustýringu í upplýsinga- og fjarskiptatækni sem um getur í 2. mgr.

Við gerð þessara draga að tæknilegum eftirlitsstöðlum skulu evrópsku eftirlitsstofnanirnar taka tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði og eðlis, umfangs og flækjustigs þjónustu hans, starfsemi og reksturs.

Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. janúar 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í fyrstu undirgrein í samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

III. KAFLI

Atvikastjórnun, flokkun og skýrslugjöf í tengslum við upplýsinga- og fjarskiptatækni

17. gr.

Atvikastjórnunarferli sem tengist upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu skilgreina, koma á og innleiða atvikastjórnunarferli í tengslum við upplýsinga- og fjarskiptatækni til að greina, meðhöndla og tilkynna um atvik sem tengjast upplýsinga- og fjarskiptatækni.

2. Aðilar á fjármálamarkaði skulu skrá öll atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegar netógnir. Aðilar á fjármálamarkaði skulu koma á viðeigandi verklagsreglum og ferlum til að tryggja samræmda og samþætta vöktun, meðhöndlun og eftirfylgni atvika sem tengjast upplýsinga- og fjarskiptatækni til að tryggja að borið sé kennsl á frumorsakir, þær skráðar og á þeim tekið til að koma í veg fyrir að slík atvik eigi sér stað.

3. Í stjórnunarferli upplýsinga- og fjarskiptatæknitengdra atvika sem um getur í 1. mgr. skal:

a) setja upp snemmbæra viðvörunarvísa,

b) koma á verklagsreglum til að bera kennsl á, rekja, skrá, flokka og draga í dilka atvik sem tengjast upplýsinga- og fjarskiptatækni samkvæmt forgangsröð þeirra og alvarleika og eftir mikilvægi þeirrar þjónustu sem verður fyrir áhrifum, í samræmi við viðmiðanirnar sem settar eru fram í 1. mgr. 18. gr.,

c) tilnefna hlutverk og ábyrgðarsvið sem þarf að virkja fyrir mismunandi tegundir atvika og sviðsmynda sem tengjast upplýsinga- og fjarskiptatækni,

d) setja fram áætlanir um samskipti við starfsfólk, ytri hagsmunaaðila og fjölmiðla í samræmi við 14. gr. og um tilkynningar til viðskiptavina, áætlanir um stigmögnun viðbragða innan fyrirtækisins, þ.m.t. kvartanir viðskiptavina sem tengjast upplýsinga- og fjarskiptatækni, og um miðlun upplýsinga til aðila á fjármálamarkaði sem gegna hlutverki mótaðila, eins og við á,

e) tryggja að a.m.k. alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni séu tilkynnt til viðkomandi framkvæmdastjórnar og upplýsa stjórn og/eða framkvæmdastjórn um a.m.k. alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni, útskýra áhrif, viðbrögð og viðbótarstýringar sem koma þarf á fót í kjölfar slíkra atvika sem tengjast upplýsinga- og fjarskiptatækni,

f) koma á verklagsreglum um viðbrögð við atvikum sem tengjast upplýsinga- og fjarskiptatækni til að draga úr áhrifum og tryggja að þjónusta verði starfhæf og örugg innan ásættanlegs tíma.

18. gr.

Flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum

1. Aðilar á fjármálamarkaði skulu flokka atvik sem tengjast upplýsinga- og fjarskiptatækni og skilgreina áhrif þeirra í samræmi við eftirfarandi viðmiðanir:

a) fjölda og/eða mikilvægi viðskiptavina eða fjárhagslegra mótaðila sem verða fyrir áhrifum og, eftir atvikum, fjárhæð eða fjölda viðskipta sem atvik sem tengist upplýsinga- og fjarskiptatækni hefur áhrif á og hvort það hafi haft áhrif á orðspor,

b) tímalengd atviks sem tengist upplýsinga- og fjarskiptatækni, þ.m.t. niðritími þjónustu,

c) landfræðilega dreifingu með tilliti til svæða sem atvik sem tengist upplýsinga- og fjarskiptatækni hefur áhrif á, einkum ef það hefur áhrif á fleiri en tvö aðildarríki,

d) gagnatap sem atvik sem tengist upplýsinga- og fjarskiptatækni hefur í för með sér varðandi tiltækileika, ósvikni, réttleika eða leynd gagna,

e) hve mikilvæg þjónustan er sem verður fyrir áhrifum, þ.m.t. viðskipti og rekstur aðila á fjármálamarkaði,

f) efnahagsleg áhrif af atviki sem tengist upplýsinga- og fjarskiptatækni, einkum beinan og óbeinan kostnað og tjón, bæði í algildum og hlutfallslegum skilningi.

2. Aðilar á fjármálamarkaði skulu flokka netógnir sem verulegar á grundvelli mikilvægis þeirrar þjónustu er sem er í hættu, þ.m.t. viðskipta og starfsemi aðila á fjármálamarkaði, fjölda og/eða mikilvægi markhópa viðskiptavina eða fjárhagslegra mótaðila og landfræðilegrar dreifingar svæða þar sem áhætta er fyrir hendi.

3. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og í samráði við Seðlabanka Evrópu og Netöryggisstofnun Evrópusambandsins, semja sameiginleg drög að tæknilegum eftirlitsstöðlum og tilgreina nánar eftirfarandi:

a) viðmiðanirnar sem settar eru fram í 1. mgr., þ.m.t. mikilvægismörk til að ákvarða alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eða, eftir því sem við á, alvarleg greiðslutengd rekstrar- eða öryggisatvik, sem falla undir tilkynningaskylduna sem mælt er fyrir um í 1. mgr. 19. gr.,

b) viðmiðanir sem lögbær yfirvöld skulu beita í þeim tilgangi að meta hve viðeigandi alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eru eða, eftir því sem við á, alvarleg greiðslutengd rekstrar- eða öryggisatvik, fyrir viðeigandi lögbær yfirvöld í öðrum aðildarríkjum og upplýsingar um tilkynningar um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eða, eftir því sem við á, alvarleg greiðslutengd rekstrar- eða öryggisatvik, sem á að deila með öðrum lögbærum yfirvöldum skv. 6. og 7. mgr. 19. gr.,

c) viðmiðanirnar sem settar eru fram í 2. mgr. þessarar greinar, þ.m.t. hve há mikilvægismörk skulu vera til að ákvarða verulegar netógnir.

4. Þegar sameiginlegu drögin að tæknilegum eftirlitsstöðlum sem um getur í 3. mgr. þessarar greinar eru samin skulu evrópsku eftirlitsstofnanirnar taka tillit til þeirra viðmiðana sem settar eru fram í 2. mgr. 4. gr., sem og til alþjóðlegra staðla, leiðbeininga og forskrifta sem Netöryggisstofnun Evrópusambandsins þróar og birtir, þ.m.t., eftir því sem við á, forskrifta fyrir aðra atvinnuvegi. Evrópsku eftirlitsstofnanirnar skulu, við beitingu viðmiðananna sem settar eru fram í 2. mgr. 4. gr., taka tilhlýðilegt tillit til þess hvort örfyrirtæki og lítil og meðalstór fyrirtæki þurfi að geta aflað nægilegra tilfanga og getu til að tryggja skjóta úrlausn atvika sem tengjast upplýsinga- og fjarskiptatækni.

Evrópsku eftirlitsstofnanirnar skulu leggja þessi sameiginlegu drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar 17. janúar 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í 3. gr. í samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

19. gr.

Tilkynningar um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og valfrjáls tilkynning um verulegar netógnir

1. Aðilar á fjármálamarkaði skulu tilkynna um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni til viðeigandi lögbærs yfirvalds eins og um getur í 46. gr. í samræmi við 4. mgr. þessarar greinar.

Ef aðili á fjármálamarkaði heyrir undir eftirlit fleiri en eins lögbærs landsyfirvalds, sem um getur í 46. gr., skulu aðildarríkin tilnefna eitt lögbært yfirvald sem viðkomandi lögbært yfirvald sem ber ábyrgð á því að annast þau hlutverk og skyldur sem kveðið er á um í þessari grein.

Lánastofnanir sem flokkast sem mikilvægar, í samræmi við 4. mgr. 6. gr. reglugerðar (ESB) nr. 1024/2013, skulu tilkynna alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni til viðkomandi lögbærs landsyfirvalds sem tilnefnt er í samræmi við 4. gr. tilskipunar 2013/36/ESB, sem skal án tafar senda Seðlabanka Evrópu þá skýrslu.

Að því er varðar fyrstu undirgrein skulu aðilar á fjármálamarkaði leggja fram frumtilkynningu og skýrslur sem um getur í 4. mgr. þessarar greinar, eftir að hafa aflað allra viðeigandi upplýsinga og greint þær, með því að nota sniðmátin sem um getur í 20. gr. og leggja þau fyrir lögbært yfirvald. Ef tæknilegur vandi kemur í veg fyrir að frumtilkynning sé lögð fram með sniðmátinu skulu aðilar á fjármálamarkaði tilkynna lögbæru yfirvaldi um það með öðrum leiðum.

Frumtilkynningin og skýrslurnar, sem um getur í 4. mgr., skulu innihalda allar nauðsynlegar upplýsingar til þess að lögbært yfirvald geti ákvarðað mikilvægi alvarlegs atviks sem tengist upplýsinga- og fjarskiptatækni og meta möguleg áhrif yfir landamæri.

Með fyrirvara um skýrslugjöf aðila á fjármálamarkaði til viðkomandi lögbærs yfirvalds, skv. fyrstu undirgrein, geta aðildarríki auk þess ákveðið að sumir eða allir aðilar á fjármálamarkaði skuli einnig senda frumtilkynningu og sérhverja skýrslu, sem um getur í 4. mgr. þessarar greinar, með því að nota sniðmátin sem um getur í 20. gr., til lögbærra yfirvalda eða viðbragðsteyma vegna váatvika er varða tölvuöryggi sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555.

2. Aðilar á fjármálamarkaði geta að eigin frumkvæði tilkynnt um verulegar netógnir til viðkomandi lögbærra yfirvalda þegar þeir telja að ógnin geti skipt fjármálakerfið, notendur þjónustu eða viðskiptavini máli. Viðkomandi lögbært yfirvald getur veitt öðrum viðeigandi yfirvöldum slíkar upplýsingar, sem um getur í 6. mgr.

Lánastofnanir sem flokkast sem mikilvægar, í samræmi við 4. mgr. 6. gr. reglugerðar (ESB) nr. 1024/2013, geta að eigin frumkvæði tilkynnt um verulegar netógnir til viðkomandi lögbærs landsyfirvalds, sem tilnefnt er í samræmi við 4. gr. tilskipunar 2013/36/ESB, sem skal tafarlaust senda tilkynninguna til Seðlabanka Evrópu.

Aðildarríki geta ákveðið að þeir aðilar á fjármálamarkaði sem tilkynna að eigin frumkvæði í samræmi við fyrstu undirgrein geti einnig sent þá tilkynningu til viðbragðsteyma vegna váatvika er varða tölvuöryggi, sem eru tilgreind eða komið á fót í samræmi við tilskipun (ESB) 2022/2555.

3. Þegar alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni á sér stað og hefur áhrif á fjárhagslega hagsmuni viðskiptavina skulu aðilar á fjármálamarkaði, án ástæðulausrar tafar og um leið og þeir fá vitneskju um það, upplýsa viðskiptavini sína um atvikið og um þær ráðstafanir sem gerðar hafa verið til að draga úr skaðlegum áhrifum af slíku atviki.

Ef um er að ræða verulega netógn skulu aðilar á fjármálamarkaði, eftir atvikum, upplýsa þá viðskiptavini sem hugsanlega geta orðið fyrir áhrifum um allar viðeigandi verndarráðstafanir sem þeir gætu íhugað að grípa til.

4. Aðilar á fjármálamarkaði skulu, innan þeirra tímamarka sem mælt verður fyrir um í samræmi við ii. lið a-liðar fyrstu málsgreinar 20. gr., leggja eftirfarandi fyrir viðkomandi lögbært yfirvald:

a) frumtilkynningu,

b) áfangaskýrslu eftir frumtilkynninguna sem um getur í a-lið, um leið og staða upphaflegs atviks hefur breyst verulega eða meðhöndlun alvarlegs atviks sem tengist upplýsinga- og fjarskiptatækni hefur breyst á grundvelli nýrra fyrirliggjandi upplýsinga og í kjölfarið, eftir því sem við á, með uppfærðum tilkynningum í hvert sinn sem viðeigandi stöðuuppfærsla er tiltæk og einnig að sérstakri beiðni lögbærs yfirvalds,

c) lokaskýrslu, þegar greiningu á frumorsök er lokið án tillits til þess hvort mótvægisráðstöfunum hafi þegar verið beitt og þegar raunverulegar tölur yfir áhrif eru tiltækar og geta komið í stað áætlaðra talna.

5. Aðilum á fjármálamarkaði er heimilt, í samræmi við lög Sambandsins og landsbundin sérlög, að útvista skyldum um skýrslugjöf samkvæmt þessari grein til þjónustuveitanda sem er þriðji aðili. Komi til slíkrar útvistunar ber aðilinn á fjármálamarkaði áfram fulla ábyrgð á því að kröfur um skýrslugjöf vegna atvika séu uppfylltar.

6. Við móttöku frumtilkynningar og hverrar skýrslu sem um getur í 4. mgr. skal lögbært yfirvald veita eftirfarandi viðtakendum tímanlega upplýsingar um alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni, eftir því sem við á, á grundvelli valdsviðs hvers þeirra um sig:

a) Evrópsku bankaeftirlitsstofnuninni, Evrópsku verðbréfamarkaðseftirlitsstofnuninni eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnuninni,

b) Seðlabanka Evrópu, ef um er að ræða aðila á fjármálamarkaði sem um getur í a-, b- og d-lið 1. mgr. 2. gr.,

c) lögbærum yfirvöldum, sameiginlegum tengiliðum eða viðbragðsteymum vegna váatvika er varða tölvuöryggi sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555,

d) skilastjórnvöldum, eins og um getur í 3. gr. tilskipunar 2014/59/ESB, og sameiginlegri skilastjórn að því er varðar einingar sem um getur í 2. mgr. 7. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 806/2014 ([37]) og að því er varðar einingar og samstæður sem um getur í b-lið 4. mgr. og 5. mgr. 7. gr. reglugerðar (ESB) nr. 806/2014 ef slíkar upplýsingar varða atvik sem skapa áhættu fyrir tryggingu nauðsynlegra starfsþátta í skilningi 35. liðar 1. mgr. 2. gr. tilskipunar 2014/59/ESB, og

e) annarra viðkomandi opinberra yfirvalda samkvæmt landslögum.

7. Eftir viðtöku upplýsinga í samræmi við 6. mgr. skulu Evrópska bankaeftirlitsstofnunin, Evrópska verðbréfamarkaðseftirlitsstofnunin eða Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin og Seðlabanki Evrópu, í samráði við Netöryggisstofnun Evrópusambandsins og samvinnu við viðkomandi lögbært yfirvald, meta hvort alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni skipti máli fyrir lögbær yfirvöld í öðrum aðildarríkjum. Í kjölfar matsins skulu Evrópska bankaeftirlitsstofnunin, Evrópska verðbréfamarkaðseftirlitsstofnunin eða Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin tilkynna viðkomandi lögbærum yfirvöldum í öðrum aðildarríkjum til samræmis við það eins fljótt og auðið er. Seðlabanki Evrópu skal tilkynna aðilum seðlabankakerfis Evrópu um málefni sem varða greiðslukerfið. Á grundvelli þeirrar tilkynningar skulu lögbær yfirvöld, eftir því sem við á, gera allar nauðsynlegar ráðstafanir til að vernda tafarlaust stöðugleika fjármálakerfisins.

([37]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 806/2014 frá 15. júlí 2014 um að koma á samræmdum reglum og samræmdri málsmeðferð fyrir skilameðferð lánastofnana og tiltekinna verðbréfafyrirtækja innan ramma sameiginlegs skilameðferðarkerfis og sameiginlegs skilasjóðs og um breytingu á reglugerð (ESB) nr. 1093/2010 (Stjtíð. ESB. L 225, 30.7.2014, bls. 1).

8. Tilkynningin sem Evrópska verðbréfamarkaðseftirlitsstofnunin á að senda skv. 7. mgr. þessarar greinar skal ekki hafa áhrif á ábyrgð lögbærs yfirvalds á því að senda upplýsingar um alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni án tafar til viðeigandi yfirvalds í gistiaðildarríki, ef verðbréfamiðstöð hefur umtalsverða starfsemi sem nær yfir landamæri í gistiaðildarríkinu, sé líklegt að alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni hafi alvarlegar afleiðingar fyrir fjármálamarkaði í gistiaðildarríkinu og ef samstarfssamningar eru fyrir hendi milli lögbærra yfirvalda í tengslum við eftirlit með aðilum á fjármálamarkaði.

20. gr.

Samræming á efni og sniðmátum tilkynninga

Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og í samráði við Netöryggisstofnun Evrópusambandsins og Seðlabanka Evrópu, semja:

a) sameiginleg drög að tæknilegum eftirlitsstöðlum til að:

   i. mæla fyrir um efni tilkynninga um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni svo að þær endurspegli viðmiðanirnar sem mælt er fyrir um í 1. mgr. 18. gr. og hafi að geyma fleiri þætti, s.s. upplýsingar til að ákvarða mikilvægi tilkynninga fyrir önnur aðildarríki og hvort þær teljist vera alvarlegt greiðslutengt rekstrar- eða öryggisatvik eða ekki,

   ii. skilgreina fresti fyrir frumtilkynningu og fyrir hverja skýrslu sem um getur í 4. mgr. 19. gr.,

   iii. staðfesta innihald tilkynningar að því er varðar verulegar netógnir.

   Við gerð þessara draga að tæknilegum eftirlitsstöðlum skulu evrópsku eftirlitsstofnanirnar taka tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði og eðlis, umfangs og flækjustigs þjónustu, starfsemi og reksturs hans og einkum með það í huga að tryggja, að því er varðar ii. lið a-liðar þessarar málsgreinar, að mismunandi tímamörk geti endurspeglað, eins og við á, sérkenni fjármálageira, með fyrirvara um að viðhalda samræmdri nálgun við skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni samkvæmt þessari reglugerð og tilskipun (ESB) 2022/2555. Evrópsku eftirlitsstofnanirnar skulu, eftir því sem við á, færa rök fyrir frávikum frá þeim aðferðum sem gripið er til í tengslum við þá tilskipun,

b) sameiginleg drög að tæknilegum framkvæmdarstöðlum til að koma á stöðluðum eyðublöðum, sniðmátum og verklagsreglum til að aðilar á fjármálamarkaði geti skýrt frá alvarlegu atviki sem tengist upplýsinga- og fjarskiptatækni og tilkynnt um verulega netógn.

Evrópsku eftirlitsstofnanirnar skulu leggja fyrir framkvæmdastjórnina sameiginlegu drögin að tæknilegu eftirlitsstöðlunum, sem um getur í a-lið fyrstu mgr., og sameiginleg drög að tæknilegum framkvæmdarstöðlum sem um getur í b-lið fyrstu mgr. eigi síðar en 17. júlí 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja sameiginlegu tæknilegu eftirlitsstaðlana sem um getur í a-lið fyrstu mgr., samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

Framkvæmdastjórninni er falið vald til að samþykkja sameiginlegu tæknilegu framkvæmdarstaðlana sem um getur í b-lið fyrstu mgr. í samræmi við 15. gr. í reglugerðum (ESB) nr. 1093/2010, reglugerðar) nr. 1094/2010 og reglugerðar (ESB) nr. 1095/2010.

21. gr.

Miðlæg söfnun tilkynninga um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni

1. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og í samráði við Seðlabanka Evrópu og Netöryggisstofnun Evrópusambandsins, taka saman sameiginlega skýrslu þar sem metin er hagkvæmni frekari miðstýringar á söfnun atvikatilkynninga með því að koma á fót sameiginlegri ESB-miðstöð fyrir tilkynningar aðila á fjármálamarkaði um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni. Í sameiginlegu skýrslunni skal kanna leiðir til að greiða fyrir flæði tilkynninga um upplýsinga- og fjarskiptatæknitengd atvik, draga úr tengdum kostnaði og renna stoðum undir þemabundnar greiningar með það í huga að auka samleitni eftirlits.

2. Sameiginlega skýrslan, sem um getur í 1. mgr., skal a.m.k. innihalda eftirfarandi þætti:

a) forsendur fyrir stofnun sameiginlegrar ESB-miðstöðvar,

b) ávinning, takmarkanir og áhættu, þ.m.t. áhættu sem tengist mikilli samsöfnun viðkvæmra upplýsinga,

c) nauðsynlega getu til að tryggja samvirkni með tilliti til annarrar viðeigandi tilkynningaskyldu,

d) rekstrarþætti,

e) skilyrði fyrir aðild,

f) tæknilegar ráðstafanir fyrir aðila á fjármálamarkaði og lögbær landsyfirvöld til að hafa aðgang að sameiginlegri ESB-miðstöð,

g) bráðabirgðamat á fjárhagslegum kostnaði sem stofnað er til með því að koma á fót starfsvettvangi sem styður sameiginlega ESB-miðstöð, þ.m.t. tilskilda sérfræðiþekkingu.

3. Evrópsku eftirlitsstofnanirnar skulu leggja skýrsluna sem um getur í 1. mgr. fyrir Evrópuþingið, ráð Evrópusambandsins og framkvæmdastjórnina eigi síðar en 17. janúar 2025.

22. gr.

Endurgjöf frá eftirlitsyfirvöldum

1. Með fyrirvara um tæknilegar upplýsingar, ráðgjöf eða úrræði og síðari eftirfylgni sem viðbragðsteymi vegna váatvika er varða tölvuöryggi geta veitt samkvæmt tilskipun (ESB) 2022/2555, eftir atvikum og í samræmi við landslög, skal lögbært yfirvald, við móttöku frumtilkynningar og sérhverrar skýrslu eins og um getur í 4. mgr. 19. gr., staðfesta móttöku og er heimilt, þegar það er mögulegt, að veita aðila á fjármálamarkaði tímanlega viðeigandi endurgjöf í samræmi við umfang eða almennar leiðbeiningar, einkum með því að gera aðgengilegar hvers kyns viðeigandi nafnlausar upplýsingar og greiningargögn um svipaðar ógnir, og er heimilt að ræða úrræði sem beitt er á vettvangi aðila á fjármálamarkaði og aðferðir til að lágmarka og milda neikvæð áhrif þvert á fjármálageirann. Með fyrirvara um endurgjöf frá eftirlitsyfirvaldi skulu aðilar á fjármálamarkaði bera fulla ábyrgð á meðhöndlun og afleiðingum af upplýsinga- og fjarskiptatæknitengdum atvikum sem tilkynnt er um skv. 1. mgr. 19. gr.

2. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, gefa árlega skýrslu, með nafnlausum upplýsingum á samanteknu formi, um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni en lögbær yfirvöld skulu veita nánari upplýsingar um þau í samræmi við 6. mgr. 19. gr. og tiltaka a.m.k. fjölda alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni, eðli þeirra og áhrif á starfsemi aðila á fjármálamarkaði eða viðskiptavina, þær aðgerðir til úrbóta sem gripið hefur verið til og kostnað sem stofnað hefur verið til.

Evrópsku eftirlitsstofnanirnar skulu gefa út viðvaranir og taka saman vandaðar tölfræðilegar upplýsingar til að styðja við mat á ógnum og veikleikum í upplýsinga- og fjarskiptatækni.

23. gr.

Greiðslutengd rekstrar- eða öryggisatvik sem varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki

Kröfurnar sem mælt er fyrir um í þessum kafla skulu einnig gilda um greiðslutengd rekstrar- eða öryggisatvik og um alvarleg greiðslutengd rekstrar- eða öryggisatvik ef þau varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki.

IV. KAFLI

Prófanir á stafrænum rekstrarlegum viðnámsþrótti

24. gr.

Almennar kröfur um framkvæmd prófunar á stafrænum rekstrarlegum viðnámsþrótti

1. Í þeim tilgangi að meta viðbúnað til að takast á við atvik sem tengjast upplýsinga- og fjarskiptatækni, til að greina veikleika, annmarka og gloppur í stafrænum rekstrarlegum viðnámsþrótti og framkvæma tafarlaust ráðstafanir til úrbóta skulu aðilar á fjármálamarkaði, aðrir en örfyrirtæki, með tilliti til viðmiðananna sem settar eru fram í 2. mgr. 4. gr., koma á, viðhalda og endurskoða trausta og alhliða prófunaráætlun um stafrænan rekstrarlegan viðnámsþrótt sem óaðskiljanlegan hluta af áhættustýringarramma í upplýsinga- og fjarskiptatækni sem um getur í 6. gr.

2. Prófunaráætlun um stafrænan rekstrarlegan viðnámsþrótt skal fela í sér ýmiss konar mat, prófanir, aðferðafræði, starfsvenjur og búnað sem á að beita í samræmi við 25. og 26. gr.

3. Við framkvæmd prófunaráætlunarinnar um stafrænan rekstrarlegan viðnámsþrótt, sem um getur í 1. mgr. þessarar greinar, skulu aðilar á fjármálamarkaði, aðrir en örfyrirtæki, fylgja áhættumiðaðri nálgun, að teknu tilliti til þeirra viðmiðana sem settar eru fram í 2. mgr. 4. gr., og taka tilhlýðilegt tillit til þróunar á landslagi upplýsinga- og fjarskiptatækniáhættu, hvers kyns sértækrar áhættu sem hlutaðeigandi aðili á fjármálamarkaði er eða kann að vera útsettur fyrir, mikilvægi upplýsingaeigna og veittrar þjónustu, sem og hvers kyns annarra þátta sem aðili á fjármálamarkaði telur viðeigandi.

4. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu tryggja að óháðir aðilar framkvæmi prófanir, hvort sem það eru innri eða ytri aðilar. Ef innri prófunaraðili framkvæmir prófanir skulu aðilar á fjármálamarkaði verja til þess nægilegum tilföngum og tryggja að komist sé hjá hagsmunaárekstrum á öllum stigum hönnunar og framkvæmdar prófunar.

5. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu setja sér verklagsreglur og stefnur til að forgangsraða, flokka og ráða bót á öllum vandamálum sem koma í ljós við framkvæmd prófana og koma á innri staðfestingaraðferð til að ganga úr skugga um að ráðin sé full bót á öllum auðkenndum veikleikum, annmörkum eða gloppum.

6. Aðilar á fjármálamarkaði, aðrir en örfyrirtæki, skulu tryggja, a.m.k. árlega, að viðeigandi prófanir séu gerðar á öllum upplýsinga- og fjarskiptatæknikerfum og hugbúnaði sem styður við nauðsynlega eða mikilvæga starfsemi.

25. gr.

Prófun á upplýsinga- og fjarskiptatæknibúnaði og -kerfum

1. Prófunaráætlunin um stafrænan rekstrarlegan viðnámsþrótt, sem um getur í 24. gr., skal kveða á um framkvæmd viðeigandi prófana, í samræmi við viðmiðanirnar sem settar eru fram í 2. mgr. 4. gr., s.s. mat og skönnun á veikleikum, greiningu á opnum hugbúnaði, mat á öryggi netkerfis, greiningu á gloppum, úttektir á raunlægu öryggi, spurningalista og skönnunarhugbúnaðarlausnir, úttektir á frumkóta þar sem mögulegt er, sviðsmyndatengdar prófanir, samhæfisprófanir, prófanir á frammistöðu, prófanir enda á milli og innbrotsprófanir.

2. Verðbréfamiðstöðvar og miðlægir mótaðilar skulu framkvæma veikleikamat áður en nýr eða fyrirliggjandi hugbúnaður og innviðir eru innleiddir eða endurinnleiddir og upplýsinga- og fjarskiptatækniþjónusta sem styður við nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði.

3. Örfyrirtæki skulu framkvæma prófanirnar, sem um getur í 1. mgr., með því að blanda saman áhættutengdri nálgun og stefnumótandi áætlanagerð um prófanir á upplýsinga- og fjarskiptatækni, með því að taka annars vegar tilhlýðilegt tillit til þarfarinnar á að viðhalda jafnvægi milli umfangs tilfanga og þess tíma sem verður úthlutað til prófana á upplýsinga- og fjarskiptatækni og kveðið er á um í þessari grein og hins vegar hve áríðandi prófanirnar teljast, tegundar áhættu, mikilvægis upplýsingaeignarinnar og veittrar þjónustu, sem og annarra viðeigandi þátta, þ.m.t. getu aðila á fjármálamarkaði til að taka meðvitaða áhættu.

26. gr.

Auknar prófanir á upplýsinga- og fjarskiptatæknibúnaði, -kerfum og -ferlum sem byggjast á ógnamiðaðri innbrotsprófun

1. Aðilar á fjármálamarkaði, aðrir en þeir sem um getur í fyrstu undirgrein 1. mgr. 16. gr. og aðrir en örfyrirtæki sem eru auðkennd í samræmi við þriðju undirgrein 8. mgr. þessarar greinar, skulu framkvæma aukna prófun með ógnamiðaðri innbrotsprófun á a.m.k. þriggja ára fresti. Á grundvelli áhættusniðs aðila á fjármálamarkaði og með tilliti til rekstrarlegra aðstæðna er lögbæru yfirvaldi heimilt, ef nauðsyn krefur, að óska eftir því við aðilann á fjármálamarkaði að hann dragi úr eða auki þessa tíðni.

2. Sérhver ógnamiðuð innbrotsprófun skal taka til nokkurra eða allra þátta nauðsynlegrar eða mikilvægrar starfsemi aðila á fjármálamarkaði og skal framkvæmd á framleiðslukerfum í rauntíma sem styðja slíka starfsemi.

Aðilar á fjármálamarkaði skulu tilgreina öll viðkomandi undirliggjandi upplýsinga- og fjarskiptatæknikerfi, -ferla og -tækni sem styðja við nauðsynlega eða mikilvæga starfsemi og upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. þá sem styður við nauðsynlega eða mikilvæga starfsemi sem hefur verið útvistað eða samið um við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

Aðilar á fjármálamarkaði skulu meta hvaða nauðsynlega eða mikilvæga starfsemi þarf að falla undir ógnamiðaða innbrotsprófun. Í niðurstöðum þessa mats skal ákvarða nákvæmt svið ógnamiðaðrar innbrotsprófunar og skulu lögbær yfirvöld staðfesta þær.

3. Þegar þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu falla undir gildissvið ógnamiðaðrar innbrotsprófunar skal aðili á fjármálamarkaði gera nauðsynlegar ráðstafanir og verndarráðstafanir til að tryggja þátttöku slíkra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu í ógnamiðuðu innbrotsprófuninni og skal ávallt bera fulla ábyrgð á því að tryggja að farið sé að þessari reglugerð.

4. Með fyrirvara um fyrstu og aðra undirgrein 2. mgr., ef ástæða er til að ætla að þátttaka þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í ógnamiðaðri innbrotsprófun, sem um getur í 3. mgr., hafi neikvæð áhrif á gæði eða öryggi þjónustu sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu veitir viðskiptavinum sem eru einingar sem falla utan gildissviðs þessarar reglugerðar eða á trúnað um gögn sem tengjast slíkri þjónustu, geta aðilinn á fjármálamarkaði og þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu samþykkt skriflega að þriðji aðilinn geri samning beint við utanaðkomandi prófunaraðila til að gera, undir stjórn eins tilnefnds aðila á fjármálamarkaði, samsetta ógnamiðaða innbrotsprófun með þátttöku fleiri aðila á fjármálamarkaði (samsett prófun) sem þriðji aðili veitir upplýsinga- og fjarskiptatækniþjónustu.

Samsetta prófunin skal ná yfir viðeigandi svið upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi sem aðilarnir á fjármálamarkaði hafa gert samning um við viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Litið skal á samsettu prófanirnar sem ógnamiðaða innbrotsprófun sem aðilar á fjármálamarkaði sem taka þátt í samsettu prófununum framkvæma.

Fjöldi aðila á fjármálamarkaði sem taka þátt í samsettum prófunum skal stilltur af á viðeigandi hátt að teknu tilliti til flækjustigs og tegunda viðkomandi þjónustu.

5. Aðilar á fjármálamarkaði skulu, í samstarfi við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og aðra aðila sem hlut eiga að máli, þ.m.t. prófunaraðila en þó ekki lögbær yfirvöld, beita skilvirkri áhættustýringu til að milda áhættu af hugsanlegum áhrifum á gögn, skaða á búnaði og röskun á nauðsynlegri eða mikilvægri starfsemi, þjónustu eða starfsemi hjá aðilanum á fjármálamarkaði sjálfum, mótaðilum eða fjármálageiranum.

6. Við lok prófana, þegar skýrslur og áætlanir um úrbætur hafa verið samþykktar skulu aðilinn á fjármálamarkaði og, eftir atvikum, hinir ytri prófunaraðilar veita yfirvaldinu, sem tilgreint er í samræmi við 9. eða 10. mgr., samantekt á viðeigandi niðurstöðum, áætlunum um úrbætur og gögnum sem sýna fram á að ógnamiðuð innbrotsprófun hafi verið framkvæmd í samræmi við kröfurnar.

7. Yfirvöld skulu veita aðilum á fjármálamarkaði staðfestingu á því að prófunin hafi verið gerð í samræmi við kröfurnar eins og sýnt er fram á í gögnunum til að heimila gagnkvæma viðurkenningu á ógnamiðuðum innbrotsprófunum milli lögbærra yfirvalda. Aðili á fjármálamarkaði skal tilkynna viðkomandi lögbæru yfirvaldi um staðfestingu, samantekt á viðeigandi niðurstöðum og áætlanir um úrbætur.

Með fyrirvara um slíka staðfestingu skulu aðilar á fjármálamarkaði ávallt bera fulla ábyrgð á áhrifum af þeim prófunum sem um getur í 4. mgr.

8. Aðilar á fjármálamarkaði skulu gera verktakasamninga við prófunaraðila um að gera ógnamiðaða innbrotsprófun í samræmi við 27. gr. Þegar aðilar á fjármálamarkaði nota innri prófunaraðila til að gera ógnamiðaða innbrotsprófun skulu þeir fá ytri prófunaraðila fyrir þriðju hverja prófun.

Lánastofnanir sem flokkast sem mikilvægar í samræmi við 4. mgr. 6. gr. reglugerðar (ESB) nr. 1024/2013 skulu eingöngu nota utanaðkomandi prófunaraðila í samræmi við a- til e-lið 1. mgr. 27. gr.

Lögbær yfirvöld skulu tilgreina aðila á fjármálamarkaði sem ber skylda til að gera ógnamiðaða innbrotsprófun með hliðsjón af viðmiðununum sem settar eru fram í 2. mgr. 4. gr., á grundvelli mats á eftirfarandi:

a) áhrifatengdum þáttum, einkum að hve miklu leyti sú þjónusta sem veitt er og starfsemi sem aðili á fjármálamarkaði stundar hefur áhrif á fjármálageirann,

b) hvort fjármálastöðugleika sé hugsanlega hætta búin, þ.m.t. kerfislægt eðli aðila á fjármálamarkaði á vettvangi Sambandsins eða á landsvísu, eftir því sem við á,

c) sértæku áhættusniði fyrir upplýsinga- og fjarskiptatækni, þroska upplýsinga- og fjarskiptatækni hjá aðilanum á fjármálamarkaði eða tækniþáttum sem um ræðir.

9. Aðildarríki geta tilnefnt eitt opinbert yfirvald í fjármálageiranum til að bera ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun í fjármálageiranum á landsvísu og skulu fela því allar valdheimildir og verkefni í því skyni.

10. Ef tilnefning í samræmi við 9. mgr. þessarar greinar hefur ekki verið gerð, og með fyrirvara um valdheimildir til að tilgreina þá aðila á fjármálamarkaði sem skulu framkvæma ógnamiðaða innbrotsprófun, er lögbæru yfirvaldi heimilt að úthluta framkvæmd sumra eða allra verkefnanna, sem um getur í þessari grein og 27. gr., til annars landsbundins yfirvalds í fjármálageiranum.

11. Evrópsku eftirlitsstofnanirnar skulu, í samráði við Seðlabanka Evrópu, semja sameiginleg drög að tæknilegum eftirlitsstöðlum í samræmi við TIBER-EU-rammann til að tilgreina nánar:

a) þær viðmiðanir sem eru notaðar við beitingu annarrar undirgreinar 8. mgr.,

b) þær kröfur og staðla sem gilda um notkun á innri prófunaraðilum,

c) kröfur í tengslum við:

   i. gildissvið þeirrar ógnamiðuðu innbrotsprófunar sem um getur í 2. mgr.,

   ii. prófunaraðferð og nálgun sem skal nota fyrir sérhvern tiltekinn áfanga í prófunarferlinu,

   iii. niðurstöður, loka- og úrbótastig prófunar,

d) tegund samvinnu eftirlitsaðila og annarrar viðeigandi samvinnu sem þörf er á við innleiðingu ógnamiðaðra innbrotsprófana, og til að greiða fyrir gagnkvæmri viðurkenningu á þeim prófunum, í tengslum við aðila á fjármálamarkaði sem starfa í fleiri en einu aðildarríki til að leyfa hæfilega aðkomu eftirlitsyfirvalda og sveigjanlega innleiðingu í því skyni að koma til móts við sérstaka eiginleika fjármálaundirgeira eða staðbundinna fjármálamarkaða.

Við gerð þessara draga að tæknilegum eftirlitsstöðlum skulu evrópsku eftirlitsstofnanirnar taka tilhlýðilegt tillit til hvers kyns sérkenna sem leiða af sérstöku eðli starfseminnar þvert á ólíka fjármálaþjónustugeira.

Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. júlí 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í fyrstu undirgrein í samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

27. gr.

Kröfur fyrir prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun

1. Aðilar á fjármálamarkaði skulu eingöngu nota prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun sem:

a) búa yfir sem bestri hæfni og orðspori,

b) búa yfir tæknilegri og skipulagslegri getu og sýna fram á sértæka sérþekkingu á ógnagreiningum, innbrotsprófunum og rauðteymisprófunum,

c) hafa fengið vottun faggildingaraðila í aðildarríki eða fylgja formlegum hátternisreglum eða siðferðilegum ramma,

d) veita óháða staðfestingu eða úttektarskýrslu í tengslum við trausta áhættustýringu í tengslum við framkvæmd á ógnamiðaðri innbrotsprófun, þ.m.t. tilhlýðilega vernd trúnaðarupplýsinga viðkomandi aðila á fjármálamarkaði og úrlausn vegna viðskiptaáhættu aðila á fjármálamarkaði,

e) falla að öllu leyti og réttilega undir viðeigandi starfsábyrgðartryggingar, þ.m.t. vegna hættu á misferli og gáleysi.

2. Þegar innri prófunaraðilar eru notaðir skulu aðilar á fjármálamarkaði tryggja að eftirfarandi skilyrði séu uppfyllt, til viðbótar við kröfurnar í 1. mgr.:

a) að viðkomandi lögbært yfirvald eða eitt opinbert yfirvald sem er tilnefnt í samræmi við 9. og 10. mgr. 26. gr. hafi samþykkt slíka notkun,

b) að viðkomandi lögbært yfirvald hafi sannreynt að aðilinn á fjármálamarkaði hafi nægileg sérgreind tilföng og hafi tryggt að komist sé hjá hagsmunaárekstrum á öllum stigum hönnunar og framkvæmdar prófunar og

c) að sá aðili sem veitir ógnagreiningargögn sé utanaðkomandi aðilanum á fjármálamarkaði.

3. Aðilar á fjármálamarkaði skulu tryggja að samningar sem gerðir eru við ytri prófunaraðila krefjist traustrar stjórnunar á niðurstöðum úr ógnamiðaðri innbrotsprófun og að öll gagnavinnsla úr þeim, þ.m.t. hvers kyns myndun, geymsla, söfnun, drög, skýrslugerð, miðlun eða eyðing, skapi ekki áhættu fyrir viðkomandi aðila á fjármálamarkaði.

V. KAFLI

Stýring upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila

I. þáttur

Helstu meginreglur um trausta stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila

28. gr.

Almennar meginreglur

1. Aðilar á fjármálamarkaði skulu stýra upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila sem óaðskiljanlegum hluta upplýsinga- og fjarskiptatækniáhættu innan áhættustýringarramma í upplýsinga- og fjarskiptatækni eins og um getur í 1. mgr. 6. gr. og í samræmi við eftirfarandi meginreglur:

a) aðilar á fjármálamarkaði sem hafa innleitt samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptaþjónustu til að reka viðskiptastarfsemi sína skulu ætíð bera fulla ábyrgð á því að uppfylla og standa við allar skuldbindingar samkvæmt þessari reglugerð og gildandi lögum um fjármálaþjónustu,

b) við stýringu á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila skulu aðilar á fjármálamarkaði hafa meginreglu um meðalhóf að leiðarljósi með hliðsjón af:

i. eðli, umfangi, flækjustigi og mikilvægi hæðis tengdu upplýsinga- og fjarskiptatækni,

ii. áhættu sem leiðir af samningum sem gerðir eru við þriðju aðila um upplýsinga- og fjarskiptatækniþjónustu, að teknu tilliti til þess hversu nauðsynleg eða mikilvæg viðkomandi þjónusta, ferli eða starfsemi er, og mögulegra áhrifa á samfellu og aðgengileika fjármálaþjónustu og -starfsemi, á eininga- og samstæðustigi.

2. Aðilar á fjármálamarkaði, aðrir en þeir sem um getur í fyrstu undirgrein 1. mgr. 16. gr. og aðrir en örfyrirtæki, skulu, sem hluti af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, samþykkja og endurskoða reglulega stefnuáætlun um upplýsinga- og fjarskiptatækniáhættu vegna þriðja aðila, með hliðsjón af fjölbreytileikastefnunni m.t.t. veitenda sem um getur í 9. mgr. 6. gr., eftir atvikum. Stefnuáætlunin um upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila skal fela í sér stefnu um notkun upplýsinga- og fjarskiptaþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veita og skal gilda á einingagrunni og, ef við á, á undirsamstæðu- og samstæðugrunni. Stjórn og/eða framkvæmdastjórn skal, á grundvelli mats á heildaráhættusniði aðilans á fjármálamarkaði og umfangi og flækjustigi viðskiptaþjónustunnar, endurskoða reglulega áhættu sem borin er kennsl á með tilliti til samningsbundins fyrirkomulags um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi.

3. Aðilar á fjármálamarkaði skulu, sem hluta af áhættustýringarramma í upplýsinga- og fjarskiptatækni, viðhalda og uppfæra á einingastigi og á undirsamstæðu- og samstæðustigi, upplýsingaskrá í tengslum við allt samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem þriðju aðilar veita.

Samningsbundna fyrirkomulagið sem um getur í fyrstu undirgrein skal skjalfest á viðeigandi hátt og gera skal greinarmun á því sem tekur til upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi og því sem ekki gerir það.

Aðilar á fjármálamarkaði skulu a.m.k. árlega gefa lögbærum yfirvöldum skýrslu um fjölda nýrra ráðstafana um notkun upplýsinga- og fjarskiptatækniþjónustu, flokka þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, tegund samningsbundins fyrirkomulags og þá þjónustu og starfsemi upplýsinga- og fjarskiptatækni sem veitt er.

Aðilar á fjármálamarkaði skulu, að fenginni beiðni þar um, gera fullnaðarskrá yfir upplýsingar aðgengilega lögbæra yfirvaldinu eða, ef óskað er, tiltekna hluta hennar ásamt öllum upplýsingum sem taldar eru nauðsynlegar til að gera skilvirkt eftirlit með aðilum á fjármálamarkaði mögulegt.

Aðilar á fjármálamarkaði skulu upplýsa lögbært yfirvald tímanlega um hvers kyns fyrirhugað samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi, sem og þegar starfsemi er orðin nauðsynleg eða mikilvæg.

4. Áður en aðilar á fjármálamarkaði gera samningsbundið fyrirkomulag um notkun á upplýsinga- og fjarskiptatækniþjónustu skulu þeir:

a) meta hvort samningsbundna fyrirkomulagið tekur til notkunar á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi,

b) meta hvort skilyrði eftirlitsyfirvalda vegna samningsgerðar hafi verið uppfyllt,

c) greina og meta alla viðeigandi áhættu í tengslum við samningsbundna fyrirkomulagið, þ.m.t. möguleikann á að slíkt samningsbundið fyrirkomulag geti stuðlað að því að auka samþjöppunaráhættu í upplýsinga- og fjarskiptatækni eins og um getur í 29. gr.,

d) gera allar nauðsynlegar áreiðanleikakannanir á þeim þriðju aðilum sem til greina kemur að veiti þeim upplýsinga- og fjarskiptatækniþjónustu og tryggja, í öllu val- og matsferlinu, að þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu sé hæfur,

e) greina og meta hagsmunaárekstra sem samningsbundna fyrirkomulagið gæti valdið.

5. Aðilum á fjármálamarkaði er aðeins heimilt að gera samning við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem fylgja viðeigandi stöðlum um upplýsingaöryggi. Ef samningsbundið fyrirkomulag varðar nauðsynlega eða mikilvæga starfsemi ættu aðilar á fjármálamarkaði að taka tillit til notkunar þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu á stöðlum um upplýsingaöryggi sem eru nútímalegastir og af hæstu gæðum áður en gengið er frá fyrirkomulaginu.

6. Þegar aðilar á fjármálamarkaði nýta sér rétt til aðgangs, eftirlits og úttektar gagnvart þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu skulu þeir, á grundvelli áhættumiðaðrar nálgunar, ákvarða fyrirfram tíðni úttekta og eftirlits, sem og þau svið sem skoða skal með því að fylgja almennt viðurkenndum endurskoðunarstöðlum í samræmi við öll fyrirmæli eftirlitsyfirvalda um notkun slíkra endurskoðunarstaðla og upptöku þeirra.

Ef samningsbundið fyrirkomulag, sem gert er við þriðju aðila um notkun upplýsinga- og fjarskiptatækniþjónustu, hefur í för með sér mikið tæknilegt flækjustig skal aðili á fjármálamarkaði sannreyna að endurskoðendur, hvort heldur þeir eru innri eða ytri aðilar, eða hópur endurskoðenda, búi yfir nægilegri hæfni og þekkingu til að framkvæma viðeigandi endurskoðanir og mat með skilvirkum hætti.

7. Aðilar á fjármálamarkaði skulu tryggja að hægt sé að segja upp samningsbundnu fyrirkomulagi um notkun á upplýsinga- og fjarskiptatækniþjónustu við eftirfarandi aðstæður:

a) við veruleg brot þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu á gildandi lögum, reglum eða samningsskilmálum,

b) við aðstæður sem greinast við vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila og teljast geta breytt framkvæmd starfsþátta sem veittir eru í gegnum samningsbundið fyrirkomulag, þ.m.t. efnislegar breytingar sem hafa áhrif á fyrirkomulagið eða stöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

c) ef í ljós koma veikleikar hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu að því er varðar heildaráhættustýringu í upplýsinga- og fjarskiptatækni, einkum hvernig hann tryggir tiltækileika, ósvikni, réttleika eða leynd gagna, hvort sem um er að ræða persónuupplýsingar eða annars konar viðkvæm gögn eða ópersónulegar upplýsingar,

d) ef lögbært yfirvald getur ekki lengur haft skilvirkt eftirlit með aðilanum á fjármálamarkaði vegna skilyrða eða aðstæðna í tengslum við viðkomandi samningsbundið fyrirkomulag.

8. Þegar um er að ræða upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi skulu aðilar á fjármálamarkaði gera útgönguáætlanir. Í útgönguáætlunum skal taka tillit til áhættu sem getur komið fram hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, einkum að því er varðar hugsanlegan misbrest af þeirra hálfu, minnkandi gæði veittrar þjónustu í upplýsinga- og fjarskiptatækni, hvers kyns röskun á viðskiptum vegna óviðeigandi eða misheppnaðrar veitingar upplýsinga- og fjarskiptatækniþjónustu eða hvers kyns verulegrar áhættu sem kemur upp í tengslum við viðeigandi og stöðuga nýtingu á viðkomandi upplýsinga- og fjarskiptatækniþjónustu, eða slit á samningsbundnu fyrirkomulagi við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu við einhverjar þeirra aðstæðna sem taldar eru upp í 7. mgr.

Aðilar á fjármálamarkaði skulu tryggja að þeir geti sagt upp samningsbundnu fyrirkomulagi án þess að:

a) röskun verði á atvinnustarfsemi þeirra,

b) takmarka hlítni við kröfur samkvæmt reglum,

c) skaða samfellu og gæði þjónustu sem veitt er viðskiptavinum.

Áætlanir um útgöngu skulu vera yfirgripsmiklar, skjalfestar og vera nægilega vel prófaðar og yfirfarnar reglulega, í samræmi við viðmiðanirnar sem settar eru fram í 2. mgr. 4. gr.

Aðilar á fjármálamarkaði skulu greina aðrar lausnir og þróa umbreytingaráætlanir sem gera þeim kleift að taka umsamda upplýsinga- og fjarskiptatækniþjónustu og viðeigandi gögn af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og flytja þau, á öruggan og heildstæðan hátt, til annarra veitenda eða taka hana upp innanhúss á ný.

Aðilar á fjármálamarkaði skulu hafa viðeigandi viðbúnaðarráðstafanir til staðar til að viðhalda samfelldum rekstri ef upp koma aðstæður sem um getur í fyrstu undirgrein.

9. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, semja drög að tæknilegum framkvæmdarstöðlum til að koma á stöðluðum sniðmátum að því er varðar upplýsingaskrána sem um getur í 3. mgr., þ.m.t. upplýsingar sem eru sameiginlegar öllu samningsbundnu fyrirkomulagi um notkun upplýsinga- og fjarskiptatækniþjónustu. Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum framkvæmdarstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. janúar 2024.

Framkvæmdastjórninni er veitt vald til að samþykkja tæknilegu framkvæmdarstaðlana sem um getur í fyrstu undirgrein í samræmi við 15. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010.

10. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, semja drög að tæknilegum eftirlitsstöðlum til að tilgreina nánar ítarlegt efni stefnunnar sem um getur í 2. mgr. að því er varðar samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veita.

Við gerð þessara draga að tæknilegum eftirlitsstöðlum skulu evrópsku eftirlitsstofnanirnar taka tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði og eðlis, umfangs og flækjustigs þjónustu hans, starfsemi og reksturs. Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. janúar 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í fyrstu undirgrein í samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

29. gr.

Bráðabirgðamat á samþjöppunaráhættu í upplýsinga- og fjarskiptatækni á einingastigi

1. Við greiningu og mat á áhættunni sem um getur í c-lið 4. mgr. 28. gr. skulu aðilar á fjármálamarkaði einnig taka tillit til þess hvort fyrirhuguð gerð samningsbundins fyrirkomulags í tengslum við upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi myndi leiða til einhvers eftirfarandi:

a) að gerður sé samningur við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem er ekki auðvelt að skipta út, eða

b) að til staðar verði fjöldi samningsbundinna fyrirkomulaga í tengslum við veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi hjá sama þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða hjá nátengdum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu.

Aðilar á fjármálamarkaði skulu meta ávinning og kostnað af öðrum lausnum, s.s. notkun mismunandi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, með tilliti til þess hvort og hvernig fyrirhugaðar lausnir samræmast viðskiptaþörfum og -markmiðum sem sett eru fram í stefnuáætlun þeirra um stafrænan viðnámsþrótt.

2. Feli samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi í sér möguleikann á að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu semji enn frekar við aðra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu um undirverktöku sem styður nauðsynlega eða mikilvæga starfsemi, skulu aðilar á fjármálamarkaði meta ávinning og áhættu sem kann að koma upp í tengslum við slíka undirverktöku, einkum þegar um er að ræða undirverktaka á sviði upplýsinga- og fjarskiptatækni með staðfestu í þriðja landi.

Ef samningsbundið fyrirkomulag varðar upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi skulu aðilar á fjármálamarkaði taka tilhlýðilegt tillit til ákvæða gjaldþrotalaga sem myndu gilda ef til gjaldþrots þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu kæmi, sem og hvers konar takmarkana sem kunna að koma upp varðandi brýna endurreisn aðila á fjármálamarkaði á gögnum.

Ef samningsbundið fyrirkomulag um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi er gert við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi skulu aðilar á fjármálamarkaði, til viðbótar við þau sjónarmið sem um getur í annarri undirgrein, einnig taka til athugunar hvort farið sé að persónuverndarreglum Sambandsins og hvort lögum þriðja landsins sé framfylgt með skilvirkum hætti.

Ef samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptaþjónustu sem styður nauðsynlega eða mikilvæga starfsemi kveður á um undirverktöku, skulu aðilar á fjármálamarkaði meta hvort og hvernig hugsanlega langar eða flóknar keðjur undirverktöku geta haft áhrif á getu þeirra til að hafa fullt eftirlit með samningsbundnum starfsþáttum og getu lögbærs yfirvalds til að hafa skilvirkt eftirlit með aðila á fjármálamarkaði í því tilliti.

30. gr.

Helstu samningsákvæði

1. Réttindi og skyldur aðila á fjármálamarkaði og þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu skulu afmarkaðar með skýrum hætti og tilgreindar skriflega. Samningurinn í heild skal fela í sér samkomulag um þjónustustig og skjalfestur í einu skriflegu skjali sem skal vera aðilunum aðgengilegt á pappír eða í skjali á öðru niðurhalanlegu, varanlegu og aðgengilegu sniði.

2. Samningsbundið fyrirkomulag á notkun upplýsinga- og fjarskiptatækniþjónustu skal fela í sér a.m.k. eftirfarandi þætti:

a) skýra og ítarlega lýsingu á öllum starfsþáttum og upplýsinga- og fjarskiptaþjónustu sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu á að veita, þar sem tilgreint er hvort undirverktakastarfsemi í upplýsinga- og fjarskiptatækniþjónustu, sem styður við nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hans, sé heimil og þau skilyrði sem gilda um slíka undirverktöku þegar svo er,

b) staðsetningar, þ.e. landsvæði eða lönd þar sem þeir starfsþættir og sú upplýsinga- og fjarskiptaþjónusta sem samningar eða undirverktökusamningar eru gerðir um verða unnin og þar sem vinna á gögn, þ.m.t. geymslustaður og sú krafa að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu tilkynni aðila á fjármálamarkaði fyrirfram ef hann hyggst breyta um staðsetningu,

c) ákvæði um tiltækileika, ósvikni, réttleika og leynd í tengslum við vernd gagna, þ.m.t. persónuupplýsinga,

d) ákvæði um að tryggja aðgang, endurreisn og skil á auðaðgengilegu sniði á persónuupplýsingum og ópersónulegum gögnum sem aðili á fjármálamarkaði vinnur, ef til ógjaldfærni, skilameðferðar eða slita á starfsemi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu kemur eða samningsbundið fyrirkomulag fellur úr gildi,

e) lýsingar á þjónustustigi, þ.m.t. uppfærslur og endurskoðanir á því,

f) skyldu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að veita aðila á fjármálamarkaði aðstoð án viðbótarkostnaðar eða á fyrirframákveðnu verði þegar upp kemur atvik sem tengist þeirri upplýsinga- og fjarskiptatækniþjónustu sem aðilanum er veitt,

g) skyldu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að eiga fullt samstarf við lögbær yfirvöld og skilastjórnvöld aðila á fjármálamarkaði, þ.m.t. aðila sem þau tilnefna,

h) uppsagnarrétt og tengdan lágmarksfrest til að segja upp samningsbundnu fyrirkomulagi í samræmi við væntingar lögbærra yfirvalda og skilastjórnvalda,

i) skilyrði fyrir þátttöku þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í áætlunum aðilans á fjármálamarkaði um öryggisvitund í upplýsinga- og fjarskiptatækni og þjálfun í stafrænum rekstrarlegum viðnámsþrótti í samræmi við 6. mgr. 13. gr.

3. Samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi skal taka til a.m.k. eftirfarandi, til viðbótar við þá þætti sem um getur í 2. mgr.:

a) heildarlýsingar á þjónustustigi, þ.m.t. uppfærslna og endurskoðana á þeim, með nákvæmum megindlegum og eigindlegum frammistöðumarkmiðum innan samþykktra þjónustustiga, til að gera aðilanum á fjármálamarkaði kleift að hafa skilvirkt eftirlit með upplýsinga- og fjarskiptatækniþjónustu og grípa til viðeigandi aðgerða til úrbóta án ótilhlýðilegrar tafar ef samþykktu þjónustustigi er ekki náð,

b) uppsagnarfrests og gagnaskilakvaða þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til aðila á fjármálamarkaði, þ.m.t. tilkynningar um hvers konar þróun sem gæti haft veruleg áhrif á getu þriðja aðila til að veita skilvirka upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi í samræmi við samþykkt þjónustustig,

c) krafna til þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu um að framkvæma og prófa viðbragðsáætlanir og hafa til staðar öryggisráðstafanir, -búnað og -stefnur fyrir upplýsinga- og fjarskiptatækni sem veita aðilanum á fjármálamarkaði viðeigandi öryggi fyrir veitingu þjónustu innan regluramma síns,

d) skuldbindingar þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu um að taka þátt í og eiga fullt samstarf innan ógnamiðaðrar innbrotsprófunar aðila á fjármálamarkaði, eins og um getur í 26. og 27. gr.,

e) réttar til að vakta frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu á áframhaldandi grundvelli, sem felur í sér eftirfarandi:

i. ótakmarkaðan rétt aðila á fjármálamarkaði eða tilnefnds þriðja aðila og lögbærs yfirvalds til aðgangs, eftirlits og úttektar og rétt til að taka afrit af viðeigandi skjölum á vettvangi ef þau skipta sköpum fyrir starfsemi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og aðrar samningsbundnar ráðstafanir eða framkvæmdarstefnur koma ekki í veg fyrir eða takmarka að sé nýttur í reynd,

ii. rétt til að samþykkja annars konar fullvissustig ef réttindi annarra viðskiptavina verða fyrir áhrifum,

iii. skyldu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að hafa fullt samstarf við vettvangsathuganir og úttektir sem lögbær yfirvöld, aðaleftirlitsaðilinn, aðilinn á fjármálamarkaði eða tilnefndur þriðji aðili framkvæmir, og

iv. skyldu til að veita upplýsingar um umfang, verklag sem á að fylgja og tíðni slíkra skoðana og úttekta,

f) útgönguáætlana, einkum að komið sé á tilskildu, fullnægjandi umbreytingartímabili:

i. þar sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu heldur áfram að sinna viðkomandi starfsþáttum eða upplýsinga- og fjarskiptaþjónustu, með það fyrir augum að draga úr hættu á röskun hjá aðila á fjármálamarkaði eða tryggja skilvirka skilameðferð og endurskipulagningu hans,

ii. sem heimilar aðila á fjármálamarkaði að flytjast til annars þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða breyta yfir í innri lausnir í samræmi við flækjustig veittrar þjónustu.

Þrátt fyrir e-lið geta þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu og aðili á fjármálamarkaði sem er örfyrirtæki gert með sér samkomulag um að hægt sé að framselja rétt aðila á fjármálamarkaði til aðgangs, skoðunar og úttektar til óháðs þriðja aðila, sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu tilnefnir, og að aðilinn á fjármálamarkaði geti hvenær sem er óskað eftir upplýsingum og fullvissu um frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og geti hvenær sem er krafist upplýsinga frá þriðja aðila.

4. Við samningaviðræður um samningsbundið fyrirkomulag skulu aðilar á fjármálamarkaði og þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu íhuga að nota föst samningsákvæði sem opinber yfirvöld hafa þróað fyrir tiltekna þjónustu.

5. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, semja drög að tæknilegum eftirlitsstöðlum til að tilgreina nánar þá þætti sem um getur í a-lið 2. mgr., sem aðili á fjármálamarkaði þarf að ákvarða og meta þegar hann semur við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi.

Við gerð þessara draga að tæknilegum eftirlitsstöðlum skulu evrópsku eftirlitsstofnanirnar taka tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði og eðlis, umfangs og flækjustigs þjónustu hans, starfsemi og reksturs.

Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. júlí 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í fyrstu undirgrein í samræmi við 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

II. þáttur

Eftirlitsrammi mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu

31. gr.

Tilnefning mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu

1. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og að fengnum tilmælum frá eftirlitsvettvangnum sem komið var á fót skv. 1. mgr. 32. gr.:

a) útnefna þá þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru mikilvægir fyrir aðila á fjármálamarkaði, í kjölfar mats sem tekur tillit til viðmiðananna sem tilgreindar eru í 2. mgr.,

b) skipa sem aðaleftirlitsaðila fyrir sérhvern mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu þá evrópsku fjármálaeftirlitsstofnun sem er ábyrg, í samræmi við reglugerðir (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 eða (ESB) nr. 1095/2010, fyrir þeim aðilum á fjármálamarkaði sem eiga samtals stærstan hluta heildareigna af verðmæti heildareigna allra aðila á fjármálamarkaði sem nota þjónustu viðeigandi mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, eins og sést á samtölu einstakra efnahagsreikninga þessara aðila á fjármálamarkaði.

2. Útnefningin, sem um getur í a-lið 1. mgr., skal byggjast á öllum eftirfarandi viðmiðunum í tengslum við upplýsinga- og fjarskiptatækniþjónustu þriðja aðila:

a) kerfislægum áhrifum á stöðugleika, samfellu eða gæði veitingar fjármálaþjónustu, ef viðkomandi þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu stæði frammi fyrir umfangsmikilli rekstrarbilun við veitingu þjónustu, að teknu tilliti til fjölda aðila á fjármálamarkaði og heildarvirðis eigna aðila á fjármálamarkaði sem viðkomandi þriðji aðili veitir upplýsinga- og fjarskiptatækniþjónustu,

b) kerfiseiginleikum eða mikilvægi aðila á fjármálamarkaði sem reiða sig á viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, metið í samræmi við eftirfarandi breytur:

   i. fjölda kerfislega mikilvægra stofnana á alþjóðavísu eða annarra kerfislega mikilvægra stofnana sem reiða sig á viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

   ii. víxltengsla á milli kerfislega mikilvægra stofnana á alþjóðavísu eða annarra kerfislega mikilvægra stofnana sem um getur í i. lið, og annarra aðila á fjármálamarkaði, þ.m.t. aðstæðna þar sem kerfislega mikilvægar stofnanir á alþjóðavísu eða aðrar kerfislega mikilvægar stofnanir veita öðrum aðilum á fjármálamarkaði þjónustu á sviði fjármálainnviða,

c) hversu mikið aðilar á fjármálamarkaði reiða sig á þjónustu viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í tengslum við nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði sem á endanum felur í sér sama þriðja aðila, án tillits til þess hvort aðilar á fjármálamarkaði reiða sig á þessa þjónustu beint eða óbeint í gegnum undirverktakasamninga,

d) hversu mikil staðgönguhæfni þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu er, að teknu tilliti til eftirfarandi breytna:

   i. skortur á raunverulegum valkostum, jafnvel að hluta til, vegna takmarkaðs fjölda þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem starfa á tilteknum markaði, eða markaðshlutdeildar viðkomandi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu eða vegna þess hversu tæknilega flókin eða háþróuð starfsemi þeirra er, þ.m.t. í tengslum við tækni sem einkaleyfi er fyrir, eða vegna sérstakra eiginleika í skipulagi eða starfsemi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

   ii. erfiðleika í tengslum við að flytja, að hluta eða öllu leyti, viðkomandi gögn og vinnuálag frá viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til annars þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, annaðhvort vegna verulegs fjárhagslegs kostnaðar, tíma eða annarra tilfanga sem gætu fylgt flutningnum eða aukinnar upplýsinga- og fjarskiptatækniáhættu eða annarrar rekstraráhættu sem aðili á fjármálamarkaði gæti orðið fyrir vegna slíkra skipta.

3. Ef þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu tilheyrir samstæðu skulu viðmiðanirnar sem um getur í 2. mgr. skoðaðar í tengslum við þá upplýsinga- og fjarskiptatækniþjónustu sem samstæðan veitir í heild.

4. Mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru hluti samstæðu skulu tilnefna einn lögaðila sem samræmingaraðila til að tryggja fullnægjandi fyrirsvar og samskipti við aðaleftirlitsaðila.

5. Aðaleftirlitsaðili skal tilkynna þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu um niðurstöðu matsins sem leiðir til útnefningarinnar sem um getur í a-lið 1. mgr. Þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu getur lagt fram hjá aðaleftirlitsaðila rökstudda yfirlýsingu með hvers konar viðeigandi upplýsingum að því er varðar matið, innan sex vikna frá dagsetningu tilkynningar. Aðaleftirlitsaðili skal taka þá rökstuddu yfirlýsingu til athugunar og getur óskað eftir að viðbótarupplýsingar verði lagðar fram innan 30 almanaksdaga frá viðtöku slíkrar yfirlýsingar.

Þegar evrópsku eftirlitsstofnanirnar hafa útnefnt þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem mikilvægan skulu þær, fyrir milligöngu sameiginlegu nefndarinnar, tilkynna þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu um slíka útnefningu og frá hvaða degi þær munu í reynd falla undir eftirlitsaðgerðir. Sá upphafsdagur skal vera eigi síðar en einum mánuði eftir að tilkynning berst. Þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal tilkynna þeim aðilum á fjármálamarkaði sem hann veitir þjónustu um tilnefningu hans sem mikilvægs aðila.

6. Framkvæmdastjórninni er falið vald til að samþykkja framseldar gerðir, í samræmi við 57. gr., til að bæta við þessa reglugerð með því að tilgreina nánar þær viðmiðanir sem um getur í 2. mgr. þessarar greinar, eigi síðar en 17. júlí 2024.

7. Ekki skal nota útnefninguna sem um getur í a-lið 1. mgr. fyrr en framkvæmdastjórnin hefur samþykkt framselda gerð í samræmi við 6. mgr.

8. Útnefningin sem um getur í a-lið 1. mgr. skal ekki gilda um eftirfarandi:

i. aðila á fjármálamarkaði sem veita öðrum aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu,

ii. þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og falla undir eftirlitsramma sem komið er á fót í þeim tilgangi að styðja við verkefnin sem um getur í 2. mgr. 127. gr. sáttmálans um starfshætti Evrópusambandsins,

iii. veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu,

iv. þriðju aðila sem veita eingöngu upplýsinga- og fjarskiptatækniþjónustu í einu aðildarríki til aðila á fjármálamarkaði sem starfa eingöngu í því aðildarríki.

9. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, koma á fót, birta og uppfæra árlega skrá yfir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu á vettvangi Sambandsins.

10. Að því er varðar a-lið 1. mgr. skulu lögbær yfirvöld senda skýrslurnar, sem um getur í þriðju undirgrein 3. mgr. 28. gr., árlega og í samanteknu formi á eftirlitsvettvanginn sem komið var á fót skv. 32. gr. Eftirlitsvettvangurinn skal meta hversu háðir aðilar á fjármálamarkaði eru þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu miðað við upplýsingar frá lögbærum yfirvöldum.

11. Þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu en eru ekki tilgreindir í skránni sem um getur í 9. mgr. geta óskað eftir því að vera útnefndir sem mikilvægir í samræmi við a-lið 1. mgr.

Að því er fyrstu undirgrein varðar skal þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu leggja fram rökstudda umsókn til Evrópsku bankaeftirlitsstofnunarinnar, Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunarinnar sem skal, fyrir milligöngu sameiginlegu nefndarinnar, ákveða hvort útnefna eigi viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem mikilvægan í samræmi við a-lið 1. mgr.

Ákvörðunin sem um getur í annarri undirgrein skal samþykkt og tilkynnt hinum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu innan sex mánaða frá móttöku umsóknarinnar.

12. Aðilar á fjármálamarkaði skulu aðeins nýta sér þjónustu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi og sem hefur verið útnefndur sem mikilvægur í samræmi við a-lið 1. mgr. ef sá síðarnefndi hefur stofnað dótturfélag í Sambandinu innan 12 mánaða frá útnefningu.

13. Mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu og um getur í 12. mgr. skal tilkynna aðaleftirlitsaðila um allar breytingar á stjórnskipulagi dótturfélags sem komið er á fót í Sambandinu.

32. gr.

Skipulag eftirlitsramma

1. Sameiginlega nefndin skal, í samræmi við 1. mgr. 57. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010, koma eftirlitsvettvangnum á fót sem undirnefnd til að styðja við starf sameiginlegu nefndarinnar og aðaleftirlitsaðilans, sem um getur í b-lið 1. mgr. 31. gr., á sviði upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila í öllum fjármálageirum. Á eftirlitsvettvangnum skal semja drög að sameiginlegri afstöðu og sameiginlegum gerðum sameiginlegu nefndarinnar á því sviði.

Á eftirlitsvettvangnum skal reglulega ræða viðkomandi þróun á áhættu og veikleikum í upplýsinga- og fjarskiptatækni og stuðla að samræmdri nálgun við vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila á vettvangi Sambandsins.

2. Á eftirlitsvettvangnum skal á ársgrundvelli gera sameiginlegt mat á útkomu og niðurstöðum eftirlitsaðgerða sem gerðar eru hjá öllum mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og stuðla að samræmingarráðstöfunum til að auka stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði, hlúa að bestu starfsvenjum við að takast á við samþjöppunaráhættu í upplýsinga- og fjarskiptatækni og kanna aðgerðir til að milda yfirfærslu áhættu þvert á atvinnugreinar.

3. Á eftirlitsvettvangnum skal leggja fram ítarlegar viðmiðanir fyrir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem sameiginlega nefndin á að samþykkja sem sameiginlega afstöðu evrópsku eftirlitsstofnananna í samræmi við 1. mgr. 56. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010.

4. Eftirlitsvettvangurinn skal samanstanda af:

a) formönnum evrópsku eftirlitsstofnananna,

b) einum háttsettum fulltrúa frá núverandi starfsfólki viðkomandi lögbærs yfirvalds sem, um getur í 46. gr., frá hverju aðildarríki,

c) framkvæmdastjóra allra evrópsku eftirlitsstofnananna og einum fulltrúa frá framkvæmdastjórninni, Evrópska kerfisáhætturáðinu, Seðlabanka Evrópu og Netöryggisstofnun Evrópusambandsins sem áheyrnarfulltrúa,

d) eftir því sem við á, einum viðbótarfulltrúa lögbærs yfirvalds, sem um getur í 46. gr., frá hverju aðildarríki sem áheyrnarfulltrúa,

e) eftir atvikum, einum fulltrúa þeirra lögbæru yfirvalda sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555 og bera ábyrgð á eftirliti með nauðsynlegri eða mikilvægri rekstrareiningu sem fellur undir þá tilskipun og hefur verið tilnefnd sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu, sem áheyrnarfulltrúa.

Eftirlitsvettvangurinn getur, eftir því sem við á, leitað ráða hjá óháðum sérfræðingum sem skipaðir eru í samræmi við 6. mgr.

5. Sérhvert aðildarríki skal tilnefna hið viðkomandi lögbæra yfirvald sem sendir starfsmann sinn til að vera háttsetti fulltrúinn sem um getur í b-lið fyrstu undirgreinar 4. mgr. og skal tilkynna aðaleftirlitsaðila um það.

Evrópsku eftirlitsstofnanirnar skulu birta á vefsetri sínu skrá yfir háttsetta fulltrúa úr hópi núverandi starfsfólks þess viðeigandi lögbæra yfirvalds sem aðildarríkin tilnefna.

6. Eftirlitsvettvangurinn skal tilnefna óháðu sérfræðingana, sem um getur í annarri undirgrein 4. mgr., úr hópi sérfræðinga sem valdir eru í kjölfar opinbers og gagnsæs umsóknarferlis.

Óháðu sérfræðingarnir skulu skipaðir á grundvelli sérþekkingar sinnar á fjármálastöðugleika, stafrænum rekstrarlegum viðnámsþrótti og öryggismálum í upplýsinga- og fjarskiptatækni. Þeir skulu starfa með sjálfstæðum og hlutlægum hætti í þágu alls Sambandsins og skulu hvorki leita eftir né taka við fyrirmælum frá stofnunum eða aðilum Sambandsins, frá ríkisstjórn aðildarríkis eða nokkrum öðrum opinberum aðila eða einkaaðila.

7. Að því er varðar þennan þátt skulu evrópsku eftirlitsstofnanirnar, í samræmi við 16. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010, eigi síðar en 17. júlí 2024 gefa út viðmiðunarreglur um samstarf evrópsku eftirlitsstofnananna og lögbærra yfirvalda, sem taka til nákvæmra verklagsreglna og skilyrða fyrir ráðstöfun og framkvæmd verkefna milli lögbærra yfirvalda og evrópsku eftirlitsstofnananna og ítarlegra upplýsinga um upplýsingaskipti sem eru nauðsynleg lögbærum yfirvöldum til að tryggja eftirfylgni með tilmælum, skv. d-lið 1. mgr. 35. gr., sem beint er til mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

8. Kröfurnar sem settar eru fram í þessum þætti skulu ekki hafa áhrif á beitingu tilskipunar (ESB) 2022/2555 og annarra reglna Sambandsins um eftirlit sem gildir um veitendur skýjavinnsluþjónustu.

9. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar og á grundvelli undirbúningsvinnu eftirlitsvettvangsins, leggja árlega skýrslu fyrir Evrópuþingið, ráðið og framkvæmdastjórnina um beitingu þessa þáttar.

33. gr.

Verkefni aðaleftirlitsaðila

1. Aðaleftirlitsaðilinn, sem skipaður er í samræmi við b-lið 1. mgr. 31. gr., skal hafa eftirlit með útnefndum mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og vera helsti tengiliður þessara mikilvægu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, að því er varðar öll mál sem tengjast eftirlitinu.

2. Að því er varðar 1. mgr. skal aðaleftirlitsaðili meta hvort sérhver mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hafi sett heildstæðar, traustar og skilvirkar reglur, verklagsreglur, fyrirkomulag og ráðstafanir til að stýra þeirri upplýsinga- og fjarskiptatækniáhættu sem hann kann að valda aðilum á fjármálamarkaði.

Matið sem um getur í fyrstu undirgrein skal einkum beinast að upplýsinga- og fjarskiptatækniþjónustu hins mikilvæga þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði. Ef nauðsyn krefur til að taka á allri viðeigandi áhættu skal það mat ná til annarra stoðþátta upplýsinga- og fjarskiptatækniþjónustu en þeirra sem eru nauðsynlegir eða mikilvægir.

3. Matið sem um getur í 2. mgr. skal taka til:

a) upplýsinga- og fjarskiptatæknikrafna til að tryggja einkum öryggi, aðgengi, samfellu, skalanleika og gæði upplýsinga- og fjarskiptatækniþjónustu sem mikilvægur þriðji aðili veitir aðilum á fjármálamarkaði, auk getu til að viðhalda ávallt ströngum kröfum um tiltækileika, ósvikni, réttleika eða leynd gagna,

b) raunlægs öryggis sem stuðlar að því að tryggja öryggi í upplýsinga- og fjarskiptatækni, þ.m.t. öryggi athafnasvæða, aðstöðu, gagnavera,

c) áhættustýringarferla, þ.m.t. áhættustýringarstefna í upplýsinga- og fjarskiptatækni, stefnu um rekstrarsamfellu og viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni,

d) stjórnunarhátta, þ.m.t. stjórnskipulags með skýra, gagnsæja og samræmda skiptingu ábyrgðar og reglna um ábyrgð sem gera skilvirka stýringu upplýsinga- og fjarskiptatækniáhættu mögulega,

e) greiningar, vöktunar og tafarlausrar tilkynningar um mikilvæg atvik sem tengjast upplýsinga- og fjarskiptatækni til aðila á fjármálamarkaði, stjórnun og úrlausn þessara atvika, einkum netárása,

f) fyrirkomulags varðandi flytjanleika gagna, flytjanleika og samvirkni forrita, sem tryggir að aðilar á fjármálamarkaði geti neytt uppsagnarréttar með skilvirkum hætti,

g) prófunar á kerfum, innviðum og eftirlitsaðferðum í upplýsinga- og fjarskiptatækni,

h) úttekta á upplýsinga- og fjarskiptatækni,

i) notkunar á landsbundnum og alþjóðlegum stöðlum sem gilda um veitingu upplýsinga- og fjarskiptatækniþjónustu til aðila á fjármálamarkaði.

4. Á grundvelli matsins, sem um getur í 2. mgr., og í samráði við sameiginlega eftirlitskerfið (JON), sem um getur í 1. mgr. 34. gr., skal aðaleftirlitsaðili innleiða skýra, ítarlega og rökstudda, sérsniðna eftirlitsáætlun þar sem lýst er árlegum eftirlitsmarkmiðum og helstu eftirlitsaðgerðum sem eru fyrirhugaðar fyrir sérhvern mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Sú áætlun skal árlega tilkynnt mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

Áður en eftirlitsáætlun er samþykkt skal aðaleftirlitsaðili senda drög að eftirlitsáætluninni til mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

Þegar mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur móttekið drög að eftirlitsáætlun er honum heimilt að leggja fram rökstudda yfirlýsingu innan 15 almanaksdaga sem sýnir fram á áætluð áhrif á viðskiptavini sem eru aðilar sem falla utan gildissviðs þessarar reglugerðar og, eftir því sem við á, móta lausnir til að draga úr áhættu.

5. Þegar árlegu eftirlitsáætlanirnar, sem um getur í 4. mgr., hafa verið samþykktar og tilkynntar mikilvægum þriðju aðilum í upplýsinga- og fjarskiptatækni geta lögbær yfirvöld aðeins gert ráðstafanir varðandi slíka mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu í samráði við aðaleftirlitsaðila.

34. gr.

Rekstrarleg samræming á milli aðaleftirlitsaðila

1. Til að tryggja samræmda nálgun við eftirlitsaðgerðir og gera kleift að samræma almennar stefnuáætlanir um eftirlit og heildstæðar rekstrar- og vinnuaðferðir skulu aðaleftirlitsaðilarnir þrír, sem tilnefndir eru í samræmi við b-lið 1. mgr. 31. gr., setja upp sameiginlegt eftirlitskerfi (JON) til að samræma sín á milli við undirbúning og til að samræma eftirlitsaðgerðir hjá mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem þeir hafa eftirlit með, sem og við hverja þá aðgerð sem kann að vera þörf á skv. 42. gr.

2. Að því er varðar 1. mgr. skulu aðaleftirlitsaðilar semja sameiginlegar reglur um eftirlit sem tilgreina ítarlegt verklag sem fylgja skal við framkvæmd á samræmingu frá degi til dags og til að tryggja skjót skipti og viðbrögð. Reglurnar skulu endurskoðaðar reglulega svo þær endurspegli rekstrarlegar þarfir, einkum þróun á hagnýtu eftirlitsfyrirkomulagi.

3. Aðaleftirlitsaðilar geta, eftir þörfum, óskað eftir því að Seðlabanki Evrópu og Netöryggisstofnun Evrópusambandsins veiti tækniráðgjöf, miðli hagnýtri reynslu eða taki þátt í sérstökum samræmingarfundum sameiginlega eftirlitskerfisins (JON).

35. gr.

Heimildir aðaleftirlitsaðila

1. Í þeim tilgangi að sinna þeim skyldum sem mælt er fyrir um í þessum þætti skal aðaleftirlitsaðili hafa eftirfarandi valdheimildir að því er varðar mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu:

a) til að óska eftir öllum viðeigandi upplýsingum og gögnum í samræmi við 37. gr.,

b) til að gera almennar rannsóknir og skoðanir í samræmi við 38. og 39. gr., eftir því sem við á,

c) til að óska eftir skýrslum þegar eftirlitsaðgerðum er lokið, þar sem tilgreindar eru aðgerðir sem gripið hefur verið til eða úrræði sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafa beitt í tengslum við tilmælin sem um getur í d-lið þessarar málsgreinar,

d) til að gefa út tilmæli á þeim sviðum sem um getur í 3. mgr. 33. gr., einkum að því er varðar eftirfarandi:

   i. notkun sértækra öryggis- eða gæðakrafna eða -ferla í upplýsinga- og fjarskiptatækni, einkum í tengslum við útgáfu á bótum, uppfærslum, dulkóðun og öðrum öryggisráðstöfunum sem aðaleftirlitsaðili telur skipta máli til að tryggja öryggi í upplýsinga- og fjarskiptatækni í þjónustu sem aðilum á fjármálamarkaði er veitt,

   ii. notkun skilyrða og skilmála, þ.m.t. tæknileg framkvæmd þeirra, sem gilda um það þegar mikilvægir þriðju aðilar veita aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu sem aðaleftirlitsaðili telur skipta máli til að koma í veg fyrir myndun stakra bilanapunkta, mögnun þeirra eða til að lágmarka hugsanleg kerfislæg áhrif í fjármálageira Sambandsins ef upp kemur samþjöppunaráhætta í upplýsinga- og fjarskiptatækni,

   iii. hvers kyns fyrirhugaða undirverktöku, ef aðaleftirlitsaðili telur að frekari undirverktakastarfsemi, þ.m.t. undirverktakasamningar sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hyggjast gera við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu eða undirverktaka í upplýsinga- og fjarskiptatækni með staðfestu í þriðja landi, geti valdið áhættu fyrir þjónustu aðilans á fjármálamarkaði eða áhættu fyrir fjármálastöðugleika, á grundvelli könnunar á upplýsingunum sem safnað er í samræmi við 37. og 38. gr.,

   iv. að forðast að gera frekari undirverktakasamninga ef eftirfarandi samanlögð skilyrði eru uppfyllt:

      — fyrirhugaður undirverktaki er þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu eða undirverktaki í upplýsinga- og fjarskiptatækni með staðfestu í þriðja landi,

      — undirverktakastarfsemi varðar nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði, og

— aðaleftirlitsaðili telur að notkun slíkra undirverktakasamninga hafi í för með sér skýra og alvarlega áhættu fyrir fjármálastöðugleika Sambandsins eða fyrir aðila á fjármálamarkaði, þ.m.t. getu aðila til að fullnægja eftirlitskröfum.

Að því er varðar iv. lið þessa liðar skulu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu senda upplýsingar varðandi undirverktakastarfsemi til aðaleftirlitsaðila með því að nota sniðmátið sem um getur í b-lið 1. mgr. 41. gr.

2. Þegar aðaleftirlitsaðili beitir þeim valdheimildum, sem um getur í þessari grein, skal hann:

a) tryggja reglulega samræmingu innan sameiginlega eftirlitskerfisins (JON), einkum skal leitast við að beita samræmdum aðferðum, eins og við á, að því er varðar eftirlit með mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,

b) taka tilhlýðilegt tillit til rammans sem komið er á með tilskipun (ESB) 2022/2555 og, ef nauðsyn krefur, hafa samráð við viðkomandi lögbær yfirvöld sem eru tilnefnd eða komið á fót í samræmi við þá tilskipun, til að draga úr tvíverknaði við tækni- og skipulagsráðstafanir sem gætu gilt um mikilvæga þriðju aðila á sviði upplýsinga- og fjarskiptatækni samkvæmt þeirri tilskipun,

c) leitast við að lágmarka, að því marki sem mögulegt er, hættu á röskun á þjónustu sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veita viðskiptavinum sem eru aðilar sem falla utan gildissviðs þessarar reglugerðar.

3. Aðaleftirlitsaðili skal hafa samráð við eftirlitsvettvanginn áður en hann beitir þeim valdheimildum sem um getur í 1. mgr.

Áður en tilmæli eru gefin út í samræmi við d-lið 1. mgr. skal aðaleftirlitsaðili gefa þjónustuveitanda þriðja aðila í upplýsinga- og fjarskiptatækni tækifæri til að veita viðeigandi upplýsingar innan 30 almanaksdaga, sem sýna fram á væntanleg áhrif á viðskiptavini sem eru aðilar sem falla utan gildissviðs þessarar reglugerðar og, eftir því sem við á, setja fram lausnir til að draga úr áhættu.

4. Aðaleftirlitsaðili skal tilkynna sameiginlega eftirlitskerfinu (JON) um niðurstöðu beitingar þeirra valdheimilda sem um getur í a- og b-lið 1. mgr. Aðaleftirlitsaðili skal, án ástæðulausrar tafar, senda skýrslurnar sem um getur í c-lið 1. mgr. til sameiginlega eftirlitskerfisins (JON) og til lögbærra yfirvalda á fjármálamarkaði sem nota upplýsinga- og fjarskiptatækniþjónustu þess mikilvæga þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

5. Mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skulu starfa með aðaleftirlitsaðila í góðri trú og aðstoða hann við að leysa verkefni sín.

6. Ef ekki er farið að öllum eða hluta ráðstafana sem grípa þarf til samkvæmt beitingu valdheimildanna sem kveðið er á um í a-, b- og c-lið 1. mgr. og þegar a.m.k. 30 almanaksdagar eru liðnir frá þeim degi sem mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu barst tilkynning um viðkomandi ráðstafanir, skal aðaleftirlitsaðili samþykkja ákvörðun um að leggja á févíti til að neyða mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að hlíta þeim ráðstöfunum.

7. Févítinu sem um getur í 6. mgr. skal beitt daglega þar til skilyrðin eru uppfyllt og eigi lengur en í sex mánuði eftir að tilkynnt er um ákvörðun um að leggja févíti á mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

8. Fjárhæð févítis, reiknuð út frá þeim degi sem mælt er fyrir um í ákvörðun um álagningu févíta, skal vera allt að 1% af meðaldagsveltu á heimsvísu hjá mikilvæga þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu á næstliðnu rekstrarári. Við ákvörðun á fjárhæð févítis skal aðaleftirlitsaðili taka tillit til eftirfarandi viðmiðana um að ekki sé farið að þeim ráðstöfunum sem um getur í 6. mgr.:

a) alvarleika og tímalengdar vanefnda,

b) hvort vanefndir á ákvæðum hafi verið framdar af ásetningi eða gáleysi,

c) vilja þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til samstarfs við aðaleftirlitsaðila.

Að því er varðar fyrstu undirgrein skal aðaleftirlitsaðili hafa samráð innan sameiginlega eftirlitskerfisins (JON) til að tryggja samræmda nálgun.

9. Févíti skulu vera stjórnsýslulegs eðlis og framfylgjanleg. Framfylgd skal vera í samræmi við gildandi réttarfarsreglur í einkamálum í aðildarríkinu þar sem eftirlit og aðgengi mun fara fram. Dómstólar hlutaðeigandi aðildarríkis skulu hafa lögsögu í kvörtunum vegna óeðlilegrar háttsemi við framfylgd laga. Fjárhæðir févíta skulu renna til fjárlaga Evrópusambandsins.

10. Aðaleftirlitsaðili skal birta opinberlega öll févíti sem hafa verið lögð á, nema slík birting upplýsinga myndi tefla fjármálamarkaðnum í tvísýnu eða valda hlutaðeigandi aðilum óhóflegum skaða.

11. Áður en til greiðslu févítis skv. 6. mgr. kemur skal aðaleftirlitsaðili gefa fulltrúum mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, og sætir málsmeðferð, tækifæri til að tjá sig um niðurstöðurnar og skal hann einungis byggja ákvarðanir sínar á þeim niðurstöðum sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu og sætir málsmeðferð hefur fengið tækifæri til að gera athugasemdir við.

Réttur aðilanna sem falla undir málsmeðferðina til varnar skal virtur að fullu í málsmeðferðinni. Mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu og sætir málsmeðferð skal eiga rétt á aðgangi að málsskjölunum, með fyrirvara um lögmæta hagsmuni annarra aðila til verndar viðskiptaleyndarmála sinna. Réttur til aðgangs að málsskjölunum nær hvorki til trúnaðarupplýsinga né innri undirbúningsskjala aðaleftirlitsaðila.

36. gr.

Beiting valdheimilda aðaleftirlitsaðila utan Sambandsins

1. Þegar ekki er hægt að ná eftirlitsmarkmiðum með samskiptum við dótturfélag sem komið er á fót að því er varðar 12. mgr. 31. gr. eða með eftirlitsaðgerðum á athafnasvæði sem staðsett er í Sambandinu getur aðaleftirlitsaðili beitt valdheimildum sínum, sem um getur í eftirfarandi ákvæðum, á athafnasvæði sem staðsett er í þriðja landi sem er í eigu, eða notað með einhverjum hætti, í þeim tilgangi að mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu geti veitt aðilum á fjármálamarkaði Sambandsins þjónustu í tengslum við viðskiptaþjónustu, starfsemi eða þjónustu, þ.m.t. stjórnsýslu-, viðskipta- eða rekstrarskrifstofur, athafnasvæði, lóðir, byggingar eða aðrar eignir:

a) í a-lið 1. mgr. 35. gr., og

b) í b-lið 1. mgr. 35. gr., í samræmi við a-, b- og d-lið 2. mgr. 38. gr. og í 1. mgr. og a-lið 2. mgr. 39. gr.

Heimilt er að beita þeim heimildum sem um getur í fyrstu undirgrein að uppfylltum öllum eftirfarandi skilyrðum:

i. aðaleftirlitsaðili telur framkvæmd skoðunar í þriðja landi nauðsynlega til að hann geti uppfyllt skyldur sínar að fullu og með skilvirkum hætti samkvæmt þessari reglugerð,

ii. eftirlit í þriðja landi er í beinum tengslum við veitingu upplýsinga- og fjarskiptatækniþjónustu til aðila á fjármálamarkaði í Sambandinu,

iii. viðkomandi mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu samþykkir að eftirlitsúttekt fari fram í þriðja landi, og

iv. aðaleftirlitsaðili hefur formlega tilkynnt viðkomandi yfirvaldi hlutaðeigandi þriðja lands um það og það ekki hreyft andmælum við því.

2. Með fyrirvara um viðkomandi valdsvið stofnana Sambandsins og aðildarríkja, að því er varðar 1. mgr., skulu Evrópska bankaeftirlitsstofnunin, Evrópska verðbréfamarkaðseftirlitsstofnunin eða Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin gera ráðstafanir til samvinnu á sviði stjórnsýslu við viðeigandi yfirvald í þriðja landi til að auðvelda aðaleftirlitsaðila og tilnefndum hópum hans snurðulausa framkvæmd skoðana í hlutaðeigandi þriðja landi að því er varðar verkefni hans í því þriðja landi. Samstarfssamningarnir skulu hvorki stofna til lagaskyldna fyrir Sambandið og aðildarríki þess né skal það hindra að aðildarríkin og lögbær yfirvöld þeirra gangi frá tvíhliða eða marghliða samkomulagi við þessi þriðju lönd og viðkomandi yfirvöld þeirra.

Samstarfssamningarnir skulu tilgreina a.m.k. eftirfarandi þætti:

a) verklag um samræmingu eftirlitsstarfsemi sem framkvæmd er samkvæmt þessari reglugerð og hvers kyns hliðstæðs eftirlits með upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila í fjármálageiranum sem viðkomandi yfirvald hlutaðeigandi þriðja lands framkvæmir, þ.m.t. upplýsingar um framsendingu samþykkis þess síðarnefnda til að gera aðaleftirlitsaðila og tilnefnda hópnum hans kleift að framkvæma almennar rannsóknir og vettvangsskoðanir, eins og um getur í fyrstu undirgrein 1. mgr., á yfirráðasvæði innan lögsögu þess,

b) fyrirkomulag við sendingu viðeigandi upplýsinga milli Evrópsku bankaeftirlitsstofnunarinnar, Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunarinnar og viðeigandi yfirvalds hlutaðeigandi þriðja lands, einkum í tengslum við upplýsingar sem aðaleftirlitsaðili gæti óskað eftir skv. 37. gr.,

c) fyrirkomulag tafarlausrar tilkynningar frá viðeigandi yfirvaldi í hlutaðeigandi þriðja landi til Evrópsku bankaeftirlitsstofnunarinnar, Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnunarinnar um tilvik þar sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi, sem telst vera mikilvægur í samræmi við a-lið 1. mgr. 31. gr., telst hafa brotið í bága við kröfurnar sem honum ber skylda til að fylgja samkvæmt gildandi lögum í hlutaðeigandi þriðja landi þegar hann veitir aðilum á fjármálamarkaði í því þriðja landi þjónustu, sem og þau úrræði og viðurlög sem beitt er,

d) reglulega afhendingu uppfærðra upplýsinga um þróun á sviði reglusetningar eða eftirlits varðandi vöktun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila hjá aðilum á fjármálamarkaði í hlutaðeigandi þriðja landi,

e) upplýsingar um framvindu eftirlits ef þörf krefur, með þátttöku eins fulltrúa viðkomandi yfirvalds í þriðja landi í eftirliti sem aðaleftirlitsaðili og tilnefndur hópur framkvæma.

3. Verði aðaleftirlitsaðili ófær um að annast eftirlitsstarfsemi utan Sambandsins, sem um getur í 1. og 2. mgr., skal hann:

a) beita valdheimildum sínum skv. 35. gr. á grundvelli allra málsatvika og skjala sem hann hefur aðgang að,

b) skjalfesta og útskýra hvers kyns afleiðingar af vanhæfni sinni til að annast fyrirhugaða eftirlitsstarfsemi eins og um getur í þessari grein.

Taka skal tillit til hugsanlegra afleiðinga, sem um getur í b-lið þessarar málsgreinar, í tilmælum aðaleftirlitsaðila sem gefin eru út skv. d-lið 1. mgr. 35. gr.

37. gr.

Beiðni um upplýsingar

1. Aðaleftirlitsaðili getur, með einfaldri beiðni eða ákvörðun, krafið mikilvæga þriðja aðila sem veita upplýsinga- og fjarskiptatækniþjónustu um allar upplýsingar sem aðaleftirlitsaðili þarf á að halda til að geta sinnt skyldum sínum samkvæmt þessari reglugerð, þ.m.t. öll viðeigandi viðskipta- eða rekstrargögn, samningar, stefnur, skjöl, skýrslur um öryggisúttektir í upplýsinga- og fjarskiptatækni, skýrslur um atvik sem tengjast upplýsinga- og fjarskiptatækni, sem og hvers kyns upplýsingar um aðila sem þessi mikilvægi þriðji aðili hefur útvistað rekstrarþáttum eða starfsemi til.

2. Þegar aðaleftirlitsaðili sendir einfalda beiðni um upplýsingar skv. 1. mgr. skal hann:

a) vísa til þessarar greinar sem lagagrundvallar beiðninnar,

b) tilgreina tilgang beiðninnar,

c) tilgreina hvaða upplýsinga er krafist,

d) setja tímamörk sem virða skal við afhendingu upplýsinganna,

e) upplýsa fulltrúa mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, og sem óskað er eftir upplýsingum frá, um að viðkomanda sé ekki skylt að veita upplýsingarnar, en ef beiðninni er svarað að eigin ákvörðun megi upplýsingarnar ekki vera rangar eða villandi.

3. Þegar krafist er afhendingar upplýsinga skv. 1. mgr. með ákvörðun skal aðaleftirlitsaðili:

a) vísa til þessarar greinar sem lagagrundvallar beiðninnar,

b) tilgreina tilgang beiðninnar,

c) tilgreina hvaða upplýsinga er krafist,

d) setja tímamörk sem virða skal við afhendingu upplýsinganna,

e) tilgreina févítin sem kveðið er á um í 6. mgr. 35. gr., ef tilskildar upplýsingar eru ófullnægjandi eða ef slíkar upplýsingar eru ekki veittar innan þeirra tímamarka sem um getur í d-lið þessarar málsgreinar,

f) tilgreina rétt til að áfrýja ákvörðuninni til kærunefndar evrópsku eftirlitsstofnunarinnar og til að fá Evrópudómstólinn til að endurskoða ákvörðunina í samræmi við 60. og 61. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010.

4. Fulltrúar mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu skulu veita umbeðnar upplýsingar. Lögmönnum sem til þess hafa fullt umboð er heimilt að veita upplýsingar fyrir hönd skjólstæðinga sinna. Hinn mikilvægi þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal bera fulla ábyrgð á því ef veittar upplýsingar eru ófullgerðar, rangar eða villandi.

5. Aðaleftirlitsaðili skal án tafar senda afrit af ákvörðun um að veita upplýsingar til lögbærra yfirvalda aðila á fjármálamarkaði, sem nota þjónustu viðkomandi mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, og sameiginlega eftirlitskerfisins (JON).

38. gr.

Almennar rannsóknir

1. Til að sinna verkefnum sínum samkvæmt þessari reglugerð getur aðaleftirlitsaðili, með aðstoð sameiginlega skoðunarhópsins sem um getur í 1. mgr. 40. gr., ef nauðsyn krefur, framkvæmt rannsóknir á mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu.

2. Aðaleftirlitsaðili skal hafa heimild til að:

a) athuga skrár, öll gögn, verklagsreglur og annað efni sem varðar framkvæmd verkefna hennar óháð því hver geymslumiðill þess er,

b) taka afrit eða fá vottuð afrit af, eða útdrætti úr, slíkum skrám, gögnum, staðfestum verklagsreglum eða hvers kyns öðru efni,

c) fara fram á að fulltrúar mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu veiti munnlegar eða skriflegar útskýringar á málavöxtum eða gögnum í tengslum við viðfangsefnið og tilgang rannsóknarinnar og til að skrá svörin,

d) taka viðtöl við aðra einstaklinga eða lögaðila sem samþykkja að veita viðtal í þeim tilgangi að safna upplýsingum að því er varðar viðfangsefni rannsóknar,

e) óska eftir skrám varðandi símtöl og gagnaumferð.

3. Embættismenn og aðrir aðilar sem aðaleftirlitsaðili hefur veitt heimild til þeirrar rannsóknar sem um getur í 1. mgr. skulu beita valdheimildum sínum að fenginni skriflegri heimild sem tilgreinir viðfangsefni og tilgang rannsóknarinnar.

Í þeirri heimild skal einnig tilgreina févíti sem kveðið er á um í 6. mgr. 35. gr. ef tilskildar skrár, gögn, skjalfestar verklagsreglur eða önnur gögn, sem framvísað hefur verið, eða svör við spurningum sem lagðar eru fyrir fulltrúa þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eru ekki veitt eða eru ófullnægjandi.

4. Fulltrúar mikilvægra þriðja aðila sem veita upplýsinga- og fjarskiptatækniþjónustu þurfa að gangast undir rannsóknir á grundvelli ákvörðunar aðaleftirlitsaðila. Ákvörðunin skal tilgreina viðfangsefni og tilgang rannsóknarinnar, févíti sem kveðið er á um í 6. mgr. 35. gr., lagaleg úrræði sem standa til boða samkvæmt reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010, auk réttarins á því að Dómstóllinn taki ákvörðunina til endurskoðunar.

5. Með góðum fyrirvara áður en rannsókn hefst skal aðaleftirlitsaðili upplýsa lögbær yfirvöld þeirra aðila á fjármálamarkaði sem nota upplýsinga- og fjarskiptatækniþjónustu þess mikilvæga þriðja aðila um fyrirhugaða rannsókn og deili á starfsmönnum með heimild.

Aðaleftirlitsaðili skal senda allar upplýsingar, sem sendar eru samkvæmt fyrstu undirgrein, til sameiginlega eftirlitskerfisins (JON).

39. gr.

Skoðanir

1. Til að sinna skyldum sínum samkvæmt þessari reglugerð getur aðaleftirlitsaðili, með aðstoð sameiginlegu skoðunarhópanna sem um getur í 1. mgr. 40. gr., farið inn á og framkvæmt allar nauðsynlegar vettvangsskoðanir á starfsstöðvum, landi eða eignum þriðja aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, s.s. á aðalskrifstofum, rekstrarstöðvum, aukastarfsstöðvum, ásamt því að framkvæma skoðanir utan vettvangs.

Við beitingu þeirra heimilda sem um getur í fyrstu undirgrein skal aðaleftirlitsaðili hafa samráð við sameiginlega eftirlitskerfið (JON).

2. Embættismenn og aðrir aðilar sem aðaleftirlitsaðili hefur veitt heimild til að framkvæma vettvangsskoðun, skulu hafa vald til að:

a) fara inn á slíkt athafnasvæði, land eða eignir, og

b) innsigla hvers kyns athafnasvæði, bókhald eða viðskiptaskjöl í þann tíma og að því marki sem nauðsynlegt er vegna skoðunarinnar.

Embættismenn og aðrir aðilar sem hafa heimild aðaleftirlitsaðila skulu beita valdheimildum sínum að fenginni skriflegri heimild sem tilgreinir viðfangsefni og tilgang skoðunarinnar, sem og févíti sem kveðið er á um í 6. mgr. 35. gr., ef fulltrúar hlutaðeigandi mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu gangast ekki undir skoðunina.

3. Aðaleftirlitsaðili skal upplýsa lögbær yfirvöld aðila á fjármálamarkaði, sem nota þennan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, með góðum fyrirvara áður en rannsókn hefst.

4. Skoðanir skulu ná yfir allt svið viðeigandi kerfa, neta, tækja, upplýsinga og gagna í upplýsinga- og fjarskiptatækni, sem annaðhvort eru notuð til að veita aðilum á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu eða stuðla að því að þeir hljóti slíka þjónustu.

5. Áður en fyrirhuguð vettvangsskoðun fer fram skal aðaleftirlitsaðili tilkynna hinum mikilvægu þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu um það með hæfilegum fyrirvara, nema slík tilkynning sé ekki möguleg vegna neyðar- eða krísuástands eða ef hún leiðir til ástands þar sem rannsókn eða úttekt myndi ekki lengur skila árangri.

6. Mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal gangast undir vettvangsskoðanir sem fyrirskipaðar eru með ákvörðun aðaleftirlitsaðila. Ákvörðunin skal tilgreina viðfangsefni og tilgang skoðunarinnar, dagsetninguna sem hefja skal skoðunina og févíti sem kveðið er á um í 6. mgr. 35. gr., tiltæk lagaleg úrræði samkvæmt reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og (ESB) nr. 1095/2010 og réttinn til að Dómstóllinn taki ákvörðunina til endurskoðunar.

7. Ef embættismenn og aðrir aðilar sem hafa heimild frá aðaleftirlitsaðila komast að raun um að mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu leggist gegn skoðun sem fyrirskipuð er samkvæmt þessari grein skal aðaleftirlitsaðili upplýsa mikilvæga þriðja aðilann sem veitir upplýsinga- og fjarskiptatækniþjónustu um afleiðingar slíkrar andstöðu, þ.m.t. möguleikann á því að lögbær yfirvöld viðkomandi aðila á fjármálamarkaði krefjist þess að aðilar á fjármálamarkaði slíti samningsbundnu fyrirkomulagi við þennan mikilvæga þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

40. gr.

Viðvarandi eftirlit

1. Við framkvæmd eftirlitsstarfsemi, einkum almennra rannsókna eða skoðana, skal aðaleftirlitsaðili njóta aðstoðar sameiginlegs skoðunarhóps sem komið er á fót fyrir hvern mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

2. Í sameiginlega skoðunarhópnum, sem um getur í 1. mgr., skulu vera starfsmenn frá:

a) Evrópsku eftirlitsstofnununum,

b) viðkomandi lögbærum yfirvöldum sem hafa eftirlit með aðilum á fjármálamarkaði sem mikilvægur þriðji aðili veitir upplýsinga- og fjarskiptatækniþjónustu,

c) lögbærum landsyfirvöldum, sem um getur í e-lið 4. mgr. 32. gr., að eigin vali,

d) einu lögbæru landsyfirvaldi frá aðildarríkinu þar sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur staðfestu, að eigin vali.

Aðilar í sameiginlega skoðunarhópnum skulu búa yfir sérþekkingu á upplýsinga- og fjarskiptatæknimálum og rekstraráhættu. Samræmingarhlutverk í sameiginlega skoðunarhópunum skal vera í höndum tilnefnds starfsmanns aðaleftirlitsaðila (hér á eftir nefndur „samræmingaraðili aðaleftirlits“).

3. Innan þriggja mánaða frá því að rannsókn eða skoðun lýkur skal aðaleftirlitsaðili, að höfðu samráði við eftirlitsvettvanginn, samþykkja tilmæli sem beint er til mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu samkvæmt valdheimildunum sem um getur í 35. gr.

4. Tilmælin sem um getur í 3. mgr. skulu tafarlaust tilkynnt mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og lögbærum yfirvöldum þeirra aðila á fjármálamarkaði sem hann veitir upplýsinga- og fjarskiptatækniþjónustu.

Í þeim tilgangi að sinna eftirlitsstarfsemi sinni getur aðaleftirlitsaðili tekið tillit til hvers kyns viðeigandi vottunar þriðja aðila og innri eða ytri úttektarskýrslna sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur gert aðgengilegar.

41. gr.

Samræming skilyrða sem gera eftirlitsstarfsemi mögulega

1. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, semja drög að tæknilegum eftirlitsstöðlum til að tilgreina:

a) upplýsingarnar sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu á að veita í umsókn að eigin frumkvæði um að verða tilgreindur sem mikilvægur skv. 11. mgr. 31. gr.,

b) efni, skipulag og snið upplýsinga sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skulu leggja fram, birta eða tilkynna skv. 1. mgr. 35. gr., þ.m.t. sniðmát fyrir upplýsingar um undirverktakasamninga,

c) viðmið til að ákvarða samsetningu sameiginlega skoðunarhópsins til að tryggja jafnvægi í þátttöku starfsmanna evrópsku eftirlitsstofnananna og viðkomandi lögbærra yfirvalda, tilnefningu þeirra, verkefni og vinnutilhögun,

d) upplýsingar um mat lögbærra yfirvalda á ráðstöfunum sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu gera á grundvelli tilmæla aðaleftirlitsaðila skv. 3. mgr. 42. gr.

2. Evrópsku eftirlitsstofnanirnar skulu leggja þessi drög að tæknilegum eftirlitsstöðlum fyrir framkvæmdastjórnina eigi síðar en 17. júlí 2024.

Framkvæmdastjórninni er veitt vald til að bæta við þessa reglugerð með því að samþykkja tæknilegu eftirlitsstaðlana sem um getur í 1. gr. í samræmi við ferlið sem um getur í 10.–14. gr. í reglugerðum (ESB) nr. 1093/2010, (ESB) nr. 1094/2010 og nr. (ESB) 1095/2010.

42. gr.

Eftirfylgni lögbærra yfirvalda

1. Innan 60 almanaksdaga frá viðtöku tilmæla frá aðaleftirlitsaðila skv. d-lið 1. mgr. 35. gr. skulu mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu annaðhvort tilkynna aðaleftirlitsaðila um þá fyrirætlan sína að fylgja tilmælunum eða gefa rökstudda skýringu á því að slíkum tilmælum sé ekki fylgt. Aðaleftirlitsaðili skal tafarlaust senda þessar upplýsingar til lögbærra yfirvalda viðkomandi aðila á fjármálamarkaði.

2. Aðaleftirlitsaðili skal upplýsa um það opinberlega ef mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu lætur hjá líða að tilkynna um aðaleftirlitsaðila í samræmi við 1. mgr. eða ef sú útskýring sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veita telst ekki fullnægjandi. Í birtum upplýsingum skal greina frá auðkenni mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu auk upplýsinga um tegund og eðli tilvika þar sem ekki er farið að tilskildum ákvæðum. Slíkar upplýsingar skulu takmarkast við það sem á við og er hóflegt til að tryggja almenningsvitund nema slík birting myndi valda hlutaðeigandi aðilum óhóflegum skaða eða gæti teflt eðlilegri starfsemi og heilleika fjármálamarkaða í tvísýnu eða stöðugleika alls eða hluta fjármálakerfis Sambandsins.

Aðaleftirlitsaðili skal tilkynna þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu um þessa opinberu birtingu.

3. Lögbær yfirvöld skulu upplýsa viðkomandi aðila á fjármálamarkaði um þá áhættu sem tilgreind er í tilmælum til mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu í samræmi við d-lið 1. mgr. 35. gr.

Við stýringu upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila skulu aðilar á fjármálamarkaði taka tillit til þeirrar áhættu sem um getur í fyrstu undirgrein.

4. Ef lögbært yfirvald telur að aðili á fjármálamarkaði taki ekki tillit til eða taki ekki nægilega vel á hinni sértæku áhættu sem tilgreind er í tilmælunum í stýringu sinni á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila skal það tilkynna viðkomandi aðila á fjármálamarkaði um möguleikann á að ákvörðun verði tekin, innan 60 almanaksdaga frá móttöku slíkrar tilkynningar skv. 6. mgr., ef ekki er fyrir hendi viðeigandi samningsbundið fyrirkomulag sem miðar að því að taka á slíkri áhættu.

5. Við móttöku skýrslnanna sem um getur í c-lið 1. mgr. 35. gr. og áður en ákvörðun er tekin, eins og um getur í 6. mgr. þessarar greinar, er lögbærum yfirvöldum heimilt að hafa samráð að eigin frumkvæði við lögbær yfirvöld sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555 og bera ábyrgð á eftirliti með nauðsynlegri eða mikilvægri rekstrareiningu sem fellur undir þá tilskipun, sem hefur verið tilnefnd sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu.

6. Lögbær yfirvöld geta, sem lokaúrræði, í kjölfar tilkynningarinnar og, ef við á, þess samráðs sem sett er fram í 4. og 5. mgr. þessarar greinar, í samræmi við 50. gr., tekið ákvörðun um að krefjast þess að aðilar á fjármálamarkaði fresti tímabundið notkun eða nýtingu þjónustu mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, annaðhvort að hluta til eða að öllu leyti, þar til brugðist hefur verið við þeirri áhættu sem tilgreind er í tilmælunum sem beint er til mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Ef nauðsyn krefur geta þau krafist þess að aðilar á fjármálamarkaði slíti viðeigandi samningsbundnu fyrirkomulagi við mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, að hluta til eða í heild.

7. Ef mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu neitar að samþykkja tilmæli, á grundvelli annarrar nálgunar en þeirrar sem aðaleftirlitsaðili mælir með, og slík önnur nálgun getur haft neikvæð áhrif á mikinn fjölda aðila á fjármálamarkaði eða verulegan hluta fjármálageirans og einstakar viðvaranir sem lögbær yfirvöld gefa út hafa ekki leitt til samræmdra aðferða til að draga úr hugsanlegri áhættu fyrir fjármálastöðugleika, getur aðaleftirlitsaðili, að höfðu samráði við eftirlitsvettvanginn, gefið út tilmæli til lögbærra yfirvalda, sem eru hvorki bindandi né opinber, til að stuðla að samræmdum og samleitnum eftirfylgniaðgerðum, eins og við á.

8. Við móttöku skýrslnanna sem um getur í c-lið 1. mgr. 35. gr. skulu lögbær yfirvöld, þegar þau taka ákvörðun eins og um getur í 6. mgr. þessarar greinar, taka tillit til tegundar og umfangs þeirrar áhættu sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu bregst ekki við, sem og þess hversu alvarlegt það er að ekki sé farið að tilmælunum, með hliðsjón af eftirfarandi viðmiðunum:

a) alvarleika og tímalengdar vanefnda,

b) hvort vanefndir hafi leitt í ljós alvarlega veikleika í verklagsreglum, stjórnunarkerfum, áhættustýringu og innra eftirliti mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

c) hvort vanefndir hafi auðveldað, leitt til eða með öðrum hætti tengst efnahagsbroti,

d) hvort vanefndir hafi verið af ásetningi eða gáleysi,

e) hvort tímabundin niðurfelling eða uppsögn samningsbundins fyrirkomulags stofni í hættu samfellu í viðskiptaþjónustu aðila á fjármálamarkaði þrátt fyrir viðleitni hennar til að forðast röskun á þjónustustarfsemi,

f) eftir atvikum, álit lögbærra yfirvalda sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555 og bera ábyrgð á eftirliti með nauðsynlegri eða mikilvægri rekstrareiningu sem fellur undir þá tilskipun, sem hefur verið tilnefnd sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu, sem beðið er um að eigin frumkvæði og í samræmi við 5. mgr. þessarar greinar.

Lögbær yfirvöld skulu gefa aðilum á fjármálamarkaði nauðsynlegan tíma til að gera þeim kleift að aðlaga samningsbundið fyrirkomulag við mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til að forðast skaðleg áhrif á stafrænan rekstrarlegan viðnámsþrótt þeirra og gera þeim kleift að taka útgönguáætlanir og umbreytingaráætlanir í notkun eins og um getur í 28. gr.

9. Ákvörðunin, sem um getur í 6. mgr. þessarar greinar, skal tilkynnt aðilum eftirlitsvettvangsins, sem um getur í a-, b- og c-lið 4. mgr. 32. gr., og sameiginlega eftirlitskerfinu.

Þeir mikilvægu þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu, sem ákvarðanirnar sem kveðið er á um í 6. mgr. hafa áhrif á, skulu hafa fullt samstarf við þá aðila á fjármálamarkaði sem verða fyrir áhrifum, einkum í tengslum við ferli tímabundinnar niðurfellingar eða uppsagnar á samningsbundnu fyrirkomulagi.

10. Lögbær yfirvöld skulu upplýsa aðaleftirlitsaðila reglulega um þær aðferðir og ráðstafanir sem gripið er til við eftirlitsverkefni í tengslum við aðila á fjármálamarkaði, sem og um samningsbundið fyrirkomulag sem aðilar á fjármálamarkaði gera ef mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafa ekki samþykkt, að hluta til eða í heild, tilmæli sem aðaleftirlitsaðili beinir til þeirra.

11. Aðaleftirlitsaðili getur, sé þess óskað, gefið nánari útskýringar á útgefnum tilmælum til leiðbeiningar fyrir lögbær yfirvöld um eftirfylgniráðstafanir.

43. gr.

Eftirlitsgjöld

1. Í samræmi við framseldu gerðina sem um getur í 2. mgr. þessarar greinar skal aðaleftirlitsaðili innheimta gjöld af mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem nægja til greiðslu nauðsynlegra útgjalda aðaleftirlitsaðila í tengslum við framkvæmd eftirlitsverkefna samkvæmt þessari reglugerð, þ.m.t. endurgreiðslu alls kostnaðar sem kann að falla til vegna vinnu sem sameiginlegi skoðunarhópurinn, sem um getur í 40. gr., innir af hendi, sem og kostnað vegna ráðgjafar sem óháðir sérfræðingar veita í tengslum við málefni sem falla undir verksvið beinnar eftirlitsstarfsemi, eins og um getur í annarri undirgrein 4. mgr. 32. gr.

Fjárhæð gjalds sem lagt er á mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu skal standa straum af öllum kostnaði sem leiðir af framkvæmd þeirra skyldna sem settar eru fram í þessum þætti og vera í réttu hlutfalli við veltu.

2. Framkvæmdastjórnin hefur vald til að samþykkja framselda gerð í samræmi við 57. gr. til að bæta við þessa reglugerð með því að ákvarða fjárhæð gjalda og hvernig þau skuli greidd fyrir 17. júlí 2024.

44. gr.

Alþjóðleg samvinna

1. Með fyrirvara um 36. gr. er Evrópsku bankaeftirlitsstofnuninni, Evrópsku verðbréfamarkaðseftirlitsstofnuninni og Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnuninni heimilt, í samræmi við 33. gr. reglugerða (ESB) nr. 1093/2010, (ESB) nr. 1095/2010 og (ESB) nr. 1094/2010, eftir því sem við á, að gera stjórnvaldsráðstafanir með reglusetningar- og eftirlitsstofnunum í þriðju löndum til að hlúa að alþjóðlegri samvinnu um upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila þvert á ólíka fjármálageira, einkum með því að þróa bestu starfsvenjur við endurskoðun á venjum og eftirliti með stýringu upplýsinga- og fjarskiptatækniáhættu, mildunarráðstafana og viðbragða vegna atvika.

2. Evrópsku eftirlitsstofnanirnar skulu, fyrir milligöngu sameiginlegu nefndarinnar, leggja sameiginlega trúnaðarskýrslu fyrir Evrópuþingið, ráðið og framkvæmdastjórnina á fimm ára fresti, með samantekt á niðurstöðum viðkomandi viðræðna við yfirvöld þriðju landa sem um getur í 1. mgr., þar sem lögð er áhersla á þróun á upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila og áhrif á fjármálastöðugleika, heilleika markaðar, fjárfestavernd og starfsemi innri markaðarins.

VI. KAFLI

Fyrirkomulag upplýsingaskipta

45. gr.

Fyrirkomulag upplýsingaskipta vegna upplýsinga og greiningargagna um netógnir

1. Aðilum á fjármálamarkaði er heimilt að skiptast á upplýsingum og greiningargögnum um netógnir, þ.m.t. vísa sem geta gefið til kynna ógn og hættu, úrræði, aðferðir og verklagsreglur, netöryggisviðvaranir og samskipunartól (e. *configuration tools*), að því marki sem slík upplýsingaskipti og miðlun vitneskju:

a) miða að því að efla stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði, einkum með vitundarvakningu í tengslum við netógnir, með því að takmarka eða hindra að netógnir geti breiðst út, styðja við varnargetu, aðferðir til að greina ógnir, stefnuáætlanir til að draga úr áhættu eða viðbragðs- og endurreisnarstig,

b) á sér stað á traustum sameiginlegum vettvangi aðila á fjármálamarkaði,

c) er framkvæmd með fyrirkomulagi til upplýsingaskipta sem verndar hugsanlega viðkvæmt eðli þeirra upplýsinga sem er deilt og falla undir hátternisreglur að teknu fullu tilliti til viðskiptaleyndar, verndar persónuupplýsinga í samræmi við reglugerð (ESB) 2016/679 og viðmiðunarreglna um samkeppnisstefnu.

2. Að því er varðar c-lið 1. mgr. skal í fyrirkomulagi upplýsingaskipta skilgreina skilyrði fyrir þátttöku og, eftir því sem við á, setja fram ítarlegar upplýsingar um þátttöku opinberra yfirvalda og heimildir þeirra til að tengjast fyrirkomulagi upplýsingaskipta, þátttöku þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, og um rekstrarþætti, þ.m.t. notkun sérstakra upplýsingatækniverkvanga.

3. Aðilar á fjármálamarkaði skulu tilkynna lögbærum yfirvöldum um þátttöku sína í fyrirkomulagi upplýsingaskipta sem um getur í 1. mgr. við staðfestingu á aðild þeirra eða, eftir því sem við á, um lok aðildar sinnar þegar þau taka gildi.

VII. KAFLI

Lögbær yfirvöld

46. gr.

Lögbær yfirvöld

Með fyrirvara um ákvæðin um eftirlitsramma fyrir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem um getur í II. þætti V. kafla þessarar reglugerðar, skulu eftirfarandi lögbær yfirvöld tryggja að farið sé að ákvæðum þessarar reglugerðar í samræmi við valdheimildir sem veittar eru með viðeigandi réttargerðum:

a) að því er varðar lánastofnanir og stofnanir sem njóta undanþágu samkvæmt tilskipun 2013/36/ESB, lögbært yfirvald sem tilnefnt er í samræmi við 4. gr. þeirrar tilskipunar og að því er varðar lánastofnanir sem flokkast sem mikilvægar í samræmi við 4. mgr. 6. gr. reglugerðar (ESB) nr. 1024/2013, Seðlabanki Evrópu í samræmi við valdheimildir og verkefni sem veitt eru með þeirri reglugerð,

b) að því er varðar greiðslustofnanir, þ.m.t. greiðslustofnanir sem njóta undanþágu samkvæmt tilskipun (ESB) 2015/2366, rafeyrisfyrirtækja sem njóta undanþágu samkvæmt tilskipun 2009/110/EB, og reikningsupplýsingaþjónustuveitenda eins og um getur í 1. mgr. 33. gr. tilskipunar (ESB) 2015/2366, það lögbæra yfirvald sem tilgreint er í samræmi við 22. gr. tilskipunar (ESB) 2015/2366,

c) að því er varðar verðbréfafyrirtæki, lögbæra yfirvaldið sem er tilnefnt í samræmi við 4. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2019/2034 ([38]),

d) að því er varðar þjónustuveitendur sýndareigna, sem hafa starfsleyfi samkvæmt reglugerð um markaði með sýndareignir og útgefendur eignatengdra tóka, lögbært yfirvald sem tilnefnt er í samræmi við viðkomandi ákvæði þeirrar reglugerðar,

e) að því er varðar verðbréfamiðstöðvar, lögbært yfirvald sem tilnefnt er í samræmi við 11. reglugerðar (ESB) nr. 909/2014,

f) að því er varðar miðlæga mótaðila, lögbært yfirvald sem tilnefnt er í samræmi við 22. gr. reglugerðar (ESB) nr. 648/2012,

g) að því er varðar viðskiptavettvanga og veitendur gagnaskýrsluþjónustu, lögbært yfirvald sem tilnefnt er í samræmi við 67. gr. tilskipunar 2014/65/ESB og lögbært yfirvald eins og það er skilgreint í 18. lið 1. mgr. 2. gr. reglugerðar (ESB) nr. 600/2014,

h) að því er varðar viðskiptaskrár, lögbært yfirvald sem tilnefnt er í samræmi við 22. gr. reglugerðar (ESB) nr. 648/2012,

i) að því er varðar rekstraraðila sérhæfða sjóða, lögbært yfirvald sem tilnefnt er í samræmi við 44. gr. tilskipunar 2011/61/ESB,

j) að því er varðar rekstrarfélög, lögbært yfirvald sem tilnefnt er í samræmi við 97. gr. tilskipunar 2009/65/EB,

k) að því er varðar vátrygginga- og endurtryggingafélög, lögbæra yfirvaldið sem tilnefnt er í samræmi við 30. gr. tilskipunar 2009/138/EB,

l) að því er varðar vátryggingamiðlara, endurtryggingamiðlara og vátryggingamiðlara í hliðarstarfsemi, lögbært yfirvald sem tilnefnt er í samræmi við 12. gr. tilskipunar (ESB) 2016/97,

m) að því er varðar stofnanir um starfstengdan lífeyri, lögbært yfirvald sem tilnefnt er í samræmi við 47. tilskipunar (ESB) 2016/2341,

n) að því er varðar lánshæfismatsfyrirtæki, lögbært yfirvald sem tilnefnt er í samræmi við 21. gr. reglugerðar (EB) nr. 1060/2009,

o) að því er varðar stjórnendur mjög mikilvægra viðmiðana, lögbært yfirvald sem tilnefnt er í samræmi við 40 og 41. gr. reglugerðar (ESB) 2016/1011,

([38]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2019/2034 frá 27. nóvember 2019 um varfærniseftirlit með verðbréfafyrirtækjum og breytingu á tilskipunum 2002/87/EB, 2009/65/EB, 2011/61/ESB, 2013/36/ESB, 2014/59/ESB og 2014/65/ESB (Stjtíð. ESB L 314, 5.12.2019, bls. 64).

p) að því er varðar þjónustuveitendur hópfjármögnunar, lögbært yfirvald sem tilnefnt er í samræmi við 29. reglugerðar (ESB) 2020/1503,

q) að því er varðar verðbréfunarskrár, lögbært yfirvald sem tilnefnt er í samræmi við 10. gr. og 1. mgr. 14. gr. reglugerðar (ESB) nr. 2017/2402.

47. gr.

Samstarf við vettvanga og yfirvöld sem komið er á fót með tilskipun (ESB) 2022/2555

1. Til að stuðla að samstarfi og gera upplýsingaskipti í eftirlitsskyni möguleg milli lögbærra yfirvalda, sem tilnefnd eru samkvæmt þessari reglugerð, og samstarfshópsins, sem komið er á fót með 14. gr. tilskipunar (ESB) 2022/2555, er evrópsku eftirlitsstofnununum og lögbærum yfirvöldum heimilt að taka þátt í starfsemi samstarfshópsins að því er varðar málefni sem snerta eftirlitsstarfsemi þeirra í tengslum við aðila á fjármálamarkaði. Evrópsku eftirlitsstofnanirnar og lögbær yfirvöld geta óskað þess að þeim sé boðin þátttaka í starfsemi samstarfshópsins í tengslum við málefni sem varða nauðsynlegar eða mikilvægar rekstrareiningar sem falla undir tilskipun (ESB) 2022/2555 og hafa einnig verið tilnefndar sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skv. 31. gr. þessarar reglugerðar.

2. Eftir því sem við á, er lögbærum yfirvöldum heimilt að hafa samráð við sameiginlega tengiliði og viðbragðsteymi vegna váatvika er varða tölvuöryggi, sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555, og deila upplýsingum með þeim.

3. Eftir því sem við á, hafa lögbær yfirvöld einnig heimild til að óska eftir hvers kyns viðeigandi tækniráðgjöf frá þeim lögbæru yfirvöldum sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555 og koma á samstarfssamningum til að leyfa að skilvirk samhæfingarkerfi fyrir skjót viðbrögð séu sett upp.

4. Í fyrirkomulaginu sem um getur í 3. mgr. þessarar greinar má m.a. tilgreina verklagsreglur um samræmingu á eftirlits- og skoðunarstarfsemi í tengslum við nauðsynlegar eða mikilvægar rekstrareiningar sem falla undir tilskipun (ESB) 2022/2555 og hafa verið tilnefndar sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skv. 31. gr. þessarar reglugerðar, þ.m.t. vegna framkvæmdar, í samræmi við landslög, á rannsóknum og vettvangsskoðunum, sem og fyrirkomulagi til upplýsingaskipta milli lögbærra yfirvalda samkvæmt þessari reglugerð og lögbærra yfirvalda sem eru tilnefnd eða komið á fót í samræmi við þá tilskipun, sem felur í sér aðgang að þeim upplýsingum sem síðarnefndu yfirvöldin fara fram á.

48. gr.

Samstarf milli yfirvalda

1. Lögbær yfirvöld skulu eiga náið samstarf sín á milli og, eftir atvikum, við aðaleftirlitsaðila.

2. Lögbær yfirvöld og aðaleftirlitsaðili skulu skiptast tímanlega á öllum viðeigandi upplýsingum um mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem eru þeim nauðsynlegar til að þau geti sinnt skyldum sínum samkvæmt þessari reglugerð, einkum í tengslum við greinda áhættu, aðferðir og ráðstafanir sem gerðar eru sem hluti af eftirlitsverkefnum aðaleftirlitsaðila.

49. gr.

Æfingar, samskipti og samvinna þvert á fjármálageira

1. Evrópsku eftirlitsstofnanirnar, fyrir milligöngu sameiginlegu nefndarinnar og í samstarfi við lögbær yfirvöld, skilastjórnvöld eins og um getur í 3. gr. tilskipunar 2014/59/ESB, Seðlabanka Evrópu, sameiginlega skilastjórn, að því er varðar upplýsingar um einingar sem falla undir gildissvið reglugerðar (ESB) nr. 806/2014, Evrópska kerfisáhætturáðið og Netöryggisstofnun Evrópusambandsins, eins og við á, geta komið á fyrirkomulagi til að gera kleift að miðla skilvirkum starfsvenjum milli fjármálageira til að auka næmi á aðstæður og greina sameiginlega veikleika í netheimum og áhættu þvert á geira.

Þær geta þróað krísustjórnunar- og viðbragðsæfingar sem fela í sér sviðsmyndir af netárásum með það fyrir augum að þróa samskiptaleiðir og gera smám saman kleift að grípa til skilvirkra, samræmdra viðbragða á vettvangi Sambandsins ef upp kemur alvarlegt atvik eða ógn sem tengist upplýsinga- og fjarskiptatækni yfir landamæri sem hefur kerfislæg áhrif á fjármálageira Sambandsins í heild.

Þessar æfingar geta, eftir því sem við á, einnig kannað hversu háður fjármálageirinn er öðrum atvinnugreinum.

2. Lögbær yfirvöld, evrópsku eftirlitsstofnanirnar og Seðlabanki Evrópu skulu starfa náið saman og skiptast á upplýsingum til að sinna skyldum sínum skv. 47.–54. gr. Þau skulu samræma eftirlit sitt með nánum hætti til að bera kennsl á og ráða bót á brotum á þessari reglugerð, þróa og stuðla að bestu starfsvenjum, auðvelda samstarf, stuðla að samkvæmni í túlkun og veita mat milli lögsagna komi upp ágreiningur.

50. gr.

Stjórnsýsluviðurlög og ráðstafanir til úrbóta

1. Lögbær yfirvöld skulu hafa allar valdheimildir til eftirlits, rannsóknar og viðurlaga sem nauðsynlegar eru til að uppfylla skyldustörf þeirra sem skyldi samkvæmt þessari reglugerð.

2. Valdheimildirnar, sem um getur í 1. mgr., skulu a.m.k. ná yfir eftirfarandi valdheimildir til að:

a) hafa aðgang að hvers kyns skjölum eða gögnum á hvaða formi sem er og lögbær yfirvöld telja að skipti máli við störf þeirra, og fá eða taka afrit af þeim,

b) framkvæma vettvangsskoðanir eða rannsóknir sem skulu fela í sér en takmarkast ekki við,

   i. að biðja fulltrúa aðila á fjármálamarkaði um munnlegar eða skriflegar útskýringar á málavöxtum eða gögnum í tengslum við viðfangsefni og tilgang rannsóknarinnar og til að skrá svörin,

   ii. að taka viðtöl við aðra einstaklinga eða lögaðila sem samþykkja að veita viðtal í þeim tilgangi að safna upplýsingum að því er varðar viðfangsefni rannsóknar,

c) krefjast ráðstafana til úrbóta vegna brota á kröfunum í þessari reglugerð.

3. Með fyrirvara um rétt aðildarríkja til að beita refsiviðurlögum í samræmi við 52. gr. skulu aðildarríki mæla fyrir um reglur um viðeigandi stjórnsýsluviðurlög og ráðstafanir til úrbóta vegna brota á þessari reglugerð og tryggja skilvirka framkvæmd þeirra.

Þessi viðurlög og ráðstafanir skulu vera skilvirk, í réttu hlutfalli við brotið og hafa varnaðaráhrif.

4. Aðildarríki skulu veita lögbærum yfirvöldum vald til að beita a.m.k. eftirfarandi stjórnsýsluviðurlögum eða ráðstöfunum til úrbóta vegna brota á þessari reglugerð:

a) gefa út fyrirmæli um að einstaklingur eða lögaðili láti af háttsemi sem felur í sér brot á reglugerðinni og endurtaki hana ekki,

b) óska eftir að bundinn verði endi á hvers konar framkvæmd eða framferði, tímabundið eða til frambúðar, sem lögbært yfirvald telur brjóta í bága við ákvæði þessarar reglugerðar og komið sé í veg fyrir að slík framkvæmd eða framferði endurtaki sig,

c) samþykkja hvers kyns ráðstafanir, þ.m.t. fjárhagslegar, til að tryggja að aðilar á fjármálamarkaði uppfylli lagaskilyrði áfram,

d) krefjast, að því marki sem það er heimilt samkvæmt landslögum, gagnaumferðarskráa sem liggja fyrir hjá fjarskiptafyrirtæki, ef rökstuddur grunur er um brot á þessari reglugerð og ef slíkar skrár geta skipt máli fyrir rannsókn á brotum á þessari reglugerð, og

e) gefa út opinberar tilkynningar, þ.m.t. opinberar yfirlýsingar sem tilgreina auðkenni viðkomandi einstaklings eða lögaðila og hvers eðlis brotið er.

5. Ef c-liður 2. mgr. og 4. mgr. eiga við um lögaðila skulu aðildarríki veita lögbærum yfirvöldum vald til að beita viðurlögum og ráðstöfunum til úrbóta, með fyrirvara um þau skilyrði sem mælt er fyrir um í landslögum, gegn meðlimum stjórnar og/eða framkvæmdastjórnar og öðrum einstaklingum sem samkvæmt landslögum bera ábyrgð á brotinu.

6. Aðildarríki skulu tryggja að hver ákvörðun um að beita stjórnsýsluviðurlögum eða ráðstöfunum til úrbóta, sem settar eru fram í c-lið 2. mgr., sé rökstudd á viðhlítandi hátt og háð málskotsrétti.

51. gr.

Beiting heimildar til að leggja á stjórnsýsluviðurlög og gera kröfu um ráðstafanir til úrbóta

1. Lögbær yfirvöld skulu beita þeim heimildum til að leggja á stjórnsýsluviðurlög og gera kröfu um ráðstafanir til úrbóta sem um getur í 50. gr. í samræmi við ramma landslaga sinna, eftir því sem við á, sem hér segir:

a) með beinum hætti,

b) í samstarfi við önnur yfirvöld,

c) á eigin ábyrgð með framsali verkefna til annarra yfirvalda, eða

d) með því að leita til lögbærra dómsyfirvalda.

2. Lögbær yfirvöld skulu, við ákvörðun tegundar og stigs stjórnsýsluviðurlaga eða ráðstafana til úrbóta sem verða lögð á skv. 50. gr., taka tillit til þess að hve miklu leyti brotið er af ásetningi eða vegna gáleysis og allra annarra aðstæðna sem máli skipta, þ.m.t eftirfarandi, eftir því sem við á:

a) mikilvægis, alvarleika og tímalengdar brots,

b) umfangs ábyrgðar einstaklingsins eða lögaðilans sem ber ábyrgð á brotinu,

c) hver fjárhagslegur styrkur einstaklingsins eða lögaðilans sem ber ábyrgð á brotinu er,

d) hagnaðar einstaklingsins eða lögaðilans sem ber ábyrgðina eða tapsins sem hann komst hjá, að því marki sem mögulegt er að ákvarða það,

e) tap þriðju aðila vegna brotsins, að svo miklu leyti sem mögulegt er að ákvarða það,

f) samstarfsvilja hins brotlega einstaklings eða lögaðila við lögbæra yfirvaldið, með fyrirvara um þörfina á að tryggja að hann endurgreiði hagnað sinn af brotinu eða tap sem viðkomandi komst hjá með því,

g) fyrri brota hins brotlega einstaklings eða lögaðila.

52. gr.

Refsiviðurlög

1. Aðildarríkjum er heimilt að ákveða að mæla ekki fyrir um reglur um stjórnsýsluviðurlög eða ráðstafanir til úrbóta vegna brota sem falla undir refsiviðurlög samkvæmt landslögum þeirra.

2. Ef aðildarríki hafa kosið að mæla fyrir um refsiviðurlög við brotum gegn þessari reglugerð skulu þau tryggja að viðeigandi ráðstafanir séu fyrir hendi þannig að viðkomandi lögbær yfirvöld hafi allar nauðsynlegar heimildir til að koma á sambandi við dómsyfirvöld, saksóknara eða yfirvöld sem berjast gegn afbrotum innan lögsögu þeirra og fái tilteknar upplýsingar sem tengjast rannsókn sakamála eða mál sem eru höfðuð vegna brota gegn þessari reglugerð og veiti öðrum lögbærum yfirvöldum og Evrópsku bankaeftirlitsstofnuninni, Evrópsku verðbréfamarkaðseftirlitsstofnuninni eða Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnuninni sömu upplýsingar til að þau geti uppfyllt skyldur sínar um samstarf hvert við annað að því er varðar þessa reglugerð.

53. gr.

Tilkynningaskylda

Aðildarríki skulu, eigi síðar en 17. janúar 2025, tilkynna framkvæmdastjórninni, Evrópsku verðbréfamarkaðseftirlitsstofnuninni, Evrópsku bankaeftirlitsstofnuninni og Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnuninni um lög og stjórnsýslufyrirmæli sem lögleiða þennan kafla, þ.m.t. öll viðkomandi ákvæði refsilaga. Aðildarríki skulu án ástæðulausrar tafar tilkynna framkvæmdastjórninni, Evrópsku verðbréfamarkaðseftirlitsstofnuninni, Evrópsku bankaeftirlitsstofnuninni og Evrópsku vátrygginga- og lífeyrissjóðaeftirlitsstofnuninni um allar síðari breytingar á þeim.

54. gr.

Birting stjórnsýsluviðurlaga

1. Lögbær yfirvöld skulu birta á opinberu vefsetri sínu, án ástæðulausrar tafar, hverja ákvörðun um stjórnsýsluviðurlög sem ekki er hægt að áfrýja eftir að aðilanum sem beittur er viðurlögum hefur verið tilkynnt um þá ákvörðun.

2. Birtingin sem um getur í 1. mgr. skal fela í sér upplýsingar um tegund og eðli brotsins, deili á þeim aðilum sem ábyrgð bera og þau viðurlög sem beitt er.

3. Ef lögbært yfirvald telur, í kjölfar mats á einstökum tilvikum, að birting auðkenna, þegar um lögaðila er að ræða, eða auðkenna og persónuupplýsinga, þegar um einstaklinga er að ræða, myndi vera í ósamræmi við brot, hafa í för með sér áhættu í tengslum við vernd persónuupplýsinga, tefla stöðugleika fjármálamarkaða eða yfirstandandi rannsókn sakamáls í tvísýnu eða valda, að því marki sem unnt er að ákvarða slíkt, hlutaðeigandi aðila óhóflegum skaða, skal það samþykkja eina af eftirfarandi lausnum að því er varðar ákvörðun um beitingu stjórnsýsluviðurlaga:

a) að birtingu sé frestað þar til engar ástæður fyrir að bíða með birtingu eru lengur fyrir hendi,

b) að það sé birt án nafngreiningar, í samræmi við landslög, eða

c) að sleppa birtingu ef valkostirnir sem settir eru fram í a- og b-lið teljast annaðhvort ófullnægjandi til að tryggja að stöðugleika fjármálamarkaða sé ekki stefnt í hættu eða ef slík birting er ekki í samræmi við mildi viðurlaganna sem hafa verið lögð á.

4. Ef um er að ræða ákvörðun um að birta stjórnsýsluviðurlög án nafngreiningar í samræmi við í b-lið 3. mgr. má fresta birtingu á viðeigandi gögnum.

5. Ef lögbært yfirvald birtir ákvörðun um beitingu stjórnsýsluviðurlaga sem er áfrýjað til viðkomandi dómsyfirvalda skulu lögbær yfirvöld þegar í stað birta þær upplýsingar á opinberu vefsetri sínu og, á síðari stigum, allar síðari tengdar upplýsingar um niðurstöðu slíkrar áfrýjunar. Einnig skal birta allar dómsniðurstöður sem ógilda ákvörðun um að beita stjórnsýsluviðurlögum.

6. Lögbær yfirvöld skulu tryggja að allar birtingar sem um getur í 1.–4. mgr. verði aðeins á opinberu vefsetri þeirra í þann tíma sem nauðsynlegur er til að beita þessari grein. Þessi tími skal ekki vera lengri en fimm ár frá birtingu.

55. gr.

Þagnarskylda

1. Um allar trúnaðarupplýsingar sem fengnar eru, skipst er á eða sendar eru í samræmi við þessa reglugerð skulu gilda ákvæði um þagnarskyldu sem mælt er fyrir um í 2. mgr.

2. Þagnarskylda gildir um alla einstaklinga sem starfa eða hafa starfað fyrir lögbær yfirvöld samkvæmt þessari reglugerð eða hvert það yfirvald eða markaðsaðila eða einstakling eða lögaðila sem lögbæru yfirvöldin hafa falið umboð sitt, þ.m.t. endurskoðendur og sérfræðingar sem þau hafa samið við.

3. Upplýsingar sem falla undir þagnarskyldu, þ.m.t. upplýsingaskipti milli lögbærra yfirvalda samkvæmt þessari reglugerð og lögbærra yfirvalda sem eru tilnefnd eða komið á fót í samræmi við tilskipun (ESB) 2022/2555, skulu ekki látnar öðrum aðila eða yfirvaldi í té nema samkvæmt ákvæðum sem mælt er fyrir um í lögum Sambandsins eða landslögum,

4. Allar upplýsingar sem lögbær yfirvöld skiptast á samkvæmt þessari reglugerð er varða viðskipta- eða rekstrarskilyrði og önnur efnahagsleg eða einkamálefni teljast vera trúnaðarupplýsingar og um þær skulu gilda skilyrði um þagnarskyldu, nema lögbæra yfirvaldið lýsi því yfir þegar samskiptin fara fram að slíkar upplýsingar megi birta eða ef slík birting upplýsinga er nauðsynleg vegna málarekstrar.

56. gr.

Persónuvernd

1. Evrópsku eftirlitsstofnununum og lögbærum yfirvöldum skal aðeins heimilt að vinna persónuupplýsingar þegar nauðsyn krefur til að uppfylla skyldur sínar samkvæmt þessari reglugerð, einkum vegna rannsóknar, skoðunar, beiðni um upplýsingar, samskipta, birtingar, úttektar, sannprófunar, mats og gerðar eftirlitsáætlana. Persónuupplýsingarnar skulu unnar í samræmi við reglugerð (ESB) 2016/679 eða reglugerð (ESB) 2018/1725, eftir því sem við á.

2. Ef ekki er kveðið á um annað í öðrum gerðum á tilteknum sviðum skulu persónuupplýsingarnar, sem um getur í 1. mgr., varðveittar þar til viðkomandi eftirlitsskyldur hafa verið inntar af hendi og í öllum tilvikum í að hámarki 15 ár, nema ef mál er til meðferðar fyrir dómstólum sem krefst frekari varðveislu slíkra gagna.

VIII. KAFLI

Framseldar gerðir

57. gr.

Beiting framsals

1. Framkvæmdastjórninni er falið vald til að samþykkja framseldar gerðir að uppfylltum þeim skilyrðum sem mælt er fyrir um í þessari grein.

2. Fela skal framkvæmdastjórninni vald til að samþykkja framseldar gerðir sem um getur í 6. mgr. 31. gr. og 2. mgr. 43. gr. í fimm ár frá 17. janúar 2024. Framkvæmdastjórnin skal taka saman skýrslu um valdaframsalið eigi síðar en níu mánuðum fyrir lok fimm ára tímabilsins. Valdaframsalið skal framlengt með þegjandi samkomulagi um jafnlangan tíma, nema Evrópuþingið eða ráðið andmæli þeirri framlengingu eigi síðar en þremur mánuðum fyrir lok hvers tímabils.

3. Evrópuþinginu eða ráðinu er hvenær sem er heimilt að afturkalla valdaframsalið sem um getur í 6. mgr. 31. gr. og 2. mgr. 43. gr. Með ákvörðun um afturköllun er bundinn endi á valdaframsalið sem tilgreint er í þeirri ákvörðun. Ákvörðunin öðlast gildi daginn eftir birtingu hennar í Stjórnartíðindum Evrópusambandsins eða síðar, eftir því sem tilgreint er í henni. Hún skal ekki hafa áhrif á gildi neinna framseldra gerða sem þegar eru í gildi.

4. Framkvæmdastjórnin skal, áður en framseld gerð er samþykkt, hafa samráð við sérfræðinga sem hvert aðildarríki hefur tilnefnt í samræmi við meginreglurnar sem mælt er fyrir um í samstarfssamningnum milli stofnana um betri lagasetningu frá 13. apríl 2016.

5. Um leið og framkvæmdastjórnin samþykkir framselda gerð skal hún tilkynna það Evrópuþinginu og ráðinu.

6. Framseld gerð sem er samþykkt skv. 6. mgr. 31. gr. og 2. mgr. 43. gr. skal því aðeins öðlast gildi að Evrópuþingið eða ráðið hafi ekki haft uppi nein andmæli innan þriggja mánaða frá tilkynningu um gerðina til Evrópuþingsins og ráðsins eða ef bæði Evrópuþingið og ráðið hafa upplýst framkvæmdastjórnina, áður en fresturinn er liðinn, um þá fyrirætlan sína að hreyfa ekki andmælum. Þessi frestur skal framlengdur um þrjá mánuði að frumkvæði Evrópuþingsins eða ráðsins.

IX. KAFLI

Umbreytingar- og lokaákvæði

I. þáttur

58. gr.

Endurskoðunarákvæði

1. Framkvæmdastjórnin skal, að höfðu samráði við evrópsku eftirlitsstofnanirnar og Evrópska kerfisáhætturáðið, eins og við á, gera endurskoðun og leggja skýrslu fyrir Evrópuþingið og ráðið ásamt, eftir því sem við á, tillögu að nýrri löggjöf, eigi síðar en 17. janúar 2028. Við endurskoðunina skal a.m.k. fjalla um eftirfarandi atriði:

a) viðmiðanir vegna tilnefningar á mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í samræmi við 2. mgr. 31. gr.,

b) að tilkynningin um verulegar netógnir, sem um getur í 19. gr., sé valfrjáls,

c) fyrirkomulagið sem um getur í 12. mgr. 31. gr. og valdheimildir aðaleftirlitsaðila, sem kveðið er á um í fyrsta undirlið iv. liðar d-liðar 1. mgr. 35. gr., með það fyrir augum að meta skilvirkni þessara ákvæða að því er varðar að tryggja skilvirkt eftirlit með mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu með staðfestu í þriðja landi og nauðsyn þess að stofna dótturfélag í Sambandinu;

Að því er varðar fyrstu undirgrein þessa liðar skal endurskoðunin fela í sér greiningu á regluverkinu sem um getur í 12. mgr. 31. gr., þ.m.t. með tilliti til aðgangs aðila á fjármálamarkaði Sambandsins að þjónustu frá þriðju löndum og aðgengi að slíkri þjónustu á markaði Sambandsins og skal hún taka tillit til frekari þróunar á mörkuðum fyrir þjónustu sem þessi reglugerð tekur til, hagnýtrar reynslu aðila á fjármálamarkaði og fjármálaeftirlitsaðila að því er varðar beitingu þessa fyrirkomulags og, eftir því sem við á, eftirlit með því og hvers kyns viðeigandi þróunar á sviði reglusetningar og eftirlits sem á sér stað á alþjóðavísu;

d) hversu viðeigandi er að innan gildissviðs þessarar reglugerðar séu aðilar á fjármálamarkaði, sem um getur í e-lið 3. mgr. 2. gr., sem nota sjálfvirk sölukerfi, í ljósi markaðsþróunar í framtíðinni varðandi notkun slíkra kerfa,

e) virkni og skilvirkni sameiginlegs eftirlitskerfis við að styðja samkvæmni í eftirliti og skilvirkni upplýsingaskipta innan eftirlitsrammans.

2. Í tengslum við endurskoðun á tilskipun (ESB) 2015/2366 skal framkvæmdastjórnin meta þörfina á auknu netviðnámsþoli greiðslukerfa og greiðsluvinnslustarfsemi og hvort viðeigandi sé að víkka út gildissvið þessarar reglugerðar þannig að það nái til rekstraraðila greiðslukerfa og eininga sem fást við greiðsluvinnslustarfsemi. Í ljósi þessa mats skal framkvæmdastjórnin, sem hluti af endurskoðun tilskipunar (ESB) 2015/2366, leggja skýrslu fyrir Evrópuþingið og ráðið eigi síðar en 17. júlí 2023.

Á grundvelli þessarar endurskoðunarskýrslu og að höfðu samráði við evrópsku eftirlitsstofnanirnar, Seðlabanka Evrópu og Evrópska kerfisáhætturáðið getur framkvæmdastjórnin, eftir því sem við á, og sem hluti af tillögu að nýrri löggjöf sem hún getur samþykkt skv. annarri málsgrein 108. gr. tilskipunar (ESB) 2015/2366, lagt fram tillögu til að tryggja að allir rekstraraðilar greiðslukerfa og einingar sem fást við greiðsluvinnslu falli undir viðeigandi eftirlit, að teknu tilliti til núverandi eftirlits af hálfu hlutaðeigandi seðlabanka.

3. Framkvæmdastjórnin skal, eigi síðar en 17. janúar 2026, að höfðu samráði við evrópsku eftirlitsstofnanirnar og Evrópunefnd eftirlitsaðila endurskoðenda, láta fara fram endurskoðun og leggja skýrslu fyrir Evrópuþingið og ráðið, ásamt tillögu að nýrri löggjöf, eftir því sem við á, um það hvort viðeigandi sé að herða kröfur til löggiltra endurskoðenda og endurskoðunarfyrirtækja að því er varðar stafrænan rekstrarlegan viðnámsþrótt, með því að fella löggilta endurskoðendur og endurskoðunarfyrirtæki undir gildissvið þessarar reglugerðar eða með breytingum á tilskipun Evrópuþingsins og ráðsins 2006/43/EB ([39]).

II. þáttur

Breytingar

59. gr.

Breytingar á reglugerð (EB) nr. 1060/2009

Reglugerð (EB) nr. 1060/2009 er breytt sem hér segir:

1) Í stað fyrstu undirgreinar 4. liðar A-þáttar í I. viðauka kemur eftirfarandi:

„Lánshæfismatsfyrirtæki skal hafa traustar stjórnunar- og bókhaldsaðferðir, innri eftirlitskerfi, skilvirkar verklagsreglur fyrir áhættumat og skilvirkt eftirlits- og öryggisfyrirkomulag fyrir stjórnun á upplýsinga- og fjarskiptatæknikerfum í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 (*).

(*) Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um viðbætur við reglugerðir (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (Stjtíð. ESB L 333, 27.12.2022, bls. 1).“

2) Í stað 12. liðar III. viðauka kemur eftirfarandi:

„12. Lánshæfismatsfyrirtæki brýtur í bága við 2. mgr. 6. gr., í tengslum við 4. lið A-þáttar I. viðauka, með því að hafa ekki traustar stjórnunar- eða bókhaldsaðferðir, innri eftirlitskerfi, skilvirkar verklagsreglur fyrir áhættumat eða skilvirkt eftirlits- eða öryggisfyrirkomulag fyrir stjórnun á upplýsinga- og fjarskiptatæknikerfum í samræmi við reglugerð (ESB) 2022/2554, eða með því að framkvæma ekki eða viðhalda tilhögun ákvarðanatöku eða stjórnskipulagi eins og krafist er í þeim lið.“

60. gr.

Breytingar á reglugerð (ESB) nr. 648/2012

Reglugerð (ESB) nr. 648/2012 er breytt sem hér segir:

1) Ákvæðum 26. gr. er breytt sem hér segir:

a) Í stað 3. mgr. kemur eftirfarandi:

„3. Miðlægur mótaðili skal viðhalda og reka stjórnskipulag sem tryggir samfellu og skipulegan rekstur þjónustu hans og starfsemi. Hann skal nota viðeigandi og hæfileg kerfi, tilföng og verklag, þ.m.t. upplýsinga- og fjarskiptatæknikerfi sem stjórnað er í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 (*).

(*) Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um viðbætur við reglugerðir (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (Stjtíð. ESB L 333, 27.12.2022, bls. 1).“

([39]) Tilskipun Evrópuþingsins og ráðsins 2006/43/EB frá 17. maí 2006 um lögboðna endurskoðun ársreikninga og samstæðureikninga, um breytingu á tilskipunum ráðsins 78/660/EBE og 83/349/EBE og um niðurfellingu á tilskipun ráðsins 84/253/EBE (Stjtíð. ESB L 157, 9.6.2006, bls. 87).

b) Ákvæði 6. liðar falla brott.

2) Ákvæðum 34. gr. er breytt sem hér segir:

a) Í stað 1. mgr. kemur eftirfarandi:

„1. Miðlægur mótaðili skal koma á, framkvæma og viðhalda viðeigandi stefnu um rekstrarsamfellu og áætlun um endurreisn eftir stóráfall, sem skal fela í sér stefnu um rekstrarsamfellu og viðbragðs- og endurreisnaráætlanir fyrir upplýsinga- og fjarskiptatækni sem komið er á og hrundið í framkvæmd í samræmi við reglugerð (ESB) 2022/2554, sem miðar að því að tryggja varðveislu starfs hans, tímanlega endurupptöku starfsemi og að skyldur miðlæga mótaðilans séu uppfylltar.“

b) Í stað fyrstu undirgreinar 3. mgr. kemur eftirfarandi:

„3. Til að tryggja samræmda beitingu þessarar greinar skal Evrópska verðbréfamarkaðseftirlitsstofnunin, að höfðu samráði við aðila að seðlabankakerfi Evrópu, semja drög að tæknilegum eftirlitsstöðlum þar sem tilgreint er lágmarksinnihald og -kröfur stefnu um rekstrarsamfellu og áætlunar um endurreisn eftir stóráfall, að undanskildum stefnu um rekstrarsamfellu og áætlunum um endurreisn eftir stóráfall í upplýsinga- og fjarskiptatækni.“

3) Í stað fyrstu undirgreinar 3. mgr. 56. gr. kemur eftirfarandi:

„3. Til að tryggja samræmda beitingu þessarar greinar skal Evrópska verðbréfamarkaðseftirlitsstofnunin semja drög að tæknilegum eftirlitsstöðlum þar sem nánar eru tilgreindar upplýsingar í umsókn um skráningu sem um getur í 1. mgr., þó ekki upplýsingar um kröfur sem tengjast stýringu upplýsinga- og fjarskiptatækniáhættu.“

4) Í stað 1. og 2. mgr. 79. gr. kemur eftirfarandi:

„1. Í viðskiptaskrá skal tilgreina uppruna rekstraráhættu og lágmarka hana, einnig með þróun á viðeigandi kerfum, stjórntækjum og verklagi, þ.m.t. upplýsinga- og fjarskiptatæknikerfum sem stjórnað er í samræmi við reglugerð (ESB) 2022/2554.

2. Viðskiptaskrá skal koma á, framkvæma og viðhalda viðeigandi stefnu um rekstrarsamfellu og áætlun um endurreisn eftir stóráfall, þ.m.t. stefnu um rekstrarsamfellu og viðbragðs- og endurreisnaráætlanir fyrir upplýsinga- og fjarskiptatækni sem komið er á fót í samræmi við reglugerð (ESB) 2022/2554, sem miðar að því að tryggja viðhald á starfsemi hans, tímanlega endurupptöku starfsemi og að skyldur viðskiptaskrár séu uppfylltar.“

5) Í 80. gr. fellur 1. mgr. brott.

6) Ákvæðum II. liðar I. viðauka er breytt sem hér segir:

a) Í stað a- og b-liðar kemur eftirfarandi:

„a) viðskiptaskrá brýtur í bága við 1. mgr. 79. gr. ef hún greinir ekki upptök rekstraráhættu eða lágmarkar þessa áhættu ekki með því að þróa viðeigandi kerfi, stjórntæki og verklag, þ.m.t. upplýsinga- og fjarskiptatæknikerfi sem stjórnað er í samræmi við reglugerð (ESB) 2022/2554,

b) viðskiptaskrá brýtur gegn 2. mgr. 79. gr. ef hún kemur ekki á, framkvæmir eða viðheldur viðeigandi stefnu um rekstrarsamfellu og áætlun um endurreisn eftir stóráfall sem komið er á í samræmi við reglugerð (ESB) 2022/2554 og miðar að því að tryggja að starfsemi hennar sé viðhaldið, tímanlega endurupptöku starfsemi og að skyldur viðskiptaskrárinnar séu uppfylltar,“

b) Ákvæði c-liðar falla brott.

7) Ákvæðum III. viðauka er breytt sem hér segir:

a) Ákvæðum II. liðar er breytt sem hér segir:

i. Í stað c-liðar kemur eftirfarandi:

„c) miðlægur mótaðili í 2. þrepi brýtur í bága við 3. mgr. 26. gr. með því að viðhalda hvorki né starfa samkvæmt stjórnskipulagi sem tryggir samfellu og skipulegan rekstur þjónustu hans og starfsemi eða með því að beita ekki viðeigandi og hæfilegum kerfum, tilföngum eða verklagsreglum, þ.m.t. upplýsinga- og fjarskiptatæknikerfum sem er stjórnað í samræmi við reglugerð (ESB) 2022/2554,“

ii. Ákvæði f-liðar falla brott.

b) Í stað a-liðar III. liðar kemur eftirfarandi:

„a) miðlægur mótaðili í 2. þrepi brýtur í bága við 1. mgr. 34. gr. með því að koma ekki á, framkvæma ekki eða viðhalda ekki fullnægjandi stefnu um rekstrarsamfellu og viðbragðs- og endurreisnaráætlunum sem teknar eru upp í samræmi við reglugerð (ESB) 2022/2554 og miða að því að tryggja varðveislu starfsemi hans, tímanlega endurupptöku starfsemi og að skyldur miðlæga mótaðilans séu uppfylltar, sem a.m.k. gerir kleift að endurheimta öll viðskipti frá þeim tíma sem röskun varð til að gera miðlæga mótaðilanum kleift að halda starfsemi áfram með vissu og ljúka uppgjöri á áætluðum degi“.

61. gr.

Breytingar á reglugerð (ESB) nr. 909/2014

Ákvæðum 45. gr. reglugerðar (ESB) nr. 909/2014 er breytt sem hér segir:

1) Í stað 1. mgr. kemur eftirfarandi:

„1. Verðbréfamiðstöð skal greina bæði innri og ytri upptök rekstraráhættu og lágmarka áhrif hennar, einnig með því að nýta viðeigandi upplýsinga- og fjarskiptatæknibúnað, -ferla og -stefnur sem komið er á fót og stjórnað í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 (*), sem og með öðrum viðeigandi búnaði, stjórntækjum og verklagi fyrir aðrar tegundir rekstraráhættu, þ.m.t. fyrir öll verðbréfauppgjörskerfi sem hún starfrækir.

(*) Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um viðbætur við reglugerðir (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (Stjtíð. ESB L 333, 27.12.2022, bls. 1).“

2) Ákvæði 2. liðar falla brott.

3) Í stað 3. og 4. mgr. kemur eftirfarandi:

„3. Verðbréfamiðstöð skal, fyrir þjónustuna sem hún veitir, sem og hvert verðbréfauppgjörskerfi sem hún starfrækir, koma á, framkvæma og viðhalda viðeigandi stefnu um rekstrarsamfellu og áætlun um endurreisn eftir stóráfall, þ.m.t. stefnu um rekstrarsamfellu og viðbragðs- og endurreisnaráætlunum sem komið er á fót í samræmi við reglugerð (ESB) 2022/2554, til að tryggja varðveislu þjónustu, tímanlega endurupptöku starfsemi og uppfyllingu á skuldbindingum verðbréfamiðstöðvarinnar, ef um er að ræða atburði sem valda umtalsverðri hættu á röskun á starfsemi.

4. Áætlunin, sem um getur í 3. mgr., skal kveða á um endurreisn allra færslna og staðna þátttakenda frá þeim tíma sem röskun varð til að gera þátttakendunum í verðbréfamiðstöð kleift að halda starfsemi áfram á öruggan hátt og ljúka uppgjöri á áætluðum degi, þ.m.t. með því að tryggja að nauðsynleg upplýsingatæknikerfi geti hafið starfsemi aftur frá þeim tíma sem röskun varð, eins og kveðið er á um í 5. og 7. mgr. 12. gr. reglugerðar (ESB) 2022/2554.“

4) Í stað 6. mgr. kemur eftirfarandi:

„6. Verðbréfamiðstöð skal greina, vakta og stýra áhættu sem lykilþátttakendur í verðbréfauppgjörskerfinu sem hún starfrækir, sem og þjónustuveitendur, aðrar verðbréfamiðstöðvar eða aðrir markaðsinnviðir gætu valdið á starfsemi hennar. Hún skal, samkvæmt beiðni, veita lögbærum og viðeigandi yfirvöldum upplýsingar um sérhverja slíka áhættu sem greind er. Hún skal einnig upplýsa lögbært yfirvald og viðeigandi yfirvöld án tafar um öll rekstraratvik sem stafa af slíkri áhættu, nema þau sem tengjast upplýsinga- og fjarskiptatækniáhættu.“

5) Í stað fyrstu undirgreinar 7. mgr. kemur eftirfarandi:

„7. Evrópska verðbréfamarkaðseftirlitsstofnunin skal, í náinni samvinnu við aðila í seðlabankakerfi Evrópu, semja drög að tæknilegum framkvæmdarstöðlum sem tilgreina þá rekstraráhættu sem um getur í 1. og 6. mgr., að undanskilinni upplýsinga- og fjarskiptatækniáhættu, og prófunaraðferðir til að takast á við eða lágmarka hvers konar áhættu, þ.m.t. þær stefnur um rekstrarsamfellu og áætlanir um endurreisn eftir stóráfall sem um getur í 3. og 4. mgr., og aðferðirnar við mat á þeim.“

62. gr.

Breytingar á reglugerð (ESB) nr. 600/2014

Reglugerð (ESB) nr. 600/2014 er breytt sem hér segir:

1) Ákvæðum 27. gr. g er breytt sem hér segir:

a) Í stað 4. mgr. kemur eftirfarandi:

„4. Viðurkennd birtingarþjónusta skal uppfylla kröfurnar varðandi öryggi net- og upplýsingakerfa sem settar eru fram í reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 (*).

(*) Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um viðbætur við reglugerðir (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (Stjtíð. ESB L 333, 27.12.2022, bls. 1).“

b) Í stað c-liðar 8. mgr. kemur eftirfarandi:

„c) raunhæfar skipulagskröfur sem mælt er fyrir um í 3. og 5. mgr.“

2) Ákvæðum 27. gr. h er breytt sem hér segir:

a) Í stað 5. mgr. kemur eftirfarandi:

„5. Þjónusta fyrir sameinaðar viðskiptaupplýsingar skal uppfylla kröfurnar varðandi öryggi net- og upplýsingakerfa sem settar eru fram í reglugerð (ESB) 2022/2554.“

b) Í stað e-liðar 8. mgr. kemur eftirfarandi:

„e) raunhæfar skipulagskröfur sem mælt er fyrir um í 4. mgr.“

3) Ákvæðum 27. gr. i er breytt sem hér segir:

a) Í stað 3. mgr. kemur eftirfarandi:

„3. Viðurkennt skýrslugjafarkerfi skal uppfylla kröfurnar varðandi öryggi net- og upplýsingakerfa sem settar eru fram í reglugerð (ESB) 2022/2554.“

b) Í stað b-liðar 5. mgr. kemur eftirfarandi:

„b) raunhæfar skipulagskröfur sem mælt er fyrir um í 2. og 4. mgr.“

63. gr.

Breyting á reglugerð (ESB) 2016/1011

Eftirfarandi málsgrein bætist við 6. gr. reglugerðar (ESB) 2016/1011:

„6. Að því er varðar mjög mikilvægar viðmiðanir skal stjórnandi hafa traustar stjórnunar- og bókhaldsaðferðir, innri eftirlitskerfi, skilvirkar verklagsreglur fyrir áhættumat og skilvirkt eftirlits- og öryggisfyrirkomulag fyrir stjórnun á upplýsinga- og fjarskiptatæknikerfum í samræmi við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 (*).

(*) Reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um viðbætur við reglugerðir (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 (Stjtíð. ESB L 333, 27.12.2022, bls. 1).“

64. gr.

Gildistaka og framkvæmd

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Hún kemur til framkvæmda frá og með 17. janúar 2025.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Strassborg 14. desember 2022.

Fyrir hönd Evrópuþingsins,	*Fyrir hönd ráðsins,*
R. METSOLA	M. BEK
forseti.	*forseti.*