REGLUR

um stafrænan viðnámsþrótt fjármálamarkaðar.

1. gr.

Gildissvið.

Reglur þessar gilda um aðila á fjármálamarkaði samkvæmt 2. gr. reglugerð (ESB) 2022/2554, sbr. lög um stafrænan viðnámsþrótt fjármálamarkaðar, nr. 78/2025, og lífeyrissjóði samkvæmt lögum um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, sbr. 36. gr. g laganna.

2. gr.

Stjórnun upplýsinga- og fjarskiptatækniáhættu, stjórnun áhættu vegna þriðju aðila, meðhöndlun og tilkynningar atvika og prófanir á stafrænu viðnámsþoli.

Um meðhöndlun og tilkynningu atvika sem tengjast upplýsinga- og fjarskiptatækni og netógnir fer samkvæmt reglugerðum (ESB) 2024/1772, 2025/301 og 2025/302, sbr. 3. gr.

Um stjórnun upplýsinga- og fjarskiptatækniáhættu fer samkvæmt reglugerð (ESB) 2024/1774, sbr. 3. gr.

Um notkun upplýsinga- og fjarskiptatækniþjónustu þriðju aðila fer eftir reglugerðum (ESB) 2024/1773 og 2025/532 við notkun, sbr. 3. gr.

Um samræmingu skilyrða sem gera eftirlitsstarfsemi evrópsku eftirlitsstofnananna mögulega fer samkvæmt reglugerðum (ESB) 2025/295 og 2025/420, sbr. 3. gr.

Um ógnamiðaðar innbrotsprófanir fer samkvæmt reglugerð (ESB) 2025/1190, sbr. 3. gr.

3. gr.

Innleiðing reglugerða.

Með reglum þessum öðlast gildi hér á landi eftirtaldar reglugerðir:

1. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1772 frá 13. mars 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina viðmið fyrir flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum, setja fram mikilvægismörk og tilgreina nánari upplýsingar um tilkynningar um alvarleg atvik, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 77/2025 frá 14. mars 2025 sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 38 frá 12. júní 2025, bls. 58. Reglugerðin er birt í fylgiskjali 1 með reglum þessum.
2. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1773 frá 13. mars 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina ítarlegt innihald stefnunnar varðandi samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 77/2025 frá 14. mars 2025 sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 38 frá 12. júní 2025, bls. 58. Reglugerðin er birt í fylgiskjali 2 með reglum þessum.
3. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1774 frá 13. mars 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreind eru nánar búnaður, aðferðir, ferlar og stefnur til stýringar á upplýsinga- og fjarskiptatækniáhættu og einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 77/2025 frá 14. mars 2025 sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 38 frá 12. júní 2025, bls. 58. Reglugerðin er birt í fylgiskjali 3 með reglum þessum.
4. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/295 frá 24. október 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla um samræmingu skilyrða sem gera eftirlitsstarfsemi mögulega, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 137/2025 frá

13. júní 2025 sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 61 frá 2. október 2025, bls. 40. Reglugerðin er birt í fylgiskjali 4 með reglum þessum.

5. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/301 frá 23. október 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreint er innihald og tímamörk frumtilkynningar, og áfanga- og lokaskýrslu, um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og inntak valfrjálsrar tilkynningar um verulegar netógnir, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 137/2025 frá 13. júní 2025 sem birt er í EES-viðbæti við Stjórnartíðindi Evrópusambandsins nr. 61 frá 2. október 2025, bls. 40. Reglugerðin er birt í fylgiskjali 5 með reglum þessum.
6. Framkvæmdarreglugerð framkvæmdastjórnarinnar (ESB) 2025/302 frá 23. október 2024 um tæknilega framkvæmdarstaðla fyrir beitingu reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar stöðluð eyðublöð, sniðmát og verklagsreglur fyrir aðila á fjármálamarkaði til að tilkynna um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og til að tilkynna um verulega netógn, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 36/2026 frá 6. febrúar 2026. Reglugerðin er birt í fylgiskjali 6 með reglum þessum.
7. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/420 frá 16. desember 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla til að tilgreina nánar 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, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 299/2025 frá 5. desember 2025 sem birt er í fylgiskjali 7 með reglum þessum, með þeim aðlögunum sem leiða af ákvörðun sameiginlegu EES-nefndarinnar. Reglugerðin er birt í fylgiskjali 8 með reglum þessum.
8. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/532 frá 24. mars 2025 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina nánar þá þætti sem aðili á fjármálamarkaði þarf að ákvarða og meta þegar hann semur við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 299/2025 frá 5. desember 2025. Reglugerðin er birt í fylgiskjali 9 með reglum þessum.
9. Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/1190 frá 13. febrúar 2025 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreind eru viðmið sem notuð eru til að auðkenna aðila á fjármálamarkaði sem skylt er að framkvæma ógnamiðaðar innbrotsprófanir, kröfur og staðlar sem gilda um notkun á innri prófunaraðilum, kröfur í tengslum við umfang, prófunaraðferðir og nálgun fyrir hvern fasa í prófunum, niðurstöður, l7kunar- og úrbótastig prófunar og tegund eftirlitssamvinnu og annarrar viðeigandi samvinnu sem þörf er á við innleiðingu ógnamiðaðra innbrotsprófana og til að greiða fyrir gagnkvæmri viðurkenningu, sem tekin var upp í EES-samninginn með ákvörðun sameiginlegu EES-nefndarinnar nr. 299/2025 frá 5. desember 2025. Reglugerðin er birt í fylgiskjali 10 með reglum þessum.

4. gr.

Gildistaka.

Reglur þessar, sem settar eru með heimild í 1.-8. tölul. 2. mgr. 11. gr. laga um stafrænan viðnámsþrótt fjármálamarkaðar nr. 78/2025 og 6. mgr. 36. gr. g laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, taka gildi þegar í stað.

Seðlabanka Íslands, 27. mars 2026.

Björk Sigurgísladóttir
varaseðlabankastjóri fjármálaeftirlits.

Guðmundur Óli Blöndal
forstöðumaður.

Fylgiskjal 1.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2024/1772

frá 13. mars 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina viðmið fyrir flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum, setja fram mikilvægismörk og tilgreina nánari upplýsingar um tilkynningar um alvarleg atvik

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum þriðju undirgrein 4. mgr. 18. gr.,

og að teknu tilliti til eftirfarandi:

1) Reglugerð (ESB) 2022/2554 miðar að því að samræma og einfalda kröfur um skýrslugjöf um atvik sem tengjast upplýsinga- og fjarskiptatækni og greiðslutengd rekstrar- eða öryggisatvik sem varða lánastofnanir, greiðslustofnanir, reikningsupplýsingaþjónustuveitendur og rafeyrisfyrirtæki („atvik“). Í ljósi þess að skýrslugjafarkröfurnar ná yfir 20 mismunandi tegundir aðila á fjármálamarkaði ætti að skilgreina flokkunarviðmið og mikilvægismörk til að ákvarða alvarleg atvik og verulegar netógnir á einfaldan, samræmdan og samkvæman hátt sem tekur tillit til sérstöðu þjónustunnar og starfsemi allra viðkomandi aðila á fjármálamarkaði.

2) Til að tryggja meðalhóf ættu flokkunarviðmið og mikilvægismörk að endurspegla stærð og heildaráhættusnið og eðli, umfang og flækjustig þjónustu allra aðila á fjármálamarkaði. Auk þess ættu viðmiðin og mikilvægismörkin að vera hönnuð þannig að þau eigi við alla aðila á fjármálamarkaði með samræmdum hætti, óháð stærð þeirra og áhættusniði, og valdi minni aðilum á fjármálamarkaði ekki óhóflegri skýrslugjafarbyrði. Til að taka á aðstæðum þar sem verulegur fjöldi viðskiptavina verður fyrir áhrifum af atviki sem fer sem slíkt ekki yfir gildandi viðmiðunarmörk ætti þó að setja algild viðmiðunarmörk sem beinast aðallega að stærri aðilum á fjármálamarkaði.

3) Í tengslum við ramma utan um skýrslugjöf vegna atvika, sem voru til áður en reglugerð (ESB) 2022/2554 tók gildi, ætti að tryggja samfellu fyrir aðila á fjármálamarkaði. Því ættu flokkunarviðmið og mikilvægismörk að vera aðlöguð að og innblásin af viðmiðunarreglum Evrópsku bankaeftirlitsstofnunarinnar um skýrslugjöf um alvarleg atvik samkvæmt tilskipun Evrópuþingsins og ráðsins (ESB) 2015/2366 ([2]), leiðbeiningum um reglubundnar upplýsingar og tilkynningar um verulegar breytingar sem viðskiptaskrár verða að senda til Evrópsku verðbréfamarkaðseftirlitsstofnunarinnar, ramma Seðlabanka Evrópu/samræmdrar eftirlitsráðstöfunar um skýrslugjöf vegna netatvika (e. *ECB/SSM Cyber Incident Reporting Framework*) og öðrum viðeigandi leiðbeiningum. Flokkunarviðmið og viðmiðunarmörk ættu einnig að henta fyrir þá aðila á fjármálamarkaði sem hafa ekki áður fallið undir kröfur um skýrslugjöf vegna atvika fyrr en nú, undir reglugerð (ESB) 2022/2554.

4) Að því er varðar flokkunarviðmiðið „fjárhæð og fjöldi viðskipta sem verða fyrir áhrifum“ er hugtakið viðskipti víðtækt og nær yfir ólíka starfsemi og þjónustu í geirabundnum gerðum sem gilda um aðila á fjármálamarkaði. Að því er þetta flokkunarviðmið varðar ætti það að ná yfir greiðslur og allar gerðir viðskipta með fjármálagerninga, sýndareignir, hrávörur eða hvers kyns aðrar eignir, einnig í formi tryggingarfjár, veðs eða trygginga, bæði gegn reiðufé og öðrum eignum. Taka ætti tillit til allra viðskipta sem varða eignir sem hægt er að gefa upp sem fjárhæð í flokkunartilgangi.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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, 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, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

5) Með flokkunarviðmiðunum ætti að tryggja að allar viðeigandi tegundir alvarlegra atvika séu fangaðar. Ekki eru endilega mörg flokkunarviðmið sem ná utan um netárásir sem tengjast innbrotum í net- eða upplýsingakerfi. Þær eru hins vegar mikilvægar þar sem hvers kyns innbrot í net- og upplýsingakerfi geta skaðað aðila á fjármálamarkaði. Til samræmis við það ætti að skilgreina flokkunarviðmiðin „mikilvæg þjónusta sem verður fyrir áhrifum“ og „gagnatap“ þannig að þau nái yfir þessar tegundir alvarlegra atvika, einkum innrás óviðkomandi aðila sem getur haft alvarlegar afleiðingar, jafnvel þótt áhrifin liggi ekki strax fyrir, einkum gagnabrot og gagnaleka.

6) Þar sem lánastofnanir falla bæði undir ramma utan um flokkun á atvikum skv. 18. gr. reglugerðar (ESB) 2022/2554 og ramma um rekstraráhættu samkvæmt framseldri reglugerð framkvæmdastjórnarinnar (ESB) 2018/959 ([3]) ætti nálgun við mat á efnahagslegum áhrifum atviks, byggt á útreikningi á kostnaði og tapi að vera eins samræmt og mögulegt er milli beggja ramma til að forðast að ósamrýmanlegar eða misvísandi kröfur.

7) Viðmið í tengslum við landfræðilega útbreiðslu atviks eins og sett er fram í c-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554 ætti að leggja áherslu á áhrif atviksins yfir landamæri, þar sem önnur viðmið í þeirri grein munu ná yfir áhrif af atviki á starfsemi aðila á fjármálamarkaði innan einnar lögsögu.

8) Þar sem flokkunarviðmiðin eru innbyrðis háð og tengd hvert öðru ætti aðferðin við að greina alvarleg atvik sem ber að tilkynna í samræmi við 1. mgr. 19. gr. reglugerðar (ESB) 2022/2554 að byggjast á samsetningu viðmiða þar sem sum viðmið, sem eru nátengd skilgreiningum á atviki sem tengist upplýsinga- og fjarskiptatækni og alvarlegu atviki sem tengist upplýsinga- og fjarskiptatækni eins og sett fram í 8. og 10. mgr. 3. gr. reglugerðar (ESB) 2022/2554, ættu að vega þyngra í flokkun á alvarlegum atvikum en önnur.

9) Til að tryggja að skýrslur og tilkynningar um alvarleg atvik sem berast lögbærum yfirvöldum skv. 1. mgr. 19. gr. reglugerðar (ESB) 2022/2554 þjóni tilgangi bæði í eftirlitsskyni og til að koma í veg fyrir smitáhrif í fjármálageiranum ættu mikilvægismörkin að gera kleift að fanga alvarleg atvik, m.a. með því að leggja áherslu á áhrifin á einingarsértæka mikilvæga þjónustu, tiltekin algild og hlutfallsleg mörk viðskiptavina eða fjárhagslegra mótaðila, viðskipti sem sýna umtalsverð áhrif á aðila á fjármálamarkaði og þýðingu áhrifanna í öðrum aðildarríkjum.

10) Líta ætti á atvik sem hafa áhrif á upplýsinga- og fjarskiptatækniþjónustu eða net- og upplýsingakerfi sem styðja nauðsynlega eða mikilvæga starfsemi eða fjármálaþjónustu sem krefst leyfis, eða óheimilan aðgang í illum tilgangi að net- og upplýsingakerfum sem styðja nauðsynlega eða mikilvæga starfsemi, sem atvik sem hafa áhrif á mikilvæga þjónustu aðila á fjármálamarkaði. Óheimill aðgangur í illum tilgangi að net- og upplýsingakerfum sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði hefur í för með sér alvarlega áhættu fyrir þá og ætti alltaf að teljast alvarlegt atvik sem ber að tilkynna, þar sem aðgangurinn getur haft áhrif á aðra aðila á fjármálamarkaði.

11) Endurtekin atvik sem virðast tengjast í gegnum svipaðar frumorsakir, sem hvert um sig er ekki alvarlegt atvik, geta bent til verulegra annmarka og veikleika í verklagsreglum aðila á fjármálamarkaði við atvika- og áhættustýringu. Endurtekin atvik ættu því að teljast vera alvarleg ef þau koma ítrekað fyrir yfir tiltekið tímabil.

12) Í ljósi þess að netógnir geta haft neikvæð áhrif á aðila á fjármálamarkaði og fjármálageirann ættu þær verulegu netógnir sem aðilar á fjármálamarkaði kunna að tilkynna að gefa til kynna líkurnar á því að þær raungerist og alvarleika mögulegra áhrifa. Til samræmis við það ætti flokkun netógnar sem verulegrar að fara eftir líkunum á því að flokkunarviðmið fyrir alvarleg atvik og viðmiðunarmörk þeirra myndu vera uppfyllt ef ógnin raungerðist, eftir tegund netógnar og eftir þeim upplýsingum sem eru tiltækar fyrir aðila á fjármálamarkaði, til að tryggja skýrt og samræmt mat á þýðingu netógna.

([3]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2018/959 frá 14. mars 2018 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) nr. 575/2013 að því er varðar tæknilega eftirlitsstaðla um lýsingu á aðferðafræði varðandi mat sem lögbær yfirvöld skulu nota til að heimila stofnunum að nota þróaðar mæliaðferðir fyrir rekstraráhættu (Stjtíð. ESB L 169, 6.7.2018, bls. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

13) Í ljósi þess að tilkynna þarf lögbærum yfirvöldum í öðrum aðildarríkjum um atvik sem hafa áhrif á aðila á fjármálamarkaði og viðskiptavini í lögsögu þeirra ætti mat á áhrifum í öðru lögsagnarumdæmi í samræmi við 7. mgr. 19. gr. reglugerðar (ESB) 2022/2554 að byggjast á frumorsökum atviksins, á hugsanlegum smitáhrifum í gegnum veitendur sem eru þriðja aðilar og á innviðum fjármálamarkaðar, sem og á áhrifum atviksins á mikilvæga hópa viðskiptavina eða fjárhagslega mótaðila.

14) Skýrslugjafar- og tilkynningarferlin sem um getur í 6. og 7. mgr. 19. gr. reglugerðar (ESB) 2022/2554 ættu að gera viðkomandi viðtakendum kleift að leggja mat á áhrifin af atvikunum. Því ættu sendar upplýsingar að ná yfir allar upplýsingar úr atvikaskýrslum sem aðili á fjármálamarkaði sendir til lögbærs yfirvalds.

15) Ef atvik felur í sér öryggisbrest við meðferð persónuupplýsinga, samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 ([4]) og tilskipun Evrópuþingsins og ráðsins 2002/58/EB ([5]), ætti þessi reglugerð ekki að hafa áhrif á skráningar- og tilkynningarskyldur vegna öryggisbrests við meðferð persónuupplýsinga sem settar eru fram í þeim lögum Sambandsins. Lögbær yfirvöld ættu að starfa með og skiptast á upplýsingum um öll viðeigandi mál við þau yfirvöld sem um getur í reglugerð (ESB) 2016/679 og tilskipun 2002/58/EB.

16) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem evrópsku eftirlitsstofnanirnar, í samráði við Netöryggisstofnun Evrópusambandsins og Seðlabanka Evrópu hafa lagt fyrir framkvæmdastjórnina.

17) Sameiginleg nefnd evrópsku eftirlitsstofnananna sem um getur í 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([6]), 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([7]) og 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([8]) hefur haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint hugsanlegan kostnað og ávinning af fyrirhuguðum stöðlum og óskað eftir ráðgjöf hagsmunahóps um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010, hagsmunahóps í vátryggingum og hagsmunahóps um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1094/2010 og hagsmunahóps á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1095/2010.

([4]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Tilskipun Evrópuþingsins og ráðsins 2002/58/EB frá 12. júlí 2002 um vinnslu persónuupplýsinga og um verndun einkalífs á sviði rafrænna fjarskipta (tilskipun um friðhelgi einkalífsins og rafræn fjarskipti) (Stjtíð. EB L 201, 31.7.2002, bls. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

18) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([9]) og skilaði hún áliti 24. janúar 2024.

SAMÞYKKT REGLUGERÐ ÞESSA:

I. KAFLI

FLOKKUNARVIÐMIÐ

1. gr.

Viðskiptavinir, fjárhagslegir mótaðilar og viðskipti

1. Fjöldi viðskiptavina sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal endurspegla fjölda allra viðskiptavina sem verða fyrir áhrifum, óháð því hvort þeir eru einstaklingar eða lögaðilar, sem geta ekki eða gátu ekki nýtt sér þá þjónustu sem aðili á fjármálamarkaði veitti á meðan atvikinu stóð eða sem atvikið hafði neikvæð áhrif á. Sá fjöldi skal einnig taka til þriðju aðila sem falla sérstaklega undir samningsbundið samkomulag á milli aðila á fjármálamarkaði og viðskiptavinarins sem viðtakanda viðkomandi þjónustu.

2. Fjöldi fjárhagslegra mótaðila sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal endurspegla fjölda allra fjárhagslegra mótaðila sem verða fyrir áhrifum og hafa gert samning við viðkomandi aðila á fjármálamarkaði.

3. Í tengslum við mikilvægi viðskiptavina og fjárhagslegra mótaðila sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal viðkomandi aðili á fjármálamarkaði taka tillit til þess að hvaða marki áhrif á viðskiptavin eða fjárhagslegan mótaðila snerta framkvæmd viðskiptamarkmiða aðila á fjármálamarkaði sem og hugsanlegra áhrifa atviksins á skilvirkni markaðar.

4. Í tengslum við fjárhæð eða fjölda viðskipta sem atvikið hefur áhrif á, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skal viðkomandi aðili á fjármálamarkaði taka tillit til allra viðskipta sem verða fyrir áhrifum og fela í sér peningafjárhæð þar sem a.m.k. einn hluti viðskiptanna fer fram í Sambandinu.

5. Ef ekki er hægt að ákvarða raunverulegan fjölda viðskiptavina eða fjárhagslegra mótaðila eða raunverulegan fjölda eða fjárhæð viðskipta sem verða fyrir áhrifum skal aðili á fjármálamarkaði leggja mat á fjöldann eða fjárhæðina miðað við tiltæk gögn frá sambærilegum viðmiðunartímabilum.

2. gr.

Áhrif á orðspor

1. Til að skera úr um áhrif atviksins á orðspor, eins og um getur í a-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði líta svo á að áhrif hafi orðið á orðspor ef a.m.k. eitt eftirfarandi viðmið er uppfyllt:

a) fjallað hefur verið um atvikið í fjölmiðlum,

b) atvikið hefur valdið endurteknum kvörtunum frá mismunandi viðskiptavinum eða fjárhagslegum mótaðilum varðandi þjónustu með beinum samskiptum við viðskiptavini eða mikilvæg viðskiptasambönd,

c) aðili á fjármálamarkaði mun ekki geta, eða líklegt er að hann geti ekki, uppfyllt kröfur samkvæmt reglum vegna atviksins,

d) aðili á fjármálamarkaði mun, eða er líklegur til að, missa viðskiptavini eða fjárhagslega mótaðila sem hafa umtalsverð áhrif á viðskipti hans vegna atviksins.

([9]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. Við mat á áhrifum atviks á orðspor skulu aðilar á fjármálamarkaði taka tillit til þess hversu sýnilegt það er eða er líklegt til að verða í tengslum við hvert viðmið sem tilgreint er í 1. mgr.

3. gr.

Tímalengd og niðritími þjónustu

1. Aðilar á fjármálamarkaði skulu mæla tímalengd atviks eins og um getur í 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554 frá því augnabliki sem atvikið átti sér stað og þar til úr því hefur verið leyst.

Ef aðilar á fjármálamarkaði geta ekki ákvarðað hvenær atvikið átti sér stað skulu þeir mæla tímalengd atviksins frá því að það uppgötvaðist. Ef aðilar á fjármálamarkaði komast að því síðar að atvikið hafi átt sér stað áður en það uppgötvaðist skulu þeir mæla tímalengdina frá því að atvikið var skráð í net- eða kerfisskrár eða aðrar gagnalindir.

Ef aðilar á fjármálamarkaði vita ekki enn hvenær leyst verður úr atvikinu eða geta ekki sannprófað skrár í kerfisskrám eða öðrum gagnalindum skulu þeir nota mat.

2. Aðilar á fjármálamarkaði skulu mæla niðritíma þjónustu, eins og um getur í b-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, frá því þegar þjónustan er að öllu leyti eða hluta til óaðgengileg viðskiptavinum, aðilum á fjármálamarkaði eða öðrum innri eða ytri notendum þar til regluleg starfsemi eða rekstur hefur verið færður aftur á sama þjónustustig og var veitt á undan atvikinu. Ef niðritími þjónustu veldur töfum á þjónustustarfsemi eftir að regluleg starfsemi eða rekstur hefur verið færður aftur í sama horf skal mæla niðritímann frá upphafi atviks þangað til að seinkuð þjónusta er aftur veitt að fullu.

Ef aðilar á fjármálamarkaði geta ekki ákvarðað hvenær niðritími þjónustu hófst skulu þeir mæla niðritíma þjónustunnar frá því að það uppgötvaðist.

4. gr.

Landfræðileg útbreiðsla

Til að ákvarða landfræðilega útbreiðslu að því er varðar svæðin sem atvikið hefur áhrif á, eins og um getur í c-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði leggja mat á hvort atvik hafi, eða hafi haft, áhrif í öðrum aðildarríkjum og einkum þýðingu áhrifanna í tengslum við eftirfarandi:

a) viðskiptavini og fjárhagslega mótaðila í öðrum aðildarríkjum,

b) útibú eða aðra aðila á fjármálamarkaði innan samstæðunnar, sem annast starfsemi í öðrum aðildarríkjum,

c) innviði fjármálamarkaðar eða veitendur sem eru þriðju aðilar, sem gæti haft áhrif á aðila á fjármálamarkaði í öðrum aðildarríkjum þar sem þeir veita þjónustu, að því marki sem slíkar upplýsingar eru tiltækar.

5. gr.

Tap á gögnum

Til að ákvarða gagnatapið sem atvik hefur í för með sér, eins og um getur í d-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði taka tillit til eftirfarandi:

a) í tengslum við tiltækileika gagna, hvort atvikið hafi gert gögn sem aðili á fjármálamarkaði, viðskiptavinir hans eða mótaðilar höfðu óskað eftir tímabundið eða varanlega ótiltæk eða ónothæf,

b) í tengslum við ósvikni gagna, hvort atvikið hafi skert trúverðugleika gagnalindarinnar,

c) í tengslum við réttleika gagna, hvort atvikið hafi valdið óheimilaðri breytingu á gögnum sem hafi gert þau ónákvæm eða ófullnægjandi,

d) í tengslum við leynd gagna, hvort atvikið hafi leitt til þess að óviðkomandi aðili eða kerfi hafi fengið aðgang að gögnum eða fengið þau afhent.

6. gr.

Mikilvægi þjónustu sem verður fyrir áhrifum

Til að ákvarða mikilvægi þjónustunnar sem verður fyrir áhrifum, eins og um getur í e-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði meta hvort atvikið:

a) hafi eða hafi haft áhrif á upplýsinga- og fjarskiptatækniþjónustu eða net- og upplýsingakerfi sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði,

b) hafi eða hafi haft áhrif á fjármálaþjónustu sem aðili á fjármálamarkaði veitir, sem þarfnast starfsleyfis, skráningar eða sem er undir eftirliti lögbærra yfirvalda,

c) feli eða hafi falið í sér árangursríkan, óheimilan aðgang í illum tilgangi að net- og upplýsingakerfum aðila á fjármálamarkaði.

7. gr.

Efnahagsleg áhrif

1. Til að ákvarða efnahagsleg áhrif atviks, eins og um getur í f-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði taka tillit til eftirfarandi tegunda af beinum og óbeinum kostnaði sem þeir hafa stofnað til vegna atviksins, án þess taka tillit til fjárhagslegrar endurheimtar:

a) fjármuna eða fjáreigna sem hafa verið tekin eignarnámi og þeir bera ábyrgð á, þ.m.t. eigna sem tapast vegna þjófnaðar,

b) kostnaðar við að endurnýja eða flytja hugbúnað, vélbúnað eða innviði,

c) starfsmannakostnaðar, þ.m.t. kostnaðar við að endurnýja eða flytja starfsfólk, ráða starfsfólk til viðbótar, greiða yfirvinnu og endurheimt tapaðrar eða skertrar færni,

d) gjalda sem hljótast af því að ekki er staðið við samningsbundnar skyldur,

e) kostnaðar vegna lagfæringa og bóta til viðskiptavina,

f) taps vegna tapaðra tekna,

g) kostnaðar sem tengist innri og ytri samskiptum,

h) ráðgjafarkostnaðar, þ.m.t. kostnaðar sem tengist lögfræðiráðgjöf, tæknirannsóknum og úrbótum.

2. Kostnaður og tap sem um getur í 1. mgr. skal ekki taka til kostnaðar sem er nauðsynlegur fyrir daglegan rekstur fyrirtækisins, einkum eftirfarandi:

a) kostnaðar vegna almenns viðhalds á innviðum, búnaði, vélbúnaði og hugbúnaði, og kostnaðar við að viðhalda færni starfsfólks,

b) innri eða ytri kostnaðar við að styrkja fyrirtækið eftir atvikið, þ.m.t. uppfærslur, endurbætur og framtaksverkefni í áhættumati,

c) tryggingariðgjalda.

3. Aðilar á fjármálamarkaði skulu reikna út fjárhæð kostnaðar og taps út frá þeim gögnum sem liggja fyrir við skýrslugjöf. Ef ekki er hægt að ákvarða fjárhæð fyrir raunverulegan kostnað og tap skulu aðilar á fjármálamarkaði áætla þá fjárhæð.

4. Við mat á efnahagslegum áhrifum atviksins skulu aðilar á fjármálamarkaði leggja saman þann kostnað og tap sem um getur í 1. mgr.

II. KAFLI

ALVARLEG ATVIK OG MIKILVÆGISMÖRK

8. gr.

Alvarleg atvik

1. Atvik skal teljast vera alvarlegt atvik að því er varðar 1. mgr. 19. gr. reglugerðar (ESB) 2022/2554 ef það hefur áhrif á nauðsynlega þjónustu, eins og um getur í 6. gr., og ef annaðhvort eftirfarandi skilyrða er uppfyllt:

a) mikilvægismörkin, sem um getur í b-lið 5. mgr. 9. gr., eru uppfyllt,

b) tvö eða fleiri af öðrum mikilvægismörkum, sem um getur í 1. til 6. mgr. 9. gr., eru uppfyllt.

2. Endurtekin atvik sem hvert fyrir sig er ekki alvarlegt atvik í samræmi við 1. mgr. skulu teljast eitt alvarlegt atvik ef þau uppfylla öll eftirfarandi skilyrði:

a) þau hafa átt sér stað a.m.k. tvisvar á 6 mánuðum,

b) þau hafa sömu augljósu frumorsökina, eins og um getur í b-lið fyrstu undirgr. 20. gr. reglugerðar (ESB) 2022/2554,

c) þau uppfylla samtals viðmiðin til að teljast alvarlegt atvik eins og sett er fram í 1. mgr.

Aðilar á fjármálamarkaði skulu meta tíðni endurtekinna atvika einu sinni í mánuði.

Þessi málsgrein gildir ekki um örfyrirtæki og aðila á fjármálamarkaði sem eru taldir upp í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554.

9. gr.

Mikilvægismörk til að ákvarða alvarleg atvik

1. Mikilvægismörkum fyrir viðmiðið „viðskiptavinir, fjárhagslegir mótaðilar og viðskipti“ er náð ef einhver eftirfarandi skilyrða eru uppfyllt:

a) fjöldi viðskiptavina sem verða fyrir áhrifum er meiri en 10% af öllum viðskiptavinum sem nota viðkomandi þjónustu,

b) fjöldi viðskiptavina sem verða fyrir áhrifum og nota viðkomandi þjónustu er meiri en 100 000,

c) fjöldi fjárhagslegra mótaðila sem verða fyrir áhrifum er meiri en 30% af öllum fjárhagslegum mótaðilum sem annast starfsemi sem tengist veitingu viðkomandi þjónustu,

d) fjöldi viðskipta sem verða fyrir áhrifum er meiri en 10% af meðalfjölda daglegra viðskipta sem aðili á fjármálamarkaði annast í tengslum við viðkomandi þjónustu,

e) fjárhæð viðskipta sem verða fyrir áhrifum er hærri en 10% af meðalvirði daglegra viðskipta sem aðili á fjármálamarkaði annast í tengslum við viðkomandi þjónustu,

f) viðskiptavinir eða fjárhagslegir mótaðilar sem hafa verið auðkenndir sem mikilvægir, í samræmi við 3. mgr. 1. gr., hafa orðið fyrir áhrifum.

Ef ekki er hægt að ákvarða raunverulegan fjölda viðskiptavina eða fjárhagslegra mótaðila eða raunverulegan fjölda eða fjárhæð viðskipta sem verða fyrir áhrifum skal aðili á fjármálamarkaði leggja mat á fjöldann eða fjárhæðina miðað við tiltæk gögn frá sambærilegum viðmiðunartímabilum.

2. Mikilvægismörkum fyrir viðmiðið „áhrif á orðspor“ er náð ef einhver skilyrðanna sem eru sett fram í a- til d-lið 2. gr. eru uppfyllt.

3. Mikilvægismörkum fyrir viðmiðið „tímalengd og niðritími þjónustu“ er náð ef einhver eftirfarandi skilyrða eru uppfyllt:

a) tímalengd atviksins er lengri en 24 stundir,

b) niðritími þjónustu er lengri en 2 stundir fyrir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

4. Mikilvægismörkum fyrir viðmiðið „landfræðileg útbreiðsla“ er náð ef atvikið hefur áhrif í tveimur eða fleiri aðildarríkjum í samræmi við 4. gr.

5. Mikilvægismörkum fyrir viðmiðið „gagnatap“ er náð ef einhver eftirfarandi skilyrða eru uppfyllt:

a) öll áhrif eins og um getur í 5. gr. á tiltækileika, ósvikni, réttleika eða leynd gagna hafa eða munu hafa neikvæð áhrif á framkvæmd viðskiptamarkmiða aðila á fjármálamarkaði eða á getu hans til að uppfylla kröfur samkvæmt reglum,

b) hvers konar árangursríkur og óheimill aðgangur í illum tilgangi að net- og upplýsingakerfum, sem a-liður fjallar ekki um, ef slíkur aðgangur getur valdið gagnatapi.

6. Mikilvægismörkum fyrir viðmiðið „efnahagsleg áhrif“ er náð ef kostnaður og tap sem aðili á fjármálamarkaði hefur stofnað til vegna atviksins hafa farið, eða eru líkleg til að fara, umfram 100 000 evrur.

III. KAFLI

VERULEGAR NETÓGNIR

10. gr.

Há mikilvægismörk til að ákvarða verulegar netógnir

Að því er varðar 2. mgr. 18. gr. reglugerðar (ESB) 2022/2554 skal netógn teljast veruleg ef öll eftirfarandi skilyrði eru uppfyllt:

a) ef netógnin raungerist getur hún haft eða gæti hafa haft áhrif á nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði eða haft áhrif á aðra aðila á fjármálamarkaði, veitendur sem eru þriðju aðilar, viðskiptavini eða fjárhagslega mótaðila, á grundvelli þeirra upplýsinga sem aðila á fjármálamarkaði eru tiltækar,

b) miklar líkur eru á að netógnin raungerist hjá viðkomandi aðila á fjármálamarkaði eða öðrum aðilum á fjármálamarkaði, að teknu tilliti til a.m.k. eftirfarandi þátta:

   i. gildandi áhættu sem tengist þeirri netógn sem um getur í a-lið, þ.m.t. hugsanlegra veikleika í kerfum aðila á fjármálamarkaði sem hægt er að misnota,

   ii. getu og tilgangs ógnvalda, að því marki sem aðila á fjármálamarkaði er kunnugt um,

   iii. langæi ógnarinnar og hvers kyns uppsafnaðrar vitneskju um atvik sem hafa haft áhrif á aðila á fjármálamarkaði eða veitanda hans sem er þriðji aðili, viðskiptavini eða fjárhagslega mótaðila,

c) netógnin gæti, ef hún raungerðist, uppfyllt eitthvert eftirfarandi:

   i. viðmiðið varðandi mikilvægi þjónustunnar sem sett er fram í e-lið 1. mgr. 18. gr. reglugerðar (ESB) 2022/2554, eins og tilgreint er 6. gr. þessarar reglugerðar,

   ii. mikilvægismörk sem sett eru fram í 1. mgr. 9. gr.,

   iii. mikilvægismörk sem sett eru fram í 4. mgr. 9. gr.,

Komist aðili á fjármálamarkaði að þeirri niðurstöðu að þau mikilvægismörk sem sett eru fram í 2., 3., 5. og 6. mgr. 9. gr. gætu verið uppfyllt er einnig hægt að taka tillit til þeirra marka, allt eftir gerð netógnar og fyrirliggjandi upplýsinga.

IV. KAFLI

GILDI ALVARLEGRA ATVIKA FYRIR LÖGBÆR YFIRVÖLD Í ÖÐRUM AÐILDARRÍKJUM OG UPPLÝSINGAR Í SKÝRSLUM SEM Á AÐ DEILA MEÐ ÖÐRUM LÖGBÆRUM YFIRVÖLDUM

11. gr.

Gildi alvarlegra atvika fyrir lögbær yfirvöld í öðrum aðildarríkjum

Mat á því hvort alvarleg atvik hafi gildi fyrir lögbær yfirvöld í öðrum aðildarríkjum, eins og um getur í 7. mgr. 19. gr. reglugerðar (ESB) 2022/2554, skal byggjast á því hvort atvikið eigi sér frumorsök í öðru aðildarríki eða hvort atvikið hafi eða hafi haft umtalsverð áhrif í öðru aðildarríki í tengslum við eitthvert eftirfarandi:

a) viðskiptavini eða fjárhagslega mótaðila,

b) útibú aðila á fjármálamarkaði eða annan aðila á fjármálamarkaði innan samstæðunnar,

c) innviði fjármálamarkaðar eða veitanda sem er þriðji aðili sem gæti haft áhrif á aðila á fjármálamarkaði sem þeir veita þjónustu.

12. gr.

Upplýsingar um alvarleg atvik sem ber að deila með öðrum lögbærum yfirvöldum

Upplýsingar um alvarleg atvik sem lögbærum yfirvöldum ber að senda öðrum lögbærum yfirvöldum í samræmi við 6. mgr. 19. gr. reglugerðar (ESB) 2022/2554 og tilkynningarnar sem Evrópska bankaeftirlitsstofnunin, Evrópska verðbréfamarkaðseftirlitsstofnunin eða Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin og Seðlabanki Evrópu verða að senda til viðkomandi lögbærra yfirvalda í öðrum aðildarríkjum í samræmi við 7. mgr. 19. gr. þeirrar reglugerðar skulu innihalda sömu upplýsingar, án nokkurs nafnleysis, og tilkynningar og skýrslur um alvarleg atvik sem berast frá aðilum á fjármálamarkaði í samræmi við 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554.

V. KAFLI

LOKAÁKVÆÐI

13. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í Stjórnartíðindum Evrópusambandsins.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 13. mars 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

Fylgiskjal 2.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2024/1773

frá 13. mars 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina ítarlegt innihald stefnunnar varðandi samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður við nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum þriðju undirgrein 10. mgr. 28. gr.

og að teknu tilliti til eftirfarandi:

1) Með ramma um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann, sem komið er á fót með reglugerð (ESB) 2022/2554, er þess krafist að aðilar á fjármálamarkaði setji sér tilteknar meginreglur til að stýra upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, sem er einkar mikilvægt þegar aðilar á fjármálamarkaði eru í samstarfi við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu til að styðja við nauðsynlega eða mikilvæga starfsemi þeirra.

2) Aðilar á fjármálamarkaði verða að taka upp og endurskoða reglulega stefnuáætlun um upplýsinga- og fjarskiptatækniáhættu vegna þriðju aðila, sem hluta af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni. Í samræmi við 2. mgr. 28. gr. reglugerðar (ESB) 2022/2554 skal sú stefnuáætlun fela í sér stefnu um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Hún skal gilda á einingagrundvelli og, þar sem við á, undirsamstæðu- og samstæðugrunni.

3) Aðilar á fjármálamarkaði eru afar mismunandi að því er varðar stærð, uppbyggingu og innra skipulag og eðli og flækjustig starfsemi þeirra og rekstrar. Nauðsynlegt er að taka tillit til þessarar fjölbreytni við setningu tiltekinna réttarfarslegra grundvallarkrafna sem eiga við um alla aðila á fjármálamarkaði við mótun stefnu varðandi samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu („stefnan“), og tryggja að þessum kröfum sé beitt á hlutfallslegan hátt.

4) Ef aðilar á fjármálamarkaði tilheyra samstæðu ætti móðurfyrirtækið sem ber ábyrgð á að gera samstæðu- eða undirsamstæðureikningsskil fyrir samstæðuna því að tryggja að stefnunni sé beitt á samræmdan og samfelldan hátt innan samstæðunnar.

5) Við beitingu stefnunnar ætti að líta á veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu, þ.m.t. þá sem eru að öllu leyti eða sameiginlega í eigu aðila á fjármálamarkaði innan sama stofnanaverndarkerfis, sem þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Áhættan sem stafar af veitendum upplýsinga- og fjarskiptatækniþjónustu innan samstæðu getur verið mismunandi en kröfurnar sem gilda um þá eru þær sömu skv. reglugerð (ESB) 2022/2554. Að sama skapi ætti stefnan að gilda um undirverktaka sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða veigamikla hluta hennar til þriðju aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, ef keðja af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu er til staðar.

6) Endanleg ábyrgð stjórnar og/eða framkvæmdastjórnar aðila á fjármálamarkaði á stýringu upplýsinga- og fjarskiptatækniáhættu er grundvallarmeginregla sem gildir einnig um notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu. Þessi ábyrgð ætti að endurspeglast í áframhaldandi þátttöku stjórnar og/eða framkvæmdastjórnar í eftirliti með og vöktun á áhættustýringu í upplýsinga- og fjarskiptatækni, þ.m.t. við samþykkt og endurskoðun stefnunnar a.m.k. einu sinni á ári.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

7) Til að tryggja viðeigandi skýrslugjöf til stjórnar og/eða framkvæmdastjórnar ætti stefnan að setja skýrt fram og skilgreina innri skyldur vegna samþykkis, stjórnunar, eftirlits með og skjalfestingar samningsbundins fyrirkomulags um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu („samningsbundið fyrirkomulag“), þ.m.t. upplýsinga- og fjarskiptatækniþjónusta sem veitt er samkvæmt samningunum sem um getur a-lið 1. mgr. 28. gr. reglugerðar (ESB) 2022/2554.

8) Til að taka tillit til allrar hugsanlegrar áhættu sem getur skapast þegar samið er um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi ætti uppbygging stefnunnar að fylgja öllum skrefum í hverjum meginfasa lífsferils samningsbundins fyrirkomulags við veitendur sem eru þriðju aðilar.

9) Til að draga úr áhættu sem greinst hefur ætti stefnan að kveða á um skipulagningu samningsbundins fyrirkomulags, þ.m.t. áhættumat, áreiðanleikakönnun og samþykkisferli fyrir nýjar eða veigamiklar breytingar á samningsbundna fyrirkomulaginu. Til að stýra áhættunni sem getur skapast áður en gert er samningsbundið fyrirkomulag við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu ætti stefnan að tiltaka viðeigandi og hlutfallslegt ferli til að velja og leggja mat á hæfi væntanlegra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og krefjast þess að aðili á fjármálamarkaði taki tillit til lista, sem ekki er tæmandi, yfir þætti sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu ættu að hafa til staðar. Listinn ætti að innihalda þætti sem tengjast orðspori þjónustuveitenda, fjármagni, mannauði og tækniúrræðum þeirra, upplýsingaöryggi, stjórnskipulagi, þ.m.t. áhættustýringu, og innra eftirliti þeirra.

10) Til að tryggja trausta áhættustýringu við veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu ætti stefnan að innihalda upplýsingar um framkvæmd, vöktun og stjórnun samningsbundins fyrirkomulags, þ.m.t. á samstæðu- og undirsamstæðugrunni, eftir atvikum. Þetta felur í sér kröfur um samningsákvæði um gagnkvæmar skuldbindingar aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem ætti að setja fram skriflega. Til að tryggja skilvirkt eftirlit og stuðla að viðnámi ef breytingar verða á viðskiptalíkani eða viðskiptaumhverfi ætti stefnan að tryggja réttindi aðilans á fjármálamarkaði eða tilnefndra þriðju aðila og lögbærra yfirvalda til að skoða og hafa aðgang að upplýsingum, auk þess að skýra frekar útgönguáætlanir og uppsagnarferli.

11) Að því marki sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu vinna með persónuupplýsingar er þessi stefna og hvers kyns samningsbundið fyrirkomulag með fyrirvara um, og ætti að vera viðbót við, skuldbindingar samkvæmt reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 ([2]), eins og að hafa skriflegan samning til staðar sem lýsir vinnslu persónuupplýsinga, kröfu um að tryggja öryggi við vinnslu persónuupplýsinga og ákvörðun um alla aðra þætti sem krafist er samkvæmt þeirri reglugerð.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

12) Sameiginleg nefnd evrópsku eftirlitsstofnananna sem um getur í 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([3]), 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([4]) og 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([5]) hefur haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint hugsanlegan kostnað og ávinning af fyrirhuguðum stöðlum og óskað eftir ráðgjöf hagsmunahópsins um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010, hagsmunahópsins í vátryggingum og hagsmunahópsins um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1094/2010 og hagsmunahópsins á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1095/2010.

13) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([6]) og skilaði hún áliti 24. janúar 2024.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Heildaráhættusnið og flækjustig

Stefnan um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu („stefnan“) skal taka mið af stærð og heildaráhættusniði aðila á fjármálamarkaði, og eðli, umfangi og þáttum sem auka eða draga úr flækjustigi þjónustu hans, starfsemi og rekstri, þ.m.t. þáttum sem tengjast:

a) tegund upplýsinga- og fjarskiptatækniþjónustu sem fellur undir samningsbundið fyrirkomulag um notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu („samningsbundið fyrirkomulag“) milli aðila á fjármálamarkaði og þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

b) staðsetningu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða staðsetningu móðurfélagsins,

c) hvort upplýsinga- og fjarskiptatækniþjónustan sem styður nauðsynlega eða mikilvæga starfsemi sé veitt af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í aðildarríki eða í þriðja landi, einnig að teknu tilliti til staðarins sem upplýsinga- og fjarskiptatækniþjónustan er veitt frá og staðarins þar sem gögnin eru unnin og geymd,

d) eðli gagnanna sem er deilt með þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

e) hvort þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sé hluti af sömu samstæðu og sá aðili á fjármálamarkaði sem þjónustan er veitt,

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru með starfsleyfi, eru skráðir eða falla undir eftirlit eða tilsjón lögbærs yfirvalds aðildarríkis eða lúta eftirlitsramma skv. II. þætti V. kafla reglugerðar (ESB) 2022/2554, og notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem ofangreint gildir ekki um,

g) notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru með starfsleyfi, eru skráðir eða falla undir eftirlit eða tilsjón eftirlitsstofnunar í þriðja landi, og notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem ofangreint gildir ekki um,

h) hvort veiting upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi einskorðist við stakan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða lítinn fjölda slíkra þjónustuveitenda,

i) flytjanleika upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi til annars þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. vegna tæknisértækra eiginleika,

j) hugsanlegum áhrifum truflana á veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi á samfellu í starfsemi aðila á fjármálamarkaði og framboð á þjónustu hans.

2. gr.

Beiting á samstæðugrunni

Ef þessi reglugerð gildir á undirsamstæðu- eða samstæðugrunni skal móðurfyrirtækið sem ber ábyrgð á því að gera samstæðu- eða undirsamstæðureikningsskil fyrir samstæðuna tryggja að stefnunni sé framfylgt á samræmdan hátt hjá öllum aðilum á fjármálamarkaði sem eru hluti samstæðunnar og að hún sé fullnægjandi til að unnt sé að beita reglugerðinni á öllum stigum samstæðunnar á skilvirkan hátt.

3. gr.

Fyrirkomulag stjórnarhátta

1. Stjórn og/eða framkvæmdastjórn skal fara yfir stefnuna a.m.k. einu sinni á ári og uppfæra hana eftir því sem nauðsyn krefur. Breytingar sem gerðar eru á stefnunni skulu innleiddar tímanlega og eins fljótt og auðið er innan viðkomandi samningsbundins fyrirkomulags. Aðilinn á fjármálamarkaði skal skjalfesta áætlaða tímalínu fyrir innleiðinguna.

2. Stefnan skal setja fram eða vísa til aðferðafræði til að ákvarða hvaða upplýsinga- og fjarskiptatækniþjónusta styður nauðsynlega eða mikilvæga starfsemi. Í stefnunni skal einnig koma fram hvenær þetta mat skuli gert og endurskoðað.

3. Stefnan skal fela í sér skýra úthlutun á innri ábyrgð vegna samþykkis, stjórnunar, eftirlits og skjalfestingar á viðkomandi samningsbundnu fyrirkomulagi og tryggja að aðilinn á fjármálamarkaði viðhaldi viðeigandi færni, reynslu og þekkingu til að hafa skilvirkt eftirlit með viðkomandi samningsbundnu fyrirkomulagi, þ.m.t. upplýsinga- og fjarskiptatækniþjónustu sem er veitt samkvæmt þessu fyrirkomulagi.

4. Með fyrirvara um endanlega ábyrgð aðilans á fjármálamarkaði á því að hafa skilvirkt eftirlit með viðeigandi samningsbundnu fyrirkomulagi skal stefnan innihalda kröfur um að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sé metinn hafa nægjanleg tilföng til að tryggja að aðili á fjármálamarkaði fari að öllum kröfum samkvæmt lögum og reglum varðandi veitta upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

5. Í stefnunni skal skilgreina með skýrum hætti hvaða staða eða háttsettur stjórnandi ber ábyrgð á vöktun á viðkomandi samningsbundnu fyrirkomulagi. Í stefnunni skal einnig tilgreint hvernig samstarfi stöðunnar eða háttsetta stjórnandans við eftirlitseiningarnar skal háttað, nema viðkomandi sé hluti þeirra, og koma á boðleiðum til stjórnar og/eða framkvæmdastjórnar, þ.m.t. eðli þeirra upplýsinga sem á að tilkynna og skjölin sem leggja ber fram. Í henni skal einnig setja fram tíðni slíkrar skýrslugjafar.

6. Stefnan skal tryggja að samningsbundið fyrirkomulag samræmist eftirfarandi:

a) áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 6. gr. reglugerðar (ESB) 2022/2554,

b) stefnu um upplýsingaöryggi sem um getur í 4. mgr. 9. gr. reglugerðar (ESB) 2022/2554,

c) stefnu um rekstrarsamfellu upplýsinga- og fjarskiptatækni sem um getur í 11. gr. reglugerðar (ESB) 2022/2554,

d) kröfum um tilkynningar um atvik sem settar eru fram í 19. gr. reglugerðar (ESB) 2022/2554.

7. Stefnan skal fela í sér kröfur um að upplýsinga- og fjarskiptatækniþjónusta sem styður nauðsynlega eða mikilvæga starfsemi sem veitt er af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu falli undir sjálfstæða endurskoðun og sé hluti af endurskoðunaráætluninni.

8. Í stefnunni skal skýrt tekið fram að samningsbundna fyrirkomulagið:

a) leysi aðilann á fjármálamarkaði og stjórn og/eða framkvæmdastjórn hans ekki undan lögbundnum skuldbindingum sínum og skyldum gagnvart viðskiptavinum,

b) megi ekki koma í veg fyrir skilvirkt opinbert eftirlit með aðila á fjármálamarkaði, né stangast á við neinar takmarkanir á eftirliti með þjónustu og starfsemi,

c) verði að innihalda kröfur um að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafi samstarf við lögbær yfirvöld,

d) verði að innihalda kröfur um að aðilinn á fjármálamarkaði, endurskoðendur hans og lögbær yfirvöld hafi virkan aðgang að gögnum og athafnasvæði í tengslum við notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

4. gr.

Meginfasar í lífsferli samningsbundins fyrirkomulags að því er varðar samþykkt og notkun

Stefnan skal tilgreina kröfur, þ.m.t. reglur, ábyrgð og ferla, fyrir sérhvern meginfasa í lífsferli samningsbundins fyrirkomulags, sem ná a.m.k. yfir eftirfarandi:

a) ábyrgð stjórnar og/eða framkvæmdastjórnar, þ.m.t. þátttaka hennar, eins og við á, í ákvarðanatökuferli um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,

b) skipulagningu samningsbundins fyrirkomulags, þ.m.t. áhættumat, áreiðanleikakönnun eins og sett er fram í 5. og 6. gr. og samþykkisferli varðandi nýjar eða umtalsverðar breytingar á samningsbundnu fyrirkomulagi, eins og sett er fram í 4. mgr. 8. gr.,

c) aðkomu rekstrareininga, innra eftirlits og annarra viðeigandi eininga að því er varðar samningsbundið fyrirkomulag,

d) innleiðingu, vöktun og stjórnun samningsbundins fyrirkomulags, eins og um getur í 7., 8. og 9. gr., þ.m.t. á samstæðu- og undirsamstæðugrunni, eftir atvikum,

e) skjalfestingu og skráahald, að teknu tilliti til krafna að því er varðar skráningu upplýsinga sem mælt er fyrir um í 3. mgr. 28. gr. reglugerðar (ESB) 2022/2554,

f) útgönguáætlanir og uppsagnarferli, eins og sett er fram í 10. gr.

5. gr.

Fyrirframáhættumat

1. Stefnan skal innihalda kröfur um að viðskiptaþarfir aðila á fjármálamarkaði séu skilgreindar áður en samningsbundið fyrirkomulag er gert.

2. Stefnan skal innihalda kröfur um að gert sé áhættumat á stigi aðila á fjármálamarkaði og, eftir atvikum, á samstæðu- og undirsamstæðugrunni áður en samningsbundið fyrirkomulag er gert.

Áhættumatið skal taka tillit til allra viðeigandi krafna sem mælt er fyrir um í reglugerð (ESB) 2022/2554 og gildandi geirasértækri löggjöf Sambandsins. Með því skal einkum meta þau áhrif sem þjónusta þriðju aðila, sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi, hefur á aðila á fjármálamarkaði og alla þá áhættu sem skapast af veitingu þriðju aðila á þeirri upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi, þ.m.t. eftirfarandi:

a) rekstraráhættu,

b) lagalegri áhættu,

c) upplýsinga- og fjarskiptatækniáhættu,

d) orðsporsáhættu,

e) áhættu sem tengist vernd trúnaðar- eða persónuupplýsinga,

f) áhættu sem tengist aðgengi að gögnum,

g) áhættu sem tengist þeirri staðsetningu þar sem gögn eru unnin og geymd,

h) áhættu sem tengist staðsetningu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

i) upplýsinga- og fjarskiptatækniáhættu á einingastigi.

6. gr.

Áreiðanleikakönnun

1. Stefnan skal setja fram viðeigandi og hlutfallslegt ferli fyrir val og mat á líklegum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu að teknu tilliti til þess hvort þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sé veitandi upplýsinga- og fjarskiptatækniþjónustu innan samstæðu og gera kröfu um að áður en aðili á fjármálamarkaði gerir samningsbundið fyrirkomulag, meti hann hvort þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu:

a) hafi viðskiptalegt orðspor, fullnægjandi getu, sérfræðiþekkingu og fullnægjandi fjármagn, mannauð og tækniúrræði, upplýsingaöryggisstaðla, viðeigandi stjórnskipulag, áhættustýringu og innra eftirlit og, ef við á, áskilin starfsleyfi eða skráningar til að veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi á áreiðanlegan og faglegan hátt,

b) hafi getu til að vakta viðeigandi tækniþróun og bera kennsl á leiðandi aðferðir í upplýsinga- og fjarskiptatækniöryggi og innleiða þær þar sem við á, til að hafa skilvirkan og traustan ramma fyrir stafrænan rekstrarlegan viðnámsþrótt,

c) noti eða hyggist nota undirverktaka í upplýsinga- og fjarskiptatækni til að sinna upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða umtalsverðan hluta hennar,

d) sé staðsettur eða vinni eða geymi gögn í þriðja landi og, ef svo er, hvort sú framkvæmd hafi áhrif á umfang rekstrar- eða orðsporsáhættu eða hættuna á því að verða fyrir áhrifum af takmarkandi ráðstöfunum, þ.m.t. viðskiptabönnum og refsiaðgerðum, sem kunna að hafa áhrif á getu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að veita upplýsinga- og fjarskiptatækniþjónustuna eða aðila á fjármálamarkaði til að fá þá upplýsinga- og fjarskiptatækniþjónustu,

e) samþykki samningsbundið fyrirkomulag sem tryggir að aðilinn á fjármálamarkaði sjálfur, tilnefndir þriðju aðilar og lögbær yfirvöld geti framkvæmt úttektir, þ.m.t. vettvangsathuganir, á skilvirkan hátt hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. á staðnum,

f) komi fram á siðferðislega og samfélagslega ábyrgan hátt, virði mannréttindi og réttindi barna, þ.m.t. bann við barnavinnu, virði gildandi meginreglur um umhverfisvernd og tryggi viðunandi vinnuskilyrði.

2. Stefnan skal tilgreina áskilið fullvissustig varðandi skilvirkni áhættustýringarramma þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu fyrir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. Stefnan skal innihalda kröfur um að áreiðanleikaferlið feli í sér mat á því hvort ráðstafanir séu til staðar til áhættumildunar og rekstrarsamfellu og hvernig tryggt sé að þær virki hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

3. Stefnan skal ákvarða áreiðanleikaferlið fyrir val og mat á þriðju aðilum sem til greina kemur að veiti upplýsinga- og fjarskiptatækniþjónustu og tilgreina hverjum eftirfarandi þátta eigi að beita fyrir tilskilið fullvissustig á frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu:

a) úttekt eða sjálfstætt mat sem aðili á fjármálamarkaði gerir sjálfur eða er gert fyrir hans hönd,

b) notkun óháðra endurskoðunarskýrslna sem unnar eru að beiðni þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

c) notkun endurskoðunarskýrslna sem gerðar eru af deild innri endurskoðunar hjá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

d) notkun viðeigandi vottana þriðja aðila,

e) notkun annarra viðeigandi upplýsinga sem eru aðgengilegar aðilanum á fjármálamarkaði eða annarra upplýsinga frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

4. Aðilar á fjármálamarkaði skulu tryggja viðeigandi fullvissustig fyrir frammistöðu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, að teknu tilliti til þáttanna sem eru settir fram í a- til e-lið 3. mgr. Nota skal fleiri en einn þátt sem taldir eru upp í þessum liðum, eftir því sem við á.

7. gr.

Hagsmunaárekstrar

1. Stefnan skal tilgreina viðeigandi ráðstafanir til að skilgreina, koma í veg fyrir og stjórna raunverulegum eða mögulegum hagsmunaárekstrum sem stafa af notkun á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, sem gera verður áður en viðkomandi samningsbundið fyrirkomulag er gert og skal kveða á um áframhaldandi vöktun á slíkum hagsmunaárekstrum.

2. Ef veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi skal stefnan tilgreina að ákvarðanir um skilyrði, þ.m.t. fjárhagsleg skilyrði, fyrir upplýsinga- og fjarskiptatækniþjónustunni verði að taka á hlutlægan hátt.

8. gr.

Samningsákvæði

1. Í stefnunni skal tilgreint að viðkomandi samningsbundið fyrirkomulag eigi að vera á skriflegu formi og innihalda öll atriði sem um getur í 2. og 3. mgr. 30. gr. reglugerðar (ESB) 2022/2554. Í stefnunni skulu einnig koma fram atriði varðandi kröfurnar sem um getur í a-lið 1. mgr. 1. gr. reglugerðar (ESB) 2022/2554, sem og annarra viðeigandi laga Sambandsins og landslaga eins og við á.

2. Í stefnunni skal tilgreint að viðkomandi samningsbundið fyrirkomulag verði að fela í sér rétt aðila á fjármálamarkaði til að hafa aðgang að upplýsingum, framkvæma skoðanir og úttektir og gera prófanir á upplýsinga- og fjarskiptatækni. Í því skyni skal þess krafist í stefnunni að aðili á fjármálamarkaði noti eftirfarandi aðferðir, með fyrirvara um endanlega ábyrgð aðila á fjármálamarkaði:

a) eigin innri úttekt eða úttekt tilnefnds þriðja aðila,

b) eftir því sem við á, samsettar úttektir og samsettar prófanir á upplýsinga- og fjarskiptatækni, þ.m.t. ógnamiðuð innbrotsprófun, sem eru skipulagðar í sameiningu með öðrum samningsbundnum aðilum á fjármálamarkaði eða fyrirtækjum sem nota upplýsinga- og fjarskiptatækniþjónustu frá sama þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og sem þessi samningsbundnu aðilar á fjármálamarkaði eða fyrirtæki eða þriðji aðili sem þau hafa tilnefnt framkvæma,

c) eftir því sem við á, vottanir þriðja aðila,

d) eftir því sem við á, innri endurskoðunarskýrslur eða endurskoðunarskýrslur þriðja aðila frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

3. Aðili á fjármálamarkaði skal ekki til lengri tíma reiða sig eingöngu á vottanirnar sem um getur í c-lið 2. mgr. eða endurskoðunarskýrslur sem um getur í d-lið þeirrar málsgreinar. Stefnan skal aðeins heimila notkun aðferðanna sem um getur í c- og d-lið 2. mgr. ef aðili á fjármálamarkaði:

a) telur endurskoðunaráætlun þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu fullnægjandi fyrir viðkomandi samningsbundið fyrirkomulag,

b) tryggir að umfang vottana eða endurskoðunarskýrslna nái yfir kerfin og lykilstýringar sem hann hefur skilgreint og tryggir að farið sé að viðeigandi kröfum samkvæmt reglum,

c) gerir ítarlegt mat á efni vottana eða endurskoðunarskýrslna á áframhaldandi grundvelli og sannprófar að skýrslur eða vottanir séu ekki úreltar,

d) tryggir að fjallað sé um helstu kerfi og stýringar í síðari útgáfum vottunar eða endurskoðunarskýrslu,

e) telur færni vottunar- eða endurskoðunarfyrirtækis vera fullnægjandi,

f) er fullviss um að vottanirnar séu gefnar út og úttektirnar gerðar á grundvelli almennt viðurkenndra viðeigandi fagstaðla og feli í sér prófun á rekstrarskilvirkni þeirra lykilstýringa sem er til staðar,

g) hefur samningsbundinn rétt til að óska, eins oft og sanngjarnt og lögmætt þykir út frá sjónarmiði áhættustýringar, eftir breytingum á umfangi vottunar eða endurskoðunarskýrslna á öðrum viðeigandi kerfum og eftirliti,

h) hefur samningsbundinn rétt til að framkvæma stakar og samsettar úttektir að eigin ákvörðun með tilliti til samningsbundins fyrirkomulags og nýta þau réttindi í samræmi við umsamda tíðni.

4. Stefnan skal tryggja að umtalsverðar breytingar á samningsbundnu fyrirkomulagi séu gerðar á formlegan hátt í skriflegu skjali sem er dagsett og undirritað af öllum aðilum og skal tilgreina endurnýjunarferli fyrir samningsbundið fyrirkomulag.

9. gr.

Vöktun á samningsbundnu fyrirkomulagi

1. Í stefnunni skal krefjast að samningsbundið fyrirkomulag tilgreini þær ráðstafanir og helstu vísa sem á að vakta á áframhaldandi grundvelli, frammistöðu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. ráðstafanir til að vakta hlítni við kröfur varðandi trúnað, tiltækileika, heilleika og ósvikni gagna og upplýsinga og hlítni þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu við viðeigandi stefnur og verklagsreglur aðila á fjármálamarkaði. Í stefnunni skulu einnig tilgreindar ráðstafanir sem gilda þegar þjónustusamningar eru ekki uppfylltir, þ.m.t. samningsbundin viðurlög, eftir því sem við á.

2. Stefnan skal tilgreina hvernig aðili á fjármálamarkaði skal meta hvort þeir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru notaðar fyrir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi uppfylli viðeigandi frammistöðu- og gæðastaðla í samræmi við samningsbundið fyrirkomulag og eigin stefnur aðila á fjármálamarkaði. Með stefnunni skal einkum tryggja eftirfarandi:

a) að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skili viðeigandi skýrslum um aðgerðir sínar og þjónustu til aðilans á fjármálamarkaði, þ.m.t. reglubundnum skýrslum, atvikaskýrslum, þjónustuskýrslum, skýrslum um öryggi í upplýsinga- og fjarskiptatækni og skýrslum um rekstrarsamfellu og prófun,

b) að frammistaða þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sé metin með lykilárangursvísum, lykilstýringarvísum, úttektum, sjálfvottunum og óháðum úttektum í samræmi við áhættustýringarramma aðila á fjármálamarkaði,

c) að aðili á fjármálamarkaði fái aðrar viðeigandi upplýsingar frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,

d) að aðila á fjármálamarkaði sé tilkynnt, eftir því sem við á, um atvik sem tengjast upplýsinga- og fjarskiptatækni og greiðslutengd rekstrar- eða öryggisatvik,

e) að framkvæmd sé óháð úttekt og endurskoðun til að sannreyna að farið sé að öllum kröfum samkvæmt lögum og reglum og stefnum.

3. Í stefnunni skal tilgreint að skjalfesta skuli matið sem um getur í 2. mgr. og að nota eigi niðurstöður þess til að uppfæra áhættumat aðila á fjármálamarkaði sem um getur í 6. gr.

4. Með stefnunni skal koma á fót viðeigandi ráðstöfunum sem aðili á fjármálamarkaði þarf að grípa til ef hann uppgötvar annmarka á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. atvik sem tengjast upplýsinga- og fjarskiptatækni og greiðslutengd rekstrar- eða öryggisatvik, í tengslum við veitingu upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða í samræmi við samningsbundið fyrirkomulag eða lagakröfur. Jafnframt skal tilgreina hvernig vakta eigi framkvæmd slíkra ráðstafana til að tryggja að þeim sé framfylgt með skilvirkum hætti innan tiltekins tímaramma, að teknu tilliti til þess hversu alvarlegir annmarkarnir eru.

10. gr.

Útganga úr og uppsögn á samningsbundnu fyrirkomulagi

Stefnan skal fela í sér kröfur um skjalfesta útgönguáætlun fyrir sérhvert samningsbundið fyrirkomulag og um reglubundna endurskoðun og prófun á skjalfestu útgönguáætluninni. Þegar útgönguáætlun er komið á fót skal taka skal tillit til eftirfarandi:

a) ófyrirsjáanlegra og viðvarandi truflana á þjónustu,

b) óviðeigandi eða misheppnaðrar veitingar á þjónustu,

c) óvæntrar uppsagnar á samningsbundnu fyrirkomulagi,

Útgönguáætlunin skal vera raunhæf, framkvæmanleg, byggjast á trúverðugum sviðsmyndum og raunhæfum forsendum og vera með áætlaðan framkvæmdatíma sem er í samræmi við útgöngu- og uppsagnarskilmálana sem komið er á með samningsbundna fyrirkomulaginu.

11. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í Stjórnartíðindum Evrópusambandsins.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 13. mars 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

Fylgiskjal 3.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2024/1774

frá 13. mars 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreind eru nánar búnaður, aðferðir, ferlar og stefnur til stýringar á upplýsinga- og fjarskiptatækniáhættu og einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum fjórðu undirgrein 15. gr. og fjórðu undirgrein 3. mgr. 16. gr.,

og að teknu tilliti til eftirfarandi:

1) Reglugerð (ESB) 2022/2554 nær yfir margskonar aðila á fjármálamarkaði sem eru mismunandi að því er varðar stærð, uppbyggingu, innra skipulag og eðli og flækjustig starfsemi þeirra, og hafa þannig hærra eða minna flækjustig eða áhættu. Til að tryggja tekið sé nægilegt tillit til þessarar fjölbreytni ættu allar kröfur varðandi stefnur, verklagsreglur, samskiptareglur og búnað fyrir öryggi í upplýsinga- og fjarskiptatækni, og að því er varðar einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, að vera í samræmi við stærð, uppbyggingu, innra skipulag, eðli og flækjustig þessara aðila á fjármálamarkaði og samsvarandi áhættu.

2) Af sömu ástæðu ættu aðilar á fjármálamarkaði sem falla undir reglugerð (ESB) 2022/2554 að hafa tiltekinn sveigjanleika varðandi hvernig þeir fullnægja kröfum að því er varðar stefnur, verklagsreglur, samskiptareglur og búnað fyrir öryggi í upplýsinga- og fjarskiptatækni og að því er varðar einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni. Þess vegna ættu aðilar á fjármálamarkaði að geta nýtt öll skjöl sem þeir eru þegar með til að hlíta hvers kyns kröfum um skráningu sem leiða af þessum kröfum. Af þessu leiðir að aðeins ætti að krefjast mótunar, skjalfestingar og innleiðingar á sérstökum öryggisstefnum um upplýsinga- og fjarskiptatækni fyrir tiltekna grundvallarþætti, sem taka m.a. tillit til leiðandi starfsvenja og staðla innan greinarinnar. Til að ná til sérstakra tæknilegra framkvæmdarþátta er enn fremur nauðsynlegt að móta, skjalfesta og innleiða verklagsreglur um öryggi upplýsinga- og fjarskiptatækni til að ná til sérstakra tæknilegra útfærsluþátta, þ.m.t. getu- og frammistöðustjórnunar, veikleika- og bótastjórnunar, gagna- og kerfisöryggis og aðgerðaskráningar.

3) Til að tryggja rétta innleiðingu til lengri tíma litið á stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni sem um getur í I. kafla II. bálks þessarar reglugerðar er mikilvægt að aðilar á fjármálamarkaði úthluti og viðhaldi rétt öllum hlutverkum og ábyrgð varðandi öryggi í upplýsinga- og fjarskiptatækni og að þeir mæli fyrir um afleiðingar þess að ekki sé farið að öryggisstefnum eða -verklagsreglum um upplýsinga- og fjarskiptatækni.

4) Til að takmarka hættuna á hagsmunaárekstrum ættu aðilar á fjármálamarkaði að tryggja aðgreiningu starfa við úthlutun á hlutverkum og ábyrgð í upplýsinga- og fjarskiptatækni.

5) Til að tryggja sveigjanleika og einfalda eftirlitsramma aðila á fjármálamarkaði ætti ekki að krefjast þess að aðilar á fjármálamarkaði setji sértæk ákvæði um afleiðingar þess að ekki sé farið að stefnum, verklagsreglum og samskiptareglum fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í I. kafla II. bálks þessarar reglugerðar, ef slík ákvæði eru þegar til staðar í annarri stefnu eða verklagsreglu.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

6) Í síbreytilegu umhverfi þar sem upplýsinga- og fjarskiptatækniáhætta er í stöðugri þróun er mikilvægt að aðilar á fjármálamarkaði móti sína eigin öryggisstefnu fyrir upplýsinga- og fjarskiptatækni á grundvelli leiðandi starfsvenja, og eftir atvikum, staðla eins og skilgreint er í 1. lið 2. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1025/2012 [2].Þetta ætti að gera aðilum á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, kleift að halda sér upplýstum og undirbúnum í umhverfi sem er breytingum undirorpið.

7) Til að tryggja stafrænan rekstrarlegan viðnámsþrótt sinn ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, að móta og innleiða eignastýringarstefnu í upplýsinga- og fjarskiptatækni, verklagsreglur um getu- og árangursstjórnun og stefnur og verklagsreglur fyrir upplýsinga- og fjarskiptatæknirekstur. Þessar stefnur og verklagsreglur eru nauðsynlegar til að tryggja vöktun á stöðu upplýsinga- og fjarskiptatæknieigna allt endingarskeið þeirra, þannig að eignirnar séu notaðar og viðhaldið á skilvirkan hátt (eignastýring í upplýsinga- og fjarskiptatækni). Stefnurnar og verklagsreglurnar ættu einnig að tryggja bestun á starfsemi upplýsinga- og fjarskiptatæknikerfa og að afköst upplýsinga- og fjarskiptatæknikerfa og -getu uppfylli sett markmið viðskipta- og upplýsingaöryggis (getu- og árangursstjórnun). Að lokum ættu þessar stefnur og verklagsreglur að tryggja skilvirka og snurðulausa daglega stjórnun og rekstur upplýsinga- og fjarskiptatæknikerfa (upplýsinga- og fjarskiptatæknirekstur) og lágmarka þannig hættu á tapi á leynd, réttleika og tiltækileika gagna. Þessar stefnur og verklagsreglur eru því nauðsynlegar til að tryggja öryggi netkerfa, til að gera fullnægjandi verndarráðstafanir gegn innbrotum og gagnamisnotkun og varðveita tiltækileika, ósvikni, réttleika og leynd gagna.

8) Til að tryggja viðeigandi stýringu áhættu í fornkerfum í upplýsinga- og fjarskiptatækni ættu aðilar á fjármálamarkaði að skrá og vakta lokadagsetningar stuðningsþjónustu upplýsinga- og fjarskiptatækni sem þriðju aðilar veita. Vegna hugsanlegra áhrifa sem tap á leynd, réttleika og tiltækileika gagna getur haft ættu aðilar á fjármálamarkaði að einbeita sér að þeim upplýsinga- og fjarskiptatæknieignum eða -kerfum sem eru nauðsynleg fyrir starfsemi fyrirtækja við skráningu og vöktun á þessum lokadagsetningum.

9) Dulritunarstýringar geta tryggt tiltækileika, ósvikni, réttleika og leynd gagna. Aðilar á fjármálamarkaði sem um getur í II. bálki þessarar reglugerðar ættu því að tilgreina og innleiða slíkar stýringar á grundvelli áhættumiðaðrar nálgunar. Í því skyni ættu aðilar á fjármálamarkaði að dulrita viðkomandi gögn sem eru í dvala, í flutningi eða, þar sem nauðsyn krefur, í notkun, á grundvelli niðurstaðna tveggja þátta ferlis, þ.e.a.s. gagnaflokkunar og yfirgripsmikils upplýsinga- og fjarskiptatækniáhættumats. Í ljósi þess flækjustigs þess að dulrita gögn í notkun ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, aðeins að dulrita gögn ef það er viðeigandi vegna niðurstaðna úr upplýsinga- og fjarskiptatækniáhættumati. Aðilar á fjármálamarkaði sem um getur í II. bálki þessarar reglugerðar ættu hins vegar að geta, ef dulritun á gögnum í notkun er ekki gerleg eða er of flókin, verndað leynd, réttleika og tiltækileika viðkomandi gagna með öðrum öryggisráðstöfunum í upplýsinga- og fjarskiptatækni. Með hliðsjón af hraðri tækniþróun á sviði dulritunar ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að fylgjast vel með viðeigandi þróun í dulmálsgreiningu og taka tillit til leiðandi starfsvenja og staðla. Aðilar á fjármálamarkaði sem um getur í II. bálki þessarar reglugerðar ættu því að fylgja sveigjanlegri aðferð, sem byggist á áhættumildun og vöktun, til að takast á við síbreytilegt umhverfi dulritunarógna, þ.m.t. ógnir vegna framfara í skammtafræði.

10) Rekstraröryggi og rekstrarstefnur, verklagsreglur, samskiptareglur og búnaður upplýsinga- og fjarskiptatækni eru nauðsynlegir þættir til að tryggja leynd, réttleika og tiltækileika gagna. Eitt lykilatriði er alger aðgreining á raunumhverfi í upplýsinga- og fjarskiptatækni frá umhverfi þar sem upplýsinga- og fjarskiptatæknikerfi eru þróuð og prófuð eða frá öðru umhverfi sem ekki er raunumhverfi. Aðgreiningin ætti að þjóna sem mikilvæg öryggisráðstöfun í upplýsinga- og fjarskiptatækni gegn óviljandi og óheimilum aðgangi að, breytingum á og eyðingu gagna í raunumhverfi, sem gæti valdið meiriháttar truflunum á viðskiptaþjónustu aðila á fjármálamarkaði sem um getur í II. bálki þessarar reglugerðar. Miðað við núverandi þróunaraðferðir í upplýsinga- og fjarskiptatækni ætti aðilum á fjármálamarkaði, í undantekningartilvikum þó, að vera heimilt að framkvæma prófanir í raunumhverfi, að því tilskildu að þeir geti réttlætt slíkar prófanir og fái nauðsynlegt samþykki fyrir þeim.

---

[2] Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1025/2012 frá 25. október 2012 um evrópska stöðlun og breytingu á tilskipunum ráðsins 89/686/EBE og 93/15/EBE og tilskipunum Evrópuþingsins og ráðsins 94/9/EB, 94/25/EB, 95/16/EB, 97/23/EB, 98/34/EB, 2004/22/EB, 2007/23/EB, 2009/23/EB og 2009/105/EB og niðurfellingu á ákvörðun ráðsins 87/95/EBE og ákvörðun Evrópuþingsins og ráðsins nr. 1673/2006/EB (Stjtíð. ESB L 316, 14.11.2012, bls. 12, ELI: http://data.europa.eu/eli/reg/2012/1025/oj).

11) Hröð þróun umhverfis upplýsinga- og fjarskiptatækni, veikleikar í upplýsinga- og fjarskiptatækni og netógnir krefjast fyrirbyggjandi og heildstæðrar nálgunar við að leiða í ljós, meta og taka á veikleikum í upplýsinga- og fjarskiptatækni. Án slíkrar nálgunar geta aðilar á fjármálamarkaði, viðskiptavinir þeirra, notendur eða mótaðilar verið alvarlega útsettir fyrir áhættu, sem myndi stofna stafrænum rekstrarlegum viðnámsþrótti þeirra, öryggi netkerfa og tiltækileika, ósvikni, réttleika og leynd gagna í hættu, sem öryggisstefnur og -verklagsreglur um upplýsinga- og fjarskiptatækni ættu að vernda. Því ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að greina og bæta úr veikleikum í upplýsinga- og fjarskiptatækniumhverfi sínu og bæði aðilar á fjármálamarkaði og þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu ættu að beita samfelldum, gagnsæjum og ábyrgum veikleikastjórnunarramma. Af sömu ástæðu ættu aðilar á fjármálamarkaði að vakta veikleika í upplýsinga- og fjarskiptatækni með því að nota áreiðanleg tilföng og sjálfvirkan búnað, til að sannreyna að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu tryggi að tafarlaust verði brugðist við veikleikum í veittri upplýsinga- og fjarskiptatækniþjónustu.

12) Bótastjórnun ætti að vera mikilvægur hluti af þeim öryggisstefnum og -verklagsreglum um upplýsinga- og fjarskiptatækni sem, með prófun og útfærslu í stýrðu umhverfi, eiga að leysa greinda veikleika og koma í veg fyrir truflanir við uppsetningu á bótum.

13) Til að tryggja tímanleg og gagnsæ boðskipti um hugsanlegar öryggisógnir sem gætu haft áhrif á aðila á fjármálamarkaði og hagsmunaaðila hans ættu aðilar á fjármálamarkaði að koma á fót verklagsreglum um ábyrga upplýsingagjöf um upplýsinga- og fjarskiptatækniveikleika til viðskiptavina, mótaðila og almennings. Þegar þessum verklagsreglum er komið á fót ættu aðilar á fjármálamarkaði að huga að þáttum, þ.m.t. hversu alvarlegir veikleikarnir eru, hugsanlegum áhrifum slíkra veikleika á hagsmunaaðila og hvort úrbóta- eða mótvægisráðstafanir séu tilbúnar til notkunar.

14) Til að gera kleift að veita aðgangsréttindi notenda ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að innleiða öflugar ráðstafanir til að tryggja einkvæma auðkenningu einstaklinga og kerfa sem munu fá aðgang að gögnum aðila á fjármálamarkaði. Sé það ekki gert verða aðilar á fjármálamarkaði útsettir fyrir hugsanlegum óheimilum aðgangi, gagnabrotum og svikastarfsemi, sem stefnir leynd, réttleika og tiltækileika viðkvæmra fjármálagagna í hættu. Þó svo að leyfa ætti notkun á almennum eða sameiginlegum reikningum í sérstökum undantekningartilvikum sem aðilar á fjármálamarkaði tilgreina ættu aðilar á fjármálamarkaði að tryggja að ábyrgð á aðgerðum sem framkvæmdar eru í gegnum þessa aðgangsreikninga sé viðhaldið. Án þeirrar verndarráðstöfunar munu hugsanlegir notendur í illum tilgangi geta hindrað ráðstafanir til rannsókna og úrbóta, sem gerir aðila á fjármálamarkaði viðkvæma fyrir ógreindum aðgerðum af illum ásetningi eða viðurlögum vegna vanefnda.

15) Til að takast á við hraðar framfarir í upplýsinga- og fjarskiptatækniumhverfi ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að koma á traustum stefnum og verklagsreglum um verkefnastjórnun í upplýsinga- og fjarskiptatækni til að viðhalda tiltækileika, ósvikni, réttleika og leynd gagna. Þessar stefnur og verklagsreglur um verkefnastjórnun í upplýsinga- og fjarskiptatækni ættu að tilgreina þá þætti sem eru nauðsynlegir fyrir farsæla stjórnun upplýsinga- og fjarskiptatækniverkefna, þ.m.t. breytingar, öflun, viðhald og þróun á upplýsinga- og fjarskiptatæknikerfum aðila á fjármálamarkaði, án tillits til þeirra verkefnastjórnunaraðferða í upplýsinga- og fjarskiptatækni sem hann hefur valið. Í tengslum við þessar stefnur og verklagsreglur ættu aðilar á fjármálamarkaði að tileinka sér prófunarvenjur og -aðferðir sem henta þörfum þeirra, en fylgja jafnframt áhættumiðaðri nálgun og tryggja að viðhaldið sé öruggu, áreiðanlegu og viðnámsþolnu upplýsinga- og fjarskiptatækniumhverfi. Til að tryggja örugga framkvæmd upplýsinga- og fjarskiptatækniverkefnis ættu aðilar á fjármálamarkaði að tryggja að starfsfólk af tilteknum viðskiptasviðum eða í tilteknum hlutverkum sem upplýsinga- og fjarskiptatækniverkefnið hefur áhrif á geti veitt nauðsynlegar upplýsingar og sérfræðiþekkingu. Til að tryggja skilvirkt eftirlit ætti að skila skýrslum um upplýsinga- og fjarskiptatækniverkefni, einkum um verkefni sem hafa áhrif á nauðsynlega eða mikilvæga starfsemi og um tengda áhættu, til stjórnar og/eða framkvæmdastjórnar. Aðilar á fjármálamarkaði ættu að sníða tíðni og inntak kerfisbundinnar og viðvarandi endurskoðunar og skýrslugerðar að mikilvægi og stærð viðkomandi upplýsinga- og fjarskiptatækniverkefna.

16) Nauðsynlegt er að tryggja að hugbúnaðarpakkar sem aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, afla sér og þróa séu samþættir við fyrirliggjandi upplýsinga- og fjarskiptatækniumhverfi á skilvirkan og öruggan hátt, í samræmi við sett markmið viðskipta- og upplýsingaöryggis. Aðilar á fjármálamarkaði ættu því að gera ítarlegt mat á slíkum hugbúnaðarpökkum. Í því skyni, og til að greina veikleika og hugsanlega ágalla í öryggismálum bæði í hugbúnaðarpökkum og víðtækari upplýsinga- og fjarskiptatæknikerfum, ættu aðilar á fjármálamarkaði að framkvæma öryggisprófun á upplýsinga- og fjarskiptatækni. Til að meta heilleika hugbúnaðar og tryggja að notkun á hugbúnaði valdi ekki öryggisáhættu í upplýsinga- og fjarskiptatækni, ættu aðilar á fjármálamarkaði einnig að endurskoða frumkóða keypts hugbúnaðar, þ.m.t., þar sem það er gerlegt, einkaleyfisbundins hugbúnaðar sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu veitir, með því að nota bæði kyrrstæðar og virkar prófunaraðferðir.

17) Breytingar, án tillits til umfangs þeirra, fela í sér eðlislæga áhættu og geta haft í för með sér umtalsverða hættu á tapi á leynd, réttleika og tiltækileika gagna, og gætu þannig leitt til meiriháttar rekstrartruflana. Til að vernda aðila á fjármálamarkaði fyrir hugsanlegum veilum og veikleikum upplýsinga- og fjarskiptatækni, sem gætu valdið verulegri áhættu fyrir þá, er strangt sannprófunarferli nauðsynlegt til að staðfesta að allar breytingar uppfylli nauðsynlegar öryggiskröfur í upplýsinga- og fjarskiptatækni. Því ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að hafa til staðar traustar stefnur og verklagsreglur um breytingastjórnun í upplýsinga- og fjarskiptatækni sem nauðsynlegan þátt í öryggisstefnum og -verklagsreglum sínum um upplýsinga- og fjarskiptatækni. Til að viðhalda hlutlægni og skilvirkni breytingastjórnunarferlis í upplýsinga- og fjarskiptatækni, koma í veg fyrir hagsmunaárekstra og tryggja að breytingar í upplýsinga- og fjarskiptatækni séu metnar á hlutlægan hátt er nauðsynlegt að aðgreina starfsemi sem ber ábyrgð á að samþykkja breytingarnar frá þeirri starfsemi sem krefst breytinganna og framkvæmir þær. Til að ná fram skilvirkum umskiptum, stýrðri innleiðingu breytinga á upplýsinga- og fjarskiptatækni og lágmarkstruflunum á rekstri upplýsinga- og fjarskiptatæknikerfa ættu aðilar á fjármálamarkaði að úthluta skýrum hlutverkum og ábyrgð sem tryggja að breytingar á upplýsinga- og fjarskiptatækni séu skipulagðar, nægilega prófaðar og að gæði séu tryggð. Til að tryggja að upplýsinga- og fjarskiptatæknikerfi haldi áfram að virka á skilvirkan hátt og veita öryggisnet fyrir aðila á fjármálamarkaði ættu aðilar á fjármálamarkaði einnig að þróa og innleiða varaaðferðir. Aðilar á fjármálamarkaði ættu að tilgreina þessar varaaðferðir á skýran hátt og úthluta ábyrgðarhlutverkum til að tryggja skjót og skilvirk viðbrögð við misheppnaðar upplýsinga- og fjarskiptatæknibreytingar.

18) Til þess að greina, stjórna og tilkynna atvik sem tengjast upplýsinga- og fjarskiptatækni ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að koma á atvikastefnu sem tengist upplýsinga- og fjarskiptatækni sem nær yfir þætti í stjórnunarferli atvika sem tengjast upplýsinga- og fjarskiptatækni. Í því skyni ættu aðilar á fjármálamarkaði að tilgreina alla viðeigandi tengiliði innan og utan stofnunar sem geta auðveldað rétta samræmingu og framkvæmd ólíkra fasa innan ferlisins. Til að besta greiningu á og viðbrögð við atvikum sem tengjast upplýsinga- og fjarskiptatækni og greina leitni meðal þessara atvika, sem eru mikilvæg upplýsingaveita sem gerir aðilum á fjármálamarkaði kleift að greina og taka á frumorsökum og vandamálum á skilvirkan hátt, ættu aðilar á fjármálamarkaði einkum að gera nákvæma greiningu á þeim atvikum sem tengjast upplýsinga- og fjarskiptatækni sem þeir telja mikilvægust, m.a. vegna reglubundinnar endurtekningar þeirra.

19) Til að tryggja snemmbúna og skilvirka greiningu á óvenjulegum athöfnum ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að safna, vakta og greina mismunandi upplýsingaveitur og úthluta tengdum hlutverkum og ábyrgðarsviðum. Að því er varðar innri upplýsingaveitur eru atburðaskrár einstaklega viðeigandi heimild en aðilar á fjármálamarkaði ættu ekki að reiða sig eingöngu á atburðaskrár. Þess í stað ættu aðilar á fjármálamarkaði að íhuga víðtækari upplýsingar til að hafa með það sem önnur innri starfssvið hafa tilkynnt, þar sem slík starfssvið eru oft dýrmæt uppspretta viðeigandi upplýsinga. Af sömu ástæðu ættu aðilar á fjármálamarkaði að greina og vakta upplýsingar sem er safnað frá utanaðkomandi veitum, þ.m.t. upplýsingum frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu um atvik sem hafa áhrif á kerfi og netkerfi þeirra, og öðrum upplýsingaveitum sem aðilar á fjármálamarkaði telja skipta máli. Að svo miklu leyti sem slíkar upplýsingar samanstanda af persónuupplýsingum gilda lög Sambandsins um persónuvernd og friðhelgi einkalífsins. Persónuupplýsingarnar ættu að takmarkast við það sem er nauðsynlegt til að greina atvikið.

20) Til að auðvelda greiningu á atvikum sem tengjast upplýsinga- og fjarskiptatækni ættu aðilar á fjármálamarkaði að geyma gögn um þessi atvik. Til að tryggja annars vegar að slík gögn séu geymd nægilega lengi og hins vegar til að forðast óhóflega mikla stjórnsýslubyrði ættu aðilar á fjármálamarkaði að ákvarða varðveislutímann með hliðsjón af, m.a., mikilvægi viðkomandi gagna og kröfum um varðveislu sem leiðir af lögum Sambandsins.

21) Til að tryggja að atvik sem tengjast upplýsinga- og fjarskiptatækni séu greind tímanlega ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að líta svo á að þær viðmiðanir sem settar eru til að virkja greiningu á og viðbrögð við atvikum sem tengjast upplýsinga- og fjarskiptatækni séu ekki tæmandi. Þar að auki, þrátt fyrir að aðilar á fjármálamarkaði ættu að taka tillit til allra þessara viðmiðana, ættu aðstæðurnar sem er lýst í viðmiðununum ekki að þurfa að eiga sér stað samtímis og taka ætti tilhlýðilegt tillit til mikilvægis þeirrar upplýsinga- og fjarskiptatækniþjónustu sem verður fyrir áhrifum til virkjunar greiningar- og viðbragðsferla vegna atvika sem tengjast upplýsinga- og fjarskiptatækni.

22) Við mótun á stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni ættu aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, að taka tillit til nauðsynlegra þátta áhættustýringar fyrir upplýsinga- og fjarskiptatækni, þ.m.t. atvikastjórnunar í tengslum við upplýsinga- og fjarskiptatækni og samskiptastefna, breytingastjórnunarferla í upplýsinga- og fjarskiptatækni og áhættu sem tengist þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu.

23) Nauðsynlegt er að ákvarða að þær sviðsmyndir sem aðilar á fjármálamarkaði, sem um getur í II. bálki þessarar reglugerðar, skulu taka tillit til bæði við innleiðingu viðbragðs- og endurreisnaráætlana fyrir upplýsinga- og fjarskiptatækni og við prófun á áætlun um rekstrarsamfellu í upplýsinga- og fjarskiptatækni. Þessar sviðsmyndir ættu að vera upphafspunktur fyrir aðila á fjármálamarkaði til að greina bæði hvort hver sviðsmynd sé bæði viðeigandi og raunhæf og þörfina á að þróa aðrar sviðsmyndir. Aðilar á fjármálamarkaði ættu að leggja áherslu á þær sviðsmyndir þar sem fjárfesting í ráðstöfunum fyrir viðnámsþrótt gætu verið árangursríkari og skilvirkari. Með því að prófa flutning vinnslu frá aðalinnviðum upplýsinga- og fjarskiptatækni yfir á varainnviði, öryggisafrit og varakerfi ættu fjármálastofnanir að meta hvort þeir varainnviðir, öryggisafrit og varakerfi starfi á skilvirkan hátt yfir nægilega langan tíma og tryggja að eðlileg starfsemi aðalinnviða upplýsinga- og fjarskiptatækni sé endurreist í samræmi við markmið um endurreisn.

24) Nauðsynlegt er að mæla fyrir um kröfur um rekstraráhættu og einkum kröfur vegna verkefnastjórnunar og breytingastjórnunar í upplýsinga- og fjarskiptatækni og stjórnun rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem byggist á þeim kröfum sem gilda nú þegar um miðlæga mótaðila, miðlægar verðbréfamiðstöðvar og viðskiptavettvanga samkvæmt reglugerðum Evrópuþingsins og ráðsins (ESB) nr. 648/2012 ([3]), (ESB) nr. 600/2014 ([4]) og (ESB) nr. 909/2014 ([5]), eftir því sem við á.

25) Skv. 5. mgr. 6. gr. reglugerðar (ESB) 2022/2554 er þess krafist að aðilar á fjármálamarkaði endurskoði áhættustýringarramma sinn fyrir upplýsinga- og fjarskiptatækni og skili inn skýrslu til lögbærs yfirvalds síns um endurskoðunina. Til að auðvelda lögbærum yfirvöldum að vinna auðveldlega úr upplýsingum úr skýrslunum og tryggja fullnægjandi flutning á upplýsingunum ættu aðilar á fjármálamarkaði að leggja skýrslurnar fram á leitarbæru rafrænu formi.

26) Kröfur til þeirra aðila á fjármálamarkaði sem falla undir einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem um getur í 16. gr. reglugerðar (ESB) 2022/2554, ættu að leggja áherslu á þau mikilvægu svið og þætti sem, í ljósi umfangs, áhættu, stærðar og flækjustigs þessara aðila á fjármálamarkaði, eru að lágmarki nauðsynleg til að tryggja leynd, réttleika, tiltækileika og ósvikni og þjónustu þessara aðila á fjármálamarkaði. Í því samhengi ættu þessir aðilar á fjármálamarkaði að hafa til staðar innri stjórnunar- og eftirlitsramma með skýrum ábyrgðarsviðum til að auðvelda skilvirkan og traustan áhættustýringarramma. Enn fremur, til að draga úr stjórnsýslubyrði og rekstrarlegu álagi, ættu þessir aðilar á fjármálamarkaði að móta og skjalfesta aðeins eina stefnu, sem er stefna um upplýsingaöryggi, sem tilgreinir ítarlegar meginreglur og reglur sem eru nauðsynlegar til að vernda leynd, réttleika, tiltækileika og ósvikni gagna og þjónustu þessara aðila á fjármálamarkaði.

27) Ákvæði þessarar reglugerðar tengjast sviði áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, með því að tilgreina tiltekna þætti sem gilda um aðila á fjármálamarkaði í samræmi við 15. gr. reglugerðar (ESB) 2022/2554 og hanna einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni fyrir aðilana á fjármálamarkaði sem eru settir fram í 1. mgr. 16. gr. þeirrar reglugerðar. Til að tryggja samræmi á milli venjulegs og einfaldaðs áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni og að teknu tilliti til þess að ákvæðin ættu að taka gildi á sama tíma er viðeigandi að sameina ákvæðin í einni lagagerð.

28) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem Evrópska bankaeftirlitsstofnunin, Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin og Evrópska verðbréfamarkaðseftirlitsstofnunin („Evrópsku eftirlitsstofnanirnar“) hafa lagt fyrir framkvæmdastjórnina, í samráði við Netöryggisstofnun Evrópusambandsins.

([3]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 648/2012 frá 4. júlí 2012 um OTC-afleiður, miðlæga mótaðila og afleiðuviðskiptaskrár (Stjtið. ESB L 201, 27.7.2012, bls. 1, ELI: http://data.europa.eu/eli/reg/2012/648/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2014/909/oj).

29) Sameiginleg nefnd evrópsku eftirlitsstofnananna sem um getur í 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([6]), 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([7]) og 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([8]) hefur haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint hugsanlegan kostnað og ávinning af fyrirhuguðum stöðlum og óskað eftir ráðgjöf hagsmunahópsins um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010, hagsmunahópsins í vátryggingum og hagsmunahópsins um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1094/2010 og hagsmunahópsins á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1095/2010.

30) Að því marki sem vinnsla persónuupplýsinga er nauðsynleg til að uppfylla þær skuldbindingar sem eru settar fram í þessum lögum ættu reglugerðir Evrópuþingsins og ráðsins (ESB) 2016/679 ([9]) og (ESB) 2018/1725 ([10]) að gilda að fullu. Við söfnun upplýsinga ætti t.d. að framfylgja meginreglunni um lágmörkun gagna til að tryggja fullnægjandi greiningu atvika. Einnig hefur verið haft samráð við Evrópsku persónuverndarstofnunina varðandi drögin að þessum lögum.

SAMÞYKKT REGLUGERÐ ÞESSA:

I. BÁLKUR

ALMENNAR MEGINREGLUR

1. gr.

Heildaráhættusnið og flækjustig

Við mótun og innleiðingu á stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í II. bálki, og einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem um getur í III. bálki, skal tekið tillit til stærðar og heildaráhættusniðs aðila á fjármálamarkaði og eðlis, umfangs og þátta í auknu eða minna flækjustigi þjónustu hans, starfsemi og reksturs, þ.m.t. þátta sem tengjast:

a) dulritun og dulmáli,

b) rekstraröryggi upplýsinga- og fjarskiptatækni,

c) netöryggi,

([6]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) verkefnastjórnun og breytingastjórnun í upplýsinga- og fjarskiptatækni,

e) mögulegum áhrifum upplýsinga- og fjarskiptatækniáhættu á leynd, réttleika og tiltækileika gagna og truflun á samfellu og aðgengileika starfsemi aðilans á fjármálamarkaði.

II. BÁLKUR

FREKARI SAMRÆMING Á BÚNAÐI, AÐFERÐUM, FERLUM OG STEFNUM TIL STÝRINGAR Á UPPLÝSINGA- OG FJARSKIPTATÆKNIÁHÆTTU Í SAMRÆMI VIÐ 15. GR. REGLUGERÐAR (ESB) 2022/2554

I. KAFLI

Stefnur, verklagsreglur, samskiptareglur og búnaður fyrir öryggi í upplýsinga- og fjarskiptatækni

1. þáttur

2. gr.

Almennir þættir stefna, verklagsreglna, samskiptareglna og búnaðar fyrir öryggi í upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu tryggja að öryggisstefnur þeirra í upplýsinga- og fjarskiptatækni, upplýsingaöryggi og tengdar verklagsreglur, samskiptareglur og búnaður eins og um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554 séu órjúfanlegur hluti af áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni. Aðilar á fjármálamarkaði skulu taka upp þær stefnur, verklagsreglur, samskiptareglur og búnað fyrir öryggi í upplýsinga- og fjarskiptatækni sem mælt er fyrir um í þessum kafla, sem:

a) tryggja öryggi netkerfa,

b) innihalda verndarráðstafanir gegn innbrotum og gagnamisnotkun,

c) viðhalda tiltækileika, ósvikni, réttleika og leynd gagna, þ.m.t. með notkun á dulritunaraðferðum,

d) tryggja nákvæma og skjóta gagnasendingu án meiriháttar truflana og ótilhlýðilegrar tafar.

2. Aðilar á fjármálamarkaði skulu tryggja að öryggisstefnur fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr.:

a) séu samræmdar við upplýsingaöryggismarkmið aðila á fjármálamarkaði sem er að finna í stefnuáætlun um stafrænan rekstrarlegan viðnámsþrótt sem um getur í 8. mgr. 6. gr. reglugerðar (ESB) 2022/2554,

b) tilgreini dagsetninguna sem stjórn og/eða framkvæmdastjórn samþykkir öryggisstefnur upplýsinga- og fjarskiptatækni formlega,

c) innihaldi vísa og ráðstafanir til að:

   i. vakta innleiðingu á stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni,

   ii. skrá undantekningar frá innleiðingunni,

   iii. sjá til þess að stafrænn rekstrarlegur viðnámsþróttur aðila á fjármálamarkaði sé tryggður komi til undanþága eins og um getur í ii. lið,

d) tilgreini skyldur starfsfólks á öllum stigum til að tryggja upplýsinga- og fjarskiptatækniöryggi aðilans á fjármálamarkaði,

e) tilgreini afleiðingar þess ef starfsfólk aðila á fjármálamarkaði framfylgir ekki öryggisstefnum fyrir upplýsinga- og fjarskiptatækni, ef ekki er mælt fyrir um það í öðrum stefnum aðila á fjármálamarkaði,

f) tilgreini lista yfir þau skjöl sem á að varðveita,

g) tilgreini ráðstafanir til aðgreiningar starfa í tengslum við líkanið um þrjár varnarlínur eða annað innra áhættustýringar- og eftirlitslíkan, eftir því sem við á, til að forðast hagsmunaárekstra,

h) taki mið af leiðandi starfsvenjum og, eftir atvikum, stöðlum eins og skilgreint er í 1. lið 2. gr. reglugerðar (ESB) nr. 1025/2012,

i) auðkenni hlutverk og ábyrgðarsvið fyrir mótun, innleiðingu og viðhald á stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni,

j) séu endurskoðaðar í samræmi við 5. mgr. 6. gr. reglugerðar (ESB) 2022/2554,

k) taki tillit til verulegra breytinga sem snerta viðkomandi aðila á fjármálamarkaði, þ.m.t. verulegra breytinga á starfsemi eða ferlum hans, á landslagi netógna eða gildandi lagalegum skuldbindingum.

2. þáttur

3. gr.

Stýring upplýsinga- og fjarskiptatækniáhættu

Aðilar á fjármálamarkaði skulu móta, skjalfesta og innleiða áhættustýringarstefnur og verklagsreglur fyrir upplýsinga- og fjarskiptatækni sem skulu innihalda allt eftirfarandi:

a) upplýsingar um samþykkt áhættuþolmarka upplýsinga- og fjarskiptatækniáhættu sem ákvörðuð eru í samræmi við b-lið 8. mgr. 6. gr. reglugerðar (ESB) 2022/2554,

b) verklagsreglu og aðferðafræði við framkvæmd upplýsinga- og fjarskiptatækniáhættumats, sem skilgreinir:

   i. veikleika og ógnir sem hafa áhrif eða geta haft áhrif á studda starfsemi, upplýsinga- og fjarskiptatæknikerfi og upplýsinga- og fjarskiptatæknieignir sem styðja þá starfsemi,

   ii. megindlega eða eigindlega vísa til að mæla áhrif af og líkur á veikleikum og ógnum sem um getur í i. lið,

c) verklagsreglur til að skilgreina, innleiða og skjalfesta ráðstafanir til meðhöndlunar upplýsinga- og fjarskiptatækniáhættu að því er varðar þá upplýsinga- og fjarskiptatækniáhættu sem er greind og metin, þ.m.t. ákvörðun á þeim ráðstöfunum til meðhöndlunar upplýsinga- og fjarskiptatækniáhættu sem nauðsynlegar eru til að hún verði innan þeirra áhættuþolmarka sem um getur í a-lið,

d) að því er varðar þá upplýsinga- og fjarskiptatækniáhættu sem eftir stendur að lokinni innleiðingu á þeim ráðstöfunum til meðhöndlunar upplýsinga- og fjarskiptatækniáhættu sem um getur í c-lið:

   i. ákvæði um tilgreiningu á eftirstæðri upplýsinga- og fjarskiptatækniáhættu,

   ii. úthlutun hlutverka og ábyrgðar varðandi:

      1) samþykki á eftirstæðri upplýsinga- og fjarskiptatækniáhættu sem fer umfram þau áhættuþolmörk aðila á fjármálamarkaði sem um getur í a-lið,

      2) endurskoðunarferlið sem um getur í iv. lið þessa d-liðar,

   iii. gerð lista yfir samþykkta eftirstæða upplýsinga- og fjarskiptatækniáhættu, þ.m.t. rökstuðning fyrir því að hún er samþykkt,

   iv. ákvæði um endurskoðun á samþykktri eftirstæðri upplýsinga- og fjarskiptatækniáhættu a.m.k. einu sinni á ári, þ.m.t.:

      1) tilgreining hvers kyns breytinga sem hafa orðið á þeirri eftirstæðu upplýsinga- og fjarskiptatækniáhættu,

      2) mat á tiltækum mótvægisráðstöfunum,

      3) mat á því hvort rökstuðningur fyrir samþykkt á þeirri eftirstæðu upplýsinga- og fjarskiptatækniáhættu sé gild og eigi við þegar endurskoðunin fer fram,

e) ákvæði um vöktun á:

   i. hvers kyns breytingum á landslagi upplýsinga- og fjarskiptatækniáhættu og netógna,

   ii. innri og ytri veikleikum og ógnum:

   iii. upplýsinga- og fjarskiptatækniáhætta aðilans á fjármálamarkaði sem gerir kleift að greina hratt þær breytingar sem gætu haft áhrif á upplýsinga- og fjarskiptatækniáhættusnið hans,

f) ákvæði um ferli til að tryggja að tekið sé tillit til hvers kyns breytinga á viðskiptaáætlun og stefnu um stafrænum rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði.

Að því er c-lið fyrstu málsgreinar varðar skulu verklagsreglurnar sem um getur í þeim lið tryggja:

a) vöktun á árangri innleiddra ráðstafana til meðhöndlunar upplýsinga- og fjarskiptatækniáhættu,

b) mat á því hvort settum áhættuþolmörkum aðila á fjármálamarkaði hafi verið náð,

c) mat á því hvort viðkomandi aðili á fjármálamarkaði hafi gripið til leiðréttinga eða úrbóta á ráðstöfununum þar sem við á.

3. þáttur

Eignastýring upplýsinga- og fjarskiptatækni

4. gr.

Eignastýringarstefna í upplýsinga- og fjarskiptatækni

1. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði móta, skjalfesta og innleiða stefnu um stýringu upplýsinga- og fjarskiptatæknieigna.

2. Í stefnu um stjórnun upplýsinga- og fjarskiptatæknieigna sem um getur í 1. mgr. skal:

a) mæla fyrir um vöktun og stjórnun á endingarskeiði upplýsinga- og fjarskiptatæknieigna sem eru tilgreindar og flokkaðar í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554,

b) mæla fyrir um að aðili á fjármálamarkaði skuli halda skrár yfir allt eftirfarandi:

   i. einkvæmt auðkenni sérhverrar upplýsinga- og fjarskiptatæknieignar,

   ii. upplýsingar um staðsetningu, annaðhvort raunlæga eða röklega, allra upplýsinga- og fjarskiptatæknieigna,

   iii. flokkun allra upplýsinga- og fjarskiptatæknieigna, eins og um getur í 1. mgr. 8. gr. reglugerðar (ESB) 2022/2254,

   iv. auðkenni eigenda upplýsinga- og fjarskiptatæknieigna,

   v. starfsemi eða þjónustu sem upplýsinga- og fjarskiptatæknieign styður,

   vi. kröfur til rekstrarsamfellu í upplýsinga- og fjarskiptatækni, þ.m.t. markmið um endurreisnartíma og endamark endurreisnar,

   vii. hvort upplýsinga- og fjarskiptatæknieignin geti verið eða sé aðgengileg frá ytri netkerfum, þ.m.t. internetinu,

   viii. tengsl og innbyrðis hæði meðal upplýsinga- og fjarskiptatæknieigna og þeirrar starfsemi sem notar hverja upplýsinga- og fjarskiptatæknieign fyrir sig,

   ix. þar sem við á, fyrir allar upplýsinga- og fjarskiptatæknieignir, lokadagsetningar reglubundinnar, aukinnar og sérsniðinnar stuðningsþjónustu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu en að henni liðinni fá upplýsinga- og fjarskiptatæknieignirnar ekki lengur stuðningsþjónustu frá birgi eða þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

c) að því er varðar aðra aðila á fjármálamarkaði en örfyrirtæki, mæla fyrir um að þeir aðilar á fjármálamarkaði haldi skrár yfir þær upplýsingar sem nauðsynlegar eru til að framkvæma sérstakt áhættumat á öllum fornkerfum í upplýsinga- og fjarskiptatækni eins og um getur í 7. mgr. 8. gr. reglugerðar (ESB) 2022/2554.

5. gr.

Verklagsreglur um stýringu upplýsinga- og fjarskiptatæknieigna

1. Aðilar á fjármálamarkaði skulu þróa, skjalfesta og innleiða verklagsreglur um stýringu upplýsinga- og fjarskiptatæknieigna.

2. Verklagsreglan um stýringu upplýsinga- og fjarskiptatæknieigna sem um getur í 1. mgr. skal tilgreina viðmiðanir um framkvæmd mikilvægismats á upplýsingaeignum og upplýsinga- og fjarskiptatæknieignum sem styðja starfsemi fyrirtækja. Matið skal taka tillit til eftirfarandi:

a) upplýsinga- og fjarskiptatækniáhættu sem tengist starfseminni og hve háð starfsemin er upplýsingaeignum eða upplýsinga- og fjarskiptatæknieignum,

b) hvernig tap á leynd, réttleika og tiltækileika slíkra upplýsingaeigna og upplýsinga- og fjarskiptatæknieigna myndi hafa áhrif á rekstrarferla og starfsemi aðila á fjármálamarkaði.

4. þáttur

Dulritun og dulmál

6. gr.

Dulritun og dulritunarstýringar

1. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði móta, skjalfesta og innleiða stefnu um dulritun og dulritunarstýringar.

2. Aðilar á fjármálamarkaði skulu hanna stefnuna um dulritun og dulritunarstýringar sem um getur í 1. mgr. á grundvelli niðurstaðna samþykktrar gagnaflokkunar og upplýsinga- og fjarskiptatækniáhættumats. Stefnan skal fela í sér reglur um allt eftirfarandi:

a) dulritun gagna í dvala og í flutningi,

b) dulritun gagna í notkun, þar sem nauðsyn krefur,

c) dulritun á tengingum innri netkerfa og umferðar til og frá ytri aðilum,

d) stjórnun dulritunarlykils, sem um getur í 7. gr., sem mælir fyrir um reglur um rétta notkun, vörn og endingarskeið dulritunarlykla.

Að því er varðar b-lið skulu aðilar á fjármálamarkaði vinna með gögn í notkun í sérstöku og vernduðu umhverfi eða gera samsvarandi ráðstafanir til að tryggja leynd, réttleika, ósvikni og tiltækileika gagna ef ekki er hægt að dulrita gögn í notkun.

3. Aðilar á fjármálamarkaði skulu hafa með í stefnu um dulritun og dulritunarstýringar, sem um getur í 1. mgr., viðmiðanir um val á dulritunaraðferðum og leiðir til notkunar, að teknu tilliti til leiðandi starfsvenja og staðla, eins og skilgreint er í 1. lið 2. gr. reglugerðar (ESB) nr. 1025/2012, og flokkun á viðkomandi upplýsinga- og fjarskiptatæknieignum sem komið er á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554. Aðilar á fjármálamarkaði, sem geta ekki fylgt leiðandi starfsvenjum eða stöðlum eða notað áreiðanlegustu aðferðirnar, skulu innleiða ráðstafanir til mótvægis og vöktunar sem tryggja viðnámsþrótt gegn netógnum.

4. Aðilar á fjármálamarkaði skulu hafa með í stefnu um dulritun og dulritunarstýringar, sem um getur í 1. mgr., ákvæði um að uppfæra eða breyta dulritunartækni á grundvelli þróunar í dulmálsgreiningu, ef nauðsyn krefur. Uppfærslurnar eða breytingarnar skulu tryggja að dulritunartæknin haldi viðnámsþrótti gagnvart netógnum, eins og krafist er skv. a-lið 2. mgr. 10. gr. Aðilar á fjármálamarkaði sem geta ekki uppfært eða breytt dulritunartækninni skulu innleiða ráðstafanir til mótvægis og vöktunar sem tryggja viðnámsþrótt gegn netógnum.

5. Aðilar á fjármálamarkaði skulu hafa með í stefnu um dulritun og dulritunarstýringar, sem um getur í 1. mgr., kröfu um að skrásetja innleiðingu ráðstafana til mótvægis og vöktunar sem innleiddar hafa verið í samræmi við 3. og 4. mgr. gefa rökstudda skýringu á því.

7. gr.

Stjórnun dulritunarlykils

1. Aðilar á fjármálamarkaði skulu hafa með í stefnu um stjórnun dulritunarlykils, sem um getur í d-lið 2. mgr. 6. gr., kröfur um stjórnun dulritunarlykla allt endingarskeið þeirra, þ.m.t. gerð, endurnýjun, geymslu, öryggisafritun, safnvistun, endurheimt, flutning, úreldingu, ógildingu og eyðingu dulritunarlyklanna.

2. Aðilar á fjármálamarkaði skulu tilgreina og innleiða stýringar til að verja dulritunarlykla fyrir tapi, óheimilum aðgangi, afhjúpun og breytingum allt endingarskeið þeirra. Aðilar á fjármálamarkaði skulu hanna þær stýringar á grundvelli niðurstaðna samþykktrar gagnaflokkunar og upplýsinga- og fjarskiptatækniáhættumatsins.

3. Aðilar á fjármálamarkaði skulu þróa og innleiða aðferðir til að skipta um dulritunarlykla ef þeir tapast eða ef lyklunum er stefnt í hættu eða þeir skemmdir.

4. Aðilar á fjármálamarkaði skulu stofna og viðhalda skrá yfir öll vottorð og búnað sem geymir vottorð fyrir a.m.k. þær upplýsinga- og fjarskiptatæknieignir sem styðja nauðsynlega eða mikilvæga starfsemi. Aðilar á fjármálamarkaði skulu tryggja að skráin sé ætíð rétt.

5. Aðilar á fjármálamarkaði skulu tryggja tímanlega endurnýjun vottorða áður en gildistími þeirra rennur út.

5. þáttur

Rekstraröryggi upplýsinga- og fjarskiptatækni

8. gr.

Stefnur og verklagsreglur fyrir upplýsinga- og fjarskiptatæknirekstur

1. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði þróa, skjalfesta og innleiða stefnur og verklagsreglur til að stýra upplýsinga- og fjarskiptatæknirekstri. Stefnurnar og verklagsreglurnar skulu tilgreina hvernig aðilar á fjármálamarkaði reka, vakta, stýra og endurheimta upplýsinga- og fjarskiptatæknieignir, þ.m.t. skjalfestingu á upplýsinga- og fjarskiptatæknirekstri.

2. Stefnurnar og verklagið fyrir upplýsinga- og fjarskiptatæknirekstur, sem um getur í 1. mgr., skulu einnig fela í sér allt eftirfarandi:

a) lýsingu á upplýsinga- og fjarskiptatæknieignum, þ.m.t. allt sem hér fer á eftir:

   i. kröfur varðandi örugga uppsetningu, viðhald, samskipan og fjarlægingu uppsetningar upplýsinga- og fjarskiptatæknikerfis,

   ii. kröfur varðandi stjórnun upplýsingaeigna sem upplýsinga- og fjarskiptatæknieignir nota, þ.m.t. vinnslu og meðhöndlun þeirra, bæði sjálfvirka og handvirka,

   iii. kröfur varðandi auðkenningu og eftirlit með fornkerfum í upplýsinga- og fjarskiptatækni,

b) stýringar og vöktun á upplýsinga- og fjarskiptatæknikerfum, þ.m.t. allt sem hér fer á eftir:

   i. kröfur um öryggisafritun og endurheimt upplýsinga- og fjarskiptatæknikerfa,

   ii. kröfur um áætlunargerð, að teknu tilliti til innbyrðis hæðis upplýsinga- og fjarskiptatæknikerfa,

   iii. samskiptareglur fyrir gagnaferil og upplýsingar úr kerfisskrám,

   iv. kröfur til að tryggja að framkvæmd á innri endurskoðun og annarri prófun lágmarki truflun á starfsemi,

   v. kröfur um aðgreiningu raunumhverfis í upplýsinga- og fjarskiptatækni frá þróunar-, prófunarumhverfi og öðru umhverfi sem ekki er raunumhverfi,

   vi. kröfur um framkvæmd þróunar og prófunar í umhverfi sem er aðgreint frá raunumhverfinu,

   vii. kröfur um framkvæmd þróunar og prófunar í raunumhverfi,

c) villumeðhöndlun í upplýsinga- og fjarskiptatæknikerfum, þ.m.t. allt sem hér fer á eftir:

i. verklagsreglur og samskiptareglur til að meðhöndla villur,

ii. tengiliði vegna stuðnings og stigmögnunar viðbragða, þ.m.t. ytri stuðningstengiliði ef upp koma ófyrirséð rekstrar- eða tæknivandamál,

iii. endurræsing upplýsinga- og fjarskiptatæknikerfis, afturfærsla og endurreisnarferli til að nota ef truflun verður á upplýsinga- og fjarskiptatæknikerfi.

Að því er varðar v. lið b-liðar skal aðgreiningin taka til allra þátta umhverfis, þ.m.t. aðgangsreikninga, gagna eða tenginga, eins og krafist er skv. a-lið fyrstu undirgreinar 13. gr.

Að því er varðar vii. lið b-liðar skulu stefnur og verklagsreglur sem um getur í 1. mgr. kveða á um að aðstæður þar sem prófun er gerð í raunumhverfi séu skýrt tilgreindar, rökstuddar, eigi sér stað innan afmarkaðs tíma og séu samþykktar af viðeigandi starfsviði, í samræmi við 6. mgr. 16. gr. Aðilar á fjármálamarkaði skulu tryggja tiltækileika, leynd, réttleika og ósvikni upplýsinga- og fjarskiptatæknikerfa og framleiðslugagna við þróun og prófun í raunumhverfinu.

9. gr.

Getu- og frammistöðustjórnun

1. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði þróa, skjalfesta og innleiða verklagsreglur um getu- og frammistöðustjórnun vegna eftirfarandi:

a) tilgreiningar á kröfum um getu upplýsinga- og fjarskiptatæknikerfa,

b) hámörkunar á nýtingu auðlinda,

c) vöktunarverklag fyrir viðhald og endurbætur á:

i. tiltækileika gagna og upplýsinga- og fjarskiptatæknikerfa,

ii. skilvirkni upplýsinga- og fjarskiptatæknikerfa,

iii. að koma í veg fyrir skort á upplýsinga- og fjarskiptatæknigetu.

2. Þær verklagsreglur um getu- og frammistöðustjórnun sem um getur í 1. mgr. skulu tryggja að aðilar á fjármálamarkaði geri viðeigandi ráðstafanir til að taka mið af sérstökum eiginleikum upplýsinga- og fjarskiptatæknikerfa með löngum eða flóknum innkaupa- eða samþykkisferlum eða upplýsinga- og fjarskiptatæknikerfa sem eru auðlindakræf.

10. gr.

Veikleika- og bótastjórnun

1. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði þróa, skjalfesta og innleiða verklagsreglur um veikleikastjórnun.

2. Veikleikastjórnunin sem um getur í 1. mgr. skal:

a) greina og uppfæra viðeigandi og traustar upplýsingaveitur til að skapa og viðhalda vitund um veikleika,

b) tryggja að fram fari sjálfvirk veikleikaskönnun og -mat á upplýsinga- og fjarskiptatæknieignum, þar sem tíðni og umfang þeirra aðgerða skal vera í samræmi við flokkunina sem komið er á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554 og heildaráhættusnið upplýsinga- og fjarskiptatæknieignarinnar,

c) sannprófa hvort:

i. þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu takist á við veikleika sem tengjast þeirri upplýsinga- og fjarskiptatækniþjónustu sem aðila á fjármálamarkaði er veitt,

ii. þjónustuveitendurnir tilkynni aðila á fjármálamarkaði tímanlega um a.m.k. alvarlega veikleika og tölfræðilegar upplýsingar og leitni,

d) rekja notkun á:

i. forritasöfnum þriðju aðila, þ.m.t. söfnum með opnum aðgangi sem notuð eru af upplýsinga- og fjarskiptatækniþjónustum sem styðja nauðsynlega eða mikilvæga starfsemi,

ii. upplýsinga- og fjarskiptatækniþjónustu sem aðilinn á fjármálamarkaði hefur þróað sjálfur eða sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur sérsniðið eða þróað fyrir aðilann á fjármálamarkaði,

e) koma á fót verklagsreglum fyrir ábyrga upplýsingagjöf um veikleika til viðskiptavina, mótaðila og almennings,

f) forgangsraða innleiðingu á bótum og öðrum mótvægisráðstöfunum til að taka á greindum veikleikum,

g) vakta og sannprófa úrbætur á veikleikum,

h) krefjast skráningar á öllum greindum veikleikum sem hafa áhrif á upplýsinga- og fjarskiptatæknikerfi og vöktun á úrlausn þeirra.

Að því er varðar b-lið skulu aðilar á fjármálamarkaði framkvæma sjálfvirka veikleikaskönnun og -mat á upplýsinga- og fjarskiptatæknieignum fyrir þær upplýsinga- og fjarskiptatæknieignir, sem styðja nauðsynlega eða mikilvæga starfsemi, a.m.k. einu sinni í viku.

Að því er varðar c-lið skulu aðilar á fjármálamarkaði fara fram á að þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu rannsaki viðkomandi veikleika, greini frumorsakir og framkvæmi viðeigandi mildandi aðgerð.

Að því er varðar d-lið skulu aðilar á fjármálamarkaði, eftir því sem við á, í samvinnu við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, vakta útgáfu og hugsanlegar uppfærslur á forritasöfnum þriðja aðila. Þegar um er að ræða upplýsinga- og fjarskiptatæknieignir eða -einingar, tilbúnar til notkunar (hilluvöru), sem eru keyptar og notaðar við rekstur upplýsinga- og fjarskiptatækniþjónustu sem styður ekki nauðsynlega eða mikilvæga starfsemi, skulu aðilar á fjármálamarkaði rekja notkun á forritasöfnum þriðja aðila, þ.m.t. söfnum með opnum aðgangi, að því marki sem hægt er.

Að því er varðar f-lið skulu aðilar á fjármálamarkaði taka tillit til þess hversu alvarlegur veikleikinn er, flokkunarinnar sem komið var á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554 og áhættusniðs þeirra upplýsinga- og fjarskiptatæknieigna sem greindir veikleikar hafa áhrif á.

3. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði þróa, skjalfesta og innleiða verklagsreglur um bótastjórnun.

4. Verklagsreglurnar um bótastjórnun sem um getur í 3. mgr. skulu:

a) bera kennsl á og leggja mat á tiltæka hugbúnaðar- og vélbúnaðarbætur og -uppfærslur með sjálfvirkum verkfærum, að því marki sem hægt er,

b) tilgreina verklagsreglur í neyðartilvikum fyrir bætur og uppfærslur á upplýsinga- og fjarskiptatæknieignum,

c) prófa og innleiða hugbúnaðar- og vélbúnaðarbæturnar og -uppfærslurnar sem um getur í v., vi. og vii. lið 2. mgr. 8. gr.,

d) setja tímamörk fyrir uppsetningu hugbúnaðar- og vélbúnaðarbóta og uppfærslna og ferli til stigmögnunar viðbragða ef ekki er unnt að virða þau tímamörk.

11. gr.

Gagna- og kerfisöryggi

1. Sem hluta af stefnum, verklagsreglum, samskiptareglum og búnaði fyrir öryggi í upplýsinga- og fjarskiptatækni, sem um getur í 2. mgr. 9. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði þróa, skjalfesta og innleiða verklagsreglur um gagna- og kerfisöryggi.

2. Verklagsreglan um gagna- og kerfisöryggi sem um getur í 1. mgr. skal innihalda öll eftirfarandi atriði sem tengjast gagna- og kerfisöryggi í upplýsinga- og fjarskiptatækni í samræmi við flokkunina sem komið var á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554:

a) aðgangstakmarkanirnar sem um getur í 21. gr. þessarar reglugerðar, sem styðja kröfur um vernd fyrir hvert flokkunarstig,

b) tilgreiningu á öruggu grunnviðmiði samskipunar fyrir upplýsinga- og fjarskiptatæknieignir sem lágmarkar útsetningu þeirra fyrir netógnum og ráðstafanir til að sannprófa reglulega að þessum grunnviðmiðum sé beitt á skilvirkan hátt,

c) tilgreiningu á öryggisráðstöfunum til að tryggja að eingöngu samþykktur hugbúnaður sé settur upp á upplýsinga- og fjarskiptatæknikerfum og endabúnaði,

d) tilgreiningu öryggisráðstafana vegna spillikóða,

e) tilgreiningu öryggisráðstafana til að tryggja að aðeins heimilaðir gagnageymslumiðlar, -kerfi og -endabúnaður séu notaðir til að flytja og geyma gögn aðilans á fjármálamarkaði,

f) eftirfarandi kröfur til að tryggja notkun á flytjanlegum endabúnaði og einkaendabúnaði sem ekki er flytjanlegur:

   i. kröfuna um að nota stjórnunarlausn til fjarstýringar á endabúnaði og fjareyðingar á gögnum aðilans á fjármálamarkaði,

   ii. kröfuna um að nota öryggisúrræði sem starfsfólk eða þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu geta ekki breytt, fjarlægt eða farið framhjá á óheimilan hátt,

   iii. kröfuna um að nota fjarlægjanlegan gagnageymslubúnað eingöngu ef eftirstæð upplýsinga- og fjarskiptatækniáhætta er innan áhættuþolmarka aðilans á fjármálamarkaði sem um getur í a-lið fyrstu undirgreinar 3. gr.,

g) ferlið við örugga eyðingu gagna, sem eru á athafnasvæði aðilans á fjármálamarkaði eða sem eru geymd utan þess, sem aðilinn á fjármálamarkaði þarf ekki lengur að safna eða geyma,

h) verklag við förgun eða úreldingu gagnageymslubúnaðar sem er á athafnasvæði aðila á fjármálamarkaði eða sem geymdur er utan þess og inniheldur trúnaðarupplýsingar,

i) tilgreiningu og innleiðingu öryggisráðstafana til að koma í veg fyrir gagnatap og -leka í kerfum og endabúnaði,

j) innleiðingu öryggisráðstafana til að tryggja að fjarvinnsla og notkun á einkaendabúnaði hafi ekki neikvæð áhrif á upplýsinga- og fjarskiptatækniöryggi aðila á fjármálamarkaði,

k) fyrir upplýsinga- og fjarskiptatæknieignir eða -þjónustu sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu rekur, tilgreiningu og innleiðingu krafna til að halda stafrænum rekstrarlegum viðnámsþrótti, í samræmi við niðurstöður gagnaflokkunar og upplýsinga- og fjarskiptatækniáhættumats.

Að því er b-lið varðar skal öruggt grunnviðmið samskipunar, sem um getur í þeim lið, taka mið af leiðandi starfsvenjum og viðeigandi aðferðum sem mælt er fyrir um í stöðlunum sem skilgreindir eru í 1. lið 2. gr. reglugerðar (ESB) nr. 1025/2012.

Að því er varðar k-lið skulu aðilar á fjármálamarkaði taka tillit til eftirfarandi:

a) innleiðingar á stillingum samkvæmt ráðgjöf seljanda á þeim þáttum sem aðili á fjármálamarkaði notar,

b) skýrrar úthlutunar upplýsingaöryggishlutverka og -ábyrgðar milli aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, í samræmi við meginregluna um fulla ábyrgð aðila á fjármálamarkaði á þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem um getur í a-lið 1. mgr. 28. gr. reglugerðar (ESB) 2022/2554, og fyrir aðila á fjármálamarkaði sem um getur í 2. mgr. 28. gr. reglugerðar og í samræmi við stefnu aðila á fjármálamarkaði um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga þjónustu,

c) nauðsyn þess að tryggja og viðhalda nægilegri hæfni innan aðila á fjármálamarkaði í stjórnun og öryggi þeirrar þjónustu sem er notuð,

d) tæknilegar ráðstafanir og skipulagsráðstafanir til að lágmarka áhættuna sem tengist þeim innviðum sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu notar fyrir upplýsinga- og fjarskiptatækniþjónustu sína, að teknu tilliti til leiðandi starfsvenja og staðla eins og skilgreint er í 1. lið 2. gr. reglugerðar (ESB) nr. 1025/2012.

12. gr.

Aðgerðaskráning

1. Aðilar á fjármálamarkaði skulu, sem hluta af öryggisráðstöfunum gegn innbrotum og misnotkun á gögnum, þróa, skjalfesta og innleiða verklagsreglur, samskiptareglur og verkfæri til aðgerðaskráningar.

2. Verklagsreglurnar, samskiptareglurnar og verkfærin til aðgerðarskráningar, sem um getur í 1. mgr., skulu einnig fela í sér allt eftirfarandi:

a) tilgreiningu á þeim atburðum sem á að skrá, varðveislutímabil skráninga og ráðstafanir til að tryggja og meðhöndla aðgerðarskráningargögn, að teknu tilliti til þess hvers vegna aðgerðarskrárnar voru stofnaðar,

b) að sundurliðunarstig skráninga sé í samræmi við tilgang og notkun þeirra til að hægt sé að greina af skilvirkni óvenjulegar athafnir eins og um getur í 24. gr.,

c) kröfu um að skrá atburði í tengslum við allt eftirfarandi:

   i. röklegar og raunlægar aðgangsstýringar, eins og um getur í 21. gr., og auðkenningarstjórnun,

   ii. getustýringu,

   iii. breytingastjórnun,

   iv. rekstur upplýsinga- og fjarskiptatækni, þ.m.t. starfsemi upplýsinga- og fjarskiptatæknikerfa,

   v. starfsemi sem tengist netumferð, þ.m.t. frammistöðu upplýsinga- og fjarskiptatæknineturkerfis,

d) ráðstafanir til að vernda aðgerðaskráningarkerfi og upplýsingar aðgerðaskráninga fyrir óheimilum breytingum, eyðingu og óheimilum aðgangi í dvala, í flutningi, og, ef við á, í notkun,

e) ráðstafanir til að greina bilun í aðgerðaskráningarkerfum,

f) með fyrirvara um gildandi kröfur samkvæmt reglum í samræmi við lög Sambandsins eða landslög, samstillingu á klukkum í hvers upplýsinga- og fjarskiptatæknikerfis aðilans á fjármálamarkaði við skjalfesta áreiðanlega heimild um viðmiðunartíma.

Að því er varðar a-lið skulu aðilar á fjármálamarkaði ákvarða varðveislutímann, að teknu tilliti til markmiða viðskipta- og upplýsingaöryggis, ástæðu þess að atburðurinn er skráður í aðgerðaskrárnar og niðurstaðna upplýsinga- og fjarskiptatækniáhættumats.

6. þáttur

Öryggi netkerfis

13. gr.

Öryggisstjórnun netkerfis

Aðilar á fjármálamarkaði skulu, sem hluta af öryggisráðstöfunum sem tryggja öryggi netkerfa gegn innbrotum og gagnamisnotkun, móta, skjalfesta og innleiða stefnur, verklagsreglur, samskiptareglur og verkfæri til öryggisstjórnunar netkerfis, þ.m.t. allt sem hér fer á eftir:

a) aðskilnað og lagskiptingu upplýsinga- og fjarskiptatæknikerfa og -netkerfa, að teknu tilliti til:

   i. hversu nauðsynleg eða mikilvæg virknin er sem upplýsinga- og fjarskiptatæknikerfin og- netkerfin styðja,

   ii. flokkunarinnar sem komið var á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554,

   iii. heildaráhættusniðs upplýsinga- og fjarskiptatæknieigna sem nota þessi upplýsinga- og fjarskiptatæknikerfi og -netkerfi,

b) skjalfestingu á öllum nettengingum og gagnaflæði aðilans á fjármálamarkaði,

c) notkun á aðgreindu og sérhæfðu netkerfi fyrir umsýslu upplýsinga- og fjarskiptatæknieigna,

d) sanngreiningu og innleiðingu aðgangsstýringar að netkerfum til að hindra og bera kennsl á tengingar við netkerfi aðilans á fjármálamarkaði frá óleyfilegum búnaði eða kerfum eða hvers kyns endabúnaði sem uppfyllir ekki öryggiskröfur aðilans á fjármálamarkaði,

e) dulritun nettenginga sem fara í gegnum fyrirtækjanet, almenn netkerfi, landsbundin netkerfi, netkerfi þriðja aðila og þráðlaus netkerfi fyrir þær samskiptareglur sem eru notaðar, að teknu tilliti til niðurstaðna samþykktrar gagnaflokkunar, niðurstaðna upplýsinga- og fjarskiptatækniáhættumats og dulritunar á nettengingunum sem um getur í 2. mgr. 6. gr.,

f) hönnun netkerfa í samræmi við þær öryggiskröfur sem aðili á fjármálamarkaði hefur gert, að teknu tilliti til leiðandi starfsvenja til að tryggja leynd, réttleika og tiltækileika netkerfisins,

g) tryggja örugga netumferð milli innri netkerfa og internetsins og annarra ytri tenginga,

h) tilgreiningu hlutverka og ábyrgðarsviða og skref sem taka skal við skilgreiningu, innleiðingu, samþykki, breytingar og endurskoðun á eldveggsreglum og tengingarsíum,

i) framkvæmd endurskoðana á nethögun og hönnun netkerfa einu sinni á ári, og reglulega fyrir örfyrirtæki, til að bera kennsl á hugsanlega veikleika,

j) ráðstafanir til tímabundinnar einangrunar, ef nauðsyn krefur, á undirnetum og netkerfisíhlutum og -búnaði,

k) innleiðingu á öruggu grunnviðmiði samskipunar allra netkerfisíhluta og herðingu netkerfis og netkerfisbúnaðar í samræmi við leiðbeiningar seljanda, staðla, þar sem það á við, eins og skilgreint er í 1. lið 2. gr. reglugerðar (ESB) nr. 1025/2012, og leiðandi starfsvenjur,

l) verklagsreglur til að takmarka, læsa og slíta kerfis- og fjarlotum eftir tilgreint tímabil aðgerðaleysis,

m) vegna netþjónustusamninga:

   i. auðkenning og skilgreining á ráðstöfunum vegna upplýsinga- og fjarskiptatækniöryggis og upplýsingaöryggis, þjónustustigum og stjórnunarkröfum allrar netþjónustu,

   ii. hvort veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu eða þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu veiti þá þjónustu.

Að því er varðar h-lið skulu aðilar á fjármálamarkaði reglulega endurskoða eldveggsreglur og tengingarsíur í samræmi við flokkunina sem komið var á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554 og heildaráhættusnið viðkomandi upplýsinga- og fjarskiptatæknikerfa. Fyrir upplýsinga- og fjarskiptatæknikerfi sem styðja nauðsynlega eða mikilvæga starfsemi skulu aðilar á fjármálamarkaði sannreyna að gildandi reglur um eldveggi og tengingarsíur séu fullnægjandi a.m.k. á 6 mánaða fresti.

14. gr.

Öryggi upplýsinga í flutningi

1. Sem hluta af verndarráðstöfunum til að varðveita tiltækileika, ósvikni, réttleika og leynd gagna skulu aðilar á fjármálamarkaði móta, skjalfesta og innleiða stefnur, verklagsreglur, samskiptareglur og verkfæri til að vernda upplýsingar í flutningi. Aðilar á fjármálamarkaði skulu einkum tryggja allt eftirfarandi:

a) tiltækileika, ósvikni, réttleika og leynd gagna í flutningi innan netkerfa og að komið sé á verklagsreglum til að meta hvort farið sé að þessum kröfum,

b) forvarnir og greiningu gagnaleka og öruggan flutning upplýsinga milli aðilans á fjármálamarkaði og utanaðkomandi aðila,

c) að kröfur um trúnað eða fyrirkomulag trúnaðar sem endurspegla þarfir aðilans á fjármálamarkaði á verndun upplýsinga fyrir bæði starfsfólk aðilans á fjármálamarkaði og starfsfólk þriðja aðila, séu innleiddar, skjalfestar og endurskoðaðar reglulega.

2. Aðilar á fjármálamarkaði skulu semja stefnur, verklagsreglur, samskiptareglur og verkfæri til að vernda upplýsingarnar í flutningi sem um getur í 1. mgr. á grundvelli niðurstaðna samþykktrar gagnaflokkunar og upplýsinga- og fjarskiptatækniáhættumatsins.

7. þáttur

Verkefnastjórnun og breytingastjórnun í upplýsinga- og fjarskiptatækni

15. gr.

Verkefnastjórnun í upplýsinga- og fjarskiptatækni

1. Sem hluta af verndarráðstöfunum til að varðveita tiltækileika, ósvikni, réttleika og leynd gagna skulu aðilar á fjármálamarkaði móta, skjalfesta og innleiða stefnu um verkefnastjórnun í upplýsinga- og fjarskiptatækni.

2. Stefnan um verkefnastjórnun í upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. skal tilgreina þá þætti sem tryggja skilvirka stjórnun upplýsinga- og fjarskiptatækniverkefna sem tengjast kaupum, viðhaldi og, eftir atvikum, þróun á upplýsinga- og fjarskiptatæknikerfum aðilans á fjármálamarkaði.

3. Stefnan um verkefnastjórnun í upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr., skal fela í sér allt eftirfarandi:

a) markmið upplýsinga- og fjarskiptatækniverkefna,

b) stjórnunarhætti vegna upplýsinga- og fjarskiptatækniverkefna, þ.m.t. hlutverk og ábyrgðarsvið,

c) áætlun, tímaramma og skref upplýsinga- og fjarskiptatækniverkefna,

d) áhættumat upplýsinga- og fjarskiptatækniverkefna,

e) viðkomandi áfanga,

f) kröfur um breytingastjórnun,

g) prófun á öllum kröfum, þ.m.t. öryggiskröfum, og viðkomandi samþykkisferli þegar upplýsinga- og fjarskiptatæknikerfi er tekið í notkun í raunumhverfi.

4. Stefnan um verkefnastjórnun í upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr., skal tryggja örugga framkvæmd upplýsinga- og fjarskiptatækniverkefna með miðlun nauðsynlegra upplýsinga og sérfræðiþekkingar af því rekstrarsviði eða starfssviðum sem upplýsinga- og fjarskiptatækniverkefnið hefur áhrif á.

5. Í samræmi við áhættumat upplýsinga- og fjarskiptatækniverkefnis, sem um getur í d-lið 3. mgr., skal stefnan um verkefnastjórnun í upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr., kveða á um að stofnun og framgangur upplýsinga- og fjarskiptatækniverkefna sem hafa áhrif á nauðsynleg eða mikilvæg starfssvið aðilans á fjármálamarkaði og tengda áhættu séu tilkynntar til stjórnar og/eða framkvæmdastjórnar sem hér segir:

a) hvert fyrir sig eða saman, eftir mikilvægi og stærð upplýsinga- og fjarskiptatækniverkefnanna,

b) reglulega og, ef nauðsyn krefur, eftir því sem atburðir gefa tilefni til.

16. gr.

Kaup, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum

1. Sem hluta af verndarráðstöfunum til að viðhalda tiltækileika, ósvikni, réttleika og leynd gagna skulu aðilar á fjármálamarkaði móta, skjalfesta og innleiða stefnu um kaup, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum. Stefnan skal:

a) greina öryggisverklag og -aðferðafræði sem tengist kaupum, þróun og viðhaldi á upplýsinga- og fjarskiptatæknikerfum,

b) krefjast auðkenningar á:

   i. tækniforskriftum og upplýsinga- og fjarskiptatækniforskriftum, eins og skilgreint er í 4. og 5. lið 2. gr. reglugerðar (ESB) nr. 1025/2012,

   ii. kröfum sem tengjast kaupum, þróun og viðhaldi upplýsinga- og fjarskiptatæknikerfa, með sérstakri áherslu á öryggiskröfur í upplýsinga- og fjarskiptatækni og samþykki viðkomandi viðskiptastarfsemi og eiganda upplýsinga- og fjarskiptatæknieignar á þeim í samræmi við innra fyrirkomulag stjórnarhátta aðila á fjármálamarkaði,

c) tilgreina ráðstafanir til að draga úr hættu á óviljandi breytingum eða vísvitandi misnotkun á upplýsinga- og fjarskiptatæknikerfum við þróun, viðhald og uppsetningu þessara upplýsinga- og fjarskiptatæknikerfa í raunumhverfi.

2. Aðilar á fjármálamarkaði skulu þróa, skjalfesta og innleiða verklagsreglur við kaup, þróun og viðhald upplýsinga- og fjarskiptatæknikerfa til að prófa og samþykkja öll upplýsinga- og fjarskiptatæknikerfi áður en þau eru tekin í notkun og eftir viðhald, í samræmi við v., vi. og vii. lið b-liðar 2. mgr. 8. gr. Stig prófunar skal vera í réttu hlutfalli við mikilvægi viðkomandi viðskiptaferla og upplýsinga- og fjarskiptatæknieigna. Prófunin skal hönnuð til að sannreyna að nýju upplýsinga- og fjarskiptatæknikerfin séu fullnægjandi til að virka eins og til er ætlast, þ.m.t. gæði þess hugbúnaðar sem þróaður er innanhúss.

Miðlægir mótaðilar skulu, auk krafnanna sem mælt er fyrir um í fyrstu undirgrein og eins og við á, hafa eftirfarandi aðila með í hönnun og framkvæmd prófunarinnar sem um getur í fyrstu undirgrein:

a) stöðustofnunaraðila og viðskiptavini,

b) samvirkandi miðlæga mótaðila,

c) aðra hagsmunaaðila.

Verðbréfamiðstöðvar skulu, auk krafnanna sem mælt er fyrir um í fyrstu undirgrein og, eins og við á, hafa eftirfarandi aðila með í hönnun og framkvæmd prófunarinnar sem um getur í fyrstu undirgrein:

a) notendur,

b) veitendur nauðsynlegra nytjahluta og nauðsynlegrar þjónustu,

c) aðrar verðbréfamiðstöðvar,

d) aðra markaðsinnviði,

e) allar aðrar stofnanir sem verðbréfamiðstöðvar hafa greint innbyrðis hæði við í stefnu sinni um rekstrarsamfellu.

3. Verklagsreglan sem um getur í 2. mgr. skal fela í sér úttektir á frumkóða sem ná yfir bæði kyrrstæðar og virkar prófanir. Prófunin skal fela í sér öryggisprófun á kerfum og forritum sem hafa tengingu við internetið í samræmi við v., vi. og vii. lið 2. mgr. 8. gr. Aðilar á fjármálamarkaði skulu:

a) bera kennsl á og greina veikleika og frávik í frumkóðanum,

b) innleiða aðgerðaáætlun til að taka á þessum veikleikum og frávikum,

c) vakta innleiðingu aðgerðaáætlunarinnar.

4. Verklagsreglan sem um getur í 2. mgr. skal fela í sér öryggisprófun hugbúnaðarpakka eigi síðar en í samþættingarfasanum, í samræmi við v., vi. og vii. lið b-liðar 2. mgr. 8. gr.

5. Verklagsreglan sem um getur í 2. mgr. skal kveða á um að:

a) annað umhverfi en raunumhverfi geymi eingöngu framleiðslugögn sem eru nafnlaus, dulnefnd eða valin af handahófi,

b) aðilum á fjármálamarkaði skulu vernda réttleika og leynd gagna í umhverfi sem ekki er raunumhverfi.

6. Þrátt fyrir ákvæði 5. mgr. getur verklagsreglan sem um getur í 2. mgr. kveðið á um að framleiðslugögn séu aðeins geymd fyrir tilteknar prófanir, í takmarkaðan tíma og að fengnu samþykki viðkomandi starfssviðs og skýrslugjöf um prófanirnar til áhættustýringareiningar í upplýsinga- og fjarskiptatækni.

7. Verklagsreglan sem um getur í 2. mgr. skal fela í sér innleiðingu stýringa til að vernda heilleika frumkóða upplýsinga- og fjarskiptatæknikerfa sem eru þróuð innanhúss eða af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og afhentur er aðilanum á fjármálamarkaði af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

8. Verklagsreglan sem um getur í 2. mgr. skal kveða á um að greina eigi einkaleyfisbundinn hugbúnað og, ef unnt er, frumkóða frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða úr opnum hugbúnaðarverkefnum, og prófa hann í samræmi við 3. mgr. áður en hann er tekinn til notkunar í raunumhverfinu.

9. Ákvæði 1. til 8. mgr. þessarar greinar skulu einnig gilda um upplýsinga- og fjarskiptatæknikerfi sem eru þróuð eða stjórnað af notendum utan upplýsinga- og fjarskiptatæknieiningar, með áhættumiðaðri nálgun.

17. gr.

Breytingastjórnun í upplýsinga- og fjarskiptatækni

1. Sem hluta af verndarráðstöfunum til að varðveita tiltækileika, ósvikni, réttleika og leynd gagna, skulu aðilar á fjármálamarkaði taka inn í verklagsreglur um breytingastjórnun í upplýsinga- og fjarskiptatækni, sem um getur í e-lið 4. mgr. 9. gr. reglugerðar (ESB) 2022/2554, að því er varðar allar breytingar á hugbúnaði, vélbúnaði, fastbúnaðarhlutum, kerfum eða öryggisstillingum, alla eftirfarandi þætti:

a) sannprófun á því hvort öryggiskröfur í upplýsinga- og fjarskiptatækni hafi verið uppfylltar,

b) fyrirkomulag til að tryggja sjálfstæði þeirra eininga sem samþykkja breytingar og þeirra eininga sem bera ábyrgð á því að biðja um og innleiða breytingarnar,

c) skýra lýsingu á hlutverkum og ábyrgðarsviðum til að tryggja:

   i. að breytingar séu skilgreindar og áætlaðar,

   ii. að hannað sé viðeigandi umbreytingarferli,

   iii. að breytingarnar séu prófaðar og þeim lokið á stýrðan hátt,

   iv. að gæðatrygging sé skilvirk,

d) skjalfestingu og miðlun upplýsinga um þau atriði sem breytt, þ.m.t.:

   i. tilgangi og umfangi breytingar,

   ii. tímalínu fyrir innleiðingu breytingar,

   iii. væntanlegum niðurstöðum,

e) auðkenningu á varaaðferðum og skyldum, þ.m.t. verklagsreglum og ábyrgð á að hætta við breytingar eða endurreisn eftir breytingar ef innleiðing þeirra tekst ekki,

f) verklagsreglur, samskiptareglur og verkfæri til að stjórna neyðarbreytingum sem veita fullnægjandi verndarráðstafanir,

g) verklagsreglur til að skjalfesta, endurmeta, meta og samþykkja neyðarbreytingar eftir innleiðingu þeirra, þ.m.t. bráðabirgðalausnir og bætur,

h) auðkenningu á hugsanlegum áhrifum breytinga á núverandi öryggisráðstafanir í upplýsinga- og fjarskiptatækni og mat á því hvort slíkar breytingar krefjist þess að frekari öryggisráðstafanir í upplýsinga- og fjarskiptatækni séu teknar upp.

2. Þegar miðlægir mótaðilar og verðbréfamiðstöðvar hafa gert umtalsverðar breytingar á upplýsinga- og fjarskiptatæknikerfum sínum, skulu þær beita upplýsinga- og fjarskiptatæknikerfi sín ströngum prófunum með því að herma eftir álagsaðstæðum.

Miðlægir mótaðilar skulu, eins og við á, hafa eftirfarandi aðila með í hönnun og framkvæmd prófunarinnar sem um getur í fyrstu undirgrein:

a) stöðustofnunaraðila og viðskiptavini,

b) samvirkandi miðlæga mótaðila,

c) aðra hagsmunaaðila.

Verðbréfamiðstöðvar skulu, eins og við á, hafa eftirfarandi aðila með í hönnun og framkvæmd prófunarinnar sem um getur í fyrstu undirgrein:

a) notendur,

b) veitendur nauðsynlegra nytjahluta og nauðsynlegrar þjónustu,

c) aðrar verðbréfamiðstöðvar,

d) aðra markaðsinnviði,

e) allar aðrar stofnanir sem verðbréfamiðstöðvar hafa greint innbyrðis hæði við í stefnu sinni um rekstrarsamfellu í upplýsinga- og fjarskiptatækni.

8. þáttur

18. gr.

Raunlægt og umhverfislegt öryggi

1. Sem hluta af verndarráðstöfunum til að varðveita tiltækileika, ósvikni, réttleika og leynd gagna skulu aðilar á fjármálamarkaði skilgreina, skjalfesta og innleiða stefnu um raunlægt og umhverfislegt öryggi. Aðilar á fjármálamarkaði skulu hanna stefnuna út frá netógnalandslaginu, í samræmi við flokkunina sem komið er á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554, og í ljósi heildaráhættusniðs upplýsinga- og fjarskiptatæknieigna og aðgengilegra upplýsingaeigna.

2. Stefnan um raunlægt og umhverfislegt öryggi, sem um getur í 1. mgr., skal fela í sér allt eftirfarandi:

a) tilvísun í þætti stefnunnar um stýringar aðgangsstjórnunarréttinda sem um getur í g-lið fyrstu málsgreinar 21. gr.,

b) ráðstafanir til að vernda athafnasvæði og gagnaver aðila á fjármálamarkaði og viðkvæm svæði sem aðili á fjármálamarkaði tilgreinir, þar sem upplýsinga- og fjarskiptatæknieignir og upplýsingaeignir eru staðsettar, fyrir árásum, slysum og umhverfislegum ógnum og hættum,

c) ráðstafanir til að tryggja upplýsinga- og fjarskiptatæknieignir, bæði innan og utan athafnasvæðis aðila á fjármálamarkaði, að teknu tilliti til niðurstaðna upplýsinga- og fjarskiptatækniáhættumats í tengslum við viðkomandi upplýsinga- og fjarskiptatæknieignir,

d) ráðstafanir til að tryggja tiltækileika, ósvikni, réttleika og leynd upplýsinga- og fjarskiptatæknieigna, upplýsingaeigna og búnaðar aðila á fjármálamarkaði til stýringar á raunlægum aðgangi með viðeigandi viðhaldi,

e) ráðstafanir til að varðveita tiltækileika, ósvikni, réttleika og leynd gagna, þ.m.t.:

   i. stefnu um hreint skrifborð af pappírum,

   ii. stefnu um hreinan skjá í upplýsingavinnslubúnaði.

Að því er b-lið varðar skulu ráðstafanir til að verjast umhverfislegum ógnum og hættum vera í réttu hlutfalli við mikilvægi athafnasvæðis, gagnavera, viðkvæmra, tilgreindra svæða og hversu mikilvægur reksturinn eða upplýsinga- og fjarskiptatæknikerfin, sem þar er að finna, eru.

Að því er c-lið varðar skal stefnan um raunlægt og umhverfislegt öryggi, sem um getur í 1. mgr., fela í sér ráðstafanir til að veita viðeigandi vernd fyrir eftirlitslausar upplýsinga- og fjarskiptatæknieignir.

II. KAFLI

Mannauðsstefna og aðgangsstýring

19. gr.

Mannauðsstefna

Aðilar á fjármálamarkaði skulu hafa í mannauðsstefnu sinni, eða öðrum viðeigandi stefnum, alla eftirfarandi þætti í tengslum við upplýsinga- og fjarskiptatækniöryggi:

a) auðkenningu og úthlutun á öllum sérstökum skyldum er varða upplýsinga- og fjarskiptatækniöryggi,

b) kröfur til starfsfólks aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem nota eða hafa aðgang að upplýsinga- og fjarskiptatæknieignum aðila á fjármálamarkaði um að:

i. vera upplýstir um, og fylgja, stefnum, verklagsreglum og samskiptareglum fyrir öryggi í upplýsinga- og fjarskiptatækni hjá aðilanum á fjármálamarkaði,

ii. vera meðvitað um tilkynningaleiðir sem aðili á fjármálamarkaði hefur komið á til að greina óeðlilega hegðun, þ.m.t., eftir atvikum, þær tilkynningaleiðir sem komið er á fót í samræmi við tilskipun Evrópuþingsins og ráðsins (ESB) 2019/1937 ([11]),

iii. við starfslok skili starfsfólk til aðila á fjármálamarkaði öllum upplýsinga- og fjarskiptatæknieignum og efnislegum upplýsingaeignum í vörslu þeirra sem tilheyra aðila á fjármálamarkaði.

20. gr.

Stjórnun auðkenningar

1. Hluti stýringar aðila á fjármálamarkaði á aðgangsstjórnunarréttindum skal vera að móta, skjalfesta og innleiða stefnur og verklagsreglur um stjórnun auðkenningar sem tryggja einkvæma auðkenningu og sannvottun einstaklinga og kerfa sem hafa aðgang að upplýsingum aðila á fjármálamarkaði til að hægt sé að veita aðgangsréttindi notenda í samræmi við 21. gr.

2. Stefnurnar og verklagsreglurnar um stjórnun auðkenningar, sem um getur í 1. mgr., skulu fela í sér allt eftirfarandi:

a) með fyrirvara um c-lið fyrstu málsgreinar 21. gr., skal hverjum starfsmanni aðila á fjármálamarkaði eða starfsfólki þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem hafa aðgang að upplýsingaeignum og upplýsinga- og fjarskiptatæknieignum aðilans á fjármálamarkaði, úthlutað einkvæmu auðkenni sem samsvarar einkvæmum notandareikningi,

b) ferli fyrir stjórnun á endingarskeiði auðkenna og aðgangsreikninga, sem stjórnar stofnun, breytingu, endurskoðun og uppfærslu, tímabundinni afvirkjun og lokun allra reikninga.

Að því er varðar a-lið skulu aðilar á fjármálamarkaði halda skrár yfir allar úthlutanir auðkenna. Þessar skrár skulu geymdar í kjölfar endurskipulagningar aðila á fjármálamarkaði eða eftir lok samningssambands, án þess að það hafi áhrif á kröfur um varðveislu sem kveðið er á um í gildandi lögum Sambandsins og landslögum.

Að því er varðar b-lið skulu aðilar á fjármálamarkaði, ef það er gerlegt og viðeigandi, innleiða sjálfvirkar lausnir fyrir stjórnun á endingarskeiði auðkenna.

21. gr.

Aðgangsstýring

Hluti stýringar aðila á fjármálamarkaði á aðgangsstjórnunarréttindum skal vera að móta, skjalfesta og innleiða stefnu sem felur í sér allt eftirfarandi:

a) veiting aðgangsréttinda að upplýsinga- og fjarskiptatæknieignum samkvæmt meginreglunum um vitneskjuþörf, notkunarþörf og lágmarksaðgangsheimildir, þ.m.t. fyrir fjar- og neyðaraðgang,

b) aðgreiningu starfa, sem ætlað er að koma í veg fyrir óréttmætan aðgang að nauðsynlegum gögnum eða að koma í veg fyrir að veitt sé samsetning aðgangsréttinda sem hægt er að nota til að komast framhjá stýringum,

c) ákvæði um notandaábyrgð, með því að takmarka notkun á almennum og sameiginlegum notandareikningum að því marki sem hægt er og tryggja að notendur séu ávallt persónugreinanlegir með tilliti til aðgerða sem gerðar eru í upplýsinga- og fjarskiptatæknikerfum,

([11]) Tilskipun Evrópuþingsins og ráðsins (ESB) 2019/1937 frá 23. október 2019 um verndun þeirra sem tilkynna um brot á lögum Sambandsins (Stjtíð. ESB L 305, 26.11.2019, bls. 17, ELI: http://data.europa.eu/eli/dir/2019/1937/oj).

d) ákvæði um takmörkun aðgangs að upplýsinga- og fjarskiptatæknieignum, þar sem tilgreindar eru stýringar og verkfæri til að koma í veg fyrir óheimilan aðgang,

e) verklagsreglur um reikningastjórnun til að veita, breyta eða afturkalla aðgangsréttindi fyrir notandareikninga og almenna reikninga, þ.m.t. almenna stjórnandareikninga, þ.m.t. ákvæði um allt eftirfarandi:

i. úthlutun hlutverka og ábyrgðarsviða við veitingu, endurskoðun og afturköllun aðgangsréttinda,

ii. veitingu forréttinda-, neyðar- og stjórnendaaðgangs samkvæmt notkunarþörf eða eftir þörfum fyrir öll upplýsinga- og fjarskiptatæknikerfi,

iii. tafarlausa afturköllun aðgangsréttar við starfslok eða þegar ekki er lengur þörf á aðgangi,

iv. uppfærslu aðgangsréttinda ef þörf er á breytingum og a.m.k. einu sinni á ári fyrir öll upplýsinga- og fjarskiptatæknikerfi, önnur en upplýsinga- og fjarskiptatæknikerfi sem styðja nauðsynlega eða mikilvæga starfsemi og a.m.k. á 6 mánaða fresti fyrir upplýsinga- og fjarskiptatæknikerfi sem styðja nauðsynlega eða mikilvæga starfsemi,

f) sannvottunaðferðir, þ.m.t. allt eftirfarandi:

i. notkun sannvottunaraðferða sem eru í samræmi við flokkunina, sem komið var á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554, og heildaráhættusnið upplýsinga- og fjarskiptatæknieigna og að teknu tilliti til leiðandi starfsvenja,

ii. notkun sterkra sannvottunaraðferða í samræmi við leiðandi starfsvenjur og aðferðir varðandi fjaraðgang að netkerfi aðilans á fjármálamarkaði, forréttindaaðgang, aðgang að upplýsinga- og fjarskiptatæknieignum sem styðja nauðsynlega eða mikilvæga starfsemi eða upplýsinga- og fjarskiptatæknieignum sem eru aðgengilegar almenningi,

g) ráðstafanir fyrir raunlæga aðgangsstýringu, þ.m.t.:

i. auðkenningu og skráningu einstaklinga sem hafa aðgang að athafnasvæði, gagnaverum og viðkvæmum tilgreindum svæðum þar sem upplýsinga- og fjarskiptatæknieignir og upplýsingaeignir eru til staðar og aðilinn á fjármálamarkaði tilgreinir,

ii. veiting raunlægra aðgangsréttinda að nauðsynlegum upplýsinga- og fjarskiptatæknieignum eingöngu til heimilaðs starfsfólks, í samræmi við meginreglurnar um vitneskjuþörf og lágmarksaðgangsheimildir og eftir þörfum,

iii. vöktun á raunlægum aðgangi að athafnasvæði, gagnaverum og viðkvæmum tilgreindum svæðum sem aðilinn á fjármálamarkaði, þar sem upplýsinga- og fjarskiptatæknieignir og upplýsingaeignir eða hvort tveggja eru til staðar, tilgreinir,

iv. endurskoðun á raunlægum aðgangsrétti til að tryggja að ónauðsynleg aðgangsréttindi séu tafarlaust afturkölluð.

Að því er varðar i. lið e-liðar skulu aðilar á fjármálamarkaði ákvarða varðveislutímann, að teknu tilliti til markmiða viðskipta- og upplýsingaöryggis, ástæðna þess að atburðurinn er skráður í atburðaskrár og niðurstaðna upplýsinga- og fjarskiptatækniáhættumats.

Að því er varðar ii. lið e-liðar skulu aðilar á fjármálamarkaði, þar sem unnt er, nota sértæka aðgangsreikninga til að sinna kerfisstjórnunaraðgerðum í upplýsinga- og fjarskiptatæknikerfum. Ef það er gerlegt og viðeigandi skulu aðilar á fjármálamarkaði nota sjálfvirkar lausnir til að stýra forréttindaaðgangi.

Að því er varðar i. lið g-liðar skal auðkenning og skráning vera í réttu hlutfalli við mikilvægi athafnasvæðis, gagnavera, viðkvæmra tilgreindra svæða og þess hversu nauðsynlegur reksturinn eða upplýsinga- og fjarskiptatæknikerfin sem þar er að finna eru.

Að því er varðar iii. lið g-liðar skal vöktun vera í réttu hlutfalli við þá flokkun, sem komið var á fót í samræmi við 1. mgr. 8. gr. reglugerðar (ESB) 2022/2554, og mikilvægi svæðisins sem aðgangur er að.

III. KAFLI

Greining og viðbrögð við atvikum sem tengjast upplýsinga- og fjarskiptatækni

22. gr.

Atvikastjórnunarstefna sem tengist upplýsinga- og fjarskiptatækni

Sem hluta af fyrirkomulagi til að greina óvenjulegar athafnir, þ.m.t. vandamál sem varða frammistöðu upplýsinga- og fjarskiptatækninets og atvik sem tengjast upplýsinga- og fjarskiptatækni, skulu aðilar á fjármálamarkaði móta, skjalfesta og innleiða stefnu um atvik sem tengist upplýsinga- og fjarskiptatækni, en samkvæmt henni skulu þeir:

a) skjalfesta ferli atvikastjórnunar sem tengist upplýsinga- og fjarskiptatækni, sem um getur í 17. gr. reglugerðar (ESB) 2022/2554,

b) koma á fót skrá yfir viðeigandi tengiliði með innri hlutverk og ytri hagsmunaaðila sem koma beint að öryggi í upplýsinga- og fjarskiptatæknirekstri, þ.m.t. um:

   i. greiningu og eftirlit með netógnum,

   ii. greiningu á óvenjulegum athöfnum,

   iii. veikleikastýringu,

c) koma á fót, innleiða og reka tæknilegt, skipulagslegt og rekstrarlegt fyrirkomulag til að styðja atvikastjórnunarferli sem tengist upplýsinga- og fjarskiptatækni, þ.m.t. fyrirkomulag til að greina fljótt óvenjulegar athafnir og hegðun í samræmi við 23. gr. þessarar reglugerðar,

d) varðveita öll sönnunargögn í tengslum við atvik sem tengjast upplýsinga- og fjarskiptatækni eins lengi en ekki lengur en nauðsyn krefur miðað við í hvaða tilgangi gögnunum er safnað, í réttu hlutfalli við mikilvægi þeirrar starfsemi, stuðningsferla og upplýsinga- og fjarskiptatæknieigna og upplýsingaeigna sem verða fyrir áhrifum, í samræmi við 2. mgr. 8. gr. framseldrar reglugerðar framkvæmdastjórnarinnar (ESB) 2024/1772 ([12]) og við allar gildandi kröfur um varðveislu samkvæmt lögum Sambandsins,

e) koma á fót og innleiða fyrirkomulag til að greina veruleg eða endurtekin atvik sem tengjast upplýsinga- og fjarskiptatækni og mynstur í fjölda og tíðni atvika sem tengjast upplýsinga- og fjarskiptatækni.

Að því er d-lið varðar skulu aðilar á fjármálamarkaði halda eftir sönnunargögnunum sem um getur í þeim lið á öruggan hátt.

23. gr.

Greining á óvenjulegum athöfnum og viðmiðunum til að greina og bregðast við atvikum sem tengjast upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu fastsetja skýr hlutverk og ábyrgðarsvið til að greina og bregðast við atvikum sem tengjast upplýsinga- og fjarskiptatækni og óvenjulegum athöfnum á skilvirkan hátt.

2. Fyrirkomulagið til að greina fljótt óvenjulegar athafnir, þ.m.t. vandamál sem varða frammistöðu upplýsinga- og fjarskiptatækninets og atvik sem tengjast upplýsinga- og fjarskiptatækni, eins og um getur í 1. mgr. 10. gr. reglugerðar (ESB) 2022/2554, skal gera aðilum á fjármálamarkaði kleift að:

a) safna, vakta og greina allt eftirfarandi:

   i. innri og ytri þætti, þ.m.t. a.m.k. þær aðgerðarskráningar sem er safnað í samræmi við 12. gr. þessarar reglugerðar, upplýsingar úr starfsemi og upplýsinga- og fjarskiptatæknieiningu, og hvers kyns vandamál sem notendur aðila á fjármálamarkaði tilkynna,

([12]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1772 frá 13. mars 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina viðmið fyrir flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum, setja fram mikilvægismörk og tilgreina nánari upplýsingar um tilkynningar um alvarleg atvik (Stjtíð. ESB L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

ii. mögulegar innri og ytri netógnir, að teknu tilliti til sviðsmynda sem ógnvaldar nota gjarnan og sviðsmynda sem byggjast á ógnargreiningum,

iii. tilkynningu um atvik sem tengist upplýsinga- og fjarskiptatækni frá þriðja aðila sem veitir aðila á fjármálamarkaði upplýsinga- og fjarskiptatækniþjónustu, sem greinist í upplýsinga- og fjarskiptatæknikerfum og -netkerfum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og getur haft áhrif á aðilann á fjármálamarkaði,

b) bera kennsl á óvenjulegar athafnir og hegðun og innleiða verkfæri sem búa til viðvaranir um óvenjulegar athafnir og hegðun, a.m.k. fyrir upplýsinga- og fjarskiptatæknieignir og upplýsingaeignir sem styðja nauðsynlega eða mikilvæga starfsemi,

c) forgangsraða viðvörununum sem um getur í b-lið til að gera kleift að meðhöndla greind atvik sem tengjast upplýsinga- og fjarskiptatækni innan áætlaðs lausnartíma, eins og aðilar á fjármálamarkaði tilgreina, bæði á vinnutíma og utan hans,

d) skrá, greina og leggja mat á hvers kyns viðeigandi upplýsingar um allar óvenjulegar athafnir og hegðun á sjálfvirkan eða handvirkan hátt.

Að því er b-lið varðar skulu verkfærin sem um getur í þeim lið innihalda þau verkfæri sem veita sjálfvirkar viðvaranir á grundvelli fyrirframskilgreindra reglna til að greina frávik sem hafa áhrif á heilleika og réttleika gagnalinda eða aðgerðaskráningar.

3. Aðilar á fjármálamarkaði skulu vernda allar skráningar á óvenjulegum athöfnum gegn óheimilum breytingum og óheimilum aðgangi að gögnum sem eru í dvala, flutningi og, þar sem við á, í notkun.

4. Aðilar á fjármálamarkaði skulu skrá allar viðeigandi upplýsingar um sérhverja óvenjulega athöfn sem greinist, sem gerir kleift að:

a) greina dagsetningu og tíma þegar óvenjuleg athöfn á sér stað,

b) greina dagsetningu og tíma þegar óvenjuleg athöfn greinist,

c) greina tegund óvenjulegrar athafnar.

5. Aðilar á fjármálamarkaði skulu taka tillit til allra eftirfarandi viðmiðana til virkjunar greiningar- og viðbragðsferla vegna atvika sem tengjast upplýsinga- og fjarskiptatækni sem um getur í 2. mgr. 10. gr. reglugerðar (ESB) 2022/2554:

a) vísbendinga um að aðgerðir kunni að hafa verið framkvæmdar af illum ásetningi í upplýsinga- og fjarskiptatæknikerfi eða -netkerfi eða að slíku upplýsinga- og fjarskiptatæknikerfi eða -netkerfi gæti hafa verið stofnað í hættu,

b) gagnataps sem greinist í tengslum við tiltækileika, ósvikni, réttleika og leynd gagna,

c) greindra neikvæða áhrifa á viðskipti og rekstur aðila á fjármálamarkaði,

d) ef upplýsinga- og fjarskiptatæknikerfi og -netkerfi eru ekki tiltæk.

6. Að því er 5. mgr. varðar skulu aðilar á fjármálamarkaði einnig taka tillit til mikilvægis viðkomandi þjónustu.

IV. KAFLI

Stjórnun rekstrarsamfellu í upplýsinga- og fjarskiptatækni

24. gr.

Efnisþættir stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu hafa allt eftirfarandi með í stefnu sinni um rekstrarsamfellu í upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr. 11. gr. reglugerðar (ESB) 2022/2554:

a) lýsingu á:

i. markmiði stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni, þ.m.t. samspili upplýsinga- og fjarskiptatækni og rekstrarsamfellu í heild sinni, og að teknu tilliti til niðurstaðna rekstraráhrifagreiningarinnar sem um getur í 5. mgr. 11. gr. reglugerðar (ESB) 2022/2554,

ii. umfangi fyrirkomulags, áætlana, verklagsreglna og kerfa til rekstrarsamfellu í upplýsinga- og fjarskiptatækni, þ.m.t. takmarkana og útilokana,

iii. tímarammanum fyrir fyrirkomulag, áætlanir, verklagsreglur og kerfi til rekstrarsamfellu í upplýsinga- og fjarskiptatækni,

iv. viðmiðunum til að virkja og afvirkja áætlanir um rekstrarsamfellu í upplýsinga- og fjarskiptatækni, áætlanir um viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni og áætlanir um krísusamskipti,

b) ákvæði um:

i. stjórnunarhætti og skipulag til að innleiða stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni, þ.m.t. hlutverk, ábyrgðarsvið og verklagsreglur um stigmögnun viðbragða sem tryggja að nægileg tilföng séu til staðar,

ii. samræmingu milli áætlunar um rekstrarsamfellu í upplýsinga- og fjarskiptatækni og heildaráætlunar um rekstrarsamfellu, varðandi a.m.k. allt eftirfarandi:

1) hugsanlegar bilanasviðsmyndir, þ.m.t. sviðsmyndirnar sem um getur í 2. mgr. 26. gr. þessarar reglugerðar,

2) endurreisnarmarkmið sem tilgreina að aðili á fjármálamarkaði skuli geta endurreist rekstur á nauðsynlegri eða mikilvægri starfsemi eftir truflanir innan markmiða um endurreisnartíma og endamark endurreisnar,

iii. þróun áætlana um rekstrarsamfellu vegna alvarlegra truflana á rekstri sem hluti þessara áætlana og forgangsröðun aðgerðar í rekstrarsamfellu í upplýsinga- og fjarskiptatækni með áhættumiðaðri nálgun,

iv. þróun, prófun og endurskoðun á viðbragðs- og endurreisnaráætlunum í upplýsinga- og fjarskiptatækni, í samræmi við 25. og 26. gr. þessarar reglugerðar,

v. endurskoðun á skilvirkni fyrirkomulags, áætlana, verklagsreglna og kerfa sem innleidd hafa verið til rekstrarsamfellu í upplýsinga- og fjarskiptatækni, í samræmi við 26. gr. þessarar reglugerðar,

vi. samræmingu stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni við:

1) samskiptastefnuna sem um getur í 2. mgr. 14. gr. reglugerðar (ESB) 2022/2554,

2) samskipta- og krísusamskiptaaðgerðirnar, sem um getur í e-lið 2. mgr. 11. gr. reglugerðar (ESB) 2022/2554.

2. Auk krafnanna sem um getur í 1. mgr. skulu miðlægir mótaðilar tryggja að stefna þeirra um rekstrarsamfellu í upplýsinga- og fjarskiptatækni:

a) feli í sér hámarks endurreisnartíma nauðsynlegrar starfsemi þeirra, sem er ekki lengri en 2 klukkustundir,

b) taki tillit til ytri tengsla og innbyrðis hæðis fjármálainnviða, þ.m.t. viðskiptavettvanga þar sem miðlægur mótaðili stöðustofnar, verðbréfauppgjörs- og greiðslukerfa og lánastofnana sem miðlægur mótaðili eða tengdur miðlægur mótaðili nota,

c) geri kröfu um að ráðstafanir hafi verið gerðar til að:

i. tryggja samfellu í nauðsynlegri eða mikilvægri starfsemi miðlægs mótaðila á grundvelli áfallasviðsmynda,

ii. viðhalda öðrum vinnslustað sem getur tryggt samfellu allrar nauðsynlegrar eða mikilvægrar starfsemi miðlægs mótaðila nákvæmlega eins og á aðalstaðnum,

iii. viðhalda eða hafa tafarlausan aðgang að varastarfsstöð til að gera starfsfólki kleift að tryggja samfellu þjónustunnar sé aðalstarfsstöðin ekki tiltæk,

iv. meta þörfina fyrir viðbótarvinnslustöðvar, einkum ef fjölbreytni áhættusnióa aðal- og viðbótarstaðarins veitir ekki fullnægjandi vissu fyrir að markmið miðlægs mótaðila um rekstrarsamfellu verði uppfyllt við allar aðstæður.

Að því er a-lið varðar skulu miðlægir mótaðilar ljúka ferlum og greiðslum í lok dags á tilskildum tíma og degi við allar aðstæður.

Að því er i. lið c-liðar varðar skal fyrirkomulag sem um getur í þeim lið snúa að því að nægilegt starfsfólk sé tiltækt, að hámarksniðritíma mikilvægrar starfsemi og varaham (e. *failover*) og endurreisn á öðrum stað.

Að því er ii. lið c-liðar varðar skal hinn vinnslustaðurinn sem um getur í þeim lið hafa landfræðilegt áhættusnið sem er frábrugðið áhættusniði aðalvinnslustaðarins.

3. Auk krafnanna sem um getur í 1. mgr. skulu verðbréfamiðstöðvar tryggja að stefna þeirra um rekstrarsamfellu í upplýsinga- og fjarskiptatækni:

a) taki tillit til hvers kyns tengsla og innbyrðis hæðis við notendur, veitendur nauðsynlegra nytjahluta og veitendur nauðsynlegrar þjónustu, aðrar verðbréfamiðstöðvar og aðra markaðsinnviði,

b) geri kröfu um að fyrirkomulag um rekstrarsamfellu í upplýsinga- og fjarskiptatækni tryggi að markmið um endurreisnartíma fyrir nauðsynlega eða mikilvæga starfsemi skuli ekki vera lengri en 2 tímar.

4. Auk krafnanna sem um getur í 1. mgr. skulu viðskiptavettvangar tryggja að stefna þeirra um rekstrarsamfellu í upplýsinga- og fjarskiptatækni tryggi að:

a) viðskipti geta hafist aftur innan eða nálægt 2 tímum eftir atvik sem veldur truflun,

b) hámarksmagn gagna sem kann að tapast úr upplýsingatækniþjónustu viðskiptavettvangs eftir atvik sem veldur truflun sé nálægt núlli.

25. gr.

Prófun áætlana um rekstrarsamfellu í upplýsinga- og fjarskiptatækni

1. Við prófun á áætlunum um rekstrarsamfellu í upplýsinga- og fjarskiptatækni í samræmi við 6. mgr. 11. gr. reglugerðar (ESB) 2022/2554 skulu aðilar á fjármálamarkaði taka tillit til rekstraráhrifagreiningar aðila á fjármálamarkaði og upplýsinga- og fjarskiptatækniáhættumatsins sem um getur í b-lið 1. mgr. 3. gr. þessarar reglugerðar.

2. Aðilar á fjármálamarkaði skulu meta með prófunum á áætlunum um rekstrarsamfellu, sem um getur í 1. mgr., hvort þeir geti tryggt samfellu í nauðsynlegri eða mikilvægri starfsemi aðila á fjármálamarkaði. Prófunin skal:

a) framkvæmd á grundvelli prófunarsviðsmynda sem líkja eftir hugsanlegum truflunum, þ.m.t. fullnægjandi hóps alvarlegra en trúverðugra sviðsmynda,

b) fela í sér prófun á upplýsinga- og fjarskiptatækniþjónustu frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, eftir atvikum,

c) fyrir aðila á fjármálamarkaði, aðra en örfyrirtæki, eins og um getur í annarri undirgrein 6. mgr. 11. gr. reglugerðar (ESB) 2022/2554, innihalda sviðsmyndir tilfærslu frá aðalinnviðum upplýsinga- og fjarskiptatækni yfir á varainnviði, öryggisafrit og varakerfi,

d) vera hönnuð til að reyna á þær forsendur sem áætlanir um rekstrarsamfellu byggjast á, þ.m.t. fyrirkomulag stjórnarhátta og krísusamskiptaáætlanir,

e) fela í sér verklagsreglur til að sannprófa getu starfsfólks aðila á fjármálamarkaði, þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, upplýsinga- og fjarskiptatæknikerfa og upplýsinga- og fjarskiptatækniþjónustu til að bregðast með fullnægjandi við þeim sviðsmyndum sem tekið hefur verið tillit til, í samræmi við 2. mgr. 26. gr.

Að því er a-lið varðar skulu aðilar á fjármálamarkaði ávallt taka með í prófunum þær sviðsmyndir sem teknar voru til skoðunar við gerð áætlananna um rekstrarsamfellu.

Að því er b-lið varðar skulu aðilar á fjármálamarkaði taka tilhlýðilegt tilliti til sviðsmynda í tengslum við ógjaldfærni eða misbrests þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu eða sviðsmynda sem tengjast pólitískri áhættu í lögsagnarumdæmum þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, þar sem við á.

Að því er varðar c-lið skal prófunin sannprófa hvort hægt sé að reka a.m.k. nauðsynlega eða mikilvæga starfsemi á viðeigandi hátt í nægilega langan tíma og hvort hægt sé að endurheimta eðlilega virkni.

3. Auk krafnanna sem um getur í 2. mgr. skulu miðlægir mótaðilar hafa með í prófun á áætlunum sínum um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem um getur í 1. mgr.:

a) stöðustofnunaraðila,

b) utanaðkomandi þjónustuveitendur,

c) viðeigandi stofnanir í fjármálainnviðum sem miðlægir mótaðilar hafa greint innbyrðis hæði við í stefnum sínum um rekstrarsamfellu.

4. Auk krafnanna sem um getur í 2. mgr. skulu verðbréfamiðstöðvar hafa með í prófun á áætlunum sínum um rekstrarsamfellu, sem um getur í 1. mgr., eins og við á:

a) notendur verðbréfamiðstöðva,

b) veitendur nauðsynlegra nytjahluta og nauðsynlegrar þjónustu,

c) aðrar verðbréfamiðstöðvar,

d) aðra markaðsinnviði,

e) allar aðrar stofnanir sem verðbréfamiðstöðvar hafa greint innbyrðis hæði við í stefnu sinni um rekstrarsamfellu.

5. Aðilar á fjármálamarkaði skulu skjalfesta niðurstöður prófunarinnar sem um getur í 1. mgr. Allir tilgreindir annmarkar sem koma í ljós vegna þessarar prófunar skulu greindir, tekið á þeim og þeir tilkynntir til stjórnar og/eða framkvæmdastjórnar.

26. gr.

Viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni

1. Við gerð þeirra viðbragðs- og endurreisnaráætlana í upplýsinga- og fjarskiptatækni, sem um getur í 3. mgr. 11. gr. reglugerðar (ESB) 2022/2554, skulu aðilar á fjármálamarkaði taka mið af niðurstöðum úr rekstraráhrifagreiningu aðila á fjármálamarkaði. Þessar viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni skulu:

a) tilgreina skilyrðin fyrir virkjun þeirra eða afvirkjun og allar undantekningar frá slíkri virkjun eða afvirkjun,

b) lýsa því hvaða ráðstafanir þarf að gera til að tryggja tiltækileika, réttleika, samfellu og endurreisn á a.m.k. upplýsinga- og fjarskiptatæknikerfum og -þjónustu sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði,

c) vera hannaðar til að uppfylla endurreisnarmarkmið í starfsemi aðila á fjármálamarkaði,

d) vera skjalfestar og gerðar aðgengilegar starfsfólki sem tekur þátt í framkvæmd viðbragðs- og endurreisnaráætlana upplýsinga- og fjarskiptatækni og vera aðgengilegar í neyðartilvikum,

e) kveða á um endurreisnarvalkosti til bæði skemmri og lengri tíma, þ.m.t. endurreisn kerfa að hluta,

f) mæla fyrir um markmið viðbragðs- og endurreisnaráætlana í upplýsinga- og fjarskiptatækni og skilyrðin fyrir að lýsa því yfir að framkvæmd áætlananna hafi heppnast vel.

Að því er d-lið varðar skulu aðilar á fjármálamarkaði skilgreina hlutverk og ábyrgðarsvið með skýrum hætti.

2. Viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. skulu auðkenna viðeigandi sviðsmyndir, þ.m.t. sviðsmyndir yfir meiriháttar rekstrartruflanir og auknar líkur á að truflun eigi sér stað. Þessar áætlanir skulu útfæra sviðsmyndir sem byggjast á núverandi upplýsingum um ógnir og lærdómi sem dreginn er af fyrri tilvikum rekstrartruflana. Aðilar á fjármálamarkaði skulu taka tilhlýðilegt tillit til allra eftirfarandi sviðsmynda:

a) netárása og tilfærslu milli aðalinnviða upplýsinga- og fjarskiptatækni og varainnviða, öryggisafrita og varakerfa,

b) sviðsmynda þar sem gæði í veitingu 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,

c) bilana að hluta eða allsherjarbilana á athafnasvæði, þ.m.t. í skrifstofu- og viðskiptahúsnæði og gagnaverum,

d) umtalsverðra bilana á upplýsinga- og fjarskiptatæknieignum eða samskiptainnviðum,

e) skorts á nauðsynlegum fjölda starfsfólks eða starfsmanna sem hafa umsjón með því að tryggja samfellu rekstrar,

f) áhrifa loftslagsbreytinga og atburða sem tengjast hnignun umhverfisins, náttúruhamfara, heimsfaraldurs og raunlægra árása, þ.m.t. innbrota og hryðjuverkaárása,

g) árás frá innherja,

h) pólitísks og félagslegs óstöðugleika, þ.m.t., ef við á, í lögsögu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og á staðnum þar sem gögnin er geymd og unnin,

i) víðtæks rafmagnsleysis.

3. Ef aðalendurreisnarráðstafanirnar eru ekki fýsilegar til skamms tíma vegna kostnaðar, áhættu, aðfangastjórnunar eða ófyrirséðra aðstæðna, skal í viðbragðs- og endurreisnaráætlunum í upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr., skoða aðra valkosti.

4. Sem hluta af viðbragðs- og endurreisnaráætlunum í upplýsinga- og fjarskiptatækni, sem um getur í 1. mgr., skulu aðilar á fjármálamarkaði skoða og innleiða samfelluráðstafanir til að draga úr bilunum í þjónustu þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, sem styður nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði.

V. KAFLI

Skýrsla um úttekt á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni

27. gr.

Framsetning og efni skýrslu um úttekt á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu skila skýrslu um úttekt á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem um getur í 5. mgr. 6. gr. reglugerðar (ESB) 2022/2554, á leitarbæru rafrænu formi.

2. Aðilar á fjármálamarkaði skulu hafa allar eftirfarandi upplýsingar með í skýrslunni sem um getur í 1. mgr.:

a) inngangskafla sem:

   i. tilgreinir skýrt þann aðila á fjármálamarkaði sem er viðfangsefni skýrslunnar og lýsir samstæðuskipulagi hans, þar sem við á,

   ii. lýsir samhengi skýrslunnar með tilliti til eðlis, umfangs og flækjustigs þjónustu, starfsemi og reksturs aðila á fjármálamarkaði, skipulagsheildar hans, skilgreindrar nauðsynlegrar starfsemi, stefnuáætlunar, stærri yfirstandandi verkefna eða starfsemi, tengsla og hversu háður hann er innanhúss og aðkeyptri upplýsinga- og fjarskiptatækniþjónustu og -kerfum eða þeirra afleiðinga sem heildartap eða meiriháttar hnignun á slíkum kerfum myndi hafa í för með sér með tilliti til nauðsynlegrar og mikilvægrar starfsemi og skilvirkni markaðar,

   iii. dregur saman meiriháttar breytingar á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni frá því að fyrri skýrslan var lögð fram,

   iv. veitir samantekt á stjórnendastigi á núverandi áhættusniði og skammtímaáhættusniði upplýsinga- og fjarskiptatækniáhættu, landslagi netógna, metinni skilvirkni stýringa þess og stöðu öryggismála hjá aðilanum á fjármálamarkaði,

b) dagsetningu þegar stjórn og/eða framkvæmdastjórn aðila á fjármálamarkaði samþykkti skýrsluna,

c) lýsingu á ástæðu úttektar á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni í samræmi við 5. mgr. 6. gr. reglugerðar (ESB) 2022/2554.,

d) upphafs- og lokadagsetningar úttektartímabils,

e) tilgreiningu á því hvaða starfssvið er ábyrgt fyrir úttektinni,

f) lýsingu á meiriháttar breytingum og endurbótum á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni frá fyrri úttekt,

g) samantekt á niðurstöðum endurskoðunar og ítarlega greiningu og mat á alvarleika veikleika, annmarka og gloppa í áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni á úttektartímabilinu,

h) lýsingu á ráðstöfunum til að taka á greindum veikleikum, annmörkum og gloppum, þ.m.t. öllu eftirfarandi:

   i. samantekt á ráðstöfunum sem gerðar hafa verið til að bæta úr greindum veikleikum, annmörkum og gloppum,

   ii. áætlaðri dagsetningu fyrir innleiðingu ráðstafana og dagsetninga í tengslum við innra eftirlit með innleiðingunni, þ.m.t. upplýsingum um stöðu framvindu innleiðingar á þessum ráðstöfunum á þeim degi sem skýrslan er skrifuð, með skýringu á því, eftir atvikum, hvort hætta sé á því að tímafresti verði ekki mætt,

   iii. verkfærum sem á að nota og tilgreiningu á starfssviði sem er ábyrgt fyrir framkvæmd á ráðstöfunum, þar sem tilgreint er hvort verkfærin og starfssviðin séu innanhúss eða utanhúss,

   iv. lýsingu á áhrifum af fyrirhuguðum breytingum á ráðstöfunum á fjármagn, mannauð og búnað aðila á fjármálamarkaði, þ.m.t. tilfanga sem úthlutað er til innleiðingar á hvers kyns ráðstöfunum til úrbóta,

   v. upplýsingum um ferlið við að upplýsa lögbært yfirvald, eftir því sem við á,

   vi. falli greindir veikleikar, annmarkar eða gloppur ekki undir ráðstafanir til úrbóta, ítarlega útskýringu á viðmiðunum sem notuð eru til að greina áhrif þessara veikleika, annmarka eða gloppa, til að meta tengda eftirstæða upplýsinga- og fjarskiptatækniáhættu, og viðmiðunum sem notuð eru til að samþykkja tengda eftirstæða áhættu,

i) upplýsingar um áætlaða frekari þróun áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni,

j) niðurstöður úr úttektinni á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni,

k) upplýsingar um fyrri úttektir, þ.m.t.:

   i. lista yfir fyrri úttektir hingað til,

   ii. eftir atvikum, stöðu innleiðingar á ráðstöfunum til úrbóta sem síðasta skýrsla tilgreindi,

   iii. ef tillagðar ráðstafanir til úrbóta í fyrri úttektum hafa ekki borið árangur eða leitt til óvæntra áskorana, lýsingu á því hvernig hægt er að betrumbæta þessar ráðstafanir til úrbóta eða á þessum óvæntu áskorunum,

l) upplýsingaveitur sem notaðar eru við undirbúning skýrslu, þ.m.t. allt sem hér fer á eftir:

   i. fyrir aðra aðila á fjármálamarkaði en örfyrirtæki, eins og um getur í 6. mgr. 6. gr. reglugerðar (ESB) 2022/2554, niðurstöður úr innri endurskoðunum,

   ii. niðurstöður úr mati á hlítni,

   iii. niðurstöður prófana á stafrænum rekstrarlegum viðnámsþrótti og, eftir atvikum, niðurstöður úr auknum prófunum, samkvæmt ógnamiðaðri innbrotsprófun, á verkfærum, kerfum og ferlum í upplýsinga- og fjarskiptatækni,

   iv. utanaðkomandi veitur.

Að því er c-lið varðar, ef úttektin var gerð að undangengnum fyrirmælum eftirlitsyfirvalda eða niðurstöðum úr viðeigandi prófun á stafrænum rekstrarlegum viðnámsþrótti eða endurskoðunarferlum, skal skýrslan fela í sér skýrar tilvísanir í slíkar leiðbeiningar eða niðurstöður, sem gerir kleift að greina ástæðu þess að endurskoðun var gerð. Ef úttektin var gerð í kjölfar atvika sem tengjast upplýsinga- og fjarskiptatækni skal skýrslan innihalda lista yfir öll atvik sem tengist upplýsinga- og fjarskiptatækni með greiningu á frumorsök atviks.

Að því er f-lið varðar skal lýsingin fela í sér greiningu á áhrifum breytinganna á stefnuáætlun aðila á fjármálamarkaði um stafrænan rekstrarlegan viðnámsþrótt, innri eftirlitsramma hans í upplýsinga- og fjarskiptatækni og stjórnarháttum áhættustýringar hans í upplýsinga- og fjarskiptatækni.

III. BÁLKUR

EINFALDAÐUR ÁHÆTTUSTÝRINGARRAMMI FYRIR AÐILA Á FJÁRMÁLAMARKAÐI SEM UM GETUR Í 1. MGR. 16. GR. REGLUGERÐAR (ESB) 2022/2554

I. KAFLI

Einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni

28. gr.

Stjórnunarhættir og skipulag

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu hafa til staðar innri stjórnunar- og eftirlitsramma sem tryggir skilvirka og varfærna stjórnun upplýsinga- og fjarskiptatækniáhættu til að ná háu stigi stafræns rekstrarlegs viðnámsþróttar.

2. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu, sem hluta af einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, tryggja að stjórn þeirra og/eða framkvæmdastjórn:

a) beri heildarábyrgð á því að tryggja að einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni geri aðila á fjármálamarkaði kleift að framkvæma viðskiptaáætlun sína í samræmi við áhættuvilja sinn og tryggi að tekið sé tillit til upplýsinga- og fjarskiptatækniáhættu í því samhengi,

b) fastsetji skýr hlutverk og ábyrgð fyrir öll upplýsinga- og fjarskiptatæknitengd verkefni,

c) setji fram markmið um upplýsingaöryggi og upplýsinga- og fjarskiptatæknikröfur,

d) samþykki, hafi eftirlit með og skoði reglulega:

   i. flokkun upplýsingaeigna aðila á fjármálamarkaði, eins og um getur í 1. mgr. 30. gr. þessarar reglugerðar, lista yfir helstu auðkenndu áhætturnar og rekstraráhrifagreiningu og tengdar stefnur,

   ii. áætlanir aðila á fjármálamarkaði um rekstrarsamfellu og viðbragðs- og endurreisnarráðstafanirnar sem um getur í f-lið 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554,

e) úthluti og skoði nauðsynlegar fjárveitingar til að uppfylla þarfir aðilans á fjármálamarkaði fyrir stafrænan rekstrarlegan viðnámsþrótt a.m.k. einu sinni á ári að því er varðar allar tegundir tilfanga, þ.m.t. viðeigandi áætlanir um öryggisvitund í upplýsinga- og fjarskiptatækni og þjálfun í stafrænum rekstrarlegum viðnámsþrótti og færni í upplýsinga- og fjarskiptatækni fyrir allt starfsfólk,

f) tilgreini og innleiði stefnur og ráðstafanir, sem er að finna í I., II. og III. kafla þessa bálks, til að auðkenna, leggja mat á og stýra þeirri upplýsinga- og fjarskiptatækniáhættu sem aðili á fjármálamarkaði er útsettur fyrir,

g) auðkenni og innleiði verklagsreglur, samskiptareglur í upplýsinga- og fjarskiptatækni og verkfæri sem eru nauðsynleg til að vernda allar upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir,

h) tryggi að starfsfólk aðila á fjármálamarkaði viðhaldi nægilegri þekkingu og færni til að skilja og meta upplýsinga- og fjarskiptatækniáhættu og áhrif hennar á starfsemi aðilans á fjármálamarkaði, í samræmi við þá upplýsinga- og fjarskiptatækniáhættu sem er stýrt,

i) komi á fót skýrslugjafarfyrirkomulagi, þ.m.t. tíðni, formi og efni skýrslugjafar til stjórnar og/eða framkvæmdastjórnar um upplýsingaöryggi og stafrænan rekstrarlegan viðnámsþrótt.

3. Þeim aðilum á fjármálamarkaði sem um getur í 1. mgr. er heimilt, í samræmi við lög Sambandsins og landsbundin sérlög, að útvista þeim verkefnum að sannreyna hlítni við kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu innan upplýsinga- og fjarskiptatæknisamstæðu eða til þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Komi til slíkrar útvistunar skulu aðilar á fjármálamarkaði bera áfram fulla ábyrgð á sannprófun á hlítni við kröfur um stýringu upplýsinga- og fjarskiptatækniáhættu.

4. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu tryggja viðeigandi aðskilnað og sjálfstæði eftirlitseininga og innri endurskoðunar.

5. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu tryggja að einfaldaður áhættustýringarrammi þeirra fyrir upplýsinga- og fjarskiptatækni sæti innri endurskoðun hjá endurskoðendum, í samræmi við endurskoðunaráætlun aðila á fjármálamarkaði. Endurskoðendurnir skulu hafa nægilega þekkingu, hæfni og sérþekkingu varðandi upplýsinga- og fjarskiptatækniáhættu og vera sjálfstæðir. Tíðni og áhersla endurskoðana á sviði upplýsinga- og fjarskiptatækni skal vera í réttu hlutfalli við upplýsinga- og fjarskiptatækniáhættu aðila á fjármálamarkaði.

6. Á grundvelli niðurstöðu úr endurskoðuninni sem um getur 5. mgr. skulu þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. tryggja tímanlega sannprófun og úrbætur á alvarlegum niðurstöðum úttekta á upplýsinga- og fjarskiptatækni.

29. gr.

Upplýsingaöryggisstefna og -ráðstafanir

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu móta, skjalfesta og innleiða upplýsingaöryggisstefnu í tengslum við einfaldaðan áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni. Þessi upplýsingaöryggisstefna skal tilgreina ítarlegar meginreglur og reglur sem eru nauðsynlegar til að vernda leynd, réttleika, tiltækileika og ósvikni gagna og þjónustu sem þessir aðilar á fjármálamarkaði veita.

2. Á grundvelli upplýsingaöryggisstefnu þeirra, sem um getur í 1. mgr., skulu þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. koma á fót og innleiða öryggisráðstafanir í upplýsinga- og fjarskiptatækni til að draga úr upplýsinga- og fjarskiptatækniáhættu, þ.m.t. mótvægisaðgerðir sem framkvæmdar eru af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu.

Öryggisráðstafanir í upplýsinga- og fjarskiptatækni skulu innihalda allar ráðstafanirnar sem um getur í 30. til 38. gr.

30. gr.

Flokkun upplýsingaeigna og upplýsinga- og fjarskiptatæknieigna

1. Sem hluti af einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem um getur í a-lið 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554, skulu þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. þeirrar greinar, tilgreina, flokka og skjalfesta alla nauðsynlega eða mikilvæga starfsemi, upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir sem styðja hana og innbyrðis hæði þeirra. Aðilar á fjármálamarkaði skulu endurskoða tilgreininguna og flokkunina eftir þörfum.

2. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu tilgreina alla nauðsynlega eða mikilvæga starfsemi sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu styðja.

31. gr.

Stýring upplýsinga- og fjarskiptatækniáhættu

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu hafa allt eftirfarandi með í einfölduðum áhættustýringarramma sínum fyrir upplýsinga- og fjarskiptatækni:

a) ákvörðun um áhættuþolmörk fyrir upplýsinga- og fjarskiptatækniáhættu, í samræmi við áhættuvilja aðila á fjármálamarkaði,

b) auðkenningu og mat á upplýsinga- og fjarskiptatækniáhættu sem aðili á fjármálamarkaði er útsettur fyrir,

c) nánari lýsingu á mótvægisáætlunum a.m.k. hvað varðar þá upplýsinga- og fjarskiptatækniáhættu sem er ekki innan áhættuþolmarka aðila á fjármálamarkaði,

d) vöktun á skilvirkni þeirra mótvægisáætlana sem um getur í c-lið,

e) greiningu og mat á allri upplýsinga- og fjarskiptatækniáhættu og upplýsingaöryggisáhættu sem stafar af hvers kyns meiriháttar breytingum á upplýsinga- og fjarskiptatæknikerfi eða -þjónustu, -ferlum eða verklagsreglum og niðurstöðum prófunar á upplýsinga- og fjarskiptatækniöryggi og í kjölfar allra meiriháttar atvika sem tengjast upplýsinga- og fjarskiptatækni.

2. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu reglulega framkvæma og skjalfesta upplýsinga- og fjarskiptatækniáhættumat í hlutfalli við áhættusnið upplýsinga- og fjarskiptatækni aðila á fjármálamarkaði.

3. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu hafa stöðugt eftirlit með ógnum og veikleikum sem skipta máli fyrir nauðsynlega eða mikilvæga starfsemi og upplýsingaeignir og upplýsinga- og fjarskiptatæknieignir, og skulu reglulega endurskoða áhættusviðsmyndirnar sem hafa áhrif á þessa nauðsynlega eða mikilvægu starfsemi.

4. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu fastsetja viðvörunarmörk og -viðmiðanir til að virkja og hefja viðbragðsferli vegna atvika sem tengjast upplýsinga- og fjarskiptatækni.

32. gr.

Raunlægt og umhverfislegt öryggi

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu skilgreina og innleiða ráðstafanir fyrir raunlægt öryggi, sem eru hannaðar á grundvelli landslags ógna og í samræmi við flokkunina sem um getur í 1. mgr. 30. gr. þessarar reglugerðar, heildaráhættusnið upplýsinga- og fjarskiptatæknieigna og aðgengilegar upplýsingaeignir.

2. Ráðstafanirnar sem um getur í 1. mgr. skulu vernda athafnasvæði aðila á fjármálamarkaði og, eftir atvikum, gagnaver aðila á fjármálamarkaði þar sem upplýsinga- og fjarskiptatæknieignir og upplýsingaeignir eru staðsettar gegn óheimiluðum aðgangi, árásum og slysum og gegn umhverfislegum ógnum og hættum.

3. Vörn gegn umhverfislegum ógnum og hættum skal vera í réttu hlutfalli við mikilvægi viðkomandi athafnasvæðis og, eftir atvikum, gagnavera og mikilvægis starfseminnar eða upplýsinga- og fjarskiptatæknikerfa sem þar er að finna.

II. KAFLI

Frekari þættir kerfa, samskiptareglna og verkfæra til að lágmarka áhrifin af upplýsinga- og fjarskiptatækniáhættu

33. gr.

Aðgangsstýring

Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu þróa, skjalfesta og innleiða verklagsreglur um röklegar og raunlægar aðgangsstýringar og framfylgja, vakta og endurskoða þessar verklagsreglur reglulega. Verklagsreglurnar skulu innihalda eftirfarandi þætti eftirlits með röklegum og raunlægum aðgangi:

a) aðgangsréttindum að upplýsingaeignum, upplýsinga- og fjarskiptatæknieignum og studdri starfsemi þeirra, og að nauðsynlegum rekstrarstöðum aðila á fjármálamarkaði, er stýrt samkvæmt meginreglunum um þörf fyrir vitneskju, þörf fyrir notkun og lágmarksaðgangsheimildir, þ.m.t. fyrir fjar- og neyðaraðgang,

b) notandaábyrgð, sem tryggir að hægt sé að bera kennsl á notendur fyrir aðgerðir sem gerðar eru í upplýsinga- og fjarskiptatæknikerfunum,

c) reikningsstýringaraðferðir til að veita, breyta eða afturkalla aðgangsréttindi fyrir notandareikninga og almenna reikninga, þ.m.t. almenna stjórnendareikninga,

d) sannvottunaraðferðir sem eru í réttu hlutfalli við flokkunina sem um getur í 1. mgr. 30. gr. og við heildaráhættusnið upplýsinga- og fjarskiptatæknieigna og sem byggjast á leiðandi starfsvenjum,

e) aðgangsréttindi eru yfirfarin reglulega og afturkölluð þegar þeirra er ekki lengur þörf.

Að því er c-lið varðar skal aðili á fjármálamarkaði úthluta forréttinda-, neyðar- og stjórnendaaðgangi samkvæmt þörf á notkun eða eftir þörfum fyrir öll upplýsinga- og fjarskiptatæknikerfi, og skjalfesta í samræmi við f-lið fyrstu málsgreinar 34. mgr.

Að því er varðar d-lið skulu aðilar á fjármálamarkaði nota sterkar sannvottunaraðferðir sem byggjast á leiðandi starfsvenjum fyrir fjaraðgang að netkerfi aðila á fjármálamarkaði, forréttindaaðgang og aðgang að upplýsinga- og fjarskiptatæknieignum sem styðja nauðsynlega eða mikilvæga starfsemi sem er aðgengileg öllum.

34. gr.

Rekstraröryggi upplýsinga- og fjarskiptatækni

Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu, sem hluta af kerfum sínum, samskiptareglum og verkfærum og fyrir allar upplýsinga- og fjarskiptatæknieignir:

a) vakta og stjórna endingarskeiði allra upplýsinga- og fjarskiptatæknieigna,

b) vakta hvort upplýsinga- og fjarskiptatæknieignir séu studdar af þriðju aðilum sem veita upplýsinga- og fjarskiptatækni-þjónustu til aðila á fjármálamarkaði, eftir atvikum,

c) tilgreina þörf á afkastagetu fyrir upplýsinga- og fjarskiptatæknieignir sínar og ráðstafanir til að viðhalda og bæta aðgengi og skilvirkni upplýsinga- og fjarskiptatæknikerfa og koma í veg fyrir skort á upplýsinga- og fjarskiptatæknigetu áður en hann verður,

d) framkvæma sjálfvirka skönnun og mat á veikleikum upplýsinga- og fjarskiptatæknieigna í samræmi við flokkun þeirra, eins og um getur í 1. mgr. 30. gr., og heildaráhættusnið upplýsinga- og fjarskiptatæknieignar, og innleiða bætur til að taka á greindum veikleikum,

e) stýra áhættu sem tengist úreltum eða óstuddum eignum eða forneignum í upplýsinga- og fjarskiptatækni,

f) skrá atburði sem tengjast röklegum og raunlægum aðgangsstýringum, upplýsinga- og fjarskiptatæknirekstri, þ.m.t. kerfisaðgerðir og netumferðaraðgerðir, og breytingastjórnun í upplýsinga- og fjarskiptatækni,

g) skilgreina og innleiða ráðstafanir til að vakta og greina upplýsingar um óvenjulegar athafnir og hegðun vegna nauðsynlegs eða mikilvægs upplýsinga- og fjarskiptatæknireksturs,

h) innleiða ráðstafanir til að vakta viðeigandi og uppfærðar upplýsingar um netógnir,

i) innleiða ráðstafanir til að greina hugsanlegan upplýsingaleka, spillikóða og aðrar öryggisógnir og almennt þekkta veikleika í hugbúnaði og vélbúnaði og athuga með samsvarandi nýjar öryggisuppfærslur.

Að því er f-lið varðar skulu aðilar á fjármálamarkaði aðlaga nákvæmni aðgerðarskráninga að tilgangi þeirra og notkun á upplýsinga- og fjarskiptatæknieigninni sem skilar þessum aðgerðaskrám.

35. gr.

Öryggi gagna, kerfa og netkerfa

Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu, sem hluta af kerfum sínum, samskiptareglum og verkfærum, þróa og innleiða verndarráðstafanir sem tryggja öryggi netkerfa gagnvart innbrotum og gagnamisnotkun og varðveita tiltækileika, ósvikni, réttleika og leynd gagna. Einkum skulu aðilar á fjármálamarkaði, að teknu tilliti til flokkunarinnar sem um getur í 1. mgr. 30. gr. í þessari reglugerð, koma öllu eftirfarandi á fót:

a) skilgreiningu og innleiðingu ráðstafana til að vernda gögn í notkun, flutningi eða dvala,

b) skilgreiningu og innleiðingu öryggisráðstafana varðandi notkun hugbúnaðar, gagnageymslumiðla, kerfa og endabúnaðar sem flytja og geyma gögn aðilans á fjármálamarkaði,

c) skilgreiningu og innleiðingu ráðstafana til að koma í veg fyrir og greina óheimilar tengingar við netkerfi aðilans á fjármálamarkaði og til að tryggja öryggi netumferðar milli innri netkerfa aðilans á fjármálamarkaði og internetsins og annarra ytri tenginga,

d) skilgreiningu og innleiðingu ráðstafana sem tryggja tiltækileika, ósvikni, réttleika og leynd gagna í flutningi innan netkerfa,

e) ferli við örugga eyðingu gagna af athafnasvæði eða sem eru geymd utan þess, sem aðili á fjármálamarkaði þarf ekki lengur að safna eða geyma,

f) ferli við örugga förgun eða úreldingu gagnageymslubúnaðar á athafnasvæði eða gagnageymslubúnaðar sem er geymdur utan þess, sem innihalda trúnaðarupplýsingar,

g) skilgreiningu og innleiðingu ráðstafana til að tryggja að fjarvinnsla og notkun á einkaendabúnaði hafi ekki neikvæð áhrif á getu aðila á fjármálamarkaði til að stunda nauðsynlega starfsemi sína á fullnægjandi, tímanlegan og öruggan hátt.

36. gr.

Öryggisprófun á upplýsinga- og fjarskiptatækni

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu koma á og innleiða áætlun um öryggisprófun á upplýsinga- og fjarskiptatækni til að sannreyna skilvirkni öryggisráðstafana sinna í upplýsinga- og fjarskiptatækni, sem þróaðar eru í samræmi við 33., 34. og 35. gr. og 37. og 38 gr. þessarar reglugerðar. Aðilar á fjármálamarkaði skulu tryggja að áætlunin taki mið af ógnum og veikleikum sem tilgreindir eru sem hluti af einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni, sem um getur í 31. gr. þessarar reglugerðar.

2. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu endurskoða, meta og prófa öryggisráðstafanir í upplýsinga- og fjarskiptatækni, að teknu tilliti til heildaráhættusniðs upplýsinga- og fjarskiptatæknieigna aðila á fjármálamarkaði.

3. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu vakta og meta niðurstöður úr öryggisprófunum og uppfæra öryggisráðstafanir sínar í samræmi við það, án ótilhlýðilegrar tafar ef um er að ræða upplýsinga- og fjarskiptatæknikerfi sem styðja nauðsynlega eða mikilvæga starfsemi.

37. gr.

Kaup, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum

Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu hanna og innleiða, eftir því sem við á, verklagsreglur um kaup, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum með áhættumiðaðri nálgun. Verklagsreglan skal:

a) tryggja að virknikröfur og kröfur sem ekki varða virkni, þ.m.t. kröfur um upplýsingaöryggi, séu settar skýrt fram og samþykktar af viðkomandi starfsemi, áður en nokkur kaup eða þróun á upplýsinga- og fjarskiptatæknikerfum fara fram,

b) tryggja að upplýsinga- og fjarskiptatæknikerfi séu prófuð og samþykkt fyrir fyrstu notkun þeirra og áður en breytingar eru gerðar á raunumhverfi,

c) skilgreina ráðstafanir til að draga úr hættu á óviljandi breytingum eða vísvitandi misnotkun á upplýsinga- og fjarskiptatæknikerfum við þróun og innleiðingu í raunumhverfi.

38. gr.

Verkefnastjórnun og breytingastjórnun í upplýsinga- og fjarskiptatækni

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu þróa, skjalfesta og innleiða verklagsreglur um verkefnastjórnun í upplýsinga- og fjarskiptatækni og tilgreina hlutverk og ábyrgðarsvið sem fylgja innleiðingunni. Verklagsreglurnar skulu ná yfir alla áfanga upplýsinga- og fjarskiptatækniverkefna frá upphafi til enda.

2. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu þróa, skjalfesta og innleiða verklagsreglur um meðhöndlun breytinga í upplýsinga- og fjarskiptatækni til að tryggja að allar breytingar á upplýsinga- og fjarskiptatæknikerfum séu skráðar, prófaðar, metnar, samþykktar, innleiddar og sannprófaðar á stýrðan hátt og með fullnægjandi verndarráðstöfunum til að varðveita stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði.

III. KAFLI

Stjórnun rekstrarsamfellu í upplýsinga- og fjarskiptatækni

39. gr.

Efnisþættir áætlunar um rekstrarsamfellu í upplýsinga- og fjarskiptatækni

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu þróa áætlanir sínar um rekstrarsamfellu með hliðsjón af niðurstöðum greiningar á útsetningu fyrir og hugsanleg áhrif af meiriháttar rekstrartruflunum og sviðsmyndum sem upplýsinga- og fjarskiptatæknieignir þeirra sem styðja nauðsynlega eða mikilvæga starfsemi gætu verið útsettar fyrir, þ.m.t. sviðsmyndir af netárásum.

2. Áætlanirnar um rekstrarsamfellu í upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. skulu:

a) vera samþykktar af stjórn og/eða framkvæmdastjórn aðila á fjármálamarkaði,

b) vera skjalfestar og auðveldlega aðgengilegar ef upp kemur neyðarástand eða krísa,

c) tryggja fullnægjandi tilföng til að hægt sé að framkvæma þær,

d) koma á fót áætluðum endurreisnaráföngum og tímarömmum fyrir endurreisn og endurupptöku á starfsemi og helstu innri og ytri hæðisþáttum, þ.m.t. þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,

e) tilgreina skilyrðin sem gætu leitt til virkjunar á áætlunum um rekstrarsamfellu í upplýsinga- og fjarskiptatækni og til hvaða aðgerða eigi að grípa til að tryggja tiltækileika, samfellu og endurreisn á upplýsinga- og fjarskiptatæknieignum aðila á fjármálamarkaði sem styðja nauðsynlega eða mikilvæga starfsemi,

f) tilgreina ráðstafanir til endurheimtar og endurreisnar á nauðsynlegri eða mikilvægri starfsemi, stuðningsferli, upplýsingaeignir og innbyrðis hæði þeirra til að forðast neikvæð áhrif á starfsemi aðila á fjármálamarkaði,

g) tilgreina verklag og ráðstafanir við öryggisafritun sem skilgreina umfang gagna sem falla undir öryggisafritun og lágmarkstíðni öryggisafritunar, miðað við mikilvægi starfseminnar sem notar gögnin,

h) athuga aðra valkosti ef til þess kæmi að endurreisn væri ekki fýsileg, til skamms tíma litið, vegna kostnaðar, áhættu, aðfangastjórnunar eða ófyrirséðra aðstæðna,

i) skilgreina fyrirkomulag innri og ytri samskipta, þ.m.t. áætlanir um stigmögnun viðbragða,

j) vera uppfærðar í samræmi við þann lærdóm sem hefur verið dreginn af atvikum, prófunum, nýrri áhættu og greindum ógnum, breytt endurreisnarmarkmið, meiriháttar breytingum á skipulagsheild aðila á fjármálamarkaði og upplýsinga- og fjarskiptatæknieignum sem styðja nauðsynlegar eða rekstraraðgerðir.

Að því er f-lið varðar skulu ráðstafanirnar sem um getur í þeim lið draga úr misbrestum hjá nauðsynlegum þriðju aðilum sem veita þjónustu.

40. gr.

Prófun áætlana um rekstrarsamfellu

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu prófa áætlanir sínar um rekstrarsamfellu sem um getur í 39. gr. þessarar reglugerðar, ásamt sviðsmyndunum sem um getur í þeirri grein, a.m.k. einu sinni á ári vegna verklagsreglna við öryggisafritun og endurheimt, eða eftir allar meiriháttar breytingar á áætluninni um rekstrarsamfellu.

2. Prófun á áætlunum um rekstrarsamfellu sem um getur í 1. mgr. skal sýna fram á að þeir aðilar á fjármálamarkaði sem um getur í þeirri málsgrein geti viðhaldið rekstrarhæfi starfsemi sinnar, þar til nauðsynlegum rekstri hefur aftur verið komið á, og greint hvers kyns annmarka á þessum áætlunum.

3. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. skulu skjalfesta niðurstöður prófunar á áætlunum um rekstrarsamfellu og hvers kyns annmarkar sem koma í ljós vegna þessarar prófunar skulu greindir, brugðist við þeim og þeir tilkynntir til stjórnar og/eða framkvæmdastjórnar.

IV. KAFLI

Skýrsla um úttekt á einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni

41. gr.

Framsetning og efni skýrslu um úttekt á einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni

1. Þeir aðilar á fjármálamarkaði sem um getur í 1. mgr. 16. gr. reglugerðar (ESB) 2022/2554 skulu leggja fram skýrsluna um úttekt á þeim áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 2. mgr. þeirrar greinar á leitarbæru rafrænu formi.

2. Skýrslan sem um getur í 1. mgr. skal innihalda allar eftirfarandi upplýsingar:

a) inngangskafla sem veitir:

   i. lýsingu á samhengi skýrslunnar með tilliti til eðlis, umfangs og flækjustigs þjónustu, starfsemi og reksturs aðila á fjármálamarkaði, skipulagsheildar hans, skilgreindrar nauðsynlegrar starfsemi, stefnu, meiriháttar yfirstandandi verkefna eða starfsemi, tengsla og hversu háður hann er innanhúss og útvistaðri upplýsinga- og fjarskiptatækniþjónustu og -kerfum eða þeirra afleiðinga sem heildartap eða meiriháttar hnignun á slíkum kerfum myndi hafa í för með sér á nauðsynlega og mikilvæga starfsemi og skilvirkni markaðar,

   ii. samantekt á stjórnendastigi á greindri núverandi og væntanlegri upplýsinga- og fjarskiptatækniáhættu, landslagi netógna, metinni skilvirkni stýringa og stöðu öryggismála hjá aðilanum á fjármálamarkaði,

   iii. upplýsingar um það svið sem skýrslan fjallar um,

   iv. samantekt á meiriháttar breytingum á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni frá fyrri skýrslu,

   v. samantekt og lýsingu á áhrifum af meiriháttar breytingum á einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni frá fyrri skýrslu,

b) eftir atvikum, dagsetningu þegar stjórn og/eða framkvæmdastjórn aðila á fjármálamarkaði samþykkti skýrsluna,

c) lýsingu á ástæðunum fyrir úttektinni, þ.m.t.:

   i. ef úttektin var gerð að undangengnum fyrirmælum eftirlitsyfirvalda, gögn um slík fyrirmæli,

   ii. ef úttektin var gerð eftir að atvik sem tengjast upplýsinga- og fjarskiptatækni áttu sér stað, lista yfir öll atvik sem tengjast upplýsinga- og fjarskiptatækni með tengdri greiningu á frumorsök,

d) upphafs- og lokadagsetning úttektartímabils,

e) aðilann sem ber ábyrgð á úttektinni,

f) samantekt á niðurstöðum og sjálfsmat á alvarleika veikleika, annmarka og gloppa sem komu fram í áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni fyrir úttektartímabilið, þ.m.t. ítarlega greiningu á þeim,

g) skilgreindar ráðstafanir til að taka á veikleikum, annmörkum og gloppum í einfaldaða áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni og áætlaða dagsetningu til að innleiða ráðstafanirnar, þ.m.t. eftirfylgni með veikleikum, annmörkum og gloppum sem voru tilgreind í fyrri skýrslum, ef ekki hefur enn verið bætt úr þessum veikleikum, annmörkum og gloppum,

h) heildarniðurstöður úr úttekt á einfaldaða áhættustýringarrammanum fyrir upplýsinga- og fjarskiptatækni, þ.m.t. hvers kyns frekari áætlaða þróun.

IV. BÁLKUR

LOKAÁKVÆÐI

42. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 13. mars 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

Fylgiskjal 4.

Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/295

frá 24. október 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla um samræmingu skilyrða sem gera eftirlitsstarfsemi mögulega

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum annarri undirgrein 2. mgr. 41. gr.,

og að teknu tilliti til eftirfarandi:

1) Með rammanum um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann, sem komið er á fót með reglugerð (ESB) 2022/2554 er innleiddur eftirlitsrammi Sambandsins fyrir þriðju aðila sem veita fjármálageiranum upplýsinga- og fjarskiptatækniþjónustu og sem útnefndir eru sem mikilvægir, í samræmi við 31. gr. þeirrar reglugerðar.

2) Þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sem ákveður að leggja að eigin frumkvæði fram beiðni um að verða útnefndur sem mikilvægur ætti að veita Evrópsku eftirlitsstofnuninni (ESA) sem tekur á móti beiðninni allar nauðsynlegar upplýsingar til að sýna fram á mikilvægi sitt samkvæmt meginreglum og viðmiðunum sem settar eru fram í reglugerð (ESB) 2022/2554. Af þessum sökum ættu upplýsingarnar sem skulu vera í umsókn að eigin frumkvæði að vera nægilega ítarlegar og fullgerðar til að stuðla að skýru og fullgerðu mati á mikilvægi skv. 11. mgr. 31. gr. þeirrar reglugerðar. Viðeigandi evrópsk eftirlitsstofnun ætti að hafna öllum ófullgerðum umsóknum og óska eftir upplýsingum sem vantar.

3) Lögmætt auðkenni þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu innan gildissviðs þessa tæknilega eftirlitsstaðals ætti að samræmast auðkenniskóðanum sem settur er fram í framkvæmdarreglugerð framkvæmdastjórnarinnar sem samþykkt var í samræmi við 9. mgr. 28. gr. reglugerðar (ESB) 2022/2554.

4) Til að fylgja eftir tilmælunum sem aðaleftirlitsaðilinn gaf út til mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu ætti aðaleftirlitsaðilinn að vakta hlítni mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu við tilmælin. Með það í huga að tryggja skilvirkt og árangursríkt eftirlit með aðgerðunum sem gripið hefur verið til eða úrræðum sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafa beitt í tengslum við þessi tilmæli, ætti aðaleftirlitsaðili að geta óskað eftir skýrslum sem um getur í c-lið 1. mgr. 35. gr. reglugerðar (ESB) 2022/2554 sem ætti að vera bráðabirgða framvinduskýrslur og lokaskýrslur.

5) Að því er varðar matið sem tilgreint er í 1. mgr. 42. gr. í reglugerð (ESB) 2022/2554, þar sem aðaleftirlitsaðila ber að meta hvort útskýringin sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu veitir er fullnægjandi, ætti tilkynningu mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til aðaleftirlitsaðila um fyrirætlan sína að fylgja mótteknum tilmælum að fylgja lýsing á aðgerðum og ráðstöfunum sem gripið hefur verið til til að draga úr áhættunni sem lýst er í tilmælunum, ásamt viðeigandi frestum. Slík útskýring ætti að vera í formi úrbótaáætlunar.

6) Þar sem vænst er að aðaleftirlitsaðili meti undirverktakasamninga mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu þarf að þróa sniðmát fyrir veitingu upplýsinga um þessa samninga. Sniðmátið ætti að taka tillit til þeirrar staðreyndar að mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu hafa aðra uppbyggingu en aðilar á fjármálamarkaði.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

7) Þegar aðaleftirlitsaðili hefur gefið út tilmæli til mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og lögbær yfirvöld hafa upplýst viðeigandi aðila á fjármálamarkaði um áhættuna sem tilgreind er í þeim tilmælum, ætti aðaleftirlitsaðili að vakta og meta framkvæmd mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu á aðgerðum og úrbótum til að fara að tilmælunum. Lögbær yfirvöld ættu að hafa eftirlit með og meta að hve miklu leyti aðilar á fjármálamarkaði eru í áhættu sem tilgreind er í þessum tilmælum. Með það í huga að viðhalda jafnræðisgrundvelli við framkvæmd verkefna þeirra, einkum þegar áhættan sem tilgreind er í tilmælunum er alvarleg og nær yfir stóran hóp aðila á fjármálamarkaði í mörgum aðildarríkjum, ættu bæði lögbær yfirvöld og aðaleftirlitsaðili að deila sín á milli öllum viðeigandi niðurstöðum sem nauðsynlegar eru til að þau geti sinnt verkefnum sínum. Markmiðið með upplýsingaskiptunum er að tryggja að endurgjöf aðaleftirlitsaðila til mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í tengslum við aðgerðir og úrbætur sem hinn síðarnefndi framkvæmir taki til greina áhrifin á áhættu aðila á fjármálamarkaði og að eftirlitsstarfsemi sem lögbær yfirvöld framkvæma sé með hliðsjón af matinu sem aðaleftirlitsaðili hefur framkvæmt.

8) Til að gera upplýsingaskipti árangursrík og skilvirk ættu lögbær yfirvöld að meta, sem hluta af eftirlitsstarfsemi sinni, að hve miklu leyti aðilar á fjármálamarkaði sem eru undir eftirliti þeirra gætu verið berskjaldaðir fyrir áhættu sem tilgreind er í tilmælunum. Matið ætti að framkvæma með hóflegum og áhættumiðuðum hætti. Aðaleftirlitsaðili ætti að óska eftir því að lögbær yfirvöld deili niðurstöðum þessa mats í sérstökum tilvikum þar sem áhættan í tengslum við tilmælin er alvarleg og nær yfir stóran hóp aðila á fjármálamarkaði í mörgum aðildarríkjum. Til að nýta sem best tilföng lögbærra yfirvalda þegar óskað er eftir niðurstöðum þessa mats, ætti aðaleftirlitsaðilinn ávallt að taka tillit til þess að markmið þessara beiðna er að meta framkvæmd aðgerða og endurbóta mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu.

9) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([2]) og skilaði hún áliti 22. júlí 2024.

10) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem Evrópsku eftirlitsstofnanirnar hafa lagt fyrir framkvæmdastjórnina.

11) Sameiginleg nefnd evrópsku eftirlitsstofnananna hefur haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint mögulegan tengdan kostnað og ávinning og óskað eftir áliti hagsmunahópsins um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([3]), hagsmunahópsins í vátryggingum og endurtryggingum og hagsmunahópsins um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([4]), og hagsmunahópsins á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([5]).

([2]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Upplýsingar sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal veita í umsókn um að vera útnefndur sem mikilvægur

1. Þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal veita eftirfarandi upplýsingar í rökstuddri umsókn að eigin frumkvæði skv. 11. mgr. 31. gr. reglugerðar (ESB) 2022/2554 um að vera útnefndur sem mikilvægur skv. a-lið 1. mgr. 31. gr. reglugerðar (ESB) 2022/2554:

a) heiti lögaðila,

b) auðkenniskóða lögaðila,

c) nafn tengiliðar og samskiptaupplýsingar mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

d) land þar sem lögaðili hefur skráða skrifstofu,

e) lýsingu á fyrirtækjaskipulaginu, þ.m.t. að lágmarki upplýsingar um móðurfélag þess og önnur tengd fyrirtæki sem veita aðilum á fjármálamarkaði í Sambandinu upplýsinga- og fjarskiptatækniþjónustu. Þær upplýsingar skulu innihalda, eftir atvikum:

   i. heiti lögaðila,

   ii. auðkenniskóða lögaðila,

   iii. land þar sem lögaðili hefur skráða skrifstofu,

f) mat á markaðshlutdeild þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu í fjármálageira Sambandsins og mat á markaðshlutdeild hverrar tegundar aðila á fjármálamarkaði eins og um getur í 1. mgr. 2. gr. reglugerðar (ESB) 2022/2554 frá og með árinu þegar umsókn um að vera útnefndur sem mikilvægur er lögð fram og næstliðnu ári fyrir þá umsókn,

g) lýsingu á hverri upplýsinga- og fjarskiptatækniþjónustu sem veitt er aðilum á fjármálamarkaði í Sambandinu, þ.m.t.:

   i. lýsingu á eðli viðskipta og tegund upplýsinga- og fjarskiptatækniþjónustu sem veitt er aðilum á fjármálamarkaði,

   ii. skrá yfir starfsemi aðila á fjármálamarkaði sem veitt upplýsinga- og fjarskiptatækniþjónusta styður við, eftir atvikum,

   iii. upplýsingar um hvort upplýsinga- og fjarskiptatækniþjónusta sem aðilum á fjármálamarkaði er veitt styðji við nauðsynlega eða mikilvæga starfsemi, eftir atvikum,

h) skrá yfir aðila á fjármálamarkaði sem nota upplýsinga- og fjarskiptatækniþjónustu sem veitt er af viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. eftirfarandi upplýsingar fyrir hvern aðila á fjármálamarkaði sem þjónustaður er, eftir atvikum:

   i. heiti lögaðila,

   ii. auðkenniskóði lögaðila, ef þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur vitneskju þar um,

   iii. tegund aðila á fjármálamarkaði sem tilgreindir eru í 1. mgr. 2. gr. reglugerðar (ESB) 2022/2554,

   iv. landfræðileg staðsetning þaðan sem upplýsinga- og fjarskiptatækniþjónusta er veitt þeim sérstaka lögaðila,

i) skrá yfir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem eru í nýjustu útgáfu skrár yfir slíka þjónustuveitendur sem evrópsku eftirlitsstofnanirnar gefa út skv. 9. mgr. 31. gr. reglugerðar (ESB) 2022/2554 sem treysta á þjónustuna sem umsækjandinn veitir, eftir atvikum,

j) sjálfsmat að því er varðar eftirfarandi:

   i. útskiptanleika hverrar upplýsinga- og fjarskiptatækniþjónustu sem umsækjandi veitir, að teknu tilliti til eftirfarandi:

      — markaðshlutdeildar þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu innan fjármálageira Sambandsins,

— fjölda þekktra viðkomandi samkeppnisaðila fyrir hverja tegund upplýsinga- og fjarskiptatækniþjónustu eða flokk upplýsinga- og fjarskiptatækniþjónustu,

— lýsingar á sérstökum eiginleikum í tengslum við upplýsinga- og fjarskiptatækniþjónustu sem í boði er, þ.m.t. í tengslum við alla tækni sem einkaleyfi er á eða sérstaka eiginleika skipulags eða starfsemi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

ii. þekkingu á því hvort aðrir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu eru tiltækilegir til að veita sömu upplýsinga- og fjarskiptatækniþjónustu og sá þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sem leggur fram umsóknina,

k) upplýsingar um framtíðarstarfsstefnu í tengslum við veitingu upplýsinga- og fjarskiptatækniþjónustu og innviða til aðila á fjármálamarkaði í Sambandinu, þ.m.t. allar fyrirhugaðar breytingar á samstæðu- eða stjórnskipulagi, innganga á nýja markaði eða starfsemi,

l) auðkenning undirverktaka þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem hafa verið útnefndir sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu,

m) allar aðrar ástæður sem skipta máli fyrir umsókn þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu um að vera útnefndur sem mikilvægur.

2. Ef þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu tilheyrir samstæðu skulu upplýsingarnar sem um getur í 1. mgr. veittar í tengslum við þá upplýsinga- og fjarskiptatækniþjónustu sem samstæðan veitir í heild.

2. gr.

Efni, uppbygging og sniðmát upplýsinganna sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skulu leggja fram, birta eða tilkynna

1. Mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu skulu, að fenginni beiðni, veita aðaleftirlitsaðilanum allar upplýsingar sem nauðsynlegar eru svo hann geti framkvæmt eftirlitsskyldur sínar í samræmi við kröfurnar í reglugerð (ESB) 2022/2554.

2. Í upplýsingunum, sem um getur í 1. mgr., kemur m.a. eftirfarandi fram:

a) upplýsingar um fyrirkomulag og afrit af samningsskjölum milli:

i. mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu og aðila á fjármálamarkaði sem um getur í 1. mgr. 2. gr. reglugerðar (ESB) 2022/2554,

ii. mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans, með það í huga að ná yfir tæknilega virðiskeðju upplýsinga- og fjarskiptatækniþjónustu sem veitt er aðilum á fjármálamarkaði í Sambandinu,

b) upplýsingar um skipulag og uppbyggingu samstæðu mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. auðkenning allra aðila sem tilheyra sömu samstæðu sem veitir beint eða óbeint upplýsinga- og fjarskiptatækniþjónustu til aðila á fjármálamarkaði í Sambandinu,

c) upplýsingar um stærstu hluthafa eftirfarandi aðila, þ.m.t. skipulag og landfræðilega dreifingu þeirra:

i. aðila sem eiga, sjálfir eða saman með tengdum aðilum sínum, 25% eða meira af hlutafé eða atkvæðisrétti mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

ii. aðila sem hafa rétt til að skipa eða leysa frá störfum meirihluta manna í stjórn, framkvæmdastjórn eða eftirlitsstjórn mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

iii. aðila sem hafa yfirráð, samkvæmt samkomulagi, yfir meirihluta atkvæðisréttar hluthafa eða fulltrúa í mikilvægum þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

d) upplýsingar um markaðshlutdeild mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu fyrir hverja tegund þjónustu, á viðkomandi mörkuðum þar sem hann starfar,

e) upplýsingar um innri stjórnarhætti mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. skipulag með skiptingu stjórnunarábyrgðar og reglna um ábyrgð,

f) fundargerðir stjórnar og/eða framkvæmdastjórnar hins mikilvæga þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og allra annarra mikilvægra innri nefnda sem tengjast á einhvern hátt starfsemi og áhættu varðandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem styður við starfsemi aðila á fjármálamarkaði innan Sambandsins,

g) upplýsingar um upplýsinga- og fjarskiptatækniöryggi mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. viðkomandi stefnuáætlanir, markmið, stefnur, verklagsreglur, samskiptareglur, ferlar, varnarráðstafanir til að vernda viðkvæm gögn, aðgangsstýringar, dulritunarreglur, viðbragðsáætlanir við atvikum og upplýsingar um hlítni við allar viðeigandi reglugerðir og landsbundna- og alþjóðlega staðla, eftir atvikum,

h) upplýsingar um tæknilegar ráðstafanir og skipulagsráðstafanir til að tryggja persónuvernd og gagnavernd, þ.m.t. persónulegar og ópersónulegar upplýsingar, varnarráðstafanir sem framkvæmdar eru til að vernda viðkvæmar upplýsingar, aðgangsstýringar, dulritunarreglur, viðbragðsáætlun fyrir gagnabrot, þegar, varðandi vinnslu persónuupplýsinga, þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu fellur undir lög frá þriðju löndum, þ.m.t. aðgangsbeiðni ríkisstjórnar þriðja lands, skrá yfir lönd og lög sem eiga við,

i) upplýsingar um fyrirkomulag sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu býður aðilum á fjármálamarkaði í Sambandinu fyrir flytjanleika gagna, flytjanleika og samvirkni forrita,

j) upplýsingar um staðsetningu gagnavera og framleiðslustöðva upplýsinga- og fjarskiptatækni sem notaðar eru til að veita aðilum á fjármálamarkaði þjónustu, þ.m.t. skrá yfir öll athafnasvæði og alla aðstöðu mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. utan Sambandsins,

k) upplýsingar um veitingu þjónustu frá þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu frá þriðju löndum, þ.m.t. upplýsingar um viðeigandi lagaákvæði sem eiga við um persónuupplýsingar og ópersónulegar upplýsingar sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu vinnur,

l) upplýsingar um ráðstafanir sem gripið er til, til að taka á áhættu sem stafar af veitingu upplýsinga- og fjarskiptatækniþjónustu af hendi mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka þeirra frá þriðju löndum,

m) upplýsingar um áhættustýringarrammann og atviksstýringarrammann, þ.m.t. stefnur, verklagsreglur, verkfæri, fyrirkomulag og fyrirkomulag stjórnarhátta mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans, þ.m.t. skrá yfir og lýsingu á alvarlegum atvikum með bein eða óbein áhrif á aðila á fjármálamarkaði innan Sambandsins, þ.m.t. viðkomandi upplýsingar til að ákvarða mikilvægi atviksins á aðila á fjármálamarkaði og meta möguleg áhrif yfir landamæri,

n) upplýsingar um rammann um breytingastjórnun, þ.m.t. stefnur, verkferlar og stýringar mikilvægra þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans,

o) upplýsingar um heildarramma um viðbrögð og endurreisn mikilvægra þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. áætlun um rekstrarsamfellu og tengdar ráðstafanir og verklagsreglur, stefnu um lífsferil hugbúnaðarþróunar, viðbragðs- og endurreisnaráætlanir og tengdar ráðstafanir og verklagsreglur, fyrirkomulag varðandi öryggisafritunarstefnur og verklag við öryggisafritun,

p) upplýsingar um eftirlit með frammistöðu, eftirlit með öryggi og rakning atvika ásamt upplýsinga um skýrslugjafarfyrirkomulag í tengslum við þjónustuveitingu, atvik og fylgni við samþykkta þjónustusamninga og markmið um þjónustustig eða svipaðar ráðstafanir milli mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu og aðila á fjármálamarkaði í Sambandinu,

q) upplýsingar um stjórnunarramma mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu hjá þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. áætlanir, stefnur, verklag og ferlar og stýringar, þ.m.t. upplýsingar um áreiðanleikakönnun og áhættumat sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu framkvæmir varðandi undirverktaka sína áður en gengið er til samkomulags við þá og til að hafa eftirlit með tengslunum sem nær yfir alla viðkomandi upplýsinga- og fjarskiptatækniáhættu og mótaðilaáhættu,

r) útdráttur úr vöktunar- og skönnunarkerfum mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans, sem nær yfir en takmarkast ekki við vöktun netkerfa, vöktun netþjóna, vöktun forrita, öryggisvöktun, skönnun á veikleikum, stjórnun aðgerðaskráninga, vöktun á frammistöðu, atvikastýringu og samanburður við áreiðanleikamarkmið, s.s. þjónustustigsmarkmið,

s) útdráttur úr hvers kyns framleiðslu-, forframleiðslu- og prófunarkerfum eða -hugbúnaði sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktakar hans nota beint eða óbeint til að veita þjónustu til aðila á fjármálamarkaði í Sambandinu,

t) skýrslur um reglufylgni og aðgengilegar úttektarskýrslur ásamt öllum viðkomandi niðurstöðum úttekta, þ.m.t. úttektir sem landsbundin yfirvöld framkvæma í Sambandinu og utan Sambandsins þar sem samstarfssamningar við viðkomandi yfirvöld kveða á um slík upplýsingaskipti eða vottanir sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu eða undirverktakar hans hafa fengið, þ.m.t. skýrslur frá innri- og ytri endurskoðendum, vottanir eða mat á reglufylgni við sérstaka staðla atvinnugreinarinnar. Í þessu felast upplýsingar um allar tegundir aðgengilegra, sjálfstæðra prófana á viðnámsþrótti upplýsinga- og fjarskiptatæknikerfa mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. hvers kyns ógnamiðaðar innbrotsprófanir sem þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu framkvæmir,

u) upplýsingar um mat sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu framkvæmir sé þess óskað eða mat á hæfni og heilleika einstaklinga sem gegna lykilstöðum innan mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

v) upplýsingar um úrbótaáætlun til að ráða bót á tilmælunum skv. 3. gr. og viðeigandi tengdar upplýsingar til að staðfesta að úrbætur hafi verið innleiddar,

w) upplýsingar um aðgengilegar þjálfunaráætlanir starfsfólks og áætlanir um öryggisvitund, þ.m.t., ef við á, upplýsingar um fjárfestingar, tilföng og aðferðir mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu við þjálfun starfsfólks síns til að meðhöndla viðkvæm fjármálagögn og viðhalda öflugu öryggisstigi,

x) upplýsingar um starfsemi mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og reikningsskil, þ.m.t. upplýsingar um fjárhagsáætlun og tilföng í tengslum við upplýsinga- og fjarskiptatækni og öryggi.

3. gr.

Upplýsingar frá mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu eftir útgáfu tilmælanna

1. Mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal gefa aðaleftirlitsaðilanum skýrslu sem inniheldur úrbótaáætlun í tengslum við tilmælin og úrbætur sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu fyrirhugar að innleiða til að draga úr áhættunni sem tilgreind er í tilmælunum sem um getur í d-lið 1. mgr. 35. gr. reglugerðar (ESB) 2022/2254. Skýrslan skal vera samræmd við tímalínuna sem aðaleftirlitsaðili setur fyrir hver tilmæli.

2. Til að gera kleift að vakta framkvæmd aðgerðanna sem gripið er til eða úrræðanna sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur beitt í tengslum við móttekin tilmæli skal mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu deila með aðaleftirlitsaðilanum óski hann þess:

a) bráðabirgða framvinduskýrslu og tengd fylgiskjöl sem tilgreina ferlið við framkvæmd aðgerðanna og ráðstafana sem settar eru fram í skýrslunni sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu gefur aðaleftirlitsaðilanum innan þeirra tímamarka sem aðaleftirlitsaðilinn skilgreinir,

b) lokaskýrslur og tengd fylgiskjöl sem tilgreina aðgerðir sem gripið er til eða úrræði sem hrint hefur verið í framkvæmd af hendi mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að draga úr þeirri áhættu sem er tilgreind í mótteknum tilmælum.

4. gr.

Skipulag og framsetning upplýsinganna sem mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu leggja fram

1. Mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal leggja fram umbeðnar upplýsingar til aðaleftirlitsaðila gegnum öruggar rafrænar leiðir sem aðaleftirlitsaðilinn hefur gefið upp í beiðni sinni og á því sniði sem hann óskar eftir.

2. Þegar aðaleftirlitsaðila eru veittar upplýsingar, skulu mikilvægir þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu:

a) fylgja skipulaginu sem aðaleftirlitsaðili hefur gefið upp í upplýsingabeiðni sinni,

b) staðsetja með skýrum hætti mikilvægar upplýsingar í framlögðum skjölum.

3. Upplýsingar sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu leggur fram, birtir eða tilkynnir til aðaleftirlitsaðila skulu vera á tungumáli sem hefð er fyrir að nota í alþjóðafjármálageiranum.

5. gr.

Sniðmát fyrir veitingu upplýsinga um undirverktakasamninga

Mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu sem þarf að deila upplýsingum um undirverktakasamninga skal veita upplýsingarnar til aðaleftirlitsaðila í samræmi við sniðmátið sem sett er fram í viðaukanum.

6. gr.

Mat lögbærra yfirvalda á áhættunni sem tekið er á í tilmælum aðaleftirlitsaðila

1. Sem hluti af eftirliti þeirra með aðilum á fjármálamarkaði skal lögbært yfirvald meta áhrif ráðstafana sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu grípur til á grundvelli tilmæla aðaleftirlitsaðila í samræmi við meðalhófsregluna, á aðila á fjármálamarkaði.

2. Við framkvæmd matsins sem um getur í 1. mgr. skal lögbært yfirvald taka tillit til alls eftirfarandi:

a) að ráðstafanir til leiðréttinga og úrbóta, sem aðilar á fjármálamarkaði framkvæma til að draga úr áhættunni sem tilgreind er í tilmælunum, séu viðunandi og fullnægjandi,

b) matsins sem aðaleftirlitsaðili gerir á reglufylgni mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu við ráðstafanir og aðgerðir sem innifaldar eru í skýrslunni þar sem það hefur áhrif á áhættu aðila á fjármálamarkaði sem er undir eftirliti hans gagnvart áhættunni sem tilgreind er í tilmælunum,

c) sjónarmiða annarra lögbærra yfirvalda sem haft hefur verið samráð við í samræmi við 5. mgr. 42. gr. reglugerðar (ESB) 2022/2554,

d) hvort aðaleftirlitsaðilinn hefur talið að aðgerðir og úrbætur sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur komið í framkvæmd séu nægjanlega góðar til að draga úr áhættu aðila á fjármálamarkaði undir valdsviði hans sem auðkennt er í tilmælunum.

3. Lögbæra yfirvaldið skal, að beiðni aðaleftirlitsaðilans, veita niðurstöður matsins sem sett er fram í 1. mgr. í tæka tíð. Þegar aðaleftirlitsaðili óskar eftir niðurstöðum þessa mats skal hann taka tillit til meginreglunnar um meðalhóf og magns áhættunnar í tengslum við tilmælin, þ.m.t. áhrif þessarar áhættu yfir landamæri þegar áhrifin ná til aðila á fjármálamarkaði sem starfa í fleiri en einu aðildarríki.

4. Þar sem við á skal lögbært yfirvald fara þess á leit við aðila á fjármálamarkaði að veita allar nauðsynlegar upplýsingar til að framkvæma matið sem um getur í 1. mgr.

7. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 24. október 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

———

VIÐAUKI

SNIÐMÁT FYRIR UPPLÝSINGAR UM UNDIRVERKTAKASAMNINGA

Flokkur upplýsinga	Grundavallarupplýsingaþættir
Almennar upplýsingar	— Nafn mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. — Auðkenniskóði mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. — Nafn tengiliðar og samskiptaupplýsingar mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu. — Dagsetning framlagningar sniðmátsins.
Yfirlit undirverktakasamninga	— Kortlagning undirverktakasamninga, þ.m.t. stutt lýsing á tilgangi og gildissviði undirverktakatengsla (þ.m.t. tilgreining á hversu nauðsynlegir eða mikilvægir undirverktakasamningarnir eru fyrir mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu). — Tilgreining og lýsing á tegundum upplýsinga- og fjarskiptatækniþjónustu sem er í undirverktöku og mikilvægi þeirra fyrir upplýsinga- og fjarskiptatækniþjónustu sem veitt er aðilum á fjármálamarkaði, í samræmi við tæknilega framkvæmdarstaðla sem samþykktir voru skv. 9. mgr. 28. gr. reglugerðar (ESB) 2022/2554. — Við tilgreiningu á tegundum upplýsinga- og fjarskiptatækniþjónustu skal vísa í skrána í IV. viðauka um tæknilega framkvæmdarstaðla sem samþykktir voru skv. 9. mgr. 28. gr. reglugerðar (ESB) 2022/2554.
Upplýsingar um undirverktaka	— Heiti og upplýsingar um lögaðila (þ.m.t. auðkenniskóði) hvers undirverktaka. — Samskiptaupplýsingar starfsfólks sem ber ábyrgð á hverjum undirverktakatengslum í stjórnunarfyrirkomulagi mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu. — Yfirlit fyrir hvern undirverktaka um sérfræðikunnáttu, reynslu og menntun og hæfi í tengslum við samningsbundna upplýsinga- og fjarskiptatækniþjónustu.
Lýsing á þjónustu sem undirverktakar veita	— Ítarleg lýsing á sértækri upplýsinga- og fjarskiptatækniþjónustu sem hver undirverktaki veitir. — Sundurliðun á ábyrgð og verkefnum sem úthlutað er til undirverktaka með því að útlista ólík hlutverk á mismunandi stigum upplýsinga- og fjarskiptatækniferla. — Upplýsingar um hvernig aðgang undirverktakar hafa að persónulegum eða öðrum viðkvæmum gögnum eða kerfum varðandi upplýsinga- og fjarskiptatækniþjónustuna sem veitt er aðilum á fjármálamarkaði. — Upplýsingar um svæði þaðan sem þjónusta undirverktaka er veitt og ráðstafana sem gripið er til til að taka á áhættu sem stafar af þjónustu sem veitt er utan Sambandsins.
Stjórnarhættir og eftirlit með undirverktakastarfsemi	— Lýsing á samnings- og stjórnunarramma sem er til staðar til að stjórna undirverktakatengslum, þ.m.t. ákvæði sem takmarka notkun viðkvæmra gagna. — Útskýring á verkferlunum fyrir val á, samskipti við og eftirlit með undirverktökum. — Yfirlit yfir frammistöðumælikvarða, markmið og samningar um þjónustustig og lykilárangursmælikvarðar sem notaðir eru til að meta frammistöðu undirverktaka og vöktun á áreiðanleika.
Áhættustýring og reglufylgni	— Mat á áhættusniði undirverktaka og möguleg áhrif á upplýsinga- og fjarskiptatækniþjónustu sem veitt er aðilum á fjármálamarkaði. — Útskýring á ráðstöfunum til áhættumildunar sem framkvæmdar eru til að takast á við áhættur tengdar undirverktöku. — Upplýsingar um hlítni undirverktaka við viðeigandi reglugerðir, þ.m.t. um gagnavernd og fagstaðla.

Flokkur upplýsinga	Grundavallarupplýsingaþættir
Rekstrarsamfella og gerð viðbragðsáætlana	— Yfirlit yfir áætlanir undirverktakans um rekstrarsamfellu og viðbrögð og endurreisn. — Lýsing á ráðstöfunum sem eru til staðar til að tryggja þjónustusamfellu ef um röskun hjá eða uppsagnar undirverktaka. — Tíðni prófana á áætlun um rekstrarsamfellu og viðbragðs- og endurreisnaráætlun undirverktaka, dagsetningar nýjustu prófana næstliðin 3 ár og tilgreining á því ef mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu kom að þessum prófunum.
Skýrslugjöf	— Lýsing á skýrslugjafarfyrirkomulagi og tíðni skýrslugjafar milli mikilvægs þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans.
Úrbætur og atvikastjórnun	— Yfirlit yfir verklagsreglur til að takast á við atvik tengd undirverktaka, brot eða það að ekki er farið að tilskildum ákvæðum.
Vottanir og endurskoðanir	— Upplýsingar um allar vottanir, óháða endurskoðun eða mat á undirverktökum til að staðfesta öryggisstýringu þeirra, gæðastaðla eða að þeir hlíti reglum. — Dagsetning og tíðni endurskoðunar á undirverktökum sem mikilvægur þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu framkvæmir.

Fylgiskjal 5.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2025/301

frá 23. október 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreint er innihald og tímamörk frumtilkynningar, og áfanga- og lokaskýrslu, um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og inntak valfrjálsrar tilkynningar um verulegar netógnir

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum þriðju undirgrein 20. gr.,

og að teknu tilliti til eftirfarandi:

1) Til að tryggja samræmingu og einföldun á tilkynningar- og skýrslugjafarkröfum fyrir alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem um getur í 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554, ættu tímamörk fyrir tilkynningu alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni að fylgja samræmdri nálgun fyrir allar tegundir aðila á fjármálamarkaði. Af þessum sökum ættu tímamörkin einnig, eins og framast er unnt, að fylgja samræmdri nálgun og hið minnsta að hafa sambærileg áhrif og kröfurnar sem settar eru fram í tilskipun Evrópuþingsins og ráðsins (ESB) 2022/2555 ([2]).

2) Til að forðast að leggja ótilhlýðilega skýrslugjafarbyrði á aðila á fjármálamarkaði þegar þeir meðhöndla atvik sem tengist upplýsinga- og fjarskiptatækni ætti innihald upphaflegrar tilkynningar að vera takmarkað við þær upplýsingar sem hafa mesta þýðingu. Til að grípa til tilhlýðilegra eftirlitsaðgerða verða lögbær yfirvöld að fá upplýsingar um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni eins fljótt og auðið er eftir að aðili á fjármálamarkaði hefur flokkað atvik sem tengist upplýsinga- og fjarskiptatækni sem alvarlegt. Af þessum sökum ættu tímamörk fyrir framlagningu upphaflegrar tilkynningar, eins og um getur í a-lið 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554, að vera eins stuttu og mögulegt er eftir að atvik sem tengist upplýsinga- og fjarskiptatækni hefur verið flokkað sem alvarlegt, á sama tíma og gert er ráð fyrir ákveðnum sveigjanleika, einkum fyrir viðskiptalíkön þjónustu sem er ekki sérstaklega háð tímamörkum, ef aðilar á fjármálamarkaði þurfa lengri tíma til að meðhöndla atvik sem tengist upplýsinga- og fjarskiptatækni eftir að þeir fá vitneskju um það.

3) Eftir viðtöku frumtilkynningar ættu lögbær yfirvöld að fá ítarlegri upplýsingar um atvikið sem tengist upplýsinga- og fjarskiptatækni í áfangaskýrslunni og allar viðkomandi upplýsingar í lokaskýrslunni. Upplýsingarnar í þessum skýrslum ættu að gera lögbærum yfirvöldum kleift að meta frekar atvik sem tengist upplýsinga- og fjarskiptatækni og meta eftirlitsaðgerðir sem þau gætu viljað grípa til.

4) Frestirnir sem um getur í ii. lið a-liðar fyrstu málsgreinar 20. gr. í reglugerð (ESB) 2022/2554 ættu því að mynda jafnvægi milli þarfar lögbærra yfirvalda til að veita upplýsingunum móttöku með skjótum hætti og þeirri þörf að veita aðilum á fjármálamarkaði nægan tíma til að safna heildstæðum og réttum upplýsingum.

5) Að teknu tilliti til viðmiðanna sem sett eru fram í a-lið fyrstu málsgreinar 20. gr. reglugerðar (ESB) 2022/2554 ættu frestir til skýrslugjafar ekki að leggja óhóflega byrði á örfyrirtæki og aðra aðila á fjármálamarkaði sem ekki eru mikilvægir. Til að forðast óhóflega byrði á aðila á fjármálamarkaði skulu frestir til skýrslugjafar einnig taka tillit til helga og almennra frídaga.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) 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, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

6) Þar sem tilkynningar um verulegar netógnir eru valfrjálsar ætti innihald slíkra tilkynninga ekki að leggja óhóflega byrði á aðila á fjármálamarkaði og ættu þær að vera takmarkaðri en upplýsingarnar sem óskað er eftir um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni.

7) Reglugerð þessi byggist á drögum að tæknilegum framkvæmdarstöðlum sem Evrópsku eftirlitsstofnanirnar hafa lagt fyrir framkvæmdastjórnina.

8) Evrópsku eftirlitsstofnanirnar hafa haft opið samráð við almenning um drögin að tæknilegum eftirlitsstöðlum sem þessi reglugerð byggist á, greint mögulegan tengdan kostnað og ávinning og óskað eftir ráðgjöf hagsmunahóps, sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([3]), (ESB) nr. 1094/2010 ([4]), og (ESB) nr. 1095/2010 ([5]).

9) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([6]) og skilaði hún áliti 22. júlí 2024. Öll vinnsla persónuupplýsinga innan gildissviðs þessarar reglugerðar ætti að vera í samræmi við gildandi meginreglur um gagnavernd og ákvæði reglugerðar (ESB) 2018/1725.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Almennar upplýsingar sem veita á í frumtilkynningum og í áfanga- og lokaskýrslum um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni

Aðilar á fjármálamarkaði skulu láta fylgja með í frumtilkynningu, áfangaskýrslu og lokaskýrslu, eins um getur í 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554, eftirfarandi almennar upplýsingar:

a) tegund framlagningar (frumtilkynning, áfangaskýrsla eða lokaskýrsla),

b) heiti aðila á fjármálamarkaði, LEI-auðkenni hans og tegund aðila á fjármálamarkaði, eins og um getur í 1. mgr. 2. gr. reglugerðar (ESB) 2022/2554,

c) nafn og auðkenniskóða aðila sem leggur fram frumtilkynningu eða áfanga- eða lokaskýrslu fyrir aðilann á fjármálamarkaði,

d) nafn og LEI-auðkenni allra aðila á fjármálamarkaði sem nefndir eru í samanlagðri frumtilkynningu eða áfanga- eða lokaskýrslu, eftir atvikum,

e) samskiptaupplýsingar ábyrgðaraðila fyrir samskipti við lögbært yfirvald vegna alvarlegs atviks sem tengist upplýsinga- og fjarskiptatækni,

f) deili á móðurfélagi samstæðu sem aðilinn á fjármálamarkaði tilheyrir, eftir atvikum,

g) gjaldmiðillinn sem fjárhæðirnar byggjast á, ef um peningaleg áhrif er að ræða.

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

2. gr.

Sértækar upplýsingar sem veita á í frumtilkynningum

Frumtilkynningar eins og um getur í a-lið 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554 skulu ná yfir a.m.k. allar eftirfarandi sértækar upplýsingar:

a) tilvísunarkóða atviks sem aðili á fjármálamarkaði úthlutar,

b) dagsetningu greiningar, tímasetningu greiningar og flokkun atviksins skv. 8. gr. framseldrar reglugerðar framkvæmdastjórnarinnar (ESB) 2024/1772 ([7]),

c) lýsingu á atvikinu sem tengist upplýsinga- og fjarskiptatækni,

d) viðmiðin sem mælt er fyrir um í 1.–8. gr. í framseldri reglugerð (ESB) 2024/1772, sem flokkun aðila á fjármálamarkaði á atviki sem tengist upplýsinga- og fjarskiptatækni sem alvarlegu, byggist á,

e) aðildarríkin sem verða fyrir áhrifum af atviki sem tengist upplýsinga- og fjarskiptatækni,

f) upplýsingar um hvernig varð vart við atvikið sem tengist upplýsinga- og fjarskiptatækni,

g) upplýsingar um uppruna atviks sem tengist upplýsinga- og fjarskiptatækni, þar sem við á,

h) upplýsingar um hvort aðili á fjármálamarkaði hafi virkjað áætlun um rekstrarsamfellu,

i) upplýsingar um endurflokkun á atviki sem tengist upplýsinga- og fjarskiptatækni úr alvarlegu í ekki alvarlegt, eftir atvikum,

j) allar aðrar viðeigandi upplýsingar, eftir atvikum.

3. gr.

Sértækar upplýsingar sem skal veita í áfangaskýrslunum

Áfangaskýrslur eins og um getur í b-lið 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554 skulu ná yfir a.m.k. allar eftirfarandi sértækar upplýsingar:

a) tilvísunarkóða atviks sem lögbært yfirvald veitir, eftir atvikum,

b) dagsetningu og tíma þegar atvikið sem tengist upplýsinga- og fjarskiptatækni átti sér stað,

c) dagsetningu og tíma þegar aðili á fjármálamarkaði hefur endurheimt reglulega starfsemi sína, eftir atvikum,

d) upplýsingar um hvernig viðmiðanirnar sem mælt er fyrir um í 1.–8. gr. í framseldri reglugerð (ESB) 2024/1772 eru uppfylltar, sem flokkun aðila á fjármálamarkaði á atviki sem tengist upplýsinga- og fjarskiptatækni sem alvarlegu, byggist á,

e) tegund atviks sem tengist upplýsinga- og fjarskiptatækni,

f) eftir atvikum, ógnir og aðferðir sem ógnaraðili notar,

g) starfssvið og rekstrarferla sem verða fyrir áhrifum,

h) innviðaþætti sem verða fyrir áhrifum, sem styðja við rekstrarferla,

i) áhrif á fjárhagslega hagsmuni viðskiptavina,

j) upplýsingar um skýrslugjöf um atvik sem tengist upplýsinga- og fjarskiptatækni til annarra yfirvalda,

k) tímabundnar aðgerðir eða -ráðstafanir sem aðili á fjármálamarkaði grípur til eða fyrirhugar að grípa til, til að ná sér á strik eftir atvik sem tengist upplýsinga- og fjarskiptatækni,

l) eftir atvikum, upplýsingar um vísa sem gefa til kynna vásetningu.

([7]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1772 frá 13. mars 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina viðmiðanir fyrir flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum, setja fram mikilvægismörk og tilgreina nánari upplýsingar um tilkynningar um alvarleg atvik (Stjtíð. ESB L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

4. gr.

Sértækar upplýsingar sem skal veita í lokaskýrslunum

Lokaskýrslur eins og um getur í c-lið 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554 skulu ná yfir allar eftirfarandi sértækar upplýsingar:

a) upplýsingar um frumorsakir atviksins sem tengist upplýsinga- og fjarskiptatækni,

b) dagsetningar og tíma þegar leyst var úr atvikinu sem tengist upplýsinga- og fjarskiptatækni og frumorsakir þess meðhöndlaðar,

c) upplýsingar um úrlausn atviksins sem tengist upplýsinga- og fjarskiptatækni,

d) upplýsingar sem viðeigandi eru fyrir skilastjórnvöld, eftir atvikum,

e) upplýsingar um beinan og óbeinan kostnað sem stafar af atviki sem tengist upplýsinga- og fjarskiptatækni og upplýsingar um fjárhagslegar endurbætur,

f) upplýsingar um endurtekin atvik sem tengjast upplýsinga- og fjarskiptatækni, eftir atvikum.

5. gr.

Tímamörk fyrir frumtilkynningu og fyrir áfanga- og lokaskýrslur

1. Aðilar á fjármálamarkaði skulu leggja fram frumtilkynningu og áfanga- og lokaskýrslur eins og um getur í a-, b- og c-lið 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554 innan eftirfarandi tímamarka:

a) fyrir frumtilkynningu: eins skjótt og auðið er, en í öllum tilvikum innan fjögurra klukkustunda frá flokkun atviks sem tengist upplýsinga- og fjarskiptatækni sem alvarlegs atviks og eigi síðar en 24 klukkustundum frá þeirri stundu er aðilinn á fjármálamarkaði fær vitneskju um atvikið sem tengist upplýsinga- og fjarskiptatækni,

b) fyrir áfangaskýrslu: eigi síðar en innan 72 klukkustunda frá framlagningu frumtilkynningar, jafnvel þótt staða eða meðhöndlun atviksins hafi ekki breyst eins og um getur í b-lið 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554. Aðilar á fjármálamarkaði skulu leggja fram uppfærða áfangaskýrslu án ástæðulausrar tafar og alltaf þegar eðlileg starfsemi hefur verið endurreist,

c) fyrir lokaskýrslu: eigi síðar en einum mánuði eftir annað hvort framlagningu áfangaskýrslunnar eða, eftir atvikum, eftir nýjustu uppfærðu áfangaskýrslu.

2. Ef aðili á fjármálamarkaði hefur ekki flokkað atvik sem tengist upplýsinga- og fjarskiptatækni sem alvarlegt innan 24 klukkustunda frá þeirri stundu þegar aðilinn á fjármálamarkaði fékk vitneskju um atvikið sem tengist upplýsinga- og fjarskiptatækni en flokkar það atvik sem alvarlegt á síðari stigum, skal aðili á fjármálamarkaði leggja fram frumtilkynningu innan fjögurra klukkustunda frá því að atvikið sem tengist upplýsinga- og fjarskiptatækni er flokkað sem alvarlegt atvik.

3. Aðilar á fjármálamarkaði sem geta ekki lagt fram frumtilkynningu, áfangaskýrslu eða lokaskýrslu innan þeirra tímamarka sem sett eru fram í 1. mgr. skulu upplýsa lögbær yfirvöld um það án ástæðulausrar tafar en eigi síðar en viðeigandi tímamörk fyrir framlagningu tilkynningar eða skýrslu og skal útskýra ástæður tafarinnar.

4. Ef frestur til framlagningar frumtilkynningar, áfangaskýrslu eða lokaskýrslu lendir á helgi eða almennum frídegi í aðildarríki aðilans á fjármálamarkaði sem tilkynnir, getur aðilinn á fjármálamarkaði lagt fram frumtilkynningu, áfangaskýrslu eða lokaskýrslu fyrir hádegi næsta virka dag.

5. Ákvæði 4. mgr. skulu ekki að gilda um framlagningu frumtilkynningar eða áfangaskýrslu lánastofnunar, miðlægra mótaðila, rekstraraðila viðskiptavettvanga og annarra aðila á fjármálamarkaði sem auðkenndir eru sem nauðsynlegir eða þýðingarmiklir aðilar skv. 3. gr. tilskipunar (ESB) 2022/2555.

6. Lögbær yfirvöld geta ákveðið að 4. mgr. skuli ekki gilda um framlagningu aðila á fjármálamarkaði á frumtilkynningu eða áfangaskýrslu, öðrum en þeim sem um getur í 5. mgr. sem eru mikilvægar eða hafa kerfislæga eiginleika fyrir fjármálageirann á landsvísu eða á vettvangi Sambandsins. Lögbær yfirvöld skulu tilkynna ákvörðun sína til tilgreindra aðila á fjármálamarkaði. Ákvörðun lögbæra yfirvaldsins skal einungis gilda að því er varðar atvik sem tilkynnt er um eftir tilkynningardag lögbæra yfirvaldsins um ákvörðunina til tilgreindra aðila á fjármálamarkaði.

6. gr.

Innihald valfrjálsrar tilkynningar um verulegar netógnir

Innihald valfrjálsrar tilkynningar í tengslum við verulegar netógnir eins og um getur í 2. mgr. 19. gr. reglugerðar (ESB) 2022/2554 skal ná yfir allt eftirfarandi:

a) almennar upplýsingar um aðilann á fjármálamarkaði sem tilkynnir eins og sett er fram í 1. gr.,

b) dagsetningu og tímasetningu greiningar netógnarinnar og aðra viðkomandi tímastimpla sem tengjast hinni verulegu netógn,

c) lýsingu á verulegu netógninni,

d) upplýsingar um möguleg áhrif verulegu netógnarinnar á aðila á fjármálamarkaði, viðskiptavini hans eða fjárhagslega mótaðila,

e) flokkunarviðmiðin sem hefðu leitt til skýrslu um alvarlegt atvik sem mælt er fyrir um í 1.–8. gr. framseldrar reglugerðar (ESB) 2024/1772 ef netógnin hefði raungerst,

f) upplýsingar um stöðu hinnar verulegu netógnar og allar breytingar á ógninni,

g) eftir atvikum, lýsing á aðgerðum sem aðili á fjármálamarkaði grípur til til að koma í veg fyrir að hin verulega netógn raungerist,

h) upplýsingar um allar tilkynningar um hina verulegu netógn gagnvart öðrum aðilum á fjármálamarkaði eða yfirvöldum,

i) eftir atvikum, upplýsingar um vísa sem gefa til kynna vásetningu,

j) allar aðrar viðeigandi upplýsingar, eftir atvikum.

7. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 23. október 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

Fylgiskjal 6.

FRAMKVÆMDARREGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2025/302

frá 23. október 2024

um tæknilega framkvæmdarstaðla fyrir beitingu reglugerðar Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar stöðluð eyðublöð, sniðmát og verklagsreglur fyrir aðila á fjármálamarkaði til að tilkynna um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og til að tilkynna um verulega netógn

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]) og einkum fjórðu málsgrein 20. gr.,

og að teknu tilliti til eftirfarandi:

1) Til að tryggja að aðilar á fjármálamarkaði tilkynni alvarleg atvik til lögbærra yfirvalda sinna á samkvæman hátt og til að tryggja að þeir veiti þessum yfirvöldum gögn af góðum gæðum ætti að tilgreina hvaða gagnareiti aðilar á fjármálamarkaði þurfa að fylla út á hinum ýmsu stigum tilkynningar sem um getur í 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554. Mikilvægt er að þessar upplýsingar séu settar þannig fram að unnt sé að fá eitt yfirlit yfir atvikið. Því er nauðsynlegt að mæla fyrir um eitt tilkynningarsniðmát í þessu skyni.

2) Aðilar á fjármálamarkaði ættu að fylla út þá gagnareiti í tilkynningasniðmátinu sem samsvara upplýsingakröfunum í viðkomandi tilkynningu eða skýrslu. Þó ætti að heimila aðilum á fjármálamarkaði sem þegar hafa upplýsingar sem þeim ber að skila á síðara tilkynningastigi , þ.e. í áfangaskýrslunni eða lokaskýrslunni, að leggja fram þau gögn fyrr.

3) Þar sem mörg eða endurtekin atvik geta talist alvarleg atvik, eins og um getur í 8. gr. framseldrar reglugerðar framkvæmdastjórnarinnar (ESB) 2024/1772 ([2]), ætti hönnun tilkynningarsniðmátsins og gagnareitanna að gera aðilum á fjármálamarkaði kleift að tilkynna um slík endurtekin atvik.

4) Til að tryggja nákvæmar og uppfærðar upplýsingar ætti tilkynningarsniðmátið að gera aðilum á fjármálamarkaði kleift, þegar þau leggja fram áfanga- og lokaskýrsluna, að uppfæra allar upplýsingar sem áður voru lagðar fram og, ef nauðsyn krefur, endurflokka alvarleg atvik sem ekki alvarleg.

5) Aðlaga ætti lögmæta auðkenningu aðila að auðkenningunum sem tilgreindar eru í tæknilegu framkvæmdarstöðlunum sem samþykktir eru skv. 9. mgr. 28. gr. reglugerðar (ESB) 2022/2554.

6) Ef aðilar á fjármálamarkaði útvista til þriðja aðila tilkynningaskyldu um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni ættu lögbær yfirvöld að kunna deili á þeim þriðja aðila sem tilkynnir fyrir hönd aðilans á fjármálamarkaði áður en fyrsta tilkynningin eða skýrslan er lögð fram til að sannreyna lögmæti þess þriðja aðila sem tilkynnir.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

([2]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1772 frá 13. mars 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina viðmiðanir fyrir flokkun á atvikum sem tengjast upplýsinga- og fjarskiptatækni og netógnum, setja fram mikilvægismörk og tilgreina nánari upplýsingar um tilkynningar um alvarleg atvik (Stjtíð. ESB L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

7) Til að greina auðveldlega áhrifin af atviki sem átti sér stað hjá, eða orsakaðist af, þjónustuveitanda sem er þriðji aðili og sem hefur áhrif á marga aðila á fjármálamarkaði innan eins aðildarríkis, og til að draga úr skýrslugjafarbyrði aðila á fjármálamarkaði, ætti tilkynningarsniðmátið að gera kleift að leggja fram sameinaða skýrslu með sameinuðum upplýsingum um áhrif atviksins á alla þá aðila á fjármálamarkaði sem hafa orðið fyrir áhrifum og hafa flokkað atvikið sem alvarlegt.

8) Tilkynningarsniðmátið ætti að vera hannað á hlutlausan hátt í tæknilegu tilliti til að hægt sé að innleiða það í mismunandi lausnir fyrir atvikatilkynningar sem þegar eru fyrir hendi eða sem kunna að verða þróaðar fyrir framkvæmd krafnanna í reglugerð (ESB) 2022/2554.

9) Hönnun tilkynningarsniðmátsins og gagnareitanna ætti að auðvelda þriðju aðilum, sem aðilar á fjármálamarkaði hafa útvistað tilkynningarskyldum sínum til í samræmi við 5. mgr. 19. gr. reglugerðar (ESB) 2022/2554, að tilkynna um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni.

10) Reglugerð þessi byggist á drögum að tæknilegum framkvæmdarstöðlum sem evrópsku eftirlitsstofnanirnar hafa lagt fyrir framkvæmdastjórnina.

11) Evrópsku eftirlitsstofnanirnar hafa haft opið samráð við almenning um drögin að tæknilegu framkvæmdarstöðlunum sem þessi reglugerð byggist á, greint mögulegan tengdan kostnað og ávinning og óskað eftir áliti hagsmunahóps um bankastarfsemi, sem komið var á fót í samræmi við 37. gr. reglugerða Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([3]), (ESB) nr. 1094/2010 ([4]) og (ESB) nr. 1095/2010 ([5]).

12) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([6]) og skilaði hún áliti 22. júlí 2024. Öll vinnsla persónuupplýsinga innan gildissviðs þessarar reglugerðar ætti að vera í samræmi við gildandi meginreglur um gagnavernd og ákvæði reglugerðar (ESB) 2018/1725.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Sniðmát fyrir tilkynningar um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni

1. Aðilar á fjármálamarkaði skulu nota sniðmátið sem mælt er fyrir um í I. viðauka til að leggja fram frumtilkynningu, áfangaskýrslu og lokaskýrslu sem um getur í 4. mgr. 19. gr. reglugerðar (ESB) 2022/2554 sem hér segir:

a) aðilar á fjármálamarkaði sem leggja fram frumtilkynningu skulu fylla út gagnareitina í sniðmátinu sem samsvara upplýsingunum sem veita skal í samræmi við 2. gr. framseldrar reglugerðar framkvæmdastjórnarinnar (ESB) 2025/301 ([7]) og er heimilt, ef þeir búa þegar yfir þeim upplýsingum, að fylla út í þá gagnareiti sem ekki er þörf á að fylla út fyrir frumtilkynningu en sem krafist er fyrir áfanga- eða lokaskýrslu,

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/301 frá 23. október 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreint er innihald og tímamörk frumtilkynningar, og áfanga- og lokaskýrslu, um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni og inntak valfrjálsrar tilkynningar um verulegar netógnir. Stjtíð. ESB L, 2025/301, 20.2.2025, ELI: http://data.europa.eu/eli/dec/2025/301/oj.

b) aðilar á fjármálamarkaði sem leggja fram áfangaskýrslu skulu fylla út gagnareitina í sniðmátinu sem samsvara upplýsingunum sem veita skal í samræmi við 3. gr. framseldrar reglugerðar (ESB) 2025/301 og er heimilt, ef þeir búa þegar yfir viðeigandi upplýsingum, að fylla út í þá gagnareiti sem ekki er þörf á að fylla út fyrir áfangaskýrsluna en sem krafist er fyrir lokaskýrsluna,

c) aðilar á fjármálamarkaði sem leggja fram lokaskýrslu skulu fylla út gagnareitina í sniðmátinu sem samsvara upplýsingunum sem veita skal í samræmi við 4. gr. framseldrar reglugerðar (ESB) 2025/301.

2. Aðilar á fjármálamarkaði skulu tryggja að upplýsingarnar í frumtilkynningunni og í áfangaskýrslunni og lokaskýrslunni séu fullnægjandi og réttar.

3. Aðilar á fjármálamarkaði skulu gefa upp áætluð gildi á grundvelli annarra tiltækra gagna og upplýsinga, að því marki sem mögulegt er, ef nákvæm gögn eru ekki tiltæk þegar frumtilkynningin eða áfangaskýrslan er gerð.

4. Þegar aðilar á fjármálamarkaði leggja fram áfanga- eða lokaskýrslu skulu þeir nota sniðmátið sem mælt er fyrir um í I. viðauka til að leggja fram allar tilskildar upplýsingar og uppfæra, eftir atvikum, upplýsingarnar sem áður voru veittar í frumtilkynningunni eða áfangaskýrslunni.

5. Aðilar á fjármálamarkaði skulu fylgja orðalistanum og leiðbeiningunum sem settar eru fram í II. viðauka þegar þeir fylla út sniðmátið sem mælt er fyrir um í I. viðauka.

2. gr.

Sameinuð framlagning frumtilkynningar, áfangaskýrslu og lokaskýrslu

Aðilar á fjármálamarkaði geta sameinað framlagningu frumtilkynningarinnar, áfangaskýrslunnar og lokaskýrslunnar og lagt tvær þeirra eða þær allar fram á sama tíma, ef regluleg starfsemi hefur verið endurreist eða greiningu á frumorsök er lokið og að því tilskildu að tímamörkin sem sett eru fram í 5. gr. framseldrar reglugerðar (ESB) 2025/301 séu virt.

3. gr.

Endurtekin atvik sem tengjast upplýsinga- og fjarskiptatækni

Aðilar á fjármálamarkaði sem veita upplýsingar um endurtekin atvik í tengslum við upplýsinga- og fjarskiptatækni sem ekki eru alvarleg en til samans uppfylla skilyrði fyrir að teljast eitt alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni, eins og sett er fram í 2. mgr. 8. gr. framseldrar reglugerðar (ESB) 2024/1772, skulu veita þær upplýsingar á sameinuðu formi.

4. gr.

Notkun öruggra rafrænna leiða

1. Aðilar á fjármálamarkaði skulu nota öruggar rafrænar leiðir, eins og lögbært yfirvald þeirra gerir aðgengilegar, til að leggja fram frumtilkynninguna og áfanga- og lokaskýrslurnar.

2. Aðilar á fjármálamarkaði sem geta ekki notað öruggu rafrænu leiðirnar eins og lögbært yfirvald þeirra gerir aðgengilegar skulu tilkynna lögbæru yfirvaldi sínu um alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni með öðrum öruggum leiðum í samráði við lögbæra yfirvaldið. Aðilar á fjármálamarkaði skulu, ef lögbært yfirvald krefst þess, leggja fram frumtilkynninguna eða áfanga- eða lokaskýrsluna að nýju um öruggu rafrænu leiðina sem lögbært yfirvald þeirra gerir aðgengilega þegar þeir geta gert það.

5. gr.

Endurflokkun á alvarlegum atvikum sem tengjast upplýsinga- og fjarskiptatækni

Ef aðili á fjármálamarkaði kemst að þeirri niðurstöðu, eftir frekara mat, að atvik sem tengist upplýsinga- og fjarskiptatækni sem áður var tilkynnt sem alvarlegt, uppfyllti aldrei flokkunarviðmiðin og mörkin sem sett eru fram í 8. gr. framseldrar reglugerðar (ESB) 2024/1772, skal aðilinn á fjármálamarkaði tilkynna lögbæru yfirvaldi að hann hafi endurflokkað atvikið úr alvarlegt í ekki alvarlegt með því að veita upplýsingar um þá endurflokkun í sniðmátinu sem mælt er fyrir um í II. viðauka við þessa reglugerð í tengslum við reitina „tegund tilkynningar“ og „aðrar upplýsingar“.

6. gr.

Tilkynning um útvistun á skýrslugjafarskyldum

1. Aðilar á fjármálamarkaði sem hafa útvistað skyldunni til að tilkynna alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni í samræmi við 5. mgr. 19. gr. reglugerðar (ESB) 2022/2554 skulu upplýsa lögbært yfirvald sitt um þann útvistunarsamning um leið og gengið hefur verið frá honum og eigi síðar en fyrir fyrstu tilkynninguna eða skýrslugjöfina.

2. Aðilar á fjármálamarkaði skulu láta lögbæra yfirvaldinu í té heiti, samskiptaupplýsingar og auðkenniskóða þriðja aðilans sem mun leggja fram tilkynningar eða skýrslur um alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni fyrir þá.

3. Aðilar á fjármálamarkaði skulu upplýsa lögbært yfirvald sitt um leið og þeir útvista ekki lengur skýrslugjafarskyldum sínum eins og um getur í 5. mgr. 19. gr. reglugerðar (ESB) 2022/2554.

7. gr.

Sameinuð skýrslugjöf

1. Þjónustuveitandi sem er þriðji aðili og skýrslugjafarskyldum hefur verið útvistað til, eins og um getur í 5. mgr. 19. gr. reglugerðar (ESB) 2022/2554, getur notað sniðmátið sem sett er fram í I. viðauka við þessa reglugerð til að veita sameinaðar upplýsingar um alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni og hefur áhrif á fleiri aðila á fjármálamarkaði í einni tilkynningu eða skýrslu og leggja þá tilkynningu eða skýrslu fyrir lögbæra yfirvaldið fyrir hönd allra aðila á fjármálamarkaði sem verða fyrir áhrifum, að því tilskildu að öll eftirfarandi skilyrði séu uppfyllt:

a) hið alvarlega atvik sem tengist upplýsinga- og fjarskiptatækni sem tilkynna skal megi rekja til eða sé af völdum veitanda upplýsinga- og fjarskiptatækniþjónustu sem er þriðji aðili,

b) sá þriðji aðili veiti fleiri en einum aðila á fjármálamarkaði, eða samstæðu, viðkomandi upplýsinga- og fjarskiptatækniþjónustu,

c) viðkomandi atvik sem tengist upplýsinga- og fjarskiptatækni sé flokkað sem alvarlegt hjá hverjum aðila á fjármálamarkaði sem sameinaða tilkynningin eða skýrslan tekur til,

d) hið alvarlega atvik sem tengist upplýsinga- og fjarskiptatækni hefur áhrif á aðila á fjármálamarkaði innan eins aðildarríkis og sameinaða skýrslan varðar aðila á fjármálamarkaði sem lúta eftirliti sama lögbæra yfirvalds,

e) lögbær yfirvöld hafi sérstaklega heimilað þessari tegund aðila á fjármálamarkaði að leggja fram sameinaðar skýrslur.

2. Ákvæði 1. mgr. gilda ekki um lánastofnanir sem eru taldar hafa verulegt vægi eins og um getur í 16. lið 2. gr. reglugerðar Seðlabanka Evrópu (ESB) nr. 468/2014 ([8]), rekstraraðila viðskiptavettvanga og miðlæga mótaðila, sem skulu aðeins nota sniðmátið í I. viðauka til að leggja fyrir lögbært yfirvald sitt tilkynningar eða skýrslur um einstök alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni.

3. Krefjist lögbær yfirvöld upplýsinga um áhrif eins alvarlegs atviks sem tengist upplýsinga- og fjarskiptatækni á stakan aðila á fjármálamarkaði skal aðilinn á fjármálamarkaði, að beiðni lögbæra yfirvaldsins, leggja fram staka tilkynningu eða skýrslu um hið alvarlega atvik sem tengist upplýsinga- og fjarskiptatækni.

([8]) Reglugerð Seðlabanka Evrópu (ESB) nr. 468/2014 frá 16. apríl 2014 um að koma á ramma um samstarf innan samræmdu eftirlitsráðstöfunarinnar milli Seðlabanka Evrópu og lögbærra landsyfirvalda og tilnefndra landsyfirvalda (rammareglugerð um samræmda eftirlitsráðstöfun) (SE/2014/17) (Stjtíð. ESB L 141, 14.5.2014, bls. 1, ELI: http://data.europa.eu/regeli//2014/468/oj).

8. gr.

Tilkynning um verulegar netógnir

1. Aðilar á fjármálamarkaði sem tilkynna um verulegar netógnir til lögbærra yfirvalda í samræmi við 2. mgr. 19. gr. reglugerðar (ESB) 2022/2554 skulu nota sniðmátið sem mælt er fyrir um í III. viðauka við þessa reglugerð og fylgja orðalistanum og leiðbeiningunum sem settar eru fram í IV. viðauka við þessa reglugerð.

2. Aðilar á fjármálamarkaði skulu tryggja að upplýsingarnar í tilkynningunni um verulegar netógnir séu fullnægjandi og réttar.

9. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í Stjórnartíðindum Evrópusambandsins.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 23. október 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

I. VIÐAUKI

SNIÐMÁT TILKYNNINGA UM ALVARLEG ATVIK

Númer reits	Gagnasvæði	
Almennar upplýsingar um aðilann á fjármálamarkaði		
1.1	Tegund framlagningar	
1.2	Heiti aðilans sem leggur skýrsluna fram	
1.3	Auðkenniskóði þess aðila sem leggur skýrsluna fram	
1.4	Tegund aðila á fjármálamarkaði sem varð fyrir áhrifum	
1.5	Heiti aðila á fjármálamarkaði sem varð fyrir áhrifum	
1.6	LEI-auðkenni þess aðila á fjármálamarkaði sem varð fyrir áhrifum	
1.7	Nafn aðaltengiliðar	
1.8	Netfang aðaltengiliðar	
1.9	Sími aðaltengiliðar	
1.10	Nafn annars tengiliðar	
1.11	Netfang annars tengiliðar	
1.12	Sími annars tengiliðar	
1.13	Heiti endanlegs móðurfyrirtækis	
1.14	LEI-auðkenni endanlegs móðurfyrirtækis	
1.15	Gagnaskilagjaldmiðill	
Inntak frumtilkynningarinnar		
2.1	Tilvísunarkóði atviks sem aðili á fjármálamarkaði úthlutar	
2.2	Dagsetning og tími þegar hið alvarlega atvik sem tengist upplýsinga- og fjarskiptatækni uppgötvaðist	
2.3	Dagsetning og tími þegar atvik sem tengist upplýsinga- og fjarskiptatækni var flokkað sem alvarlegt	
2.4	Lýsing á alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni	
2.5	Flokkunarviðmið sem leiddu til þess að atvikstilkynningin var send	
2.6	Mikilvægismörk fyrir flokkunarviðmiðið „landfræðileg útbreiðsla“	
2.7	Uppgötvun á alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni	

Númer reits	Gagnasvæði	
2.8	Upplýsingar um hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni sé upprunnið hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði	
2.9	Virkjun áætlunar um rekstrarsamfellu, ef hún er virkjuð	
2.10	Aðrar viðeigandi upplýsingar	
Inntak áfangaskýrslu		
3.1	Tilvísunarkóði atviks sem lögbært yfirvald veitir	
3.2	Dagsetning og tími þegar hið alvarlega atvik sem tengist upplýsinga- og fjarskiptatækni varð	
3.3	Dagsetning og tími þegar þjónusta, starfsemi eða rekstur var endurreistur	
3.4	Fjöldi viðskiptavina sem urðu fyrir áhrifum	
3.5	Hlutfall viðskiptavina sem urðu fyrir áhrifum	
3.6	Fjöldi fjárhagslegra mótaðila sem urðu fyrir áhrifum	
3.7	Hlutfall fjárhagslegra mótaðila sem urðu fyrir áhrifum	
3.8	Áhrif á viðkomandi viðskiptavini eða fjárhagslega mótaðila	
3.9	Fjöldi viðskipta sem urðu fyrir áhrifum	
3.10	Hlutfall viðskipta sem urðu fyrir áhrifum	
3.11	Virði viðskipta sem urðu fyrir áhrifum	
3.12	Upplýsingar um hvort tölurnar eru raunverulegar eða áætlaðar eða hvort engin áhrif hafi orðið	
3.13	Áhrif á orðspor	
3.14	Samhengisbundnar upplýsingar um áhrif á orðspor	
3.15	Tímalengd alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni	
3.16	Niðritími þjónustu	
3.17	Upplýsingar um hvort tölurnar um tímalengd og niðritíma þjónustu séu raunverulegar eða áætlaðar.	
3.18	Tegundir áhrifa í aðildarríkjunum	
3.19	Lýsing á því hvernig alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur áhrif í öðrum aðildarríkjum	
3.20	Mikilvægismörk fyrir flokkunarviðmiðið „gagnatap“	

Númer reits	Gagnasvæði	
3.21	Lýsing á gagnatapinu	

Númer reits	Gagnasvæði	
3.22	Flokkunarviðmiðið „mikilvæg þjónusta sem varð fyrir áhrifum“	
3.23	Tegund alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni	
3.24	Aðrar tegundir atvika	
3.25	Ógnir og aðferðir sem ógnaraðili notar	
3.26	Aðrar tegundir aðferða	
3.27	Upplýsingar um starfssvið og rekstrarferla sem urðu fyrir áhrifum	
3.28	Hlutar innviða sem styðja við rekstrarferla og urðu fyrir áhrifum	
3.29	Upplýsingar um hluta innviða sem styðja við rekstrarferla og urðu fyrir áhrifum	
3.30	Áhrif á fjárhagslega hagsmuni viðskiptavina	
3.31	Skýrslugjöf til annarra yfirvalda	
3.32	Tilgreining á „öðrum“ yfirvöldum	
3.33	Tímabundnar aðgerðir eða -ráðstafanir sem gerðar eru, eða fyrirhugað er að gera, til að ná sér á strik eftir atvikið	
3.34	Lýsing á hvers kyns tímabundnum aðgerðum og ráðstöfunum sem gerðar hafa verið til eða fyrirhugað er að gera til að ná sér á strik eftir atvikið	
3.35	Vísbendingar um vásetningu	
Inntak lokaskýrslu		
4.1	Grófflokkun á frumorsökum atviksins	
4.2	Ítarleg flokkun á frumorsökum atviksins	
4.3	Viðbótarflokkun á frumorsökum atviksins	
4.4	Aðrar tegundir frumorsaka	
4.5	Upplýsingar um frumorsakir atviksins	
4.6	Samantekt um úrlausn atviks	
4.7	Dagsetning og tími þegar tekið var á frumorsök atviksins	
4.8	Dagsetning og tími úrlausnar atviksins	
4.9	Upplýsingar um hvort dagsetning varanlegrar úrlausnar atviksins er önnur en upphaflega áætlaður framkvæmdardagur	
4.10	Mat á áhættu fyrir nauðsynlega starfsemi með tilliti til skilameðferðar	

Númer reits	Gagnasvæði	
4.11	Upplýsingar sem skipta máli fyrir skilastjórnvöld	

Númer reits	Gagnasvæði	
4.12	Mikilvægismörk fyrir flokkunarviðmiðið „efnahagsleg áhrif“	
4.13	Fjárhæð vergs beins og óbeins kostnaðar og taps	
4.14	Fjárhæð fjárhagslegrar endurheimtar	
4.15	Upplýsingar um hvort atvikin sem ekki eru alvarleg hafi endurtekið sig	
4.16	Dagsetning og tími endurtekinna atvika	

II. VIÐAUKI

ORÐALISTI OG LEIÐBEININGAR UM SKÝRSLUGJÖF UM ALVARLEG ATVIK

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
Almennar upplýsingar um aðilann á fjármálamarkaði						
1.1.	Tegund framlagningar	Tilgreina skal tegund atvikatilkynningar eða -skýrslu sem lögð er fyrir lögbæra yfirvaldið.	Já	Já	Já	Val: — frumtilkynning, — áfangaskýrsla, — lokaskýrsla, — alvarlegt atvik endurflokkað sem ekki alvarlegt.
1.2.	Heiti aðilans sem leggur skýrsluna fram	Fullt lögheiti aðilans sem leggur skýrsluna fram.	Já	Já	Já	Alstafir
1.3.	Auðkenniskóði þess aðila sem leggur skýrsluna fram	Auðkenniskóði þess aðila sem leggur skýrsluna fram. Ef aðilar á fjármálamarkaði leggja fram tilkynningu/skýrslu skal auðkenniskóðinn vera auðkenni lögaðila (LEI), sem er einkvæmur 20 alstafa kóði, sem byggist á ISO-staðli 17442-1:2020. Þjónustuveitandi sem er þriðji aðili og leggur fram skýrslu fyrir aðila á fjármálamarkaði getur notað auðkenniskóða eins og tilgreint er í tæknilegu framkvæmdarstöðlunum sem samþykktir eru skv. 9. mgr. 28. gr. reglugerðar (ESB) 2022/2554.	Já	Já	Já	Alstafir
1.4.	Tegund aðila á fjármálamarkaði sem varð fyrir áhrifum	Tegund aðilans, eins og um getur í a- til t-lið 1. mgr. 2. gr. reglugerðar (ESB) 2022/2554, sem beiðnin er lögð fram fyrir. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skal velja hinar ólíku tegundir aðila á fjármálamarkaði sem falla undir sameinuðu skýrsluna.	Já	Já	Já	Val (fjölval): — lánastofnun, — greiðslustofnun, — undanþegin greiðslustofnun, — reikningsupplýsingaþjónustuveitandi, — rafeyrisfyrirtæki, — undanþegið rafeyrisfyrirtæki, — verðbréfafyrirtæki, — þjónustuveitandi sýndareigna, — útgefandi eignatengdra tóka, — verðbréfamiðstöð, — miðlægur mótaðili, — viðskiptavettvangur, — viðskiptaskrá,

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
						— rekstraraðili sérhæfðra sjóða, — rekstrarfélag, — veitandi gagnaskýrsluþjónustu, — vátrygginga- og endurtryggingafélag, — vátryggingamiðlari, endurtryggingamiðlari og vátryggingamiðlari í hliðarstarfsemi, — stofnun um starfstengdan lífeyri, — lánshæfismatsfyrirtæki, — stjórnandi mjög mikilvægra viðmiðana, — þjónustuveitandi hópfjármögnunar, — verðbréfunarskrá.
1.5.	Heiti aðila á fjármálamarkaði sem varð fyrir áhrifum	Fullt lögheiti aðilans á fjármálamarkaði sem varð fyrir áhrifum af alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni og er skylt að tilkynna um alvarlega atvikið til lögbærs yfirvalds síns skv. 19. gr. reglugerðar (ESB) 2022/2554. Ef um er að ræða sameinaða skýrslugjöf: a) listi yfir heiti allra þeirra aðila á fjármálamarkaði sem urðu fyrir áhrifum af alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni, aðskilin með semikommu, b) þjónustuveitandi sem er þriðji aðili og leggur fram tilkynningu eða skýrsluna um alvarlegt atvik á sameinaðan hátt, eins og um getur í 7. gr. þessarar reglugerðar, skal telja upp heiti allra aðila á fjármálamarkaði sem atvikið hefur áhrif á, aðskilin með semíkommu.	Já, ef aðilinn á fjármálamarkaði sem atvikið hafði áhrif á er annar en aðilinn sem leggur fram skýrsluna og ef um er að ræða sameinaða skýrslugjöf	Já, ef aðilinn á fjármálamarkaði sem atvikið hafði áhrif á er annar en aðilinn sem leggur fram skýrsluna og ef um er að ræða sameinaða skýrslugjöf	Já, ef aðilinn á fjármálamarkaði sem atvikið hafði áhrif á er annar en aðilinn sem leggur fram skýrsluna og ef um er að ræða sameinaða skýrslugjöf	Alstafir
1.6.	LEI-auðkenni þess aðila á fjármálamarkaði sem varð fyrir áhrifum	Auðkenni lögaðila (LEI) þess aðila á fjármálamarkaði sem varð fyrir áhrifum af alvarlegu atviki sem tengist upplýsinga- og fjarskiptatækni, úthlutað í samræmi við Alþjóðlegu staðlasamtökin. Ef um er að ræða sameinaða skýrslugjöf: a) listi yfir LEI-auðkenni allra þeirra aðila á fjármálamarkaði sem urðu fyrir áhrifum af alvarlega atvikinu sem tengist upplýsinga-	Já, ef aðilinn á fjármálamarkaði sem varð fyrir áhrifum af alvarlega atvikinu sem	Já, ef aðilinn á fjármálamarkaði sem varð fyrir áhrifum af alvarlega atvikinu sem	Já, ef aðilinn á fjármálamarkaði sem varð fyrir áhrifum af alvarlega atvikinu sem	Einkvæmur 20 alstafa kóði, sem byggist á ISO-staðli 17442-1:2020

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	og fjarskiptatækni, aðskilin með semikommu.	tengist upplýsinga- og fjarskiptatækni er ekki sá sami	tengist upplýsinga- og fjarskiptatækni er ekki sá sami og aðilinn	tengist upplýsinga- og fjarskiptatækni er ekki sá sami	

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
		b) þjónustuveitandi sem er þriðji aðili og leggur fram tilkynninguna eða skýrsluna um alvarlegt atvik á sameinaðan hátt, eins og um getur í 7. gr. þessarar reglugerðar, skal telja upp LEI-auðkenni allra aðila á fjármálamarkaði sem atvikið hefur áhrif á, aðskilin með semíkommu. Uppröðun á LEI-kóðum og heitum aðila á fjármálamarkaði skal vera eins.	og aðilinn sem leggur fram skýrsluna og ef um er að ræða sameinaða skýrslugjöf	sem leggur fram skýrsluna og ef um er að ræða sameinaða skýrslugjöf	og aðilinn sem leggur fram skýrsluna og ef um er að ræða sameinaða skýrslugjöf	
1.7.	Nafn aðaltengiliðar	Nafn og kenninafn aðaltengiliðar aðilans á fjármálamarkaði. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, heiti aðaltengiliðar hjá aðilanum á fjármálamarkaði sem leggur fram sameinuðu skýrsluna.	Já	Já	Já	Alstafir
1.8.	Netfang aðaltengiliðar	Netfang aðaltengiliðar sem lögbært yfirvald getur notað til eftirfylgnisamskipta. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, netfang aðaltengiliðar hjá aðilanum á fjármálamarkaði sem leggur fram sameinuðu skýrsluna.	Já	Já	Já	Alstafir
1.9.	Sími aðaltengiliðar	Símanúmer aðaltengiliðar sem lögbært yfirvald getur notað til eftirfylgnisamskipta. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, símanúmer aðaltengiliðar hjá aðilanum á fjármálamarkaði sem leggur fram sameinuðu skýrsluna. Gefa skal upp símanúmerið með öllum landsnúmerum (t.d. +33XXXXXXXXX)	Já	Já	Já	Alstafir
1.10.	Nafn annars tengiliðar	Nafn og kenninafn annars tengiliðar eða heiti ábyrgs teymis hjá aðilanum á fjármálamarkaði eða einingar sem leggur fram skýrsluna fyrir hönd aðilans á fjármálamarkaði	Já	Já	Já	Alstafir
1.11.	Netfang annars tengiliðar	Netfang annars tengiliðar eða virkt netfang teymisins sem lögbært yfirvald getur notað til eftirfylgnisamskipta.	Já	Já	Já	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
1.12. Sími annars tengiliðar	Símanúmer annars tengiliðar eða teymis sem lögbært yfirvald getur notað til eftirfylgnisamskipta. Gefa skal upp símanúmerið með öllum landsnúmerum (t.d. +33XXXXXXXXX)	Já	Já	Já	Alstafir
1.13. Heiti endanlegs móðurfyrirtækis	Heiti endanlegs móðurfélags samstæðunnar sem aðilinn á fjármálamarkaði, sem varð fyrir áhrifum, tilheyrir, eftir atvikum.	Já, ef aðilinn á fjármálamarkaði tilheyrir samstæðu	Já, ef aðilinn á fjármálamarkaði tilheyrir samstæðu	Já, ef aðilinn á fjármálamarkaði tilheyrir samstæðu	Alstafir
1.14. LEI-auðkenni endanlegs móðurfyrirtækis	LEI-auðkenni endanlegs móðurfélags samstæðunnar sem aðilinn á fjármálamarkaði, sem varð fyrir áhrifum, tilheyrir, eftir atvikum. Úthlutað í samræmi við Alþjóðlegu staðlasamtökin.	Já, ef aðilinn á fjármálamarkaði tilheyrir samstæðu	Já, ef aðilinn á fjármálamarkaði tilheyrir samstæðu	Já, ef aðilinn á fjármálamarkaði tilheyrir samstæðu	Einkvæmur 20 alstafa kóði, sem byggist á ISO-staðli 17442-1:2020
1.15. Gagnaskilagjaldmiðill	Gjaldmiðill sem notaður er í skýrslugjöf vegna atviks	Já	Já	Já	Val sem fyllt er með því að nota gjaldmiðilskóða ISO-staðals 4217
Inntak frumtilkynningarinnar					
2.1. Tilvísunarkóði atviks sem aðili á fjármálamarkaði úthlutar	Einkvæmur tilvísunarkóði sem aðili á fjármálamarkaði gefur út sem auðkennir með ótvíræðum hætti viðkomandi alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skal gefa upp tilvísunarkóða atviksins sem þjónustuveitandi sem er þriðji aðili úthlutar.	Já	Já	Já	Alstafir
2.2. Dagsetning og tími þegar atvikið sem	Dagsetning og tími þegar aðilinn á fjármálamarkaði fékk vitneskju um atvikið sem tengist upplýsinga- og fjarskiptatækni.	Já	Já	Já	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kkk:mm:ss)

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	tengist upplýsinga- og fjarskiptatækni uppgötvaðist	Hvað varðar endurtekin atvik: dagsetning og tími þegar nýjasta atvikið sem tengist upplýsinga- og fjarskiptatækni uppgötvaðist.				
2.3.	Dagsetning og tími þegar atvikið var flokkað sem alvarlegt	Dagsetning og tími þegar atvik sem tengist upplýsinga- og fjarskiptatækni var flokkað sem alvarlegt samkvæmt flokkunarviðmiðunum sem sett voru með framseldri reglugerð (ESB) 2024/1772	Já	Já	Já	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kkk:mm:ss)
2.4.	Lýsing á atvikinu sem tengist upplýsinga- og fjarskiptatækni	Lýsing á mikilvægustu þáttum alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni. Aðilar á fjármálamarkaði skulu veita gróft yfirlit yfir eftirfarandi upplýsingar, s.s. mögulegar orsakir, tafarlaus áhrif, kerfi sem urðu fyrir áhrifum og aðrar. Aðilar á fjármálamarkaði skulu telja með, ef vitað er eða raunhæft er að ætla, hvort atvikið hafi áhrif á þjónustuveitendur sem eru þriðju aðilar eða aðra aðila á fjármálamarkaði, tegund þjónustuveitanda eða aðila á fjármálamarkaði, heiti þeirra, auðkenniskóða þeirra og tegund auðkenniskóða (t.d. LEI-auðkenni eða einkvæmur evrópskur auðkenniskóði (EUID)). Í síðari skýrslum getur innihald reitsins þróast með tímanum til að endurspegla viðvarandi skilning á atvikinu sem tengist upplýsinga- og fjarskiptatækni og lýsa öllum öðrum mikilvægum upplýsingum um atvikið sem tengist upplýsinga- og fjarskiptatækni sem gagnareitirnir fanga ekki, þ.m.t. innra mat aðilans á fjármálamarkaði á alvarleika (t.d. mjög lágt, lágt, miðlungs, hátt, mjög hátt) og upplýsingar um stig og heiti æðstu einingar innan ákvarðanatökuskipulagsins sem hafa komið að viðbrögðum við atvikinu sem tengist upplýsinga- og fjarskiptatækni.	Já	Já	Já	Alstafir
2.5.	Flokkunarviðmið sem leiddu til þess að atvikstilkynningin var send	Flokkunarviðmiðin samkvæmt framseldri reglugerð (ESB) 2024/1772 sem leiddu til þess að ákveðið var að atvikið sem tengist upplýsinga- og fjarskiptatækni væri alvarlegt og tilkynning og skýrslugjöf send í framhaldinu. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, flokkunarviðmiðin sem leiddu til þess að ákveðið var að atvikið sem tengist upplýsinga- og fjarskiptatækni	Já	Já	Já	Val (fjölval): — viðskiptavinir, fjárhagslegir mótaðilar og viðskipti sem urðu fyrir áhrifum, — áhrif á orðspor, — tímalengd og niðritími þjónustu, — landfræðileg útbreiðsla, — gagnatap,

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
		væri alvarlegt fyrir a.m.k. einn eða fleiri aðila á fjármálamarkaði.				— mikilvæg þjónusta sem varð fyrir áhrifum, — efnahagsleg áhrif.
2.6.	Mikilvægismörk fyrir flokkunarviðmiðið „landfræðileg útbreiðsla“	Aðildarríki Evrópska efnahagssvæðisins sem verða fyrir áhrifum af alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni Þegar áhrif alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni eru metin í öðrum aðildarríkjum skulu aðilar á fjármálamarkaði taka tillit til 4. og 12. gr. framseldrar reglugerðar 2024/1772.	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Val (fjölval) fyllt út með því að nota ISO-staðal 3166 ALPHA-2 þeirra landa sem urðu fyrir áhrifum
2.7.	Uppgötvun á alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni	Upplýsingar um hvernig alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni uppgötvaðist.	Já	Já	Já	Val: — upplýsingatækniöryggi, — starfsfólk, — innri endurskoðun, — ytri endurskoðun, — viðskiptavinir, — fjárhagslegir mótaðilar, — þjónustuveitandi sem er þriðji aðili, — árásaraðili, — vöktunarkerfi, — yfirvald/stofnun/löggæsluaðili, — annar.
2.8.	Upplýsingar um hvort atvikið sé upprunnið hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði	Upplýsingar um hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni sé upprunnið hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði. Aðilar á fjármálamarkaði skulu tilgreina hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni eigi uppruna sinn hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði (þ.m.t. aðilum á fjármálamarkaði sem tilheyra sömu samstæðu og skýrslugjafareiningin) og heiti, auðkenniskóði þjónustuveitandans eða aðilans og tegund auðkenniskóða (t.d. LEI-auðkenni eða einkvæmt evrópskt auðkenni (EUID)).	Já, ef atvikið er upprunnið hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði	Já, ef atvikið er upprunnið hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði	Já, ef atvikið er upprunnið hjá þjónustuveitanda sem er þriðji aðili eða öðrum aðila á fjármálamarkaði	Alstafir
2.9.	Virkjun áætlunar um rekstrarsamfellu, ef hún er virkjuð	Upplýsingar um hvort viðbragðsráðstafanir í áætlun um rekstrarsamfellu hafi verið formlega virkjaðar hjá aðilanum á fjármálamarkaði.	Já	Já	Já	Boole-gildi (Já eða Nei)

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
2.10. Aðrar viðeigandi upplýsingar	Allar frekari upplýsingar sem sniðmátið tekur ekki til. Aðilar á fjármálamarkaði sem hafa endurflokkað alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni sem ekki alvarlegt skulu lýsa ástæðunum fyrir því hvers vegna atvik sem tengist upplýsinga- og fjarskiptatækni uppfyllir ekki, og þess ekki vænst að það uppfylli, viðmiðið til að teljast alvarlegt atvik.	Já, ef um aðrar upplýsingar er að ræða sem koma ekki fram í sniðmátinu eða ef alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur verið endurflokkað sem ekki alvarlegt	Já, ef um aðrar upplýsingar er að ræða sem koma ekki fram í sniðmátinu eða ef alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur verið endurflokkað sem ekki alvarlegt	Já, ef um aðrar upplýsingar er að ræða sem koma ekki fram í sniðmátinu eða ef alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur verið endurflokkað sem ekki alvarlegt	Alstafir

Inntak áfangaskýrslu

3.1. Tilvísunarkóði atviks sem lögbært yfirvald veitir	Einkvæmur tilvísunarkóði sem lögbært yfirvald úthlutar við móttöku frumtilkynningar til að auðkenna með ótvíræðum hætti alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni.	Nei	Já, ef við á	Já, ef við á	Alstafir
3.2. Dagsetning og tími þegar atvikið varð	Dagsetning og tími þegar alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni átti sér stað, ef það var ekki á sama tíma og þegar aðilinn á fjármálamarkaði fékk vitneskju um það. Hvað varðar endurtekin atvik: dagsetning og tími þegar nýjasta alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni uppgötvaðist.	Nei	Já	Já	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kkk:mm:ss)
3.3. Dagsetning og tími þegar þjónusta, starfsemi eða rekstur	Upplýsingar um dagsetningu og tíma endurreisnar þjónustu, starfsemi eða rekstrar sem varð fyrir áhrifum af alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni.	Nei	Já, ef fyllt hefur verið út í gagnareit 3.16	Já, ef fyllt hefur verið út í gagnareit 3.16	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kkk:mm:ss)

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	var endurreistur			„niðritími þjónustu“	„niðritími þjónustu“	
3.4.	Fjöldi viðskiptavina sem urðu fyrir áhrifum	Fjöldi viðskiptavina sem urðu fyrir áhrifum af hinu alvarlega atviki sem tengist upplýsinga- og fjarskiptatækni sem nýta þjónustu viðkomandi aðila á fjármálamarkaði. Við mat á fjölda viðskiptavina sem urðu fyrir áhrifum skulu aðilar á fjármálamarkaði taka tillit til 1. mgr. 1. gr. og b-liðar 1. mgr. 9. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu. Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegan fjölda viðskiptavina sem urðu fyrir áhrifum skal nota mat sem byggt er á tiltækum gögnum frá sambærilegum viðmiðunartímabilum. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, heildarfjöldi viðskiptavina sem urðu fyrir áhrifum hjá öllum aðilum á fjármálamarkaði.	Nei	Já	Já	Heil tala
3.5.	Hlutfall viðskiptavina sem urðu fyrir áhrifum	Hlutfall viðskiptavina sem urðu fyrir áhrifum af hinu alvarlega atviki sem tengist upplýsinga- og fjarskiptatækni miðað við heildarfjölda viðskiptavina sem nýta sér þá þjónustu sem urðu fyrir áhrifum og viðkomandi aðili á fjármálamarkaði veitir. Ef fleiri en ein tegund þjónustu varð fyrir áhrifum skal þjónustan sett fram á sameinuðu formi. Aðilar á fjármálamarkaði skulu taka tillit til 1. mgr. 1. gr. og a-liðar 1. mgr. 9. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu. Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegt hlutfall viðskiptavina sem verða fyrir áhrifum skal nota mat sem byggt er á tiltækum gögnum frá sambærilegum viðmiðunartímabilum. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skal aðili á fjármálamarkaði deila summu allra viðskiptavina sem urðu fyrir áhrifum með heildarfjölda viðskiptavina allra aðila á fjármálamarkaði sem urðu fyrir áhrifum.	Nei	Já	Já	Gefið upp sem hlutfall – öll gildi, allt að 5 tölustafir sem innihalda allt að einum aukastaf, gefin upp í prósentum (t.d. 2,4 í staðinn fyrir 2,4%). Ef gildið hefur fleiri en einn tölustaf á eftir tugabrotstákni skulu skýrslugefandi mótaðilar námunda upp

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.6. Fjöldi fjárhagslegra mótaðila sem urðu fyrir áhrifum	Fjöldi fjárhagslegra mótaðila sem urðu fyrir áhrifum af hinu alvarlega atviki, sem tengist upplýsinga- og fjarskiptatækni, og hafa gert samning við viðkomandi aðila á fjármálamarkaði. Við mat á hlutfalli fjárhagslegra mótaðila sem urðu fyrir áhrifum skulu aðilar á fjármálamarkaði taka tillit til 2. mgr. 1. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu. Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegan fjölda fjárhagslegra mótaðila sem verða fyrir áhrifum skal nota mat sem byggt er á tiltækum gögnum frá sambærilegum viðmiðunartímabilum. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, heildarfjöldi fjárhagslegra mótaðila sem urðu fyrir áhrifum hjá öllum aðilum á fjármálamarkaði.	Nei	Já	Já	Heil tala

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.7.	Hlutfall fjárhagslegra mótaðila sem urðu fyrir áhrifum	Hlutfall fjárhagslegra mótaðila sem urðu fyrir áhrifum af hinu alvarlega atviki sem tengist upplýsinga- og fjarskiptatækni miðað við heildarfjölda fjárhagslegra mótaðila sem hafa gert samning við viðkomandi aðila á fjármálamarkaði. Við mat á hlutfalli fjárhagslegra mótaðila sem urðu fyrir áhrifum skulu aðilar á fjármálamarkaði taka tillit til 1. mgr. 1. gr. og c-liðar 1. mgr. 9. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu. Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegt hlutfall fjárhagslegra mótaðila sem verða fyrir áhrifum skal nota mat sem byggt er á tiltækum gögnum frá sambærilegum viðmiðunartímabilum. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skal tilgreina summu allra fjárhagslegra mótaðila sem urðu fyrir áhrifum deilt með heildarfjölda fjárhagslegra mótaðila allra aðila á fjármálamarkaði sem urðu fyrir áhrifum.	Nei	Já	Já	Gefið upp sem hlutfall – öll gildi, allt að 5 tölustafir sem innihalda allt að einum aukastaf, gefin upp í prósentum (t.d. 2,4 í staðinn fyrir 2,4%). Ef gildið hefur fleiri en einn tölustaf á eftir tugabrotstákni skulu skýrslugefandi mótaðilar námunda upp
3.8.	Áhrif á viðkomandi viðskiptavini eða fjárhagslega mótaðila	Sérhver greind áhrif á viðkomandi viðskiptavini eða fjárhagslega mótaðila eins og um getur í 3. mgr. 1. gr. og f-lið 1. mgr. 9. gr. framseldrar reglugerðar (ESB) 2024/1772.	Nei	Já, ef viðmiðunarmörkin fyrir „mikilvægi viðskiptavina og fjárhagslegra mótaðila“ eru uppfyllt	Já, ef viðmiðunarmörkin fyrir „mikilvægi viðskiptavina og fjárhagslegra mótaðila“ eru uppfyllt	Boole-gildi (Já eða Nei)
3.9.	Fjöldi viðskipta sem urðu fyrir áhrifum	Fjöldi viðskipta sem urðu fyrir áhrifum af alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni. Við mat á áhrifum á viðskipti skulu aðilar á fjármálamarkaði taka tillit til 4. mgr. 1. gr. framseldrar reglugerðar (ESB) 2024/1772, þ.m.t. allra viðskipta innanlands og yfir landamæri sem urðu fyrir áhrifum og fela í sér peningafjárhæð þar sem a.m.k. einn hluti viðskiptanna fór fram í Sambandinu.	Nei	Já, ef atvikið hefur haft áhrif á viðskipti	Já, ef atvikið hefur haft áhrif á viðskipti	Heil tala

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegan fjölda viðskipta sem verða fyrir áhrifum skal nota mat sem byggt er á tiltækum gögnum frá sambærilegum viðmiðunartímabilum. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, heildarfjöldi viðskipta sem varð fyrir áhrifum hjá öllum aðilum á fjármálamarkaði.				
3.10. Hlutfall viðskipta sem urðu fyrir áhrifum	Hlutfall viðskipta sem urðu fyrir áhrifum borið saman við meðalfjölda viðskipta innanlands og yfir landamæri sem framkvæmd eru á dag af viðkomandi aðila á fjármálamarkaði í tengslum við þá þjónustu sem varð fyrir áhrifum. Aðilar á fjármálamarkaði skulu taka tillit til 4. mgr. 1. gr. og d-liðar 1. mgr. 9. gr. framseldrar reglugerðar (ESB) 2024/1772. Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegt hlutfall viðskipta sem verða fyrir áhrifum skal nota mat. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skal aðili á fjármálamarkaði leggja saman fjölda allra viðskipta sem urðu fyrir áhrifum og deila í hana með heildarfjölda viðskipta allra aðila á fjármálamarkaði sem urðu fyrir áhrifum.	Nei	Já, ef atvikið hefur haft áhrif á viðskipti	Já, ef atvikið hefur haft áhrif á viðskipti	Gefið upp sem hlutfall – öll gildi, allt að 5 tölustafir sem innihalda allt að einum aukastaf, gefin upp í prósentum (t.d. 2,4 í staðinn fyrir 2,4%). Ef gildið hefur fleiri en einn tölustaf á eftir tugabrotstákni skulu skýrslugefandi mótaðilar námunda upp
3.11. Virði viðskipta sem urðu fyrir áhrifum	Heildarvirði viðskiptanna sem alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur haft áhrif á skal metið í samræmi við 4. mgr. 1. gr. og e-lið 1. mgr. 9. gr. framseldrar reglugerðar (ESB) 2024/1772. Aðili á fjármálamarkaði sem getur ekki ákvarðað raunverulegt virði viðskipta sem urðu fyrir áhrifum skal nota mat sem byggt er á tiltækum gögnum frá sambærilegum viðmiðunartímabilum. Aðili á fjármálamarkaði skal greina frá fjárhæðinni sem jákvæðu virði. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, heildarfjöldi viðskipta sem urðu fyrir áhrifum	Nei	Já, ef atvikið hefur haft áhrif á viðskipti	Já, ef atvikið hefur haft áhrif á viðskipti	Fjárhæð Aðilar á fjármálamarkaði skulu tilgreina gagnapunkta í einingum með lágmarksnákvæmni sem samsvarar þúsundum eininga (t.d. 2,5 í stað 2 500 evra).

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	hjá öllum aðilum á fjármálamarkaði.				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.12. Upplýsingar um hvort tölurnar eru raunverulegar eða áætlaðar eða hvort engin áhrif hafi orðið	Upplýsingar um hvort tölurnar í gagnareitum 3.4 til 3.11 eru raunverulegar eða áætlaðar eða hvort engin áhrif hafi orðið.	Nei	Já	Já	Val (fjölval): — rauntölur yfir viðskiptavini sem urðu fyrir áhrifum, — rauntölur yfir fjárhagslega mótaðila sem urðu fyrir áhrifum, — rauntölur yfir viðskipti sem urðu fyrir áhrifum, — áætlun á viðskiptavinum sem urðu fyrir áhrifum, — áætlun á fjárhagslegum mótaðilum sem urðu fyrir áhrifum, — áætlun á viðskiptum sem urðu fyrir áhrifum, — engin áhrif á viðskiptavini, — engin áhrif á fjárhagslega mótaðila, — engin áhrif á viðskipti.
3.13. Áhrif á orðspor	Upplýsingar um áhrif á orðspor vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni eins og um getur í 2. og 10. gr. framseldrar reglugerðar (ESB) 2024/1772. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, þeir flokkar áhrifa á orðspor eiga við um a.m.k. einn aðila á fjármálamarkaði.	Nei	Já, ef viðmiðið „áhrif á orðspor“ er uppfyllt	Já, ef viðmiðið „áhrif á orðspor“ er uppfyllt	Val (fjölval): — fjallað hefur verið um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni í fjölmiðlum, — alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur valdið endurteknum kvörtunum frá mismunandi viðskiptavinum eða fjárhagslegum mótaðilum varðandi þjónustu með beinum samskiptum við viðskiptavini eða mikilvæg viðskiptasambönd — aðili á fjármálamarkaði mun ekki geta, eða líklegt er að hann geti ekki, uppfyllt kröfur samkvæmt reglum vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni, — aðili á fjármálamarkaði mun, eða er líklegur til að, missa viðskiptavini eða fjárhagslega mótaðila, sem hefur umtalsverð áhrif á viðskipti hans, vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni.

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.14. Samhengisbundnar upplýsingar um áhrif á orðspor	Upplýsingar sem lýsa því hvernig alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur haft eða gæti haft áhrif á orðspor aðilans á fjármálamarkaði, þ.m.t. brot á lögum, kröfur samkvæmt reglum ekki uppfylltar, fjöldi kvartana frá viðskiptavinum og annað.	Nei	Já, ef viðmiðið „áhrif á orðspor“ er uppfyllt.	Já, ef viðmiðið „áhrif á orðspor“ er uppfyllt.	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	Þessar samhengisbundnu upplýsingar skulu tiltaka tegund miðla (t.d. hefðbundna og stafræna miðla, blogg, streymisveitur) og umfjöllun fjölmiðla, þ.m.t. útbreiðsla fjölmiðlanna (staðbundnir, landsbundnir, alþjóðlegir). Umfjöllun fjölmiðla í þessu samhengi skal ekki þýða nokkur neikvæð ummæli fylgjenda eða notenda samfélagsmiðla. Aðili á fjármálamarkaði skal einnig tiltaka hvort í umfjöllun fjölmiðla hafi verið lögð áhersla á verulega áhættu fyrir viðskiptavini hennar í tengslum við alvarlegt atvik sem tengist upplýsinga- og fjarskiptatækni, þ.m.t. hættu á ógjaldfærni aðilans á fjármálamarkaði eða hættu á tapi fjármuna. Aðilar á fjármálamarkaði skulu einnig tilgreina hvort þeir hafi veitt fjölmiðlum upplýsingar í þeim tilgangi að upplýsa almenning með áreiðanlegum hætti um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni og afleiðingar þess. Aðilar á fjármálamarkaði geta einnig tilgreint hvort rangar upplýsingar hafi verið í fjölmiðlum í tengslum við atvikið sem tengist upplýsinga- og fjarskiptatækni, þ.m.t. upplýsingar sem byggðar eru á röngum upplýsingum sem ógnaraðilar hafa vísvitandi dreift eða upplýsingar sem varða eða sýna skemmdarverk á vefsetri aðilans á fjármálamarkaði.				
3.15. Tímalengd atviksins	Aðilar á fjármálamarkaði skulu mæla tímalengd alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni frá þeirri stundu sem atvikið varð þar til leyst var úr því. Aðilar á fjármálamarkaði sem geta ekki ákvarðað hvenær alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni átti sér stað skulu mæla tímalengd alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni frá þeirri stundu sem fyrr var, þegar aðilinn á fjármálamarkaði uppgötvaði atvikið eða þegar aðilinn á fjármálamarkaði skráði atvikið í net- eða kerfisskrár eða aðrar gagnalindir. Aðilar á fjármálamarkaði sem vita ekki enn hvenær alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni verður leyst skulu áætla það. Gildið skal gefið upp í dögum, klukkustundum og mínútum.	Nei	Já	Já	DD:KK:MM

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skulu aðilar á fjármálamarkaði mæla lengstu tímalengd alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni ef hún er mismunandi milli aðila.				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.16. Niðritími þjónustu	Niðritími þjónustu skal mældur frá því þegar þjónustan var að öllu leyti eða hluta til óaðgengileg viðskiptavinum, aðilum á fjármálamarkaði eða öðrum innri eða ytri notendum þar til regluleg starfsemi eða rekstur hefur verið færður aftur á sama þjónustustig og var veitt á undan atvikinu. Ef niðritími þjónustu veldur töfum á þjónustustarfsemi eftir að regluleg starfsemi eða rekstur hefur verið færður aftur í sama horf skulu aðilar á fjármálamarkaði mæla niðritímann frá upphafi alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni þangað til að seinkuð þjónusta er aftur veitt. Aðilar á fjármálamarkaði sem geta ekki ákvarðað hvenær niðritími þjónustu hófst skulu mæla niðritíma þjónustunnar frá þeirri stundu sem fyrr var, þegar atvikið greindist eða þegar það var skráð. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skulu aðilar á fjármálamarkaði mæla lengsta niðritíma þjónustunnar ef hann er mismunandi milli aðila.	Nei	Já, ef atvikið olli því að þjónusta lá niðri	Já, ef atvikið olli því að þjónusta lá niðri	DD:KK:MM
3.17. Upplýsingar um hvort tölurnar um tímalengd og niðritíma þjónustu séu raunverulegar eða áætlaðar	Upplýsingar um hvort tilkynntu gildin í gagnareitum 3.15 og 3.16 eru raunveruleg gildi eða áætluð gildi.	Nei	Já, ef viðmiðið „tímalengd og niðritími þjónustu“ er uppfyllt	Já, ef viðmiðið „tímalengd og niðritími þjónustu“ er uppfyllt	Val: — Rauntölur, — Áætlanir, — Rauntölur og áætlanir, — Engar upplýsingar tiltækar.
3.18. Tegundir áhrifa í aðildarríkjunum	Tegundir áhrifa í viðeigandi aðildarríkjum EES. Upplýsingar um hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hafi haft áhrif í öðrum aðildarríkjum EES (öðrum en aðildarríki þess lögbæra yfirvalds sem atvikið er tilkynnt til), í samræmi við 4. gr. framseldrar reglugerðar (ESB) 2024/1772, einkum með tilliti til þess hversu mikil áhrif það hefur í tengslum við: a) viðskiptavini og fjárhagslega mótaðila í öðrum aðildarríkjum sem urðu fyrir áhrifum eða	Nei	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Val (fjölval): — viðskiptavinir, — fjárhagslegir mótaðilar, — útibú aðilans á fjármálamarkaði, — aðilar á fjármálamarkaði innan samstæðunnar sem annast starfsemi í viðkomandi aðildarríki, — innviðir fjármálamarkaðar, — þjónustuveitendur sem eru þriðju aðilar og geta verið sameiginlegir öðrum aðilum á fjármálamarkaði.

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	b) útibú eða aðrir aðilar á fjármálamarkaði innan samstæðunnar sem annast starfsemi í öðrum aðildarríkjum eða c) innviðir fjármálamarkaðar eða þjónustuveitendur sem eru þriðju aðilar, sem kann að hafa áhrif á aðila á fjármálamarkaði í öðrum aðildarríkjum þar sem þeir veita þjónustu.				
3.19. Lýsing á því hvernig atvikið hefur áhrif í öðrum aðildarríkjum	Lýsing á áhrifum og alvarleika alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni í hverju aðildarríki sem varð fyrir áhrifum, þ.m.t. mat á áhrifum og alvarleika á: a) viðskiptavini, b) fjárhagslega mótaðila, c) útibú aðilans á fjármálamarkaði, d) aðra aðila á fjármálamarkaði innan samstæðunnar sem annast starfsemi í viðkomandi aðildarríki, e) innviði fjármálamarkaðar, f) þjónustuveitendur sem eru þriðju aðilar og geta verið sameiginlegir öðrum aðilum á fjármálamarkaði eftir því sem við á í öðru aðildarríki eða öðrum aðildarríkjum.	Nei	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Já, ef viðmiðunarmörkin fyrir „landfræðilega útbreiðslu“ eru uppfyllt	Alstafir
3.20. Mikilvægismörk fyrir flokkunarviðmiðið „gagnatap“	Gerðir gagnataps sem alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur í för með sér varðandi tiltækileika, ósvikni, réttleika og leynd gagna. Aðilar á fjármálamarkaði skulu taka tillit til 5. og 13. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, gagnatap sem hefur áhrif á a.m.k. einn aðila á fjármálamarkaði.	Nei	Já, ef viðmiðið „gagnatap“ er uppfyllt	Já, ef viðmiðið „gagnatap“ er uppfyllt	Val (fjölval): — tiltækileiki, — ósvikni, — réttleiki, — leynd gagna.
3.21. Lýsing á gagnatapinu	Lýsing á áhrifum alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni á tiltækileika, ósvikni, réttleika og leynd nauðsynlegra gagna í samræmi við 5. og 13. gr. framseldrar reglugerðar (ESB) 2024/1772. Upplýsingar um áhrif á framkvæmd viðskiptamarkmiða aðilans á fjármálamarkaði eða á það að uppfylla eftirlitskröfur. Aðilar á fjármálamarkaði skulu gefa til kynna, sem hluta af veittum upplýsingum, hvort gögnin sem urðu fyrir áhrifum séu gögn um viðskiptavini, gögn annarra stofnana (t.d. fjárhagslegra mótaðila)	Nei	Já, ef viðmiðið „gagnatap“ er uppfyllt	Já, ef viðmiðið „gagnatap“ er uppfyllt	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	eða gögn um aðilann á fjármálamarkaði sjálfan.				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	Aðilinn á fjármálamarkaði getur einnig tilgreint þá tegund gagna sem tengjast atvikinu – einkum hvort gögnin séu trúnaðarmál og um hvers konar trúnaðarskyldu var að ræða (t.d. viðskiptaleynd/trúnaður um rekstrarupplýsingar, persónuupplýsingar, þagnarskylda: bankaleynd, vátryggingaleynd, greiðsluþjónustuleynd o.s.frv.). Upplýsingarnar geta einnig falið í sér mögulega áhættu í tengslum við gagnatap, s.s. hvort nota megi gögnin sem atvikið hafði áhrif á til að bera kennsl á einstaklinga og ógnaraðilinn gæti notað til að auka lánstraust eða fá lán án þeirra samþykkis, til að gera beinskeyttar vefveiðiárásir, til að birta upplýsingar opinberlega. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, almenn lýsing á áhrifum atviksins á þá aðila á fjármálamarkaði sem urðu fyrir áhrifum. Ef áhrifin eru mismunandi skal lýsingin á áhrifunum gefa skýrt til kynna hvaða sérstöku áhrif þetta hefur á mismunandi aðila á fjármálamarkaði.				
3.22. Flokkunarviðmiðið „mikilvæg þjónusta sem varð fyrir áhrifum“	Upplýsingar varðandi viðmiðið „mikilvæg þjónusta sem varð fyrir áhrifum“. Aðilar á fjármálamarkaði skulu taka tillit til 6. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu, þ.m.t. upplýsinga um: — þjónustuna eða starfsemina sem varð fyrir áhrifum, sem útheimtir starfsleyfi, skráningu eða er undir eftirliti lögbærra yfirvalda, eða — þá upplýsinga- og fjarskiptatækniþjónustu eða þau net- og upplýsingakerfi sem styðja nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði, og — eðli óheimils aðgangs í illum tilgangi að net- og upplýsingakerfum aðila á fjármálamarkaði. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, þau áhrif á mikilvæga þjónustu sem eiga við um a.m.k. einn aðila á fjármálamarkaði.	Nei	Já	Já	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.23. Tegund atviks	Flokkun atvika eftir tegund.	Nei	Já	Já	Val (fjölval): — Netöryggistengt, — Brestur í ferlum, — Kerfisbilun, — Ytri atburður, — Greiðslutengt, — Annað (tilgreina skal nánar).
3.24. Aðrar tegundir atvika	Aðrar tegundir atvika sem tengjast upplýsinga- og fjarskiptatækni: aðilar á fjármálamarkaði sem hafa valið „annað“ í tegund atviks í gagnareit 3.23 skulu tilgreina tegund atviks sem tengist upplýsinga- og fjarskiptatækni.	Nei	Já, ef „annað“ var valið sem tegund atviks í gagnareit 3.23	Já, ef „annað“ var valið sem tegund atviks í gagnareit 3.23	Alstafir
3.25. Ógnir og aðferðir sem ógnaraðili notar	Tilgreina skal ógnir og aðferðir sem ógnaraðili notar, þ.m.t.: a) samskiptablekking, þ.m.t. vefveiðar, b) (dreifð) álagsárás, c) auðkennisþjófnaður, d) dulkóðun gagna í skaðlegum tilgangi, þ.m.t. gagnagíslatökuforrit, e) óheimil notkun tilfanga, f) gagnastuldur og hagræðing gagna, að undanskildum auðkennisþjófnaði, g) gagnaeyðilegging, h) afmyndun, i) tölvuárás á aðfangakeðju, j) annað (tilgreina skal nánar).	Nei	Já, ef tegund atviks sem tengist upplýsinga- og fjarskiptatækni er „net-öryggistengt“ í reit 3.23	Já, ef tegund atviks sem tengist upplýsinga- og fjarskiptatækni er „net-öryggistengt“ í reit 3.23	Val (fjölval): — Samskiptablekking, þ.m.t. vefveiðar, — (Dreifð) álagsárás, — Auðkennisþjófnaður, — Dulkóðun gagna í skaðlegum tilgangi, þ.m.t. gagnagíslatökuforrit, — Óheimil notkun tilfanga, — Gagnastuldur og hagræðing gagna, þ.m.t. auðkennisþjófnaður, — Gagnaeyðilegging, — Afmyndun, — Tölvuárás á aðfangakeðju, — Annað (tilgreina skal nánar).
3.26. Aðrar tegundir aðferða	Aðrar tegundir aðferða Aðilar á fjármálamarkaði sem völdu „annað“ við tegund aðferðar í gagnareit 3.25 skulu tilgreina gerð aðferðar.	Nei	Já, ef „annað“ var valið sem tegund aðferðar í gagnareit 3.25	Já, ef „annað“ var valið sem tegund aðferðar í gagnareit 3.25	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.27. Upplýsingar um starfssvið og rekstrarferla sem urðu fyrir áhrifum	Upplýsingar um starfssviðin og rekstrarferlana sem atvikið hafði áhrif á, þ.m.t. vörur og þjónusta. Starfssvið skulu m.a. vera en ekki takmarkast við: a) markaðssetning og fyrirtækjaþróun, b) þjónusta við viðskiptavini, c) vörustjórnun, d) regluvarsla, e) áhættustjórnun, f) fjármál og reikningsskil, g) mannauðsstjórnun og almenn þjónusta, h) upplýsingatækni. Rekstrarferlarnir skulu m.a. vera, en ekki takmarkast við: — reikningsupplýsingar, — tryggingafræðileg þjónusta, — færsluhirðing greiðslna, — auðkenning/heimildarveiting, — heimildir, — inntaka nýrra viðskiptavina, — réttindastjórnun, — stjórnun réttindagreiðslna, — kaup og sala pakkaðra vátryggingarsamninga á milli vátrygginga, — kortagreiðslur, — reiðufjárstjórnun, — ráðstöfun eða úttektir reiðufjár, — umsýsla vátryggingakrafna, — afgreiðsla vátryggingarkrafna, — stöðustofnun, — lán til fyrirtækjasamsteypa, — sameiginlegar tryggingar, — millifærsla fjármuna, — varsla og varðveisla eigna, — innleiðing nýrra viðskiptavina, — inntaka gagna, — gagnavinnsla, — beingreiðslur, — útflutningstryggingar, — lokafrágangur viðskipta/samninga, — setning fjármálagerninga á markað, — reikningshald sjóða,	Nei	Já	Já	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	— gjaldeyrir, — fjárfestingarráðgjöf, — fjárfestingarstýring, — útgáfa greiðslumiðla, — útlánastýring, — greiðsluferli líftrygginga, — peningasendingar, — útreikningur á hreinni eign, — fyrirmæli, — greiðsluvirkjun, — vátryggingar, — stýring eignasafna, — innheimta iðgjalda, — móttaka/flutningur/framkvæmd, — endurtryggingar, — uppgjör, — vöktun viðskipta. Ef um er að ræða sameinaða skýrslugjöf eins og um getur í 7. gr. þessarar reglugerðar, þau starfssvið og rekstrarferlar sem urðu fyrir áhrifum hjá a.m.k. einum aðila á fjármálamarkaði.				
3.28. Hlutar innviða sem styðja við rekstrarferla og urðu fyrir áhrifum	Upplýsingar um hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hafi haft áhrif á hluta innviða (netþjóna, stýrikerfi, hugbúnað, hugbúnaðarþjóna, millibúnað, netkerfishluta, aðra) sem styðja rekstrarferla.	Nei	Já	Já	Val: — Já, — Nei, — Upplýsingar ekki tiltækar.
3.29. Upplýsingar um hluta innviða sem styðja við rekstrarferla og urðu fyrir áhrifum	Lýsing á áhrifum alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni á hluta innviða sem styðja rekstrarferla, þ.m.t. vélbúnað og hugbúnað. Vélbúnaður er m.a. netþjónar, tölvur, gagnaver, skiptistöðvar, beinar og netöld. Hugbúnaður er m.a. stýrikerfi, forrit, gagnagrunnar, öryggistól, netkerfisíhlutir, annað tilgreinið nánar. Lýsingarnar skulu lýsa eða nefna hluta eða kerfi viðkomandi innviðar sem varð fyrir áhrifum og, ef tiltækt er: a) upplýsingar um útgáfu, b) innri innviðir/útvistað að hluta til/útvistað að fullu – nafn þjónustuveitanda sem er þriðji aðili,	Nei	Já, ef atvikið hefur haft áhrif á hluta innviða sem styðja rekstrarferla	Já, ef atvikið hefur haft áhrif á hluta innviða sem styðja rekstrarferla	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	c) hvort innviðir séu notaðir í, eða deilt með, margs konar viðskiptastarfsemi, d) viðeigandi álagsþols-/samfellu-/endurheimtar-/staðgöngufyrirkomulag sem eru fyrir hendi.				
3.30. Áhrif á fjárhagslega hagsmuni viðskiptavina	Upplýsingar um hvort alvarlega atvikið í tengslum við upplýsinga- og fjarskiptatækni hafi haft áhrif á fjárhagslega hagsmuni viðskiptavina.	Nei	Já	Já	Val: — Já, — Nei, — Upplýsingar ekki tiltækar.
3.31. Skýrslugjöf til annarra yfirvalda	Upplýsingar um hvaða yfirvöld voru látin vita um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni. Að teknu tilliti til mismunar sem rekja má til landslöggjafar í aðildarríkjunum skal skilningur aðila á fjármálamarkaði á hugtakinu löggæsluyfirvöld vera víður til að það feli í sér opinber yfirvöld sem hafa heimildir til að sækja til saka fyrir tölvubrot, þ.m.t. lögreglu, löggæslustofnanir og saksóknara.	Nei	Já	Já	Val (fjölval): — Lögregla/löggæslustofnanir, — Viðbragðsteymi vegna váatvika er varða tölvuöryggi, — Persónuverndaryfirvöld, — Innlend netöryggisstofnun, — Engin, — Annað (tilgreina skal nánar).
3.32. Tilgreining á „öðrum“ yfirvöldum	Upplýsingar um hvaða „aðrar“ tegundir yfirvalda voru látin vita um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni. Ef „annað“ var valið í gagnareit 3.31 skal lýsingin fela í sér ítarlegri upplýsingar um yfirvaldið sem aðilinn á fjármálamarkaði sendi upplýsingar um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni.	Nei	Já, ef aðilinn á fjármálamarkaði upplýsti „aðra“ tegund yfirvalds um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni.	Já, ef aðilinn á fjármálamarkaði upplýsti „aðra“ tegund yfirvalds um alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni	Alstafir
3.33. Tímabundnar aðgerðir eða -ráðstafanir sem gerðar eru, eða fyrirhugað er að	Upplýsingar um hvort aðilinn á fjármálamarkaði hafi tekið upp (eða hyggist taka upp) tímabundnar aðgerðir sem gerðar hafa verið (eða áætlað er að gera) til að ná sér á strik eftir alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni.	Nei	Já	Já	Boole-gildi (Já eða Nei)

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
gera, til að ná sér á strik eftir atvikið					

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
3.34. Lýsing á hvers kyns tímabundnum aðgerðum og ráðstöfunum sem gerðar hafa verið til eða fyrirhugað er að gera til að ná sér á strik eftir atvikið	Upplýsingarnar skulu lýsa þeim aðgerðum sem gripið var til tafarlaust, þ.m.t. einangrun atviksins á vettvangi netkerfisins, bráðabirgðalausnum, lokun USB-tengja, virkjun vinnslustaðar til endurreisnar eftir stóráfall, og hvers konar viðbótaröryggiseftirliti sem tekið er upp tímabundið. Aðilar á fjármálamarkaði skulu tilgreina dagsetningu og tíma þegar tímabundnu aðgerðirnar voru gerðar og hvaða dag áætlað er að snúið verði til baka á aðalvinnslustaðinn. Ef um er að ræða tímabundnar aðgerðir sem hafa ekki verið innleiddar en eru ennþá fyrirhugaðar skal tilgreina dagsetninguna sem áætlað er að þær komi til framkvæmda. Ef ekki hefur verið gripið til neinna tímabundinna aðgerða/ráðstafana skal tilgreina ástæðu.	Nei	Já, ef gripið hefur verið til tímabundinna aðgerða/ráðstafana eða ef fyrirhugað er að grípa til þeirra (upplýsingareitur 3.33)	Já, ef gripið hefur verið til tímabundinna aðgerða/ráðstafana eða ef fyrirhugað er að grípa til þeirra (upplýsingareitur 3.33)	Alstafir
3.35. Vísbendingar um vásetningu	Upplýsingar varðandi meiriháttar atvik sem tengist upplýsinga- og fjarskiptatækni sem gætu hjálpað til við að greina skaðlega virkni innan net- eða upplýsingakerfis (vísbendingar um vásetningu (e. *Indicators of Compromise (IoC)*), eftir atvikum. Reiturinn á aðeins við um þá aðila á fjármálamarkaði sem falla undir gildissvið tilskipunar Evrópuþingsins og ráðsins (ESB) 2022/2555 ([1]) og þá aðila á fjármálamarkaði sem tilgreindir eru sem nauðsynlegir eða þýðingarmiklir aðilar samkvæmt landsreglum sem leiða í lög 3. gr. tilskipunar (ESB) 2022/2555, ef við á. Þær vísbendingar um vásetningu sem aðili á fjármálamarkaði lætur í té skulu innihalda eftirfarandi gagnaflokka: a) IP-tölur, b) vefslóðir, c) lén, d) skráartæti (e. *file hashes*), e) gögn um spilliforrit (e. *malware data*) (heiti spilliforrits, skráarheiti og staðsetning þeirra, sérstakir skráarlyklar sem tengjast virkni spilliforrits), f) gögn um virkni nets (tengi, samskiptareglur, vistföng, tilvísunarslóðir, aðgangsforrit, hausar, tilteknar aðgerðaskrár eða sérstakt mynstur í netumferð),	Nei	Já, ef netöryggistengt er valið sem tegund atviks í gagnareit 3.23	Já, ef netöryggistengt er valið sem tegund atviks í gagnareit 3.23	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	g) gögn um tölvupóstskilaboð (sendandi, viðtakandi, efni, yfirskrift, innihald),				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	h) beiðnir nafnaþjóns léns og skráasamskipan, i) virkni á notendareikningum (innskráningar, virkni á reikningum notenda með aukin réttindi, aukning réttinda), j) gagnagrunnsumferð (les/skrif), beiðnir til sömu skrár. Í reynd getur þessi tegund upplýsinga tekið til gagna sem varða m.a. vísa sem lýsa mynstri í netumferð sem samsvara þekktum árásum/yrkjanetsamskiptum, IP-vistföng véla sem eru sýktar af spilliforritum (yrkjum), gögn sem tengjast þjónum til „skipana og stjórnunar“ sem spilliforrit nota (vanalega lén eða IP-vistföng) og vefslóðir sem tengjast vefveiðisetrum eða vefsetrum sem vitað er að hýsi spilliforrit eða veilubragðapakka.				
Inntak lokaskýrslu					
4.1. Grófflokkun á frumorsökum atviksins	Grófflokkun frumorsaka hins alvarlega atviks í tengslum við upplýsinga- og fjarskiptatækni undir tegundum atvika, þ.m.t. eftirfarandi grófflokkar: a) aðgerðir af illum ásetningi, b) brestur í ferlum, c) kerfisbilun/truflun, d) mannleg mistök, e) ytri atburður.	Nei	Nei	Já	Val (fjölval): — aðgerðir af illum ásetningi, — brestur í ferlum, — kerfisbilun / truflun, — mannleg mistök, — ytri atburður.
4.2. Ítarleg flokkun á frumorsökum atviksins	Ítarleg flokkun á frumorsökum hins alvarlega atviks sem tengist upplýsinga- og fjarskiptatækni undir tegundum atvika, þ.m.t. eftirfarandi ítarlegir flokkar sem tengjast grófflokkunum sem eru tilkynntir í gagnareit 4.1: 1. **Aðgerðir af illum ásetningi** (ef valið skal velja eitt eða fleira af eftirfarandi): a) innri aðgerðir af ásettu ráði, b) efnislegar skemmdir af ásettu ráði/hagræðing/þjófnaður, c) sviksamlegt athæfi. 2. **Brestur í ferlum** (ef valið skal velja eitt eða fleira af eftirfarandi): a) vöktun ófullnægjandi eða vöktun og eftirlit bregst,	Nei	Nei	Já	Val (fjölval): — aðgerðir af illum ásetningi: innri aðgerðir af ásettu ráði, — aðgerðir af illum ásetningi: efnislegar skemmdir af ásettu ráði/hagræðing/þjófnaður, — aðgerðir af illum ásetningi: sviksamlegt athæfi, — brestur í ferlum: vöktun ófullnægjandi eða vöktun og eftirlit bregst, — brestur í ferlum: hlutverk og ábyrgðarsvið ófullnægjandi eða óljós, — brestur í ferlum: stýringarferli upplýsinga- og fjarskiptatækniáhættu bregst,

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
					— brestur í ferlum: upplýsinga- og fjarskiptatæknirekstur og öryggisaðgerðir upplýsinga- og fjarskiptatækni eru ófullnægjandi eða bregðast,

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	b) hlutverk og ábyrgðarsvið eru ófullnægjandi eða óljós, c) stýringarferli upplýsinga- og fjarskiptatækniáhættu bregst, d) upplýsinga- og fjarskiptatæknirekstur og öryggisaðgerðir upplýsinga- og fjarskiptatækni eru ófullnægjandi eða bregðast, e) verkefnastjórnun á sviði upplýsinga- og fjarskiptatækni ófullnægjandi eða bregst, f) ófullnægjandi innri stefnur, verklagsreglur og skjalahald, g) ófullnægjandi öflun, þróun eða viðhald á upplýsinga- og fjarskiptatæknikerfum, h) annað (tilgreina skal nánar). 3. **Kerfisbilun/truflun** (ef valið skal velja eitt eða fleira af eftirfarandi): a) geta og afköst vélbúnaðar: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem orsakast af vélbúnaði sem reynist ófullnægjandi með tilliti til afkasta eða frammistöðu til að uppfylla viðeigandi lagalegar kröfur, b) viðhald vélbúnaðar: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem stafa af ófullnægjandi eða vanræktu viðhaldi á íhlutum vélbúnaðar, öðru en „úreldingu/öldrun vélbúnaðar“, c) úrelding/öldrun vélbúnaðar: þessi tegund frumorsakar tekur til alvarlegra atvika sem tengjast upplýsinga- og fjarskiptatækni sem stafa af úreltum eða gömlum vélbúnaðaríhlutum, d) samrýmanleiki/samskipan hugbúnaðar: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem orsakast af hugbúnaðaríhlutum sem eru ósamrýmanlegir öðrum hugbúnaði eða samskipan kerfis, þ.m.t. alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem koma til vegna árekstra milli hugbúnaðar, rangra stillinga eða rangt stilltra stika sem hafa áhrif á heildarvirkni kerfisins, e) afköst hugbúnaðar: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem stafa af hugbúnaðaríhlutum sem sýna lélega frammistöðu eða óskilvirkni, af öðrum ástæðum en þeim sem tilgreindar eru í „samrýmanleiki/samskipan hugbúnaðar“, þ.m.t. atvik sem tengjast upplýsinga- og fjarskiptatækni sem orsakast af hægum við-				— brestur í ferlum: verkefnastjórnun á sviði upplýsinga- og fjarskiptatækni ófullnægjandi eða bregst, — brestur í ferlum: ófullnægjandi innri stefnur, verklagsreglur og skjalahald, — brestur í ferlum: ófullnægjandi öflun, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum, — brestur í ferlum: annað (tilgreina skal nánar), — kerfisbilun: afköst og frammistaða vélbúnaðar, — kerfisbilun: viðhald vélbúnaðar, — kerfisbilun: úrelding/öldrun vélbúnaðar, — kerfisbilun: samrýmanleiki/samskipan hugbúnaðar, — kerfisbilun: frammistaða hugbúnaðar, — kerfisbilun: netstillingar, — kerfisbilun: efnislegar skemmdir, — kerfisbilun: annað (tilgreina skal nánar), — mannleg mistök: athafnaleysi, — mannleg mistök: mistök, — mannleg mistök: færni og þekking, — mannleg mistök: starfsmannahald er ófullnægjandi, — mannleg mistök: óskilvirk samskipti, — mannleg mistök: önnur (tilgreina skal nánar), — ytri atburður: náttúruhamfarir/óviðráðanleg atvik, — ytri atburður: brestur hjá þriðja aðila, — ytri atburður: annað (tilgreina skal nánar).

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	bragðstíma, óhóflegri notkun auðlinda eða óskilvirkri inningu fyrirspurna sem hefur áhrif á frammistöðu hugbúnaðarins eða kerfisins,				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	f) netstillingar: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem stafa af röngum eða ranglega stilltum netstillingum eða innviðum, þ.m.t. alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem stafa af villum í samskipan nets, beiningarvandamálum, röngum stillingum eldveggja eða öðrum vandamálum tengdum netinu sem hafa áhrif á tengingu eða fjarskipti, g) efnislegar skemmdir: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem orsakast af efnislegum skemmdum á innviðum upplýsinga- og fjarskiptatækni sem leiða til kerfisbilana, h) annað (tilgreina skal nánar). 4. **Mannleg mistök** (ef valið skal velja eitt eða fleira af eftirfarandi): a) athafnaleysi (óviljandi), b) mistök, c) færni og þekking: alvarleg atvik í tengslum við upplýsinga- og fjarskiptatækni sem stafa af skorti á sérfræðiþekkingu eða hæfni í meðferð upplýsinga- og fjarskiptatæknikerfa eða -ferla sem geta orsakast af ónógri þjálfun, ófullnægjandi þekkingu eða skort á færni sem þarf til að framkvæma tiltekin verkefni eða takast á við tæknilegar áskoranir, d) ófullnægjandi mannauður: alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni sem verða vegna skorts á nauðsynlegum tilföngum, þ.m.t. vélbúnaði, hugbúnaði, innviðum eða starfsfólki, og þ.m.t. aðstæður þar sem ónóg tilföng hafa í för með sér rekstrarlega óskilvirkni, kerfisbilanir eða vangetu til að uppfylla viðskiptalegar kröfur, e) óskilvirk samskipti, f) annað (tilgreina skal nánar). 5. **Ytri atburður** (ef valið skal velja eitt eða fleira af eftirfarandi): a) náttúruhamfarir/óviðráðanlegar aðstæður, b) brestur hjá þriðja aðila,				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	c) annað (tilgreina skal nánar). Aðilar á fjármálamarkaði skulu hafa í huga að þegar um er að ræða endurtekin alvarleg atvik sem tengjast upplýsinga- og fjarskiptatækni skal taka mið af þeirri tilteknu frumorsök sem virðist liggja að baki atvikinu fremur en hinum víðu flokkum sem tilgreindir eru í þessum reit.				
4.3. Viðbótarflokkun á frumorsökum atviksins	Viðbótarflokkun á frumorsökum hins alvarlega atviks sem tengist upplýsinga- og fjarskiptatækni undir tegund atviksins, þ.m.t. eftirfarandi viðbótarflokkar sem tengjast ítarlegu flokkunum sem tilkynna skal í gagnareit 4.2. Reiturinn er skyldubundinn í lokaskýrslu ef greint er frá sérstökum flokkum sem krefjast frekari sundurgreiningar í gagnareit 4.2. 2.a) **Vöktun og eftirlit ófullnægjandi eða bregst:** a) eftirlit með því að stefnu sé fylgt, b) eftirlit með þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, c) vöktun og sannprófun á úrbótum á veikleikum, d) auðkenningar- og aðgangsstjórnun, e) dulkóðun og dulmál, f) aðgerðaskráning. 2. c) **Brestur í stýringarferli upplýsinga- og fjarskiptatækniáhættu:** a) ekki tilgreint rétt áhættuþol, b) ófullnægjandi mat á veikleikum og ógnum, c) ófullnægjandi ráðstafanir vegna meðferðar áhættu, d) léleg stýring á eftirstæðri upplýsinga- og fjarskiptatækniáhættu. 2. d) **Upplýsinga- og fjarskiptatæknirekstur og öryggisaðgerðir upplýsinga- og fjarskiptatækni eru ófullnægjandi eða bregðast:** a) veikleika- og bótastjórnun, b) breytingastjórnun, c) afkasta- og frammistöðustjórnun,	Nei	Nei	Já	Val (fjölval): — eftirlit með því að stefnu sé fylgt, — eftirlit með þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, — vöktun og sannprófun á úrbótum á veikleikum, — auðkenningar- og aðgangsstjórnun, — dulkóðun og dulmál, — aðgerðaskráning, — ekki tilgreint rétt áhættuþol, — ófullnægjandi mat á veikleikum og ógnum, — ófullnægjandi ráðstafanir vegna meðferðar áhættu, — léleg stýring á eftirstæðri upplýsinga- og fjarskiptatækniáhættu, — veikleika- og bótastjórnun, — breytingastjórnun, — afkasta- og frammistöðustjórnun, — stýring upplýsinga- og fjarskiptatæknieigna og flokkun upplýsinga, — öryggisafritun og endurheimt, — meðhöndlun villna, — ófullnægjandi öflun, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum, — prófanir á hugbúnaði eru ófullnægjandi eða bregðast.

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	d) stýring upplýsinga- og fjarskiptatæknieigna og flokkun upplýsinga,				

Gagnasvæði		Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
		e) öryggisafritun og endurheimt, f) meðhöndlun villna. 2. g) **Ófullnægjandi öflun, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum:** a) ófullnægjandi öflun, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum, b) prófanir á hugbúnaði ófullnægjandi eða bregðast.				
4.4.	Aðrar tegundir frumorsaka	Aðilar á fjármálamarkaði sem völdu „önnur“ við tegund frumorsakar í gagnareit 4.2 skulu tilgreina aðrar tegundir frumorsaka	Nei	Nei	Já, ef „önnur“ var valin sem tegund frumorsakar í gagnareit 4.2.	Alstafir
4.5.	Upplýsingar um frumorsakir atviksins	Lýsing á atburðarásinni sem leiddi til hins alvarlega atviks sem tengist upplýsinga- og fjarskiptatækni og lýsing á því hvernig alvarlega atvikið virðist hafa svipaða frumorsök ef það er flokkað sem endurtekið atvik, þ.m.t. gagnorð lýsing á öllum undirliggjandi ástæðum og helstu þáttum sem stuðluðu að því að atvikið átti sér stað. Ef um var að ræða aðgerðir af illum ásetningi, lýsing á aðferðafræðinni við þær aðgerðir, þ.m.t. úrræði, tækni og verklag sem notað var, ásamt innkomuvigrinum sem leiddi til alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni, þ.m.t. lýsing á rannsóknum og greiningum sem leiddu til greiningar á frumorsökunum, ef við á.	Nei	Nei	Já	Alstafir
4.6.	Úrlausn atviks	Viðbótarupplýsingar varðandi aðgerðir/ráðstafanir sem gerðar hafa verið/fyrirhugaðar eru til að leysa varanlega úr alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni og til að koma í veg fyrir að slíkt atvik eigi sér stað aftur. Lærdómur sem dreginn er af alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni.	Nei	Nei	Já	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	Í lýsingunni skulu koma fram eftirfarandi atriði: 1. **Lýsing á aðgerðum til úrlausnar** a) Aðgerðir sem gripið er til í því skyni að leysa varanlega úr alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni (að undanskildum tímabundnum aðgerðum), b) fyrir hverja aðgerð sem gripið er til, tilgreina mögulega aðkomu þjónustuveitanda sem er þriðji aðili og viðkomandi aðila á fjármálamarkaði, c) tilgreina hvort verklagsreglur hafi verið aðlagaðar í kjölfar alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni, d) tilgreina skal allar viðbótarráðstafanir sem voru gerðar eða eru fyrirhugaðar með tengdri tímaáætlun framkvæmdar. Möguleg vandamál sem greinast að því er varðar traustleika þeirra upplýsingatæknikerfa sem verða fyrir áhrifum/eða með tilliti til verklagsreglna eða eftirlits sem er til staðar, ef við á. Aðilar á fjármálamarkaði skulu tilgreina með skýrum hætti hvernig fyrirhugaðar aðgerðir til úrbóta munu taka á tilgreindum frumorsökum og hvenær búist er við að alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni verði endanlega leyst. 2. **Lærdómur** Aðilar á fjármálamarkaði skulu lýsa niðurstöðum úr greiningu í kjölfar atviks.				
4.7. Dagsetning og tími þegar tekið var á frumorsök atviksins	Dagsetning og tími þegar tekið var á frumorsök atviksins.	Nei	Nei	Já	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kk:mm:ss)
4.8. Dagsetning og tími úrlausnar atviksins	Dagsetning og tími úrlausnar atviksins.	Nei	Nei	Já	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kk:mm:ss)

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
4.9. Upplýsingar um hvort dagsetning varanlegrar úrlausnar atvikanna er önnur en upphaflega áætlaður framkvæmdardagur	Lýsingar á ástæðum þess að dagsetning endanlegrar úrlausnar á alvarlega atvikinu sem tengist upplýsinga- og fjarskiptatækni er frábrugðin upphaflega áætlaðri dagsetningu framkvæmdar, eftir atvikum.	Nei	Nei	Já	Alstafir
4.10. Mat á áhættu fyrir nauðsynlega starfsemi með tilliti til skilameðferðar	Mat á því hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni feli í sér áhættu fyrir nauðsynlega starfsemi í skilningi 35. liðar 1. mgr. 2. gr. tilskipunar Evrópuþingsins og ráðsins 2014/59/ESB ([2]). Aðilar, eins og um getur í 1. mgr. 1. gr. tilskipunar 2014/59/ESB, skulu tilgreina hvort atvikið feli í sér áhættu fyrir nauðsynlega starfsemi í skilningi 35. liðar 1. mgr. 2. gr. tilskipunar 2014/59/ESB og eins og greint er frá í sniðmáti Z07.01 í framkvæmdarreglugerð framkvæmdastjórnarinnar (ESB) 2018/1624 ([3]) og tengt við tiltekna aðila í sniðmáti Z07.02.	Nei	Nei	Já, ef atvikið skapar áhættu fyrir nauðsynlega starfsemi aðila á fjármálamarkaði skv. 35. lið 1. mgr. 2. gr. tilskipunar 2014/59/ESB	Alstafir
4.11. Upplýsingar sem skipta máli fyrir skilastjórnvöld	Lýsing á því hvort og þá hvernig alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hefur haft áhrif á skilabærni einingarinnar eða samstæðunnar. Einingar, eins og um getur í 1. mgr. 1. gr. tilskipunar 2014/59/ESB, skulu veita upplýsingar um hvort og þá hvernig alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hafi haft áhrif á skilabærni einingarinnar eða samstæðunnar. Þessar einingar skulu einnig tilgreina hvort alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni hafi áhrif á gjaldfærni eða lausafjárstöðu aðilans á fjármálamarkaði og mögulega mælingu áhrifanna. Þessar einingar skulu einnig veita upplýsingar um áhrif á rekstrarlega samfellu, áhrif á skilabærni einingarinnar, hvers konar viðbótaráhrif á kostnað og tap vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni, þ.m.t. á eiginfjárstöðu aðilans á fjármálamarkaði, og hvort samningsbundið fyrirkomulag um	Nei	Nei	Já, ef atvikið hefur haft áhrif á skilabærni einingarinnar eða samstæðunnar	Alstafir

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	notkun upplýsinga- og fjarskiptatækniþjónustu sé enn traust og að fullu framfylgjanlegt komi til skilameðferðar einingarinnar.				

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
4.12. Mikilvægismörk fyrir flokkunarviðmiðið „efnahagsleg áhrif“	Ítarlegar upplýsingar um viðmiðunarmörk sem alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni náði að lokum í tengslum við viðmiðið „efnahagsleg áhrif“ sem um getur í 7. og 14. gr. framseldrar reglugerðar (ESB) 2024/1772.	Nei	Nei	Já	Alstafir
4.13. Fjárhæð vergs beins og óbeins kostnaðar og taps	Heildarfjárhæð vergs beins og óbeins kostnaðar og taps sem aðilinn á fjármálamarkaði hefur orðið fyrir vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni, þ.m.t.: a) fjárhæð fjármuna eða fjáreigna sem teknar hafa verið eignarnámi og aðilinn á fjármálamarkaði ber ábyrgð á, b) fjárhæð kostnaðar við að endurnýja eða flytja hugbúnað, vélbúnað eða innviði, c) fjárhæð starfsmannakostnaðar, þ.m.t. kostnaðar við að endurnýja eða flytja starfsfólk, ráða starfsfólk til viðbótar, greiða yfirvinnu og endurheimta tapaða eða skerta færni starfsfólks, d) fjárhæð gjalda sem hljótast af því að ekki er staðið við samningsbundnar skyldur, e) fjárhæð kostnaðar við að rétta hlut viðskiptavina og greiða bætur, f) fjárhæð taps vegna tapaðra tekna, g) fjárhæð kostnaðar sem tengist innri og ytri samskiptum, h) fjárhæð ráðgjafarkostnaðar, þ.m.t. kostnaðar sem tengist lögfræðiráðgjöf, tæknirannsóknum og úrbótum, i) fjárhæð annars kostnaðar og taps, þ.m.t.: i. bein útgjöld, þ.m.t. virðisrýrnun og uppgjörsgjöld, í rekstrarreikningi og niðurfærslur vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni, ii. varúðarniðurfærslur eða varasjóðir sem gert er grein fyrir í rekstrarreikningi vegna hugsanlegs taps í tengslum við alvarlega atvikið sem tengist upplýsinga- og fjarskiptatækni,	Nei	Nei	Já	Fjárhæð

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	iii. yfirvofandi tap, tap sem varð til vegna alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni og er bókað til bráðabirgða á tímabundnum reikningum eða biðreikningum og endurspeglast ekki enn í rekstrarreikningi sem áætlað er að telja eigi með innan tímabils sem endurspeglar stærð og aldur liðarins sem er í biðstöðu, iv. verulegar útistandandi tekjur sem tengjast samningsbundnum skyldum við þriðju aðila, þ.m.t. ákvörðunin um að greiða bætur til viðskiptavinar í kjölfar alvarlega atviksins sem tengist upplýsinga- og fjarskiptatækni frekar en að endurgreiða eða greiða beint, með því að fella niður tekjuaðlögun þar sem samningsbundin gjöld eru felld niður eða lækkuð í tiltekið tímabil fram í tímann, v. tap vegna fyrri tímabila, þegar það nær yfir lengri tíma en eitt fjárhagslegt uppgjörsár og getur valdið lagalegri áhættu. Aðilar á fjármálamarkaði skulu taka tillit til 1. og 2. mgr. 7. gr. framseldrar reglugerðar (ESB) 2024/1772 í mati sínu. Aðilar á fjármálamarkaði skulu ekki taka með í þessa tölu fjárhagslega endurheimt af neinu tagi. Aðilar á fjármálamarkaði skulu greina frá fjárhæðinni sem jákvæðu virði. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skulu aðilar á fjármálamarkaði taka tillit til heildarfjárhæðar kostnaðar og taps hjá öllum aðilum á fjármálamarkaði. Aðilar á fjármálamarkaði skulu tilgreina gagnapunkta í einingum með lágmarksnákvæmni sem samsvarar þúsundum eininga.				
4.14. Fjárhæð fjárhagslegrar endurheimtar	Heildarfjárhæð fjárhagslegrar endurheimtar. Fjárhagslegar endurheimtur skulu miðast við upphaflegt tap af völdum atviksins, óháð því hvenær fjárhagslegar endurheimtur í formi fjármagns eða innstreymis efnahagslegs ávinnings berast.	Nei	Nei	Já	Fjárhæð Aðilar á fjármálamarkaði skulu tilgreina gagnapunkta í einingum með lágmarksnákvæmni sem samsvarar þúsundum eininga

Gagnasvæði	Lýsing	Skyldubundið í frumtilkynningu	Skyldubundið í áfangaskýrslu	Skyldubundið í lokaskýrslu	Tegund reits
	Aðilar á fjármálamarkaði skulu greina frá fjárhæðinni sem jákvæðu virði. Ef um er að ræða sameinaða skýrslugjöf, eins og um getur í 7. gr. þessarar reglugerðar, skulu aðilar á fjármálamarkaði taka tillit til heildarfjárhæðar fjárhagslegrar endurheimtar hjá öllum aðilum á fjármálamarkaði.				
4.15. Upplýsingar um hvort atvikin sem ekki eru alvarleg hafi endurtekið sig	Upplýsingar um hvort fleiri en eitt atvik tengt upplýsinga- og fjarskiptatækni sem ekki er alvarlegt hafi endurtekið sig og teljist til samans alvarlegt atvik í skilningi 2. mgr. 8. gr. framseldrar reglugerðar (ESB) 2024/1772. Aðilar á fjármálamarkaði skulu upplýsa um hvort atvik sem tengjast upplýsinga- og fjarskiptatækni og ekki eru alvarleg hafi endurtekið sig og séu til samans talin eitt alvarlegt atvik. Aðilar á fjármálamarkaði skulu einnig tilgreina hve oft þessi ekki alvarlegu atvik í tengslum við upplýsinga- og fjarskiptatækni hafa orðið.	Nei	Nei	Já, ef alvarlega atvikið samanstendur af fleiri en einu endurteknu atviki sem ekki telst vera alvarlegt.	Alstafir
4.16. Dagsetning og tími endurtekinna atvika	Ef aðilar á fjármálamarkaði tilkynna um endurtekin atvik sem tengjast upplýsinga- og fjarskiptatækni, dagsetning og tími þegar fyrsta atvikið átti sér stað.	Nei	Nei	Já, fyrir endurtekin atvik	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kkk:mm:ss)

([1]) 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, http://data.europa.eu/eli/dir/2022/2555/oj).

([2]) 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, http://data.europa.eu/eli/dir/2014/59/oj).

([3]) Framkvæmdarreglugerð framkvæmdastjórnarinnar (ESB) 2018/1624 frá 23. október 2018 um tæknilega framkvæmdarstaðla að því er varðar verklagsreglur og stöðluð eyðublöð og sniðmát fyrir tilhögun upplýsingamiðlunar að því er varðar skilaáætlanir fyrir lánastofnanir og verðbréfafyrirtæki samkvæmt tilskipun Evrópuþingsins og ráðsins 2014/59/ESB og um niðurfellingu á framkvæmdarreglugerð framkvæmdastjórnarinnar (ESB) 2016/1066 (Stjtíð. ESB L 277, 7.11.2018, bls. 1, http://data.europa.eu/eli/reg_impl/2018/1624/oj).

III. VIÐAUKI

SNIÐMÁT FYRIR TILKYNNINGAR UM VERULEGAR NETÓGNIR

Númer reits	Gagnasvæði	
1	Heiti aðilans sem leggur tilkynninguna fram	
2	Auðkenniskóði þess aðila sem leggur tilkynninguna fram	
3	Tegund aðila á fjármálamarkaði sem leggur fram tilkynninguna	
4	Heiti aðilans á fjármálamarkaði	
5	LEI-auðkenni aðilans á fjármálamarkaði	
6	Nafn aðaltengiliðar	
7	Netfang aðaltengiliðar	
8	Sími aðaltengiliðar	
9	Nafn annars tengiliðar	
10	Netfang annars tengiliðar	
11	Sími annars tengiliðar	
12	Dagsetning og tími þegar netógnin uppgötvaðist	
13	Lýsing á verulegu netógninni	
14	Upplýsingar um möguleg áhrif	
15	Möguleg flokkunarviðmið atviks	
16	Staða netógnarinnar	
17	Aðgerðir framkvæmdar til að koma í veg fyrir að hún raungerist	
18	Tilkynning til annarra hagsmunaaðila	
19	Vísbendingar um vásetningu	
20	Aðrar viðeigandi upplýsingar	

IV. VIÐAUKI

ORÐALISTI OG LEIÐBEININGAR UM TILKYNNINGU UM VERULEGAR NETÓGNIR

Gagnasvæði	Lýsing	Skyldubundinn reitur	Tegund reits
1. Heiti aðilans sem leggur tilkynninguna fram	Fullt lögheiti aðilans sem leggur tilkynninguna fram.	Já	Alstafir
2. Auðkenniskóði þess aðila sem leggur tilkynninguna fram	Auðkenniskóði þess aðila sem leggur tilkynninguna fram. Ef aðilar á fjármálamarkaði leggja fram tilkynningu/skýrslu skal auðkenniskóðinn vera auðkenni lögaðila (LEI), sem er einkvæmur 20 alstafa kóði, sem byggist á ISO-staðli 17442-1:2020. Ef þjónustuveitandi sem er þriðji aðili leggur fram skýrslu fyrir aðila á fjármálamarkaði getur hann notað auðkenniskóða eins og tilgreint er í tæknilegu framkvæmdarstöðlunum sem samþykktir eru skv. 9. mgr. 28. gr. reglugerðar (ESB) 2022/2554.	Já	Alstafir
3. Tegund aðila á fjármálamarkaði sem leggur fram skýrsluna	Tegund aðilans, eins og um getur í a- til t-lið 1. mgr. 2. gr. reglugerðar (ESB) 2022/2554, sem leggur skýrsluna fram.	Já, ef skýrslan er ekki send af viðkomandi aðila á fjármálamarkaði með beinum hætti.	Val (fjölval): — lánastofnun, — greiðslustofnun, — undanþegin greiðslustofnun, — reikningsupplýsingaþjónustuveitandi, — rafeyrisfyrirtæki, — undanþegið rafeyrisfyrirtæki, — verðbréfafyrirtæki, — þjónustuveitandi sýndareigna, — útgefandi eignatengdra tóka, — verðbréfamiðstöð, — miðlægur mótaðili, — viðskiptavettvangur, — viðskiptaskrá, — rekstraraðili sérhæfðra sjóða, — rekstrarfélag, — veitandi gagnaskýrsluþjónustu,

Gagnasvæði	Lýsing	Skyldubundinn reitur	Tegund reits
			— vátrygginga- og endurtryggingafélag, — vátryggingamiðlari, endurtryggingamiðlari og vátryggingamiðlari í hliðarstarfsemi, — stofnun um starfstengdan lífeyri, — lánshæfismatsfyrirtæki, — stjórnandi mjög mikilvægra viðmiðana, — þjónustuveitandi hópfjármögnunar, — verðbréfunarskrá.
4. Heiti aðilans á fjármálamarkaði	Fullt lögheiti aðilans á fjármálamarkaði sem tilkynnir um hina verulegu netógn.	Já, ef aðilinn á fjármálamarkaði er annar en sá sem leggur fram tilkynninguna	Alstafir
5. LEI-auðkenni aðilans á fjármálamarkaði	Auðkenni lögaðila (LEI) þess aðila á fjármálamarkaði sem tilkynnir verulega netógn, úthlutað í samræmi við Alþjóðlegu staðlasamtökin.	Já, ef aðilinn á fjármálamarkaði sem tilkynnir um hina verulegu netógn er annar en aðilinn sem leggur fram skýrsluna	Einkvæmur 20 alstafa kóði, sem byggist á ISO-staðli 17442-1:2020
6. Nafn aðaltengiliðar	Nafn og kenninafn aðaltengiliðar aðilans á fjármálamarkaði.	Já	Alstafir
7. Netfang aðaltengiliðar	Netfang aðaltengiliðar sem lögbært yfirvald getur notað til eftirfylgnisamskipta.	Já	Alstafir
8. Sími aðaltengiliðar	Símanúmer aðaltengiliðar sem lögbært yfirvald getur notað til eftirfylgnisamskipta. Gefa skal upp símanúmerið með öllum landsnúmerum (t.d. +33XXXXXXXXX)	Já	Alstafir
9. Nafn annars tengiliðar	Nafn og kenninafn annars tengiliðar hjá aðilanum á fjármálamarkaði eða aðilanum sem leggur fram tilkynninguna fyrir hönd aðilans á fjármálamarkaði, ef tiltækt er.	Já, ef fyrir liggur nafn og kenninafn annars tengiliðar aðilans á fjármálamarkaði eða aðilans sem leggur fram tilkynninguna fyrir hönd hans	Alstafir

Gagnasvæði	Lýsing	Skyldubundinn reitur	Tegund reits
10. Netfang annars tengiliðar	Netfang annars tengiliðar eða virkt netfang teymisins sem lögbært yfirvald getur notað til eftirfylgnisamskipta, ef tiltækt er.	Já, ef fyrir liggur netfang annars tengiliðar eða virkt netfang teymisins sem lögbært yfirvald getur notað til eftirfylgnisamskipta	Alstafir
11. Sími annars tengiliðar	Símanúmer annars tengiliðar sem lögbært yfirvald getur notað til eftirfylgnisamskipta, ef tiltækt er. Gefa skal upp símanúmerið með öllum landsnúmerum (t.d. +33XXXXXXXXX).	Já, ef fyrir liggur símanúmer annars tengiliðarins sem lögbært yfirvald getur notað til eftirfylgnisamskipta	Alstafir
12. Dagsetning og tími þegar netógnin uppgötvaðist	Dagsetning og tími þegar aðilinn á fjármálamarkaði fékk vitneskju um hina verulegu netógn.	Já	Samræmdur heimstími samkvæmt ISO-staðli 8601 (ÁÁÁÁ-MM-DD Kkk:mm:ss)
13. Lýsing á verulegu netógninni	Lýsing á mikilvægustu þáttum hinnar verulegu netógnar. Aðilar á fjármálamarkaði skulu veita: a) gróft yfirlit yfir mikilvægustu þætti hinnar verulegu netógnar, b) tengda áhættu sem stafar af henni, þ.m.t. mögulega veikleika í kerfum aðilans á fjármálamarkaði sem hægt er að notfæra sér, c) upplýsingar um líkurnar á að hin verulega netógn raungerist og d) upplýsingar um uppsprettu upplýsinga um netógnina.	Já	Alstafir
14. Upplýsingar um möguleg áhrif	Upplýsingar um möguleg áhrif netógnarinnar á aðilann á fjármálamarkaði, viðskiptavini hans eða fjárhagslega mótaðila ef netógnin hefur raungerst	Já	Alstafir
15. Möguleg flokkunarviðmið atviks	Flokkunarviðmiðin sem hefðu valdið því að gerð hefði verið tilkynning um alvarlegt atvik ef netógnin hefði raungerst.	Já	Val (fjölval): — viðskiptavinir, fjárhagslegir mótaðilar og viðskipti sem urðu fyrir áhrifum, — áhrif á orðspor, — tímalengd og niðritími þjónustu, — landfræðileg útbreiðsla, — gagnatap, — mikilvæg þjónusta sem varð fyrir áhrifum, — efnahagsleg áhrif.

Gagnasvæði	Lýsing	Skyldubundinn reitur	Tegund reits
16. Staða net-ógnarinnar	Upplýsingar um stöðu netógnarinnar gagnvart aðilanum á fjármálamarkaði og hvort breytingar hafi orðið á virkni ógnarinnar. Ef netógnin er hætt að hafa samskipti við upplýsingakerfi aðilans á fjármálamarkaði má merkja stöðuna sem óvirka. Ef aðilinn á fjármálamarkaði hefur upplýsingar um að ógnin sé enn virk gagnvart öðrum aðilum eða fjármálakerfinu í heild skal merkja stöðuna sem virka.	Já	Val: — virk, — óvirk.
17. Aðgerðir framkvæmdar til að koma í veg fyrir að hún raun-gerist	Helstu upplýsingar um aðgerðir sem aðili á fjármálamarkaði framkvæmir til að koma í veg fyrir að veruleg netógn raungerist, ef við á.	Já	Alstafir
18. Tilkynning til annarra hagsmuna-aðila	Upplýsingar um tilkynningu um netógn til annarra aðila á fjármálamarkaði eða yfirvalda.	Já, ef aðrir aðilar á fjármála-markaði eða yfirvöld hafa verið upplýst um netógnina)	Alstafir
19. Vísbendingar um vásetn-ingu	Upplýsingar sem tengjast umtalsverðri ógn sem gætu verið hjálp við að greina skaðlega virkni innan net- eða upplýsingakerfis (vísbendingar um vásetningu), eftir atvikum. Þær vísbendingar um vásetningu sem aðili á fjármálamarkaði lætur í té kunna að innihalda, en takmarkast ekki við, eftirfarandi gagnaflokka: a) IP-tölur, b) vefslóðir, c) lén, d) skráartæti (e. *file hashes*), e) gögn um spilliforrit (e. *malware data*) (heiti spilliforrits, skráarheiti og staðsetning þeirra, sérstakir skráarlyklar sem tengjast virkni spilliforrits), f) gögn um virkni nets (tengi, samskiptareglur, vistföng, tilvísunarslóðir, aðgangsforrit, hausar, tilteknar aðgerðaskrár eða sérstakt mynstur í netumferð), g) gögn um tölvupóstskilaboð (sendandi, viðtakandi, efni, yfirskrift, innihald), h) beiðnir nafnaþjóns léns og skráasamskipan, i) virkni á notendareikningum (innskráningar, virkni á reikningum notenda með aukin réttindi, aukning réttinda), j) gagnagrunnsumferð (les/skrif), beiðnir til sömu skrár. Þessi tegund upplýsinga getur tekið til gagna sem varða vísa sem lýsa mynstri í netumferð sem samsvara þekktum árásum/yrkjanetsamskiptum, IP-vistföng véla sem eru sýktar af spilliforritum (yrkjum), gögn sem tengjast þjónum til „skipana og stjórnunar“ sem spilliforrit nota (vanalega lén eða IP-vistföng) og vefslóðir sem tengjast vefveiðisetrum eða vefsetrum sem vitað er að hýsi spilliforrit eða veilubragðapakka.	Já, ef upplýsingar um vísbend-ingar um vásetningu sem tengist netógn eru til staðar)	Alstafir

Gagnasvæði	Lýsing	Skyldubundinn reitur	Tegund reits
20. Aðrar viðeigandi upplýsingar	Allar aðrar viðeigandi upplýsingar um hina verulegu netógn	Já, ef við á og aðrar upplýsingar eru fyrir hendi sem ekki er að finna í sniðmátinu	Alstafir

Fylgiskjal 7.

ÁKVÖRÐUN SAMEIGINLEGU EES-NEFNDARINNAR
nr. 299/2025

frá 5. desember 2025

um breytingu á IX. viðauka (Fjármálaþjónusta) við EES-samninginn

SAMEIGINLEGA EES-NEFNDIN HEFUR,

með vísan til samningsins um Evrópska efnahagssvæðið („EES-samningurinn“), einkum 98. gr.,

og að teknu tilliti til eftirfarandi:

1) Fella ber inn í EES-samninginn framselda reglugerð framkvæmdastjórnarinnar (ESB) 2025/420 frá 16. desember 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla til að tilgreina nánar 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 ([1]).

2) Fella ber inn í EES-samninginn framselda reglugerð framkvæmdastjórnarinnar (ESB) 2025/532 frá 24. mars 2025 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina nánar þá þætti sem aðili á fjármálamarkaði þarf að ákvarða og meta þegar hann semur við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi ([2]).

3) Fella ber inn í EES-samninginn framselda reglugerð framkvæmdastjórnarinnar (ESB) 2025/1190 frá 13. febrúar 2025 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreind eru viðmið sem notuð eru til að auðkenna aðila á fjármálamarkaði sem skylt er að framkvæma ógnamiðaðar innbrotsprófanir, kröfur og staðlar sem gilda um notkun á innri prófunaraðilum, kröfur í tengslum við umfang, prófunaraðferðir og nálgun fyrir hvern áfanga í prófunum, niðurstöður, loka- og úrbótastig prófunar og tegund samvinnu eftirlitsaðila og annarrar viðeigandi samvinnu sem þörf er á við innleiðingu ógnamiðaðra innbrotsprófana og til að greiða fyrir gagnkvæmri viðurkenningu ([3]).

4) IX. viðauki við EES-samninginn breytist því í samræmi við það,

SAMÞYKKT ÁKVÖRÐUN ÞESSA:

([1]) Stjtíð. ESB L, 2025/420, 24.3.2025, ELI: http://data.europa.eu/eli/reg_del/2025/420/oj
([2]) Stjtíð. ESB L, 2025/532, 2.7.2025, ELI: http://data.europa.eu/eli/reg_del/2025/532/oj
([3]) Stjtíð. ESB L, 2025/1190, 18.6.2025, ELI: http://data.europa.eu/eli/reg_del/2025/1190/oj

1. gr.

Eftirfarandi er bætt við á eftir lið 31qh (framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/301) í IX. viðauka við EES-samninginn:

„31qi. **32025 R 0420**: Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/420 frá 16. desember 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla til að tilgreina nánar 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 (Stjtíð. ESB L, 2025/420, 24.3.2025).

Ákvæði framseldu reglugerðarinnar skulu, að því er samning þennan varðar, aðlöguð sem hér segir:

Í b-lið 3. mgr. 3. gr. er orðunum „eða Eftirlitsstofnun EFTA, eftir því sem við á“ bætt við á eftir orðunum „Evrópsku eftirlitsstofnananna“.

31qj. **32025 R 0532**: Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/532 frá 24. mars 2025 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina nánar þá þætti sem aðili á fjármálamarkaði þarf að ákvarða og meta þegar hann semur við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi (Stjtíð. ESB L, 2025/532, 2.7.2025).

31qk. **32025 R 1190**: Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/1190 frá 13. febrúar 2025 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreind eru viðmið sem notuð eru til að auðkenna aðila á fjármálamarkaði sem skylt er að framkvæma ógnamiðaðar innbrotsprófanir, kröfur og staðlar sem gilda um notkun á innri prófunaraðilum, kröfur í tengslum við umfang, prófunaraðferðir og nálgun fyrir hvern áfanga í prófunum, niðurstöður, loka- og úrbótastig prófunar og tegund samvinnu eftirlitsaðila og annarrar viðeigandi samvinnu sem þörf er á við innleiðingu ógnamiðaðra innbrotsprófana og til að greiða fyrir gagnkvæmri viðurkenningu (Stjtíð. ESB L, 2025/1190, 18.6.2025).“

2. gr.

Íslenskur og norskur texti framseldra reglugerða (ESB) 2025/420, (ESB) 2025/532 og (ESB) 2025/1190, sem verður birtur í EES-viðbæti við *Stjórnartíðindi Evrópusambandsins*, telst fullgildur.

3. gr.

Ákvörðun þessi öðlast gildi 6. desember 2025, að því tilskildu að allar tilkynningar samkvæmt 1. mgr. 103. gr. EES-samningsins hafi farið fram (*).

4. gr.

Ákvörðun þessi skal birt í EES-deild *Stjórnartíðinda Evrópusambandsins* og EES-viðbæti við þau.

Gjört í Brussel, 5. desember 2025.

Fyrir hönd sameiginlegu EES-nefndarinnar

Stefán Haukur Jóhannesson

Formaður

(*) Engin stjórnskipuleg skilyrði gefin til kynna.

Fylgiskjal 8.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2025/420

frá 16. desember 2024

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla til að tilgreina nánar 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

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum aðra undirgrein 2. mgr. 41. gr.,

og að teknu tilliti til eftirfarandi:

1) Eftirlitsramminn sem komið er á með reglugerð (ESB) 2022/2554 ætti að byggjast á skipulegu og stöðugu samstarfi milli evrópsku eftirlitsstofnananna (ESA) og lögbærra yfirvalda fyrir milligöngu eftirlitsvettvangsins og sameiginlegu skoðunarhópanna.

2) Yfirvöldin sem um getur í 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554 ættu að tryggja að starfsmenn þeirra sem fyrirhugað er að skipa í sameiginlega skoðunarhópinn, sem um getur í 1. mgr. 40. gr. þeirrar reglugerðar, búi yfir þeirri tæknilegu sérfræðikunnáttu sem krafist er í lýsingum sem þarf í sameiginlegu skoðunarhópunum. Ef sýnt er fram á það að yfirvald hefur ekki starfsmenn sem uppfylla kröfurnar um þá tæknilegu sérfræðikunnáttu sem nauðsynleg er í sameiginlega skoðunarhópunum ætti aðaleftirlitsaðilinn að líta á það sem rökstuðning fyrir því að afnema, á þeim tímapunkti, skyldu yfirvaldanna til að tilnefna starfsmenn í sameiginlegu skoðunarhópana. Í slíku tilviki ætti yfirvaldið þó að leggja sig fram eftir bestu getu um að taka á þessum skorti á sérfræðiþekkingu og leitast við að auka getu sína til að leggja sitt af mörkum til sameiginlegu skoðunarhópanna í tengslum við næstu athugun.

3) Starfsmenn yfirvaldanna sem um getur í 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554 sem tilnefndir eru í sameiginlegan skoðunarhóp eins og um getur í 1. mgr. 40. gr. þeirrar reglugerðar ættu að halda áfram að vera starfsmenn yfirvaldsins sem tilnefnir þá og falla þar af leiðandi undir vinnutíma og varanlega starfsstöð eins og um getur í ráðningarsamningi þeirra.

4) Til að tryggja sem skilvirkasta notkun auðlinda við framkvæmd eftirlitsstarfsemi ættu aðilar í sameiginlegum skoðunarhópum að geta verið þátttakendur í mörgum sameiginlegum skoðunarhópum og geta haft eftirlit með mörgum mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu. Fjöldi mikilvægra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem skal úthluta tilteknum aðila sameiginlega skoðunarhópsins og heildarþörf fyrir starfsfólk ætti að vera með tilliti til áhættulýsinga mikilvægu þriðju aðilanna sem veita upplýsinga- og fjarskiptatækniþjónustu og fyrirhugaðs umfangs eftirlitsstarfsemi. Í stefnumarkandi eftirlitsáætluninni til margra ára, sem uppfærð er árlega af aðaleftirlitsaðilanum eftir því sem þurfa þykir, er tekið tillit til möguleikans á að hafa eftirlit með mörgum mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og er hún endurspegluð í hverri árlegri eftirlitsáætlun. Til að tryggja áreiðanleika áætlaðrar og viðvarandi skuldbindingar tilnefningaryfirvaldanna um að veita tilföng til að tryggja mönnun sameiginlegu skoðunarhópanna ætti aðaleftirlitsaðilinn að hafa samráð við bæði sameiginlega eftirlitskerfið og eftirlitsvettvanginn um stefnumarkandi eftirlitsáætlunina til margra ára.

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

5) Aðaleftirlitsaðilinn ætti að beita blöndu viðmiða og meginreglna við tilgreiningu á fjölda starfsmanna í hverjum sameiginlegum skoðunarhópi og samsetningunni sem af henni leiðir. Í ljósi fjölbreyttrar tæknilegrar og landfræðilegrar dreifingar og notkunar ýmissa aðila á fjármálamarkaði á mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu ættu þessi viðmið og þessar meginreglur að taka tillit til tæknilegs eðlis eftirlitsverkefna, mismunandi stigs hæðis fjármálastofnana að því er varðar þjónustu mikilvægu þriðju aðilanna sem veita upplýsinga- og fjarskiptatækniþjónustu, landfræðilegrar dreifingar, stærðar og fjölda aðila á fjármálamarkaði sem reiða sig á þessa þjónustu og, þegar það er mögulegt, hlutfallslegs fyrirsvars þvert á atvinnugreinar. Þegar aðaleftirlitsaðilinn sinnir því verkefni ætti hann að reiða sig á upplýsingar frá lögbærum yfirvöldum í tengslum við tilgreiningu mikilvægu þriðju aðilanna sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. upplýsingar sem þarf að því er varðar öll undirviðmiðin eins og mælt er fyrir um í framseldri reglugerð framkvæmdastjórnarinnar (ESB) 2024/1502 ([2]) og taka tillit til mikilvægis þriðju aðilanna sem veita upplýsinga- og fjarskiptatækniþjónustu fyrir veitingu tiltekinnar fjármálaþjónustu bæði á vettvangi aðildarríkis og Sambandsins.

6) Til að tryggja að skipulag og samsetning sameiginlegu skoðunarhópanna þjóni tilgangi sínum og til að tryggja viðvarandi hagkvæmni og skilvirkni eftirlitsrammans ætti aðaleftirlitsaðilinn og aðilar í sameiginlegu skoðunarhópunum að meta reglulega árangur sameiginlegu skoðunarhópanna. Aðaleftirlitsaðilinn og tilnefningaryfirvöldin ættu að nota þessi möt til að sannreyna hvort aðilar í sameiginlegu skoðunarhópunum séu enn til þess fallnir að sinna verkefnum þeirra og gera breytingar á aðilum í sameiginlegu skoðunarhópunum, eftir því sem við á.

7) Til að tryggja að aðilarnir í sameiginlegu skoðunarhópunum starfi sem eitt teymi og eftirlitsstarfsemi sé framkvæmd á stöðugan hátt ættu Evrópsku eftirlitsstofnanirnar að skilgreina verklagsreglur um eftirlit sem aðilar í sameiginlegu skoðunarhópunum og aðaleftirlitsaðilinn skulu fara að er þeir sinna verkefnum sínum.

8) Þar sem eftirlitsverkefni fela í sér vinnslu trúnaðarupplýsinga ætti aðaleftirlitsaðilinn að veita aðilum í sameiginlega skoðunarhópnum aðgengi að slíkum upplýsingum og viðkomandi upplýsingatæknitilföngum (þ.m.t. tækjum, forritum og gagnasöfnum) og tilföngum sem eru ekki upplýsingatækni (þ.m.t. stefnum, verklagsreglum og skjalahaldi) á grundvelli meginreglunnar um þörf á vitneskju og innan tiltekins umfangs verkefna þeirra sem þörf er á fyrir aðila í sameiginlega skoðunarhópnum til að aðstoða aðaleftirlitsaðilann við að uppfylla lögboðið hlutverk sitt eða inna verkefni sín af hendi. Við gerð fyrirkomulags aðaleftirlitsaðilans og lögbærra yfirvalda um að koma þessari reglugerð í framkvæmd, í samræmi við framselda reglugerð framkvæmdastjórnarinnar (ESB) 2024/1505 ([3]), til að tryggja fullnægjandi fjármögnun kostnaðar í tengslum við tilföngin sem tilnefningaryfirvöldin leggja fram, ætti aðaleftirlitsaðilinn að fella inn í slíkt samkomulag þátt sem lýsir aðferðinni við endurgreiðslu á beinum og óbeinum kostnaði allra yfirvalda sem taka þátt í að tilnefna aðila í sameiginlegu skoðunarhópana. Til að tryggja gagnsæja og trúverðuga framkvæmd eftirlitsstarfsemi ætti þetta samkomulag einnig að tryggja að aðilar í sameiginlegu skoðunarhópunum séu lausir við hagsmunaárekstra er þeir sinna skyldum sínum.

9) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem Evrópska bankaeftirlitsstofnunin, Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin og Evrópska verðbréfamarkaðseftirlitsstofnunin hafa lagt fyrir framkvæmdastjórn Evrópusambandsins.

([2]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1502 frá 22. febrúar 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 með því að tilgreina nánar viðmiðanirnar fyrir útnefningu á þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem mikilvægra fyrir aðila á fjármálamarkaði (Stjtíð. ESB L, 2024/1502, 30.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1502/oj).

([3]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2024/1505 frá 22. febrúar 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 um að ákvarða fjárhæð eftirlitsgjalda sem aðaleftirlitsaðili innheimtir af mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu og með hvaða hætti þau gjöld skulu greidd (Stjtíð. ESB L, 2024/1505, 30.5.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1505/oj).

10) Sameiginleg nefnd evrópsku eftirlitsstofnananna sem um getur í 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([4]), 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([5]) og 54. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([6]) hefur haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint hugsanlegan kostnað og ávinning af fyrirhuguðum stöðlum og óskað eftir ráðgjöf hagsmunahópsins um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1093/2010, hagsmunahópsins í vátryggingum og endurtryggingum og hagsmunahópsins um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1094/2010 og hagsmunahópsins á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar (ESB) nr. 1095/2010.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Verkefni aðila í sameiginlega skoðunarhópnum

1. Aðilar í sameiginlega skoðunarhópnum skulu inna verkefni sín af hendi undir samræmingarstjórn samræmingaraðila aðaleftirlitsaðilans. Þessi verkefni eru m.a. viðvarandi stuðningur við starfsemi sem aðaleftirlitsaðilinn innir af hendi og framkvæmd sértækra verkefna. Verkefnin skulu vera:

a) að aðstoða aðaleftirlitsaðilann við undirbúning og gerð sérsniðinna árlegra eftirlitsáætlana sem um getur í 4. mgr. 33. gr. reglugerðar (ESB) 2022/2554,

b) að aðstoða aðaleftirlitsaðilann við framkvæmd matsins sem um getur í 2. mgr. 33. gr. reglugerðar (ESB) 2022/2554,

c) að meta upplýsingarnar sem aðaleftirlitsaðilinn fær frá mikilvæga þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu skv. 37. gr. reglugerðar (ESB) 2022/2554 og II. kafla framseldrar reglugerðar framkvæmdastjórnarinnar (ESB) 2025/295 ([7]),

d) að framkvæma almennar rannsóknir á mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sem um getur í 38. gr. reglugerðar (ESB) 2022/2554,

e) að framkvæma skoðanirnar sem um getur í 1. mgr. 39. gr. reglugerðar (ESB) 2022/2554,

f) að skrifa tilmælin sem um getur í d-lið 1. liðar 35. gr. reglugerðar (ESB) 2022/2554,

g) að meta úrbótaáætlunina og framvinduskýrslurnar sem um getur í 4. gr. framseldrar reglugerðar (ESB) 2025/295,

h) að undirbúa og skrifa beiðnir og ákvarðanir sem um getur í 35. gr. (6. mgr.), 37. gr. (1. mgr.), 38. gr. (4. mgr.) og 39. gr. (6. mgr.) reglugerðar (ESB) 2022/2554,

i) að aðstoða aðaleftirlitsaðilann við framlag hans til þverlægrar eftirlitsstarfsemi, þ.m.t. við þróun ítarlegra viðmiðana sem um getur í 3. mgr. 32. gr. reglugerðar (ESB) 2022/2554,

([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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([7]) Framseld reglugerð framkvæmdastjórnarinnar (ESB) 2025/295 frá 24. október 2024 um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla um samræmingu skilyrða sem gera eftirlitsstarfsemi mögulega (Stjtíð. ESB L, 2025/295, 13.2.2025, ELI: http://data.europa.eu/eli/reg_del/2025/295/oj).

j) að tryggja að viðeigandi upplýsingum varðandi aðila á fjármálamarkaði sem nota þjónustuna sem veitt er af mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu sé deilt með aðaleftirlitsaðilanum,

k) að aðstoða aðaleftirlitsaðilann við óundirbúna starfsemi eftir þörfum sem aðaleftirlitsaðilinn telur vera þörf á í tilgangi eftirlits.

2. Ef aðaleftirlitsaðilinn endurskoðar verulega sérsniðna árlega eftirlitsáætlun á árinu skal hann hafa aðila í sameiginlega skoðunarhópnum með við framkvæmd sérsniðnu árlegu eftirlitsáætlunarinnar og endurskoðun hennar.

2. gr.

Stofnun sameiginlega skoðunarhópsins

1. Eftir að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu er fyrst tilgreindur sem mikilvægur í samræmi við a-lið 1. mgr. 31. gr. reglugerðar (ESB) 2022/2554 skal aðaleftirlitsaðilinn, í samráði við sameiginlega eftirlitskerfið sem um getur í 1. mgr. 34. gr. reglugerðar (ESB) 2022/2554, koma á fót sameiginlega skoðunarhópnum sem ber ábyrgð á framkvæmd eftirlitsstarfsemi varðandi þann mikilvæga þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

2. Ef verulegar breytingar verða að því er varðar stöðu mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu getur aðaleftirlitsaðilinn, í samráði við sameiginlega eftirlitskerfið, uppfært samsetningu sameiginlega skoðunarhópsins sem ber ábyrgð á framkvæmd eftirlitsstarfsemi varðandi þann mikilvæga þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu.

Í þeim tilgangi skulu verulegar breytingar að því er varðar mikilvæga þriðja aðilann sem veitir upplýsinga- og fjarskiptatækniþjónustu tengjast einhverju af eftirfarandi:

a) þjónustunni sem viðkomandi þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu veitir,

b) starfsemi aðila á fjármálamarkaði sem upplýsinga- og fjarskiptatækniþjónusta mikilvæga þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu styður við,

c) skránni yfir mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem um getur í 9. mgr. 31. gr. reglugerðar (ESB) 2022/2554.

3. Yfirvöldin sem um getur í 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554 skulu tilnefna einn eða fleiri einstaklinga úr hópi starfsmanna sinna sem skal skipa sem aðila í sameiginlega skoðunarhópnum. Einstakling má tilnefna og skipa sem aðila að einum eða fleiri sameiginlegum skoðunarhópum.

4. Aðaleftirlitsaðilinn skal skipa einstaklingana sem tilnefndir eru sem aðilar í sameiginlega skoðunarhópnum annað hvort í fullt starf eða hlutastarf, með hliðsjón af tiltækileika þeirra, sértækra þarfa aðaleftirlitsaðilans og samkomulagsins milli tilnefningaryfirvaldsins og aðaleftirlitsaðilans.

5. Við tilnefningu aðila í sameiginlegu skoðunarhópana skulu yfirvöldin sem um getur í 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554 meta tæknilega sérfræðikunnáttu, réttindi og hæfi og færni þeirra í upplýsinga- og fjarskiptatækni og á viðeigandi sviðum, þ.m.t. samskipta- og samstarfsfærni, sem og á sviði endurskoðunar og eftirlits.

6. Aðaleftirlitsaðilinn getur krafist þess að tilnefningaryfirvöldin breyti aðeins tilnefningum sínum í rökstuddum tilvikum og þegar eiginleikar tilnefndu einstaklinganna passa ekki við lýsinguna á þeim mannauði sem þörf er á.

7. Aðaleftirlitsaðilinn og yfirvöldin skulu gera allar viðeigandi og mögulegar ráðstafanir til að tryggja fullnægjandi mönnun sameiginlega skoðunarhópsins í samræmi við sérsniðnu árlegu eftirlitsáætlunina.

3. gr.

Aðilar í sameiginlega skoðunarhópnum

1. Aðaleftirlitsaðilinn skal ákvarða fjölda aðila í sameiginlega skoðunarhópnum og samsetningu hans í samráði við sameiginlega eftirlitskerfið sem um getur í 1. mgr. 34. gr. reglugerðar (ESB) 2022/2554 og í samráði við eftirlitsvettvanginn sem um getur í 1. mgr. 32. gr. þeirrar reglugerðar.

2. Aðaleftirlitsaðilinn skal ákvarða fjöldann í ferlinu við stofnun sameiginlega skoðunarhópsins, og eftir því sem þörf krefur, með tilliti til:

a) verkefnanna sem felast í sérsniðnum árlegum eftirlitsáætlunum sem gerðar eru fyrir hvern mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem fellur undir eftirlit sameiginlega skoðunarhópsins,

b) stefnumarkandi markmiða í eftirlitsáætluninni til margra ára sem gerð er fyrir alla mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem fellur undir eftirlit allra sameiginlegu skoðunarhópanna.

3. Til að ákvarða fjölda og samsetningu aðila í sameiginlega skoðunarhópnum skal aðaleftirlitsaðilinn taka a.m.k. allt eftirfarandi til greina:

a) fyrirhugað umfang eftirlitsstarfsemi sem verður stunduð í tengslum við alla mikilvæga þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu,

b) stærð og flækjustig þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu sem fellur undir eftirlit sameiginlega skoðunarhópsins og Evrópsku eftirlitsstofnananna sem aðaleftirlitsaðila,

c) sértæka sérsniðna eftirlitsþörf í tengslum við tiltekinn mikilvægan þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu, samkvæmt mati aðaleftirlitsaðilans,

d) stöðugleika samsetningar sameiginlega skoðunarhópsins, sem tryggir viðeigandi varðveislu þekkingar,

e) nauðsynlega færni sem krafist er til að inna af hendi verkefni sameiginlega skoðunarhópsins, að teknu tilliti til krafna um tækniþekkingu og þekkingu sem er ekki tæknilegs eðlis á sviði upplýsinga- og fjarskiptatækni,

f) aðildarríkin þar sem mikilvægur þriðji aðili veitir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði og lögbæru yfirvöldin sem hafa eftirlit með þeim aðilum á fjármálamarkaði sem nota þá þjónustu,

g) mismunandi tegundir, stærðir og fjölda aðila á fjármálamarkaði sem mikilvægur þriðji aðili veitir upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi,

h) lögbær yfirvöld sem hafa eftirlit með aðilum á fjármálamarkaði sem eru mest háðir upplýsinga- og fjarskiptatækniþjónustunni sem veitt er af mikilvægum þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu,

i) að yfirvöld sem tilnefna fulltrúa í sameiginlega skoðunarhópinn séu hlutfallslega dreifð eftir atvinnugreinum.

4. Við tilnefningu aðila í sameiginlega skoðunarhópinn skulu yfirvöldin sem um getur í 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554 a.m.k. taka tillit til c-, d-, e-, g- og h-liðar í 3. mgr.

4. gr.

Breyting á aðild að sameiginlegum skoðunarhóp

Aðaleftirlitsaðilinn skal, að höfðu samráði við aðila í sameiginlega skoðunarhópnum, með reglulegu millibili, eða þegar aðaleftirlitsaðilinn breytist, eða þegar verulegar breytingar, eins og tilgreint er í 2. mgr. 2. gr., eiga sér stað meta árangur aðila í sameiginlega skoðunarhópnum. Bæði tilnefningaryfirvöldin og aðaleftirlitsaðilinn skulu nota niðurstöður þess mats til að taka ákvörðun um það hvort viðeigandi sé að gera breytingar á aðild að sameiginlega skoðunarhópnum.

5. gr.

Vinnutilhögun aðilanna í sameiginlega skoðunarhópnum

1. Aðilar í sameiginlega skoðunarhópnum skulu inna verkefni sín, sem tilgreind eru í sérsniðnu árlegu eftirlitsáætluninni, af hendi af tilhlýðilegri færni, aðgát og kostgæfni, án hlutdrægni og í samræmi við leiðbeiningar samræmingaraðila aðaleftirlitsaðilans sem um getur í annarri undirgrein 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554.

2. Þegar aðilar í sameiginlega skoðunarhópnum inna eftirlitsverkefni sín af hendi skulu þeir fylgja verklagsreglum um eftirlit sem Evrópsku eftirlitsstofnanirnar hafa samið í sameiningu í tengslum við framkvæmd eftirlitsstarfsemi og viðkomandi starfssvæði, þ.m.t. nákvæmar skilgreiningar í tengslum við notkun upplýsingatæknitóla og -búnaðar og tímastjórnun.

3. Aðilar í sameiginlega skoðunarhópnum skulu fylgja nákvæmum skilgreiningum á upplýsinga- og gagnameðhöndlun og leiðbeiningum sem samræmingaraðili aðaleftirlitsaðilans, sem um getur í annarri undirgrein 2. mgr. 40. gr. reglugerðar (ESB) 2022/2554, leggur fram og hlíta trúnaðarregluverki Evrópsku eftirlitsstofnananna.

4. Aðaleftirlitsaðilinn og tilnefningaryfirvöldin skulu koma á fyrirkomulagi fyrir framkvæmd krafnanna sem mælt er fyrir um í þessari reglugerð, þ.m.t. fyrirkomulagi um tímann sem sameiginlegi skoðunarhópurinn ver í eftirlitsstarfsemi og kostnað í tengslum við hana, þjálfun og þætti varðandi siðferði og framferði í tengslum við hlutverk aðila í sameiginlega skoðunarhópnum, eftir því sem við á.

5. Aðaleftirlitsaðilinn og tilnefningaryfirvöldin skulu tryggja að fyrirkomulagið sem um getur í 4. mgr. sé framkvæmt, endurskoðað og uppfært tímanlega.

6. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 16. desember 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

Fylgiskjal 9.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2025/532

frá 24. mars 2025

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla sem tilgreina nánar þá þætti sem aðili á fjármálamarkaði þarf að ákvarða og meta þegar hann semur við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum fjórðu undirgrein 5. mgr. 30. gr.,

og að teknu tilliti til eftirfarandi:

1) Veiting upplýsinga- og fjarskiptatækniþjónustu til aðila á fjármálamarkaði byggist oft á flókinni keðju undirverktaka í upplýsinga- og fjarskiptatækni, þar sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu geta gert einn eða fleiri undirverktakasamninga við aðra þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu. Að vera óbeint háðir undirverktökum í upplýsinga- og fjarskiptatækni getur haft áhrif á getu aðila á fjármálamarkaði til að greina, meta og stýra áhættum, þ.m.t. áhættum sem tengjast eyðum í upplýsingum frá þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, og á takmarkaða getu aðila á fjármálamarkaði til að afla upplýsinga frá þeim undirverktökum í upplýsinga- og fjarskiptatækni sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi eða efnislega hluta hennar. Hvað þetta varðar, þegar veiting upplýsinga- og fjarskiptatækniþjónustu byggist á hugsanlega langri eða flókinni keðju undirverktaka í upplýsinga- og fjarskiptatækni, er mikilvægt að aðilar á fjármálamarkaði tilgreini heildarkeðju undirverktaka í upplýsinga- og fjarskiptatækni sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

2) Meðal undirverktakanna sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi ættu aðilar á fjármálamarkaði einkum og stöðugt að einbeita sér að þeim undirverktökum sem styðja með skilvirkum hætti upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi, þ.m.t. öllum undirverktökum sem veita upplýsinga- og fjarskiptatækniþjónustu þar sem truflun myndi skerða öryggi eða samfellu þjónustunnar, eins og mælt er fyrir um í upplýsingaskránni sem um getur í 3. mgr. 28. gr. reglugerðar (ESB) 2022/2554.

3) Aðilar á fjármálamarkaði eru afar mismunandi að því er varðar stærð, uppbyggingu og innra skipulag og eðli og flækjustig starfsemi þeirra. Til að tryggja meðalhóf ætti að taka mið af þessari fjölbreytni þegar tilgreint er hvaða þætti aðili á fjármálamarkaði ætti að ákvarða og meta þegar samið er við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

4) Þegar aðilar á fjármálamarkaði hafa heimilað þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu að nota undirverktaka í upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi, í samræmi við 2. mgr. 30. gr. reglugerðar (ESB) 2022/2554, dregur það ekki úr endanlegri ábyrgð stjórnenda aðila á fjármálamarkaði á að stýra áhættu sinni og uppfylla lagalegar skuldbindingar og eftirlitsskyldur sínar. Ef heimilt er að semja við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi, er mikilvægt að aðilar á fjármálamarkaði hafi skýra heildaryfirsýn yfir áhættuna sem tengist því að útvista þjónustu sem styður nauðsynlega eða mikilvæga starfsemi svo að þeir geti vaktað, stýrt og dregið úr slíkri áhættu. Því ættu þeir að leggja mat á áhættuna áður en samið er við undirverktaka um starfsemina.

5) Líta ætti á undirverktaka í upplýsinga- og fjarskiptatækni innan samstæðu sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, þ.m.t. undirverktaka í upplýsinga- og fjarskiptatækni innan samstæðu sem eru að öllu leyti eða sameiginlega í eigu aðila á fjármálamarkaði innan sama stofnanaverndarkerfis, sem undirverktaka í upplýsinga- og fjarskiptatækni.

6) Eftir atvikum, þegar um samstæðu er að ræða, ætti móðurfyrirtæki aðila á fjármálamarkaði að tryggja að stefnunni um notkun undirverktaka í upplýsinga- og fjarskiptatækni, sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, sé beitt á samræmdan og samfelldan hátt innan samstæðunnar.

7) Mikilvægt er að tryggja alhliða stýringu á þeim áhættum sem geta komið upp þegar upplýsinga- og fjarskiptatækniþjónusta sem styður nauðsynlega eða mikilvæga starfsemi er falin undirverktaka. Af þessum sökum ættu aðilar á fjármálamarkaði að fylgja stigum lífsferils samningsbundins fyrirkomulags um notkun á upplýsinga- og fjarskiptatækniþjónustu sem styður starfsemina og er veitt af þriðju aðilum sem veita upplýsinga- og fjarskiptatækniþjónustu, þ.m.t. fyrir undirverktakasamninga. Því er nauðsynlegt að mæla fyrir um kröfur til aðila á fjármálamarkaði sem ættu að endurspeglast í samningsbundnu fyrirkomulagi þeirra við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu þar sem heimilt er að fela undirverktaka að veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi.

8) Til að vega upp á móti áhættu sem tengist undirverktakastarfsemi er nauðsynlegt að tilgreina við hvaða skilyrði þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu geta notað undirverktaka til að veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi. Í því skyni ætti samningsbundið fyrirkomulag um upplýsinga- og fjarskiptatækni milli aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu að mæla fyrir um slík skilyrði, þ.m.t. skipulagningu undirverktakasamninga, áhættumat, áreiðanleikakönnun og samþykkisferli fyrir nýjum undirverktakasamningum í upplýsinga- og fjarskiptatækni um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar eða efnislegar breytingar á gildandi samningsbundnu fyrirkomulagi sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur gert.

9) Til að greina áhættu sem kann að koma upp áður en aðili á fjármálamarkaði gerir samning við undirverktaka í upplýsinga- og fjarskiptatækni ættu þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu að meta hæfi hugsanlegra undirverktaka á viðeigandi og hlutfallslegan hátt, hæfi hugsanlegra undirverktaka á grundvelli þess samningsbundna fyrirkomulags um upplýsinga- og fjarskiptatækni sem þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur gert við aðilann á fjármálamarkaði. Í samningsbundna fyrirkomulaginu um upplýsinga- og fjarskiptatækni ætti því að vera gerð krafa um að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu eða aðilinn á fjármálamarkaði sjálfur, eins og við á, leggi mat á tilföng hugsanlegs undirverktaka, þ.m.t. sérþekkingu viðkomandi og hvort hann hafi fullnægjandi fjármagn, mannauð og tækniúrræði, upplýsingaöryggi hans og stjórnskipulag, þ.m.t. áhættustýringu og innra eftirlit sem undirverktakinn ætti að hafa til staðar.

10) Til að draga út veikleikum og ógnum sem kunna að skapa áhættu fyrir upplýsinga- og fjarskiptatæknikerfi og rekstur aðila á fjármálamarkaði ættu þeir að geta haft eftirlit með frammistöðu upplýsinga- og fjarskiptatækniþjónustu og verið upplýstir um allar breytingar sem máli skipta í undirverktakakeðju upplýsinga- og fjarskiptatækni þegar slíkar breytingar varða nauðsynlega eða mikilvæga starfsemi.

11) Til að gera aðilum á fjármálamarkaði kleift að leggja mat á áhættuna sem tengist undirverktakasamningum eða efnislegum breytingum á þeim ættu þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu að upplýsa aðila á fjármálamarkaði sem þeir veita upplýsinga- og fjarskiptatækniþjónustu um alla slíka nýja samninga eða breytingar með góðum fyrirvara áður en slíkir samningar eða breytingar taka gildi. Af sömu ástæðu ættu aðilar á fjármálamarkaði að hafa rétt til að slíta samningi við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu ef niðurstaða áhættumats þeirra sýnir að nýr samningur eða efnislegar breytingar feli í sér áhættu sem er umfram áhættuþol þeirra.

12) Evrópsku eftirlitsstofnanirnar hafa haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint mögulegan tengdan kostnað og ávinning og óskað eftir ráðgjöf viðkomandi hagsmunahópa evrópsku eftirlitsstofnananna sem komið er á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([2]), 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([3]), og 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([4]).

13) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([5]) og skilaði hún áliti 20. ágúst 2024.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Heildaráhættusnið og flækjustig

Aðilar á fjármálamarkaði skulu taka mið af stærð sinni og heildaráhættusniði og eðli, umfangi og þáttum aukins eða lækkaðs flækjustigs í þjónustu sinni, starfsemi og rekstri, þ.m.t. þáttum að því er varðar:

a) tegund upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi sem samningsbundið fyrirkomulag milli aðilans á fjármálamarkaði og þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu nær yfir,

b) tegund upplýsinga- og fjarskiptatækniþjónustu sem samningsbundið fyrirkomulag milli þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans nær yfir,

c) staðsetningu undirverktakans í upplýsinga- og fjarskiptatækni sem styður nauðsynlega eða mikilvæga starfsemi, eða efnislegan hluta hennar eða móðurfélags hans,

d) lengd og flækjustig keðju undirverktaka sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar og nýtt er af þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu,

e) eðli gagnanna sem er deilt með undirverktökunum í upplýsinga- og fjarskiptatækni sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar,

f) hvort upplýsinga- og fjarskiptatækniþjónustan sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar sé veitt af undirverktökum sem staðsettir eru í aðildarríki eða í þriðja landi, þ.m.t. staðsetninguna sem upplýsinga- og fjarskiptatækniþjónustan er í raun veitt frá og staðinn þar sem gögnin eru í raun unnin og geymd,

g) hvort undirverktakarnir í upplýsinga- og fjarskiptatækni sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar eru hluti sömu samstæðu og sá aðili á fjármálamarkaði sem þjónustan er veitt,

([2]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

h) hvort undirverktakarnir í upplýsinga- og fjarskiptatækni sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislegan hluta hennar hafi starfsleyfi, séu skráðir eða falli undir eftirlit eða tilsjón eftirlitsstofnunar í aðildarríki eða falli undir eftirlitsramma skv. II. þætti V. kafla reglugerðar (ESB) 2022/2554,

i) hvort þriðju aðilarnir sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar hafi starfsleyfi, séu skráðir eða falli undir eftirlit eða tilsjón eftirlitsstofnunar í þriðja landi,

j) hvort veiting upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi eða efnislega hluta hennar einskorðist við einstakan undirverktaka þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða lítinn fjölda slíkra undirverktaka,

k) hvort undirverktaka upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar myndi hafa áhrif á flytjanleika upplýsinga- og fjarskiptatækniþjónustunnar til annars þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

l) hugsanleg áhrif truflana á samfellu og aðgengileika að upplýsinga- og fjarskiptatækniþjónustu, sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, þegar slík þjónusta er veitt af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sem nýtir undirverktaka til að veita upplýsinga- og fjarskiptatækniþjónustuna sem styður nauðsynlega eða mikilvæga starfsemi eða efnislegan hluta hennar.

2. gr.

Hópumsókn

Ef þessi reglugerð gildir á undirsamstæðu- eða samstæðugrunni skal móðurfyrirtækið sem ber ábyrgð á því að gera samstæðu- eða undirsamstæðureikningsskil fyrir samstæðuna tryggja að skilyrði fyrir undirverktöku á notkun upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislegan hluta hennar, þar sem slík undirverktakastarfsemi er heimil samkvæmt samningsbundnu fyrirkomulagi um notkun upplýsinga- og fjarskiptatækniþjónustu, sé framfylgt á samræmdan hátt hjá öllum aðilum á fjármálamarkaði sem eru hluti samstæðunnar og að hún sé fullnægjandi til að unnt sé að beita reglugerðinni á öllum stigum samstæðunnar á skilvirkan hátt.

3. gr.

Áreiðanleikakönnun og áhættumat varðandi notkun undirverktaka sem styðja nauðsynlega eða mikilvæga starfsemi

1. Áður en aðili á fjármálamarkaði gerir samningsbundið fyrirkomulag við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu skal hann ákveða hvort þeim þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu sé heimilt að semja við undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislegan hluta hennar. Aðili á fjármálamarkaði skal aðeins gera slíkt samningsbundið fyrirkomulag ef hann hefur metið að öll eftirfarandi skilyrði hafi verið uppfyllt:

a) áreiðanleikaferli á þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu tryggja að hann geti valið og lagt mat á rekstrarlega og fjárhagslega getu hugsanlegra undirverktaka í upplýsinga- og fjarskiptatækni til að veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, þ.m.t. með því að taka þátt í prófunum á stafrænum rekstrarlegum viðnámsþrótti, eins og um getur í IV. kafla reglugerðar (ESB) 2022/2554, að kröfu aðilans á fjármálamarkaði,

b) þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu getur tilgreint alla undirverktaka sem styðja nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, tilkynnt og upplýst aðilann á fjármálamarkaði um undirverktakana og getur veitt aðilanum á fjármálamarkaði allar upplýsingar sem kunna að vera nauðsynlegar til að meta skilyrðin samkvæmt þessari grein,

c) þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu tryggir að samningsbundið fyrirkomulag við undirverktakana sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega og mikilvæga starfsemi eða efnislega hluta hennar geri aðilanum á fjármálamarkaði kleift að uppfylla eigin skuldbindingar, sem leiða af reglugerð (ESB) 2022/2554 og gildandi lögum Sambandsins og landslöggjöf,

d) undirverktakinn veitir aðilanum á fjármálamarkaði og lögbærum yfirvöldum og skilastjórnvöldum sama samningsbundna

e) án þess að það hafi áhrif á endanlega ábyrgð aðilans á fjármálamarkaði á því að farið sé eftir skyldum samkvæmt lögum og reglum, þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur sjálfur fullnægjandi getu, sérþekkingu og nægilega fjármuni, mannauð og tæknigetu til að hafa eftirlit með upplýsinga- og fjarskiptatækniáhættu undirverktaka, þ.m.t. með því að beita viðeigandi upplýsingaöryggisstöðlum og hafa til staðar viðeigandi stjórnskipulag, áhættustýringu og innra eftirlit, sem og tilkynningar um atvik og viðbrögð,

f) aðilinn á fjármálamarkaði hefur fullnægjandi getu, sérþekkingu og nægilega fjármuni, mannauð og tæknigetu til að hafa eftirlit með upplýsinga- og fjarskiptatækniáhættu að því er varðar þjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar sem hefur verið falin undirverktaka, þ.m.t. með því að beita viðeigandi upplýsingaöryggisstöðlum og hafa til staðar viðeigandi stjórnskipulag, áhættustýringu, viðbrögð við atvikum, stjórnun rekstrarsamfellu og innra eftirlit,

g) aðilinn á fjármálamarkaði hefur lagt mat á hvaða áhrif hugsanlegur misbrestur hjá undirverktaka sem veitir upplýsinga- og fjarskiptatækniþjónustu, sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, hefði á stafrænan rekstrarlegan viðnámsþrótt aðilans á fjármálamarkaði og fjárhagslegt heilbrigði hans,

h) aðilinn á fjármálamarkaði hefur lagt mat á áhættuna sem tengist staðsetningu hugsanlegra undirverktaka í tengslum við upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar sem þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu veitir,

i) aðilinn á fjármálamarkaði hefur lagt mat á samþjöppunaráhættu í upplýsinga- og fjarskiptatækni hjá aðilanum í samræmi við 29. gr. reglugerðar (ESB) 2022/2554,

j) aðilinn á fjármálamarkaði hefur metið hvort einhverjar hindranir séu fyrir því að lögbær yfirvöld, skilastjórnvöld eða aðilinn á fjármálamarkaði beiti endurskoðun, eftirlitsúttekt og aðgangsrétti, þ.m.t. aðilar tilnefndir af þeim.

2. Aðilar á fjármálamarkaði sem nota þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem fela undirverktaka upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar skulu reglulega framkvæma áhættumatið sem um getur í f- til j-lið 1. mgr. varðandi hugsanlegar breytingar á viðskiptaumhverfi sínu, þ.á m. varðandi breytingar á studdri starfsemi, á áhættumötum sem taka til upplýsinga- og fjarskiptatækniógna, samþjöppunaráhættu í upplýsinga- og fjarskiptatækni og landfræðipólitískra áhættuþátta.

3. Þótt aðilar á fjármálamarkaði treysti á niðurstöður áhættumatsins sem þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu framkvæma á undirverktökum sínum, þegar þeir uppfylla skuldbindingarnar sem settar eru fram í þessari grein, skal það ekki takmarka endanlega ábyrgð þeirra á að uppfylla skyldur sínar samkvæmt lögum og reglum samkvæmt reglugerð (ESB) 2022/2554.

4. gr.

Skilyrði fyrir því að hægt sé að semja við/fela undirverktaka um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar

1. Í samningsbundnu fyrirkomulagi á milli aðilans á fjármálamarkaði og þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu skal tilgreint hvaða upplýsinga- og fjarskiptatækniþjónustur sem styðja nauðsynlega eða mikilvæga starfsemi eru hæfar til undirverktakastarfsemi og með hvaða skilyrðum. Eftirfarandi skal tilgreint í samningnum:

a) að þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu beri ábyrgð á veitingu þjónustunnar sem undirverktakarnir veita,

b) að gerð sé krafa um að þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu hafi eftirlit með allri upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi og falin er undirverktökum eða efnislega hluta hennar til að tryggja að samningsbundnar skyldur við aðilans á fjármálamarkaði séu stöðugt uppfylltar,

c) skyldur þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu um vöktun og skýrslugjöf gagnvart aðilanum á fjármálamarkaði varðandi undirverktaka sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar,

d) að þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu skuli leggja mat á alla áhættu sem tengist staðsetningu núverandi eða hugsanlegra undirverktaka sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar og móðurfélags þeirra og staðsetningunni þaðan sem viðkomandi upplýsinga- og fjarskiptatækniþjónusta er veitt frá,

e) staðsetning gagna sem undirverktakinn vinnur eða geymir, eftir því sem við á,

f) að þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu skuli tilgreina í samningi sínum við undirverktaka skyldur um vöktun og skýrslugjöf sem undirverktakinn hefur gagnvart þriðja aðilanum sem veitir upplýsinga- og fjarskiptatækniþjónustu og, þegar sammælst er um slíkt, gagnvart aðilanum á fjármálamarkaði,

g) að þriðji aðilinn sem veitir upplýsinga- og fjarskiptatækniþjónustu skuli tryggja samfellu í upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi í allri keðju undirverktaka, ef undirverktaki í upplýsinga- og fjarskiptatækni stendur ekki við samningsbundnar skyldur sínar,

h) að samningsbundið fyrirkomulag milli þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans feli í sér kröfur um viðbragðsáætlanir sem um getur í c-lið 3. mgr. 30. gr. reglugerðar (ESB) 2022/2554 og tilgreini þjónustustig sem undirverktakar í upplýsinga- og fjarskiptatækni skulu uppfylla í tengslum við áætlanirnar,

i) að samningsbundna fyrirkomulagið milli þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og undirverktaka hans tilgreini öryggisstaðla í upplýsinga- og fjarskiptatækni og allar viðbótaröryggiskröfur sem um getur í c-lið 3. mgr. 30. gr. reglugerðar (ESB) 2022/2554,

j) að undirverktaki skuli veita aðilanum á fjármálamarkaði og viðeigandi lögbærum og skilastjórnvöldum sama rétt til aðgengis, eftirlitsúttektar og endurskoðunar og þeim sem um getur í e-lið 3. mgr. 30. gr. reglugerðar (ESB) 2022/2554,

k) að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skuli tilkynna aðila á fjármálamarkaði um hvers kyns efnislegar breytingar á undirverktakasamningum,

l) að aðili á fjármálamarkaði hafi rétt til að rifta samningi við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu ef skilyrðin sem mælt er fyrir um í annaðhvort 6. gr. þessarar reglugerðar eða skilyrðin sem mælt er fyrir um í 7. mgr. 28. gr. reglugerðar (ESB) 2022/2554 hafa verið uppfyllt.

2. Breytingar sem tengjast samningum milli aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar, sem nauðsynlegar eru til að uppfylla kröfur þessarar reglugerðar, skulu innleiddar tímanlega og eins fljótt og unnt er. Aðili á fjármálamarkaði skal skjalfesta fyrirhugaða tímalínu innleiðingarinnar.

5. gr.

Efnislegar breytingar á undirverktakasamningum um upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar

1. Í samningsbundnu fyrirkomulagi skal kveðið á um að þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skuli upplýsa aðila á fjármálamarkaði um allar fyrirhugaðar efnislegar breytingar á undirverktakasamningum með nægum fyrirvara til að aðilinn á fjármálamarkaði geti lagt mat á:

a) áhrifin á þá áhættu sem hann er undir eða kann að standa frammi fyrir,

b) hvort slíkar efnislegar breytingar geti haft áhrif á getu þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu til að uppfylla samningsbundnar skyldur sínar gagnvart aðila á fjármálamarkaði.

2. Í samningsbundna fyrirkomulaginu skal kveðið á um hæfilegan uppsagnarfrest fyrir aðila á fjármálamarkaði til að samþykkja eða andmæla breytingunum.

3. Þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu skal aðeins framkvæma efnislegar breytingar á undirverktakasamningum sínum eftir að aðili á fjármálamarkaði hefur annaðhvort samþykkt eða ekki andmælt breytingunum við lok uppsagnarfrestsins.

4. Ef aðili á fjármálamarkaði er þeirrar skoðunar að þær efnislegu breytingar sem um getur í 1. mgr. fari umfram áhættuþol aðila á fjármálamarkaði skal hann, áður en uppsagnarfresturinn rennur út:

a) upplýsa þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu um það,

b) andmæla breytingunum og óska eftir breytingum á þeim áður en þær eru innleiddar.

6. gr.

Uppsögn samnings milli aðila á fjármálamarkaði og þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu

Aðili á fjármálamarkaði skal hafa rétt til að kveða á um í samningsbundnu fyrirkomulagi við þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu að samningsbundnu fyrirkomulagi skuli slitið í sérhverju eftirfarandi tilvika:

a) aðili á fjármálamarkaði hefur andmælt efnislegum breytingum á undirverktakasamningum sem styðja nauðsynlega eða mikilvæga starfsemi og óskað eftir breytingum á samningunum, en þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur engu að síður innleitt þessar efnislegu breytingar,

b) þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu hefur innleitt efnislegar breytingar á undirverktakasamningum sem styðja nauðsynlega eða mikilvæga starfsemi eða efnislega hluta hennar áður en uppsagnarfrestur rennur út án samþykkis aðilans á fjármálamarkaði,

c) þriðji aðili sem veitir upplýsinga- og fjarskiptatækniþjónustu felur undirverktaka upplýsinga- og fjarskiptatækniþjónustu sem styður nauðsynlega eða mikilvæga starfsemi eða efnislegan hluta hennar, án þess að það sé sérstaklega heimilt samkvæmt samningi milli aðilans á fjármálamarkaði og þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu.

7. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 24. mars 2025.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

Fylgiskjal 10.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2025/1190

frá 13. febrúar 2025

um viðbætur við reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 að því er varðar tæknilega eftirlitsstaðla þar sem tilgreind eru viðmið sem notuð eru til að auðkenna aðila á fjármálamarkaði sem skylt er að framkvæma ógnamiðaðar innbrotsprófanir, kröfur og staðlar sem gilda um notkun á innri prófunaraðilum, kröfur í tengslum við umfang, prófunaraðferðir og nálgun fyrir hvern fasa í prófunum, niðurstöður, lokunar- og úrbótastig prófunar og tegund eftirlitssamvinnu og annarrar viðeigandi samvinnu sem þörf er á við innleiðingu ógnamiðaðra innbrotsprófana og til að greiða fyrir gagnkvæmri viðurkenningu

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 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 ([1]), einkum fjórðu undirgrein 11. mgr. 26. gr.,

og að teknu tilliti til eftirfarandi:

1) Þessi reglugerð er samin í samræmi við TIBER-EU-rammann og endurspeglar aðferðafræði, ferli og uppbyggingu ógnamiðaðrar innbrotsprófunar (TLPT) eins og lýst er í TIBER-EU. Aðilar á fjármálamarkaði sem falla undir ógnamiðaða innbrotsprófun geta vísað til og beitt TIBER-EU-rammanum, eða einhverri landsbundinni innleiðingu hans, að því marki sem sá rammi eða sú innleiðing er í samræmi við kröfurnar sem settar eru fram í 26. og 27. gr. reglugerðar (ESB) 2022/2554 og þessari reglugerð. Tilnefning eins opinbers yfirvalds í fjármálageiranum til að bera ábyrgð á málum sem tengjast ógnamiðaðri innbrotsprófun á landsvísu í samræmi við 9. mgr. 26. gr. reglugerðar (ESB) 2022/2554 ætti ekki að hafa áhrif á valdheimildir lögbærra yfirvalda sem þeim er falið á vettvangi Sambandsins til að hafa eftirlit með tilteknum aðilum á fjármálamarkaði í samræmi við 46. gr. þeirrar reglugerðar svo sem, t.d., Seðlabanka Evrópu að því er varðar mikilvægar lánastofnanir sem teljast hæfar vegna málefna sem tengjast ógnamiðaðri innbrotsprófun. Þegar aðeins sumum verkefnum í tengslum við ógnamiðaða innbrotsprófun er úthlutað til annars lögbærs yfirvalds í fjármálageiranum skv. 10. mgr. 26. gr. reglugerðar (ESB) 2022/2554 ætti lögbært yfirvald aðilans á fjármálamarkaði sem um getur í 46. gr. þeirrar reglugerðar að vera yfirvald verkefna í tengslum við ógnamiðaða innbrotsprófun sem ekki hefur verið úthlutað.

2) Með hliðsjón af því hversu flókin ógnamiðuð innbrotsprófun er og þeirri áhættu sem henni fylgir ætti notkun hennar að vera takmörkuð við þá aðila á fjármálamarkaði þar sem hún er réttlætanleg. Þar af leiðandi ættu yfirvöldin sem bera ábyrgð á málefnum í tengslum við ógnamiðaða innbrotsprófun (yfirvöld á sviði ógnamiðaðrar innbrotsprófunar, annað hvort á vettvangi Sambandsins eða á landsvísu) að undanskilja frá umfangi ógnamiðaðrar innbrotsprófunar þá aðila á fjármálamarkaði sem starfa innan undirgeira kjarnafjármálaþjónustu þar sem ekki er unnt að réttlæta ógnamiðaða innbrotsprófun. Það þýðir að lánastofnanir, greiðslustofnanir og rafeyrisfyrirtæki, verðbréfamiðstöðvar, miðlægir mótaðilar, viðskiptavettvangar, vátrygginga- og endurtryggingafélög, jafnvel þótt aðilarnir uppfylli megindlegar viðmiðanir, gætu losnað undan kröfum um ógnamiðaða innbrotsprófun í ljósi heildarmats á áhættusniði og þroska upplýsinga- og fjarskiptatækni þeirra, áhrifum á fjármálageirann og tengdum áhyggjum af fjármálastöðugleika.

3) Yfirvöld á sviði ógnamiðaðrar innbrotsprófunar ættu að meta, í ljósi heildarmats á áhættusniði og þroska upplýsinga- og fjarskiptatækni, áhrifum á fjármálageirann og tengdum áhyggjum af fjármálastöðugleika, hvort einhver önnur tegund aðila á fjármálamarkaði en lánastofnanir, greiðslustofnanir, rafeyrisfyrirtæki, miðlægir mótaðilar, verðbréfamiðstöðvar, viðskiptavettvangar, vátryggingafélög og endurtryggingafélög ættu að falla undir ógnamiðaða innbrotsprófun. Matið á því hvort slíkir aðilar á fjármálamarkaði uppfylli þessar eigindlegu viðmiðanir ætti að miða að því að bera kennsl á aðila á fjármálamarkaði sem viðeigandi er að beita ógnamiðaða innbrotsprófun á með því að nota vísa sem eru þvert á

([1]) Stjtíð. ESB L 333, 27.12.2022, bls. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

atvinnugreinar og hlutlægir. Á sama tíma ætti matið á því hvort aðili á fjármálamarkaði uppfyllir þessar eigindlegu viðmiðanir að takmarka aðilana sem falla undir ógnamiðaða innbrotsprófun við þá aðila sem réttlætanlegt er að prófa. Einnig ætti að meta hvort aðili á fjármálamarkaði uppfyllir þessar eigindlegu viðmiðanir í ljósi þróunar á nýjum mörkuðum og aukins mikilvægis nýrra markaðsaðila fyrir fjármálageirann í framtíðinni, þ.m.t. þjónustuveitendur sýndareigna sem hafa starfsleyfi í samræmi við 59. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2023/1114 ([2]).

4) Aðilar á fjármálamarkaði geta haft sama veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu eða tilheyrt sömu samstæðu og reitt sig á samnýtt upplýsinga- og fjarskiptatæknikerfi. Í þeim tilvikum er mikilvægt að yfirvöld á sviði ógnamiðaðrar innbrotsprófunar taki tillit til uppbyggingar og kerfislægra eiginleika eða mikilvægis viðkomandi aðila á fjármálamarkaði á landsvísu eða á vettvangi Sambandsins við mat á því hvort aðili á fjármálamarkaði ætti að falla undir ógnamiðaða innbrotsprófun og hvort framkvæma ætti ógnamiðaða innbrotsprófun á eininga- eða samstæðustigi (með sameiginlegri ógnamiðaðri innbrotsprófun).

5) Í því skyni að endurspegla TIBER-EU-rammann er nauðsynlegt að aðferðafræði prófunar kveði á um þátttöku eftirfarandi aðalþátttakenda: aðilans á fjármálamarkaði, með stýrihópi (sem endurspeglar „stýrihóp“ TIBER-EU) og blátt teymi (sem endurspeglar „blátt teymi“ TIBER-EU), og yfirvaldsins á sviði ógnamiðaðrar innbrotsprófunar, í formi netöryggisteymis ógnamiðaðrar innbrotsprófunar (sem endurspeglar „TIBER-netöryggisteymi“ TIBER-EU), aðila sem veitir ógnagreiningargögn og prófunaraðila (þar sem prófunaraðilarnir endurspegla „þann sem útvegar rautt teymi“ í TIBER-EU).

6) Til að tryggja að reynslan sem fengist hefur með innleiðingu TIBER-EU-rammans nýtist við ógnamiðuðu innbrotsprófunina og til að draga úr áhættu í tengslum við framkvæmd hennar ætti að tryggja að ábyrgð netöryggisteymis ógnamiðaðrar innbrotsprófunar sem koma skal á fót á stigi yfirvalda ógnamiðaðrar innbrotsprófunar samsvari eins nákvæmlega og hægt er ábyrgð netteyma TIBER-EU. Þar af leiðandi ættu netöryggisteymi ógnamiðaðrar innbrotsprófunar að hafa prófunarstjóra sem bera ábyrgð á umsjón með einstökum ógnamiðuðum innbrotsprófunum og á skipulagningu og samræmingu einstakra prófana. Netöryggisteymi ógnamiðaðrar innbrotsprófunar ættu að vera sameiginlegur tengiliður fyrir samskipti í tengslum við prófun fyrir innri og ytri hagsmunaaðila, fyrir söfnun og úrvinnslu endurgjafar og lærdóms af áður framkvæmdum prófunum og ættu að styðja við aðila á fjármálamarkaði sem gangast undir ógnamiðaða innbrotsprófun.

7) Til að endurspegla aðferðafræði TIBER-EU-rammans ættu prófunarstjórar að búa yfir nauðsynlegri hæfni og getu til að veita ráðgjöf og til að gagnrýna tillögur prófunaraðila. Reynslan af TIBER-EU-rammanum hefur sýnt fram á gildi þess að hafa teymi sem samanstendur af í það minnsta tveimur prófunarstjórum sem úthlutað er á hverja prófun. Til að endurspegla að ógnamiðuð innbrotsprófun er notuð til að stuðla að lærdómsreynslu, til að vernda trúnað prófana, nema um sé að ræða vandamál varðandi tilföng eða sérfræðiþekkingu, eru yfirvöld ógnamiðaðrar innbrotsprófunar eindregið hvött til að hafa í huga að meðan á ógnamiðaðri innbrotsprófun stendur ættu prófunarstjórar ekki að sinna eftirlitsstarfsemi að því er varðar þann aðila á fjármálamarkaði sem undirgengst ógnamiðaða innbrotsprófun.

8) Til að tryggja samræmi við TIBER-EU-rammann er mikilvægt að yfirvald ógnamiðaðrar innbrotsprófunar fylgist náið með prófuninni á öllum stigum hennar. Að teknu tilliti til eðlis prófunarinnar og áhættunnar sem henni fylgir er mikilvægt að yfirvald ógnamiðaðrar innbrotsprófunar sé þátttakandi í sérhverjum áfanga prófunarinnar. Einkum ætti að hafa samráð við yfirvald ógnamiðaðrar innbrotsprófunar og það ætti að staðfesta þau möt eða ákvarðanir aðilans á fjármálamarkaði sem gætu annars vegar sett mark sitt á skilvirkni prófunarinnar og hins vegar haft áhrif á áhættur tengdar prófuninni. Þau grundvallarskref sem krefjast sérstakrar aðkomu yfirvalds ógnamiðaðrar innbrotsprófunar eru m.a. sannreyning á tiltekinni grundvallarskjölun prófunarinnar og val á veitendum ógnagreiningargagna og prófunaraðilum og áhættustýringarráðstöfununum. Aðkoma yfirvalda ógnamiðaðrar innbrotsprófunar, einkum varðandi sannreyningu, ætti ekki að hafa í för með sér óþarfa byrði fyrir þau yfirvöld og því ætti að takmarka hana við þá skjalfestingu og þær ákvarðanir sem hafa bein áhrif á framkvæmd ógnamiðaðrar innbrotsprófunar. Með virkri þátttöku í hverjum áfanga prófunarinnar geta yfirvöld ógnamiðaðrar innbrotsprófunar metið á skilvirkan hátt hlítni aðila á fjármálamarkaði við viðeigandi kröfur, sem ætti að gera yfirvöldunum kleift að gefa út staðfestingu skv. 7. mgr. 26. gr. reglugerðar (ESB) 2022/2554.

([2]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2023/1114 frá 31. maí 2023 um markaði fyrir sýndareignir og um breytingu á reglugerðum (ESB) nr. 1093/2010 og (ESB) nr. 1095/2010 og tilskipunum 2013/36/ESB og (ESB) 2019/1937 (Stjtíð. ESB L 150, 9.6.2023, bls. 40, ELI: http://data.europa.eu/eli/reg/2023/1114/oj).

9) Leynd ógnamiðuðu innbrotsprófunarinnar er afar mikilvæg til að tryggja að prófunarskilyrðin séu sem raunverulegust. Af þessum sökum ætti prófunin að vera leynileg og gera ætti varúðarráðstafanir til að halda ógnamiðuðu innbrotsprófuninni leyndri, þ.m.t. með vali á dulnefnum sem ætti að útfæra svo að koma megi í veg fyrir að þriðju aðilar geti áttað sig á ógnamiðuðu innbrotsprófuninni. Verði starfsfólk sem ber ábyrgð á öryggi fjármálateymisins vart við fyrirhugaða eða yfirstandandi ógnamiðaða innbrotsprófun er líklegt að það verði athugulla og betur á verði en við eðlilegar vinnuaðstæður, sem hefur þar af leiðandi í för með sér breytta niðurstöðu prófunar. Starfsfólk aðila á fjármálamarkaði utan stýrihópsins ætti því aðeins að fá að vita um fyrirhugaða eða yfirstandandi ógnamiðaða innbrotsprófun ef um er að ræða brýnar ástæður og með fyrirvara um fyrirframsamþykki prófunarstjóranna, m.a. til að tryggja leynd prófunarinnar ef aðili innan bláa teymisins hefur uppgötvað prófunina.

10) Eins og reynslan af TIBER-EU-rammanum hefur sýnt að því er varðar „stýrihópinn“ er nauðsynlegt að velja hæfan hópstjóra stýrihóps til að framkvæmd ógnamiðaðrar innbrotsprófunar verði sem öruggust. Hópstjóri stýrihópsins ætti að hafa fullnægjandi umboð innan aðilans á fjármálamarkaði til að stýra öllum þáttum prófunarinnar, án þess að stofna leynd hennar í hættu. Af sömu ástæðu ættu aðilar stýrihópsins að búa yfir yfirgripsmikilli þekkingu á aðilanum á fjármálamarkaði, hlutverki og leiðandi stöðu hópstjóra stýrihópsins, vera nægilega háttsettir og hafa aðgang að yfirstjórn aðila. Til að draga úr líkum á því að ógnamiðaðri innbrotsprófun verði stofnað í hættu ætti stýrihópurinn að vera eins lítill og mögulegt er.

11) Ógnamiðaðri innbrotsprófun fylgja eðlislægir áhættuþættir, þar sem nauðsynleg starfsemi er prófuð í raunumhverfi í rauntíma, sem gætu valdið álagsárásum (e. *denial-of-service*), óvæntu kerfishruni, skemmdum á nauðsynlegum virkum þjónustukerfum eða tapi, breytingu eða birtingu gagna. Þessi áhætta undirstrikar þörfina fyrir traustar áhættustýringarráðstafanir. Til að tryggja að ógnamiðuð innbrotsprófun sé framkvæmd á stýrðan hátt allt prófunarferlið er mjög mikilvægt að aðilar á fjármálamarkaði séu á öllum tímum meðvitaðir um þá sértæku áhættu sem kemur upp við ógnamiðaða innbrotsprófun og að dregið sé úr þeirri áhættu. Að því leyti, og án þess að það hafi áhrif á innri ferla aðilans á fjármálamarkaði og þá ábyrgð og þau umboð sem þegar hafa verið veitt hópstjóra stýrihópsins, kann að vera viðeigandi að upplýsingar um áhættustýringarráðstafanir vegna ógnamiðaðrar innbrotsprófunar, eða í sérstökum tilvikum samþykki stjórnar og/eða framkvæmdastjórnar aðilans á fjármálamarkaði á þeim áhættustýringarráðstöfunum, séu veittar. Til að geta veitt skilvirka og hæfustu sérfræðiþjónustu og til að draga úr þeirri áhættu er einnig nauðsynlegt að prófunaraðilar og veitendur ógnagreiningargagna (saman kallaðir veitendur ógnamiðaðrar innbrotsprófunar) búi yfir hæfni, sérfræðiþekkingu og viðeigandi reynslu á hæsta stigi í ógnagreiningum og ógnamiðaðri innbrotsprófun í fjármálaþjónustugeiranum.

12) Hefðbundin innbrotsprófun veitir ítarlegt og gagnlegt mat á tæknilegum veikleikum og veikleikum í uppsetningu, oft á einu kerfi eða umhverfi í einangrun, en ólíkt greiningargagnamiðuðum prófunum rauðs teymis meta þau ekki heildarsviðsmynd markvissrar árásar á aðila í heild, þ.m.t. allt umfang fólks, ferla og tækni. Við valferli á veitendum ógnamiðaðrar innbrotsprófunar ættu aðilar á fjármálamarkaði því að tryggja að þessir veitendur hafi nauðsynlega hæfni til að framkvæma greiningargagnamiðaða prófun rauðs teymis og ekki eingöngu innbrotsprófanir. Því er nauðsynlegt að mæla fyrir um ítarlegar viðmiðanir fyrir prófunaraðila, bæði innri og ytri, og veitendur ógnagreiningargagna, sem eru ávallt utanaðkomandi. Þegar veitendur ógnamiðaðrar innbrotsprófunar tilheyra sama félagi ætti að aðgreina með fullnægjandi hætti starfsfólkið sem er falið að gera ógnamiðaða innbrotsprófun.

13) Það geta verið undantekningartilvik þar sem aðilar á fjármálamarkaði geta ekki ráðið veitendur ógnamiðaðrar innbrotsprófunar sem uppfylla þessar ítarlegu viðmiðanir. Aðilar á fjármálamarkaði ættu því, eftir að hafa fært sönnur á því að engir slíkir veitendur ógnagreiningargagna eru tiltækir, að hafa heimild til að ráða aðila sem uppfylla ekki allar ítarlegu viðmiðanirnar, að því tilskildu að þeir dragi með fullnægjandi hætti úr viðbótaráhættunni sem því fylgir og að yfirvald ógnamiðaðrar innbrotsprófunar meti allar þessar viðmiðanir.

14) Ef margir aðilar á fjármálamarkaði og mörg yfirvöld ógnamiðaðrar innbrotsprófunar taka þátt í ógnamiðaðri innbrotsprófun ætti að tilgreina hlutverk allra aðila í ferlinu til að framkvæmd prófunarinnar verði sem skilvirkust og öruggust. Í tilgangi samsettrar prófunar er nauðsynlegt að gera sértækar kröfur um að tilgreina hlutverk tilnefnds aðila á fjármálamarkaði, nánar tiltekið ætti hann að bera ábyrgð á veitingu allra nauðsynlegra skjala til leiðandi yfirvalds ógnamiðaðrar innbrotsprófunar og vöktun á prófunarferlinu. Tilnefndi aðilinn á fjármálamarkaði ætti einnig að bera ábyrgð á sameiginlegum þáttum matsins á áhættustýringu. Þrátt fyrir hlutverk tilnefnda aðilans á fjármálamarkaði ættu skuldbindingar sérhvers aðila á fjármálamarkaði sem tekur þátt í samsettu ógnamiðuðu innbrotsprófuninni að vera óbreyttar á meðan á samsettu prófuninni stendur. Sama meginreglan ætti að gilda um sameiginlega ógnamiðaða innbrotsprófun.

15) Eins og reynslan af innleiðingu TIBER-EU-rammans hefur sýnt er skilvirkasta leiðin til að tryggja viðeigandi framkvæmd prófunarinnar að halda staðfundi eða fjarfundi, með öllum hlutaðeigandi hagsmunaaðilum (aðilum á fjármálamarkaði, yfirvöldum, prófunaraðilum og veitendum ógnagreiningargagna). Því ætti að halda staðfundi og fjarfundi á mismunandi stigum ferlisins, einkum í undirbúningsfasanum við upphaf ógnamiðuðu innbrotsprófunarinnar og til að fastmóta umfang hennar, á meðan á prófunarferlinu stendur, til að ljúka við gerð skýrslunnar um ógnagreiningargögn og prófunaráætlun rauða teymisins, og fyrir vikulegar stöðuuppfærslur, og í lokunarfasanum til að endurspila aðgerðir prófunaraðila og bláa teymisins, teymisvinnu fjólubláa teymisins og til að skiptast á endurgjöf um ógnamiðuðu innbrotsprófunina.

16) Til að tryggja snurðulausa framkvæmd ógnamiðuðu innbrotsprófunarinnar ætti yfirvald ógnamiðaðrar innbrotsprófunar að setja væntingar sínar um prófunina skýrt fram til aðilans á fjármálamarkaði. Hvað það varðar ættu prófunarstjórarnir að tryggja að komið sé á viðeigandi upplýsingaflæði til stýrihóps aðilans á fjármálamarkaði og veitenda ógnamiðaðra innbrotsprófana.

17) Aðilinn á fjármálamarkaði ætti að velja nauðsynlega eða mikilvæga starfsemi sem mun falla undir ógnamiðuðu innbrotsprófunina. Við val á þessari starfsemi ætti aðilinn á fjármálamarkaði að byggja á ýmsum viðmiðunum sem varða mikilvægi hverrar starfsemi fyrir aðilann sjálfan og fyrir fjármálageirann, á vettvangi Sambandsins og á landsvísu, ekki aðeins með hliðsjón af efnahagslegum skilyrðum heldur einnig með tilliti til táknrænnar eða pólitískrar stöðu starfseminnar. Til að stuðla að snurðulausri yfirfærslu yfir í fasa söfnunar ógnagreiningargagna ætti stýrihópurinn að veita prófunaraðilum og veitendum ógnagreiningargagna sem taka ekki þátt í ferlinu við að ákvarða umfangið, ítarlegar upplýsingar um samþykkt umfang.

18) Til að veita prófunaraðilunum nauðsynlegar upplýsingar til að herma eftir raunverulegri og raunhæfri árás á kerfi aðilans á fjármálamarkaði í rauntíma, sem eru undirstaða nauðsynlegrar eða mikilvægrar starfsemi, ætti veitandi ógnagreiningargagna að safna greiningargögnum eða upplýsingum um a.m.k. tvö lykilþætti: árásarmörkin, með því að greina mögulega árásarfleti á aðilann á fjármálamarkaði, og ógnirnar, með því að greina viðeigandi ógnvalda og mögulegar ógnasviðsmyndir. Til að tryggja að veitandi ógnagreiningargagna taki viðeigandi ógnir gagnvart aðilanum á fjármálamarkaði til greina ættu prófunaraðilarnir, stýrihópurinn og prófunarstjórarnir að veita endurgjöf um drögin að skýrslunni um ógnagreiningargögn. Ef það er tiltækt getur veitandi ógnagreiningargagna notað almennt landslag netógna sem yfirvald ógnamiðaðrar innbrotsprófunar leggur fram fyrir fjármálageira aðildarríkis sem grunnviðmið fyrir landsbundið landslag netógna. Á grundvelli beitingar TIBER-EU-rammans varir söfnun ógnagreiningargagna venjulega u.þ.b. fjórar vikur.

19) Til að gera prófunaraðilunum kleift að öðlast innsýn og endurskoða enn frekar skjalið um skilgreiningu umfangs prófunar og skýrsluna um markvissar ógnagreiningar til að ljúka við prófunaráætlun rauða teymisins er nauðsynlegt, áður en prófunarfasi rauða teymisins í ógnamiðuðu innbrotsprófuninni hefst, að prófunaraðilarnir fái frá veitanda ógnagreiningargagnanna ítarlegar útskýringar á skýrslunni um markviss ógnagreiningargögn og greiningu á mögulegum ógnasviðsmyndum.

20) Til að gera prófunaraðilum kleift að framkvæma raunsæja og ítarlega prófun þar sem allir árásarfasar eru framkvæmdir og skilgreindum markmiðum náð (hér á eftir nefnt „flagg“) ætti að veita nægan tíma fyrir prófunarfasa rauða teymisins. Á grundvelli reynslunnar af TIBER-EU-rammanum ætti tíminn sem er veittur að vera a.m.k. 12 vikur og skal hann ákvarðaður með hliðsjón af fjölda aðila sem eiga í hlut, umfangi ógnamiðuðu innbrotsprófunarinnar, tilfanga hlutaðeigandi aðila á fjármálamarkaði, hvers konar utanaðkomandi kröfum og tiltækileika stuðningsupplýsinga sem aðilinn á fjármálamarkaði veitir.

21) Meðan á prófunarfasa rauðs teymis stendur ættu prófunaraðilarnir að beita ýmsum úrræðum, tæknilausnum og aðferðum til að prófa með fullnægjandi hætti framleiðslukerfi aðilans á fjármálamarkaði í rauntíma. Úrræðin, tæknilausnirnar og aðferðirnar ættu að fela í sér, eins og við á, frumkönnun (þ.e. að safna eins miklum upplýsingum og mögulegt er um árásarmark), undirbúning árásar (þ.e. að greina upplýsingar um innviði, aðstöðu og starfsfólk og undirbúa aðgerðir sem beinast sérstaklega að árásarmarkinu), framkvæmd (þ.e. virkt upphaf heildaraðgerða gegn árásarmarkinu), misnotkun (þ.e. ef markmið prófunaraðila er að stofna netþjónum og netkerfi aðilans á fjármálamarkaði í hættu og misnota starfsfólk með bragðvísi), stjórn og tilfærslu (þ.e. tilraunir til tilfærslu frá vásettum kerfum til kerfa sem eru viðkvæmari eða mikilvæg) og aðgerðir gegn árásarmarkinu (þ.e. að fá frekari aðgang að vásettum kerfum og fá aðgang að fyrirframákveðnum upplýsingum og gögnum, eins og áður var samþykkt í prófunaráætlun rauða teymisins).

22) Við framkvæmd á ógnamiðaðri innbrotsprófun ættu prófunaraðilar að aðhafast í samræmi við þann tíma sem er tiltækur til að framkvæma árásina, tilföngin og siðferðisleg og lagaleg mörk. Ef prófunaraðilarnir geta ekki haldið áfram á næsta fyrirhugaða stig árásarinnar ætti stýrihópurinn stöku sinnum að geta veitt liðsinni að fengnu samþykki yfirvalds ógnamiðuðu innbrotsprófunarinnar, með „hjálparhönd“. Hjálparhönd má flokka gróft í upplýsinga- og aðgangsaðstoð og getur falið í sér veitingu aðgangs að upplýsinga- og fjarskiptatæknikerfum eða innri netkerfum til að geta haldið áfram með prófunina og einblínt á næstu skref árásarinnar.

23) Meðan vinna rauða teymisins er í prófunarfasanum ætti, ef þörf krefur til að hægt sé að halda áfram ógnamiðuðu innbrotsprófuninni sem síðasta úrræði við sérstakar aðstæður og þegar allir aðrir kostir hafa verið nýttir, að beita prófun sem er samstarfsverkefni með þátttöku bæði prófunaraðilanna og bláa teymisins. Í tengslum við slíka takmarkaða fjólubláa teymisvinnu er unnt að nota eftirfarandi aðferðir: „fangað og sleppt“ (e. *catch-and-release*) þar sem prófunaraðilar reyna að halda sviðsmyndinni áfram, það kemst upp um þá en þeir halda prófuninni áfram, „stríðsleikir“ (e. *war gaming*) sem gera það kleift að gera flóknari sviðsmyndir til að prófa stefnumarkandi ákvarðanatöku eða „samstarf um sönnun á hugmyndum“ (e. *collaborative proof-of-concept*) sem gerir prófunaraðilum og aðilum blás teymis kleift að sannprófa tilteknar öryggisráðstafanir, tæki eða tækni í stýrðu samstarfsumhverfi.

24) Ógnamiðaða innbrotsprófun ætti að nota til lærdóms í því skyni að auka stafrænan rekstrarlegan viðnámsþrótt aðila á fjármálamarkaði. Í því tilliti ætti bláa teymið og prófunaraðilar að endurtaka árásina og endurskoða skrefin sem tekin eru til að læra af prófuninni í samstarfi við prófunaraðilana. Í þeim tilgangi og til að gera fullnægjandi undirbúning mögulegan ætti að gera prófunarskýrslu rauða teymisins og prófunarskýrslu bláa teymisins aðgengilegar öllum aðilum sem taka þátt í endurtekningunni, áður en þeir framkvæma endurtekninguna. Þar að auki ætti fjólublá teymisvinna að fara fram í lokunarfasanum til að hámarka lærdóminn. Aðferðirnar sem nota má í fjólubláu teymisvinnunni í lokunarfasanum ættu m.a. að vera umræða um aðrar mögulegar árásarsviðsmyndir, athugun á kerfum í öðrum sviðsmyndum í rauntíma eða endurathugun á fyrirhuguðum sviðsmyndum í rauntíma sem prófunaraðilarnir náðu ekki að ljúka eða framkvæma í prófunarfasanum.

25) Til að stuðla enn frekar að lærdómi allra þátttakenda í ógnamiðuðu innbrotsprófuninni, til hagsbóta fyrir prófanir í framtíðinni og til að auka stafrænan rekstrarlegan viðnámsþrótt enn frekar ættu hlutaðeigandi aðilar að veita hver öðrum endurgjöf um heildarferlið og einkum tilgreina hvaða aðgerðir gengu vel eða hvaða aðgerðir mætti bæta og hvaða þættir ógnamiðuðu innbrotsprófunarinnar virkuðu vel eða hvaða þætti mætti bæta.

26) Lögbæru yfirvöldin sem um getur í 46. gr. reglugerðar (ESB) 2022/2554 og yfirvöld ógnamiðaðrar innbrotsprófunar ættu, ef þau eru ekki þau sömu, að hafa samstarf um að fella ítarlega prófun í formi ógnamiðaðrar innbrotsprófunar inn í gildandi eftirlitsferli. Í því tilliti og til að deila réttum skilningi á niðurstöðum ógnamiðuðu innbrotsprófunarinnar og hvernig ætti að túlka þær þykir rétt, einkum að því er varðar yfirlitsskýrsluna um prófunina og úrbótaáætlanir, að koma á nánu samstarfi milli prófunarstjóra sem tóku þátt í ógnamiðuðu innbrotsprófuninni og þeirra eftirlitsaðila sem bera ábyrgð.

27) Í samræmi við fyrstu undirgrein 8. mgr. 26. gr. reglugerðar (ESB) 2022/2554 er þess krafist að aðilar á fjármálamarkaði geri verktakasamning við ytri prófunaraðila um þriðju hverja prófun. Ef aðilar á fjármálamarkaði hafa bæði innri og ytri prófunaraðila í prófunarteymi sínu ætti að líta á það sem ógnamiðaða innbrotsprófun sem framkvæmd er af innri prófunaraðilum að því er varðar þá grein.

28) Reglugerð þessi byggist á drögum að tæknilegum eftirlitsstöðlum sem Evrópska bankaeftirlitsstofnunin, Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin og Evrópska verðbréfamarkaðseftirlitsstofnunin (Evrópsku eftirlitsstofnanirnar) hafa lagt fyrir framkvæmdastjórnina, í samráði við Seðlabanka Evrópu.

29) Evrópsku eftirlitsstofnanirnar hafa haft opið samráð við almenning um drögin að tæknilegu eftirlitsstöðlunum sem þessi reglugerð byggist á, greint mögulegan tengdan kostnað og ávinning og óskað eftir áliti hagsmunahópsins um bankastarfsemi sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 ([3]), hagsmunahópsins í vátryggingum og endurtryggingum og hagsmunahópsins um starfstengdan lífeyri sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 ([4]), og hagsmunahópsins á verðbréfamarkaði sem komið var á fót í samræmi við 37. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 ([5]).

30) Samráð var haft við Evrópsku persónuverndarstofnunina í samræmi við 1. mgr. 42. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) 2018/1725 ([6]) og skilaði hún áliti 20. ágúst 2024.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

Skilgreiningar

Í þessari reglugerð er merking eftirfarandi hugtaka sem hér segir:

1) „stýrihópur“: teymi skipað starfsfólki aðilans á fjármálamarkaði sem verið er að prófa og, ef við á með hliðsjón af umfangi ógnamiðuðu innbrotsprófunarinnar, starfsfólki þriðja aðila sem veitir þjónustu og sérhvers annars aðila sem stjórnar prófuninni,

2) „hópstjóri stýrihóps“: sá starfsmaður aðilans á fjármálamarkaði sem ber ábyrgð á framkvæmd allrar starfsemi varðandi ógnamiðaða innbrotsprófun á aðilanum á fjármálamarkaði í tengslum við tiltekna prófun,

3) „blátt teymi“: starfsfólk aðilans á fjármálamarkaði og, ef við á, starfsfólk þriðja aðila sem veitir þjónustu og sérhvers annars aðila sem máli skiptir með hliðsjón af umfangi ógnamiðuðu innbrotsprófunarinnar, sem annast varnir vegna notkunar aðila á fjármálamarkaði á netkerfi og upplýsingakerfi með því að viðhalda öryggisstöðu gegn hermdum eða raunverulegum árásum og eru ekki upplýstir um ógnamiðuðu innbrotsprófunina,

4) „verkefni blás teymis“: verkefni sem blátt teymi annast að jafnaði s.s. öryggisstjórnstöðvar (SOC), innviðaþjónusta á sviði upplýsinga- og fjarskiptatækni, þjónusta á þjónustuborði, atvikastjórnun á rekstrarstigi,

5) „rautt teymi“: prófunaraðilar, innri eða ytri, sem samið hefur verið við um að framkvæma, eða hafa fengið úthlutað, ógnamiðaða innbrotsprófun,

6) „fjólublá teymisvinna“: samstarf við prófanir með þátttöku bæði prófunaraðila og bláa teymisins,

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

7) „yfirvald ógnamiðaðrar innbrotsprófunar“: eitthvað af eftirtöldu:

   a) eitt opinbert yfirvald í fjármálageiranum sem tilnefnt er í samræmi við 9. mgr. 26. gr. reglugerðar (ESB) nr. 2022/2554,

   b) yfirvaldið í fjármálageiranum sem hefur verið falið að annast sum eða öll verkefnin í tengslum við ógnamiðaða innbrotsprófun í samræmi við 10. mgr. 26. gr. reglugerðar (ESB) 2022/2554,

   c) öll lögbær yfirvöld sem um getur í 46. gr. reglugerðar (ESB) nr. 2022/2554,

8) „netöryggisteymi ógnamiðaðrar innbrotsprófunar“: starfsfólk yfirvalda ógnamiðaðrar innbrotsprófunar sem ber ábyrgð á málefnum í tengslum við ógnamiðaða innbrotsprófun,

9) „prófunarstjórar“: starfsfólk sem tilnefnt er til að leiða starfsemi yfirvalds ógnamiðaðrar innbrotsprófunar varðandi tiltekna ógnamiðaða innbrotsprófun til að fylgjast með hlítni við þessa reglugerð,

10) „veitandi ógnagreiningargagna“: sérfræðingarnir sem aðilinn á fjármálamarkaði semur við að því er varðar sérhverja ógnamiðaða innbrotsprófun og eru utan aðilans á fjármálamarkaði og þjónustuveitenda upplýsinga- og fjarskiptatækni innan samstæðu, ef um slíka er að ræða, sem safna og greina markviss ógnagreiningargögn sem skipta máli fyrir aðilann á fjármálamarkaði innan umfangs tiltekinnar ógnamiðaðrar innbrotsprófunar og þróa samsvarandi viðeigandi og raunsæjar sviðsmyndir ógna,

11) „veitendur ógnamiðaðrar innbrotsprófunar“: prófunaraðilar og veitendur ógnagreiningargagna,

12) „hjálparhönd“: aðstoð eða upplýsingar sem stýrihópurinn veitir prófunaraðilunum til að gera þeim kleift að halda áfram árásarleið sem þeir hefðu ekki getað haldið áfram með af sjálfsdáðum, og enginn annar kostur er í stöðunni, þ.m.t. vegna tímaskorts eða skorts á tilföngum fyrir tiltekna ógnamiðaða innbrotsprófun,

13) „árásarleið“: sú leið sem prófunaraðilar fara í virkum prófunarfasa rauðs teymis við ógnamiðaða innbrotsprófun til að ná þeim flöggum sem tilgreind eru að því er varðar þá ógnamiðuðu innbrotsprófun,

14) „flögg“: lykilmarkmiðin í upplýsinga- og fjarskiptatæknikerfunum sem styðja við nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði sem prófunaraðilar reyna að ná við prófunina,

15) „viðkvæmar upplýsingar“: upplýsingar sem auðvelt er að nýta til að framkvæma árásir á upplýsinga- og fjarskiptatæknikerfi aðilans á fjármálamarkaði, hugverk, viðskiptagögn sem viðskiptaleynd hvílir á eða persónuupplýsingar, sem geta skaðað, beint eða óbeint, aðilann á fjármálamarkaði og vistkerfi hans ef þau myndu falla í hendur aðila með illan ásetning,

16) „hópur“: allir þeir aðilar á fjármálamarkaði sem taka þátt í samsettri ógnamiðaðri innbrotsprófun skv. 4. mgr. 26. gr. reglugerðar (ESB) 2022/2554,

17) „gistiaðildarríki“: gistiaðildarríkið í samræmi við sérlög Sambandsins sem gilda um sérhvern aðila á fjármálamarkaði,

18) „sameiginleg ógnamiðuð innbrotsprófun“: ógnamiðuð innbrotsprófun, önnur en samsett ógnamiðuð innbrotsprófun eins og um getur í 4. mgr. 26. gr. reglugerðar (ESB) 2022/2554, með þátttöku fleiri aðila á fjármálamarkaði sem nota sama þjónustuveitanda innan samstæðu sem veitir upplýsinga- og fjarskiptatækniþjónustu eða tilheyra sömu samstæðu og deila upplýsinga- og fjarskiptatæknikerfum.

2. gr.

Tilgreining á aðilum á fjármálamarkaði sem skylt er að framkvæma ógnamiðaða innbrotsprófun

1. Yfirvöld ógnamiðaðrar innbrotsprófunar skulu meta hvort gera skuli kröfu um framkvæmd ógnamiðaðrar innbrotsprófunar að teknu tilliti til áhrifa þessara aðila á fjármálamarkaði, kerfislægra eiginleika þeirra og áhættusniðs upplýsinga- og fjarskiptatækni, á grundvelli allra eftirfarandi viðmiðana:

a) áhrifatengdra þátta og þátta sem tengjast kerfislægum eiginleikum:

   i. stærð aðilans á fjármálamarkaði, sem ákvörðuð er á grundvelli þess hvort aðilinn á fjármálamarkaði veitir fjármálaþjónustu í einu eða fleiri aðildarríkjum og með því að bera starfsemi aðilans á fjármálamarkaði saman við starfsemi annarra aðila á fjármálamarkaði sem veita sambærilega þjónustu,

   ii. umfang og eðli samtengingar aðilans á fjármálamarkaði við aðra aðila á fjármálamarkaði innan fjármálageirans í einu eða fleiri aðildarríkjum,

iii. nauðsyn og mikilvægi þjónustunnar sem aðilinn á fjármálamarkaði veitir fyrir fjármálageirann,

iv. útskiptanleiki þjónustunnar sem aðilinn á fjármálamarkaði veitir,

v. flækjustig viðskiptalíkans aðilans á fjármálamarkaði og tengdrar þjónustu og ferla,

vi. hvort aðilinn á fjármálamarkaði sé hluti af samstæðu með kerfislæga eiginleika á vettvangi Sambandsins eða á landsvísu innan fjármálageirans og deilir upplýsinga- og fjarskiptatæknikerfum,

b) þátta sem tengjast upplýsinga- og fjarskiptatækniáhættu:

i. áhættusnið aðilans á fjármálamarkaði,

ii. landslag netógna aðilans á fjármálamarkaði,

iii. hversu háð upplýsinga- og fjarskiptatæknikerfum og -ferlum nauðsynleg eða mikilvæg starfsemi aðila á fjármálamarkaði, eða stoðstarfsemi hennar, er,

iv. hversu flókin högun upplýsinga- og fjarskiptatækni aðilans á fjármálamarkaði er,

v. upplýsinga- og fjarskiptatækniþjónustu og starfsemi sem studd er af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og magns og tegundar samninga við þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu eða þjónustuveitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu,

vi. niðurstöður allra eftirlitsathugana sem skipta máli fyrir mat á þroska upplýsinga- og fjarskiptatækni aðilans á fjármálamarkaði,

vii. þroski áætlunar um rekstrarsamfellu upplýsinga- og fjarskiptatækni og viðbragðs- og endurreisnaráætlana í upplýsinga- og fjarskiptatækni,

viii. þroski starfhæfra öryggisráðstafana upplýsinga- og fjarskiptatækni til greiningar og mótvægisráðstafana, þ.m.t. getan til að:

1) vakta með viðvarandi hætti innviði upplýsinga- og fjarskiptatækni aðila á fjármálamarkaði,

2) bera kennsl á upplýsinga- og fjarskiptatæknitengda atburði í rauntíma,

3) greina atburðina sem um getur í 2. lið,

4) bregðast tímanlega og á skilvirkan hátt við atburðunum sem um getur í 2. lið,

ix. hvort aðilinn á fjármálamarkaði sé hluti af samstæðu sem er virk innan fjármálageirans á vettvangi Sambandsins eða á landsvísu sem deilir upplýsinga- og fjarskiptatæknikerfum.

Að því er varðar i. lið a-liðar skal yfirvald ógnamiðaðrar innbrotsprófunar, þegar það er mögulegt, taka til athugunar:

a) markaðshlutdeild aðilans á fjármálamarkaði á vettvangi Sambandsins og á landsvísu,

b) umfang starfsemi sem aðilinn á fjármálamarkaði býður upp á,

c) markaðshlutdeild þjónustunnar sem aðilinn á fjármálamarkaði veitir eða starfseminnar sem stunduð er í Sambandinu eða á landsvísu.

Að því er varðar v. lið a-liðar skal yfirvald ógnamiðaðrar innbrotsprófunar, þegar það er mögulegt, taka til athugunar:

a) hvort aðilinn á fjármálamarkaði starfræki fleiri en eitt viðskiptalíkan,

b) samtengingu mismunandi viðskiptaferla og tengdrar þjónustu.

2. Yfirvöld ógnamiðaðrar innbrotsprófunar skulu krefjast þess að allir eftirfarandi aðilar á fjármálamarkaði framkvæmi ógnamiðaða innbrotsprófun, nema matið sem um getur í 1. mgr. að því er varðar aðila á fjármálamarkaði gefi til kynna að áhrif hans, áhyggjuefni varðandi fjármálastöðugleika í tengslum við þann aðila á fjármálamarkaði eða áhættusnið upplýsinga- og fjarskiptatækni réttlæti ekki framkvæmd ógnamiðaðrar innbrotsprófunar:

a) lánastofnanir sem uppfylla eitthvað af eftirfarandi skilyrðum:

i. þær hafi verið tilgreindar sem kerfislega mikilvægar stofnanir á alþjóðavísu (G-SII) í samræmi við 131. gr. tilskipunar Evrópuþingsins og ráðsins 2013/36/ESB (7),

ii. þær hafi verið tilgreindar sem aðrar kerfislega mikilvægar stofnanir (O-SII) í samræmi við 131. gr. tilskipunar 2013/36/ESB,

iii. þær eru hluti af kerfislega mikilvægri stofnun á alþjóðavísu eða annarri kerfislega mikilvægri stofnun,

(7) 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, ELI: http://data.europa.eu/eli/dir/2013/36/oj).

b) greiðslustofnanir sem á báðum næstliðnum tveimur almanaksárum fyrir mat yfirvalds ógnamiðaðrar innbrotsprófunar framkvæmdu greiðslur, eins og þær eru skilgreindar í 5. lið 4. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2015/2366 ([8]), sem voru samtals að andvirði meira en 150 milljarðar evra,

c) rafeyrisfyrirtæki sem á báðum næstliðnum tveimur almanaksárum fyrir mat yfirvalds ógnamiðaðrar innbrotsprófunar framkvæmdu greiðslur, eins og þær eru skilgreindar í 5. lið 4. gr. tilskipunar Evrópuþingsins og ráðsins (ESB) 2015/2366, sem voru samtals að andvirði meira en 150 milljarðar evra eða áttu útistandandi rafeyri að andvirði meira en 40 milljarða evra,

d) verðbréfamiðstöðvar,

e) miðlægir mótaðilar,

f) viðskiptavettvangar með rafrænt viðskiptakerfi sem uppfyllir einhverja af eftirfarandi viðmiðunum:

i. viðskiptavettvangurinn hefur mesta markaðshlutdeild með tilliti til veltu á landsvísu á hvoru tveggja næstliðnu almanaksáranna fyrir mat yfirvalds ógnamiðaðrar innbrotsprófunar að því er varðar eitthvað af eftirfarandi:

1) framseljanleg verðbréf eins og þau eru skilgreind er í a-lið 44. liðar 1. mgr. 4. gr. tilskipunar Evrópuþingsins og ráðsins 2014/65/ESB ([9]),

2) framseljanleg verðbréf eins og þau eru skilgreind í b-lið 44. liðar 1. mgr. 4. gr. tilskipunar 2014/65/ESB,

3) afleiður eins og þær eru skilgreindar í 29. lið 1. mgr. 2. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 600/2014 ([10]),

4) samsettar fjármálaafurðir eins og þær eru skilgreindar í 28. lið 1. mgr. 2. gr. reglugerðar (ESB) nr. 600/2014,

5) losunarheimildir eins og um getur í 11. lið C-þáttar I. viðauka við tilskipun 2014/65/ESB,

ii. viðskiptavettvangurinn hefur markaðshlutdeild sem er umfram 5% með tilliti til veltu á vettvangi Sambandsins á hvoru tveggja næstliðnu almanaksáranna fyrir mat yfirvalds ógnamiðaðrar innbrotsprófunar að því er varðar eitthvað af eftirfarandi:

1) hlutabréf í fyrirtækjum og önnur verðbréf sem eru ígildi hlutabréfa í fyrirtækjum, sameignarfélögum eða öðrum einingum og heimildarskírteini vegna hlutabréfa,

2) skuldabréf eða önnur tryggð skuldaskjöl, þ.m.t. heimildarskírteini vegna slíkra verðbréfa,

3) afleiður eins og skilgreint er í 29. lið 1. mgr. 2. gr. reglugerðar (ESB) nr. 600/2014,

4) samsettar fjármálaafurðir eins og þær eru skilgreindar í 28. lið 1. mgr. 2. gr. reglugerðar (ESB) nr. 600/2014,

5) losunarheimildir eins og um getur í 11. lið C-þáttar I. viðauka við tilskipun 2014/65/ESB,

([8]) 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, 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, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

([9]) 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, ELI: http://data.europa.eu/eli/dir/2014/65/oj).

([10]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 600/2014 frá 15. maí 2014 um markaði fyrir fjármálagerninga og um breytingu á reglugerð (ESB) nr. 648/2012 (Stjtíð. ESB L 173, 12.6.2014, bls. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

g) vátrygginga- og endurtryggingafélög sem uppfylla allar eftirfarandi viðmiðanir:

i. verg bókfærð iðgjöld þeirra eru umfram 1 500 000 000 evrur,

ii. vátryggingaskuld þeirra er umfram 10 000 000 000 evrur,

iii. vátryggingafélög sem stunda aðeins líftryggingastarfsemi eða stunda hvort tveggja líftryggingastarfsemi og skaðatryggingastarfsemi með heildareignir sem eru meiri en 3,5% af samtölu heildareigna, sem metnar eru í samræmi við 75. gr. tilskipunar Evrópuþingsins og ráðsins 2009/138/EB ([11]), vátrygginga- og endurtryggingafélaga með staðfestu í aðildarríkinu.

Að því er varðar ii. lið f-liðar, ef viðskiptavettvangurinn er hluti af samstæðu sem deilir upplýsinga- og fjarskiptatæknikerfum eða sama þjónustuveitanda upplýsinga- og fjarskiptatækni innan samstæðu, skal taka tillit til veltu verðbréfa og afleiðusamninga á öllum viðskiptavettvöngum sem tilheyra sömu samstæðu og eru með staðfestu í Sambandinu.

Að því er varðar g-lið skulu yfirvöld ógnamiðaðrar innbrotsprófunar tilgreina hlutmengi allra vátrygginga- og endurtryggingafélaga með því að beita viðmiðununum sem mælt er fyrir um í i., ii. og iii. lið g-liðar. Vátrygginga- og endurtryggingafélög í viðkomandi hlutmengi skulu framkvæma ógnamiðaða innbrotsprófun ef þau uppfylla einnig einhverja af eftirfarandi viðmiðunum:

a) verg bókfærð iðgjöld þeirra eru umfram 3 000 000 000 evrur,

b) vátryggingaskuld þeirra er umfram 30 000 000 000 evrur,

c) heildareignir sem eru meiri en 10% af samtölu heildareigna vátrygginga- og endurtryggingafélaga með staðfestu í aðildarríkinu, sem metnar eru í samræmi við 75. gr. tilskipunar 2009/138/EB.

3. Ef fleiri en einn aðili á fjármálamarkaði sem tilheyrir sömu samstæðu og deilir upplýsinga- og fjarskiptatæknikerfum, eða ef fleiri en einn aðili á fjármálamarkaði notar sama þjónustuveitanda upplýsinga- og fjarskiptatækni innan samstæðu, uppfyllir viðmiðanirnar sem settar eru fram í 2. mgr. skulu yfirvöld ógnamiðaðra innbrotsprófana að því er varðar þá aðila á fjármálamarkaði ákvarða, í samræmi við 2. mgr. 16. gr., hvort krafan um að framkvæma ógnamiðaða innbrotsprófun á einingargrunni eigi við um þá aðila á fjármálamarkaði.

Ef yfirvald móðurfélags í samstæðu aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar, sem um getur í fyrstu undirgrein, er annað en yfirvald aðilanna á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar skulu yfirvöld aðila á fjármálamarkaði, sem tilheyrir samstæðunni, á sviði ógnamiðaðrar innbrotsprófunar hafa samráð við það yfirvald um það hvort það þyki viðeigandi að framkvæma ógnamiðaða innbrotsprófun á einingargrunni.

3. gr.

Netöryggisteymi og prófunarstjórar ógnamiðaðrar innbrotsprófunar

1. Yfirvald ógnamiðaðrar innbrotsprófunar skal fela netöryggisteymi ógnamiðaðrar innbrotsprófunar ábyrgð á að samræma starfsemi sem tengist ógnamiðaðri innbrotsprófun. Netöryggisteymi ógnamiðaðrar innbrotsprófunar skal skipað prófunarstjórum sem er falið að hafa umsjón með sérhverri ógnamiðaðri innbrotsprófun.

2. Yfirvald ógnamiðaðrar innbrotsprófunar skal tilnefna prófunarstjóra og a.m.k. einn varamann fyrir hverja prófun.

3. Prófunarstjórarnir skulu fylgjast með því hvort, og tryggja að, farið sé að kröfunum sem mælt er fyrir um í þessari reglugerð.

([11]) 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, ELI: http://data.europa.eu/eli/dir/2009/138/oj).

4. Prófunarstjórarnir skulu senda aðilanum á fjármálamarkaði samskiptaupplýsingar netöryggisteymis ógnamiðaðrar innbrotsprófunar með tilkynningunni sem um getur í 1. mgr. 9. gr.

5. Yfirvald ógnamiðaðrar innbrotsprófunar skal taka þátt í öllum áföngum ógnamiðaðrar innbrotsprófunar.

4. gr.

Skipulagsráðstafanir fyrir aðila á fjármálamarkaði

1. Aðilar á fjármálamarkaði skulu tilnefna hópstjóra stýrihóps sem skal bera ábyrgð á daglegu utanumhaldi ógnamiðaðrar innbrotsprófunar og ákvörðunum og aðgerðum stýrihópsins.

2. Aðilar á fjármálamarkaði skulu koma á skipulagsráðstöfunum og ráðstöfunum er varða verklag til að tryggja að:

a) aðgengi að upplýsingum um fyrirhugaða eða yfirstandandi ógnamiðaða innbrotsprófun sé takmarkað, á grundvelli meginreglunnar um þörf á vitneskju, við stýrihópinn, stjórnina og/eða framkvæmdastjórnina, prófunaraðilana, veitanda ógnagreiningargagna og yfirvald ógnamiðuðu innbrotsprófunarinnar,

b) stýrihópurinn hafi samráð við prófunarstjórana áður en einhver aðili bláa teymisins fær að koma að ógnamiðaðri innbrotsprófun,

c) stýrihópurinn sé upplýstur um það ef starfsfólk aðilans á fjármálamarkaði eða þriðju aðilar sem veita þjónustu verða varir við ógnamiðaða innbrotsprófun; ef viðbrögð við atviki þróast á verri veg sér stýrihópurinn um að halda aftur af þeirri þróun eftir þörfum,

d) ráðstafanir í tengslum við leynd ógnamiðaðrar innbrotsprófunar, sem gildir um starfsfólk aðilans á fjármálamarkaði, hlutaðeigandi starfsfólk þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu, prófunaraðila og veitanda ógnagreiningargagna séu til staðar,

e) stýrihópurinn veiti prófunarstjórum allar upplýsingar um ógnamiðuðu innbrotsprófunina óski þeir þess,

f) aðilar sem eiga í hlut í ógnamiðuðu innbrotsprófuninni vísa eingöngu til hennar með dulnefni, ef það er mögulegt.

5. gr.

Áhættustýring fyrir ógnamiðaða innbrotsprófun

1. Í undirbúningsfasanum sem um getur í 9. gr. skal stýrihópurinn meta áhættuna sem fylgir prófun í rauntíma á framleiðslukerfum nauðsynlegrar eða mikilvægrar starfsemi aðilans á fjármálamarkaði, þar á meðal hugsanleg áhrif á:

a) fjármálageirann,

b) fjármálastöðugleika á vettvangi Sambandsins eða á landsvísu.

Stýrihópurinn skal rýna þessi áhrif á meðan á prófuninni stendur.

2. Að því er varðar áhættumatið og áhættustýringu skal stýrihópurinn taka tillit til a.m.k. þeirrar tegundar áhættu sem leiðir af:

a) veitingu aðgangs til veitanda ógnagreiningargagna og ytri prófunaraðila, eftir atvikum, að viðkvæmum upplýsingum um aðilann á fjármálamarkaði,

b) að ógnamiðuð innbrotsprófun sé ekki í samræmi við reglugerð (ESB) 2022/2554 og þessa reglugerð ef slíkur skortur á reglufylgni hefur í för með sér skort á staðfestingu sem um getur í 7. mgr. 26. gr. reglugerðar (ESB) 2022/2554, þ.m.t. ef slíkur skortur á reglufylgni er vegna brota á trúnaðarkvöð um ógnamiðaða innbrotsprófun eða vegna skorts á siðferðislegri háttsemi,

c) stigmögnun krísuástands og atvika,

d) virkum fasa rauða teymisins, þ.m.t. áhættu í tengslum við truflun á nauðsynlegri starfsemi og spillingu gagna vegna starfsemi prófunaraðilanna, og möguleg áhrif á þriðju aðila,

e) starfsemi blás teymis, þ.m.t. áhættu í tengslum við truflun á nauðsynlegri starfsemi og spillingu gagna vegna starfsemi bláa teymisins, og möguleg áhrif hennar á þriðju aðila,

f) ófullnægjandi enduruppbyggingu kerfa sem ógnamiðuð innbrotsprófun hefur áhrif á.

6. gr.

Áhættustýring fyrir samsettar eða sameiginlegar ógnamiðaðar innbrotsprófanir

1. Ef um er að ræða sameiginlega ógnamiðaða innbrotsprófun eða samsetta ógnamiðaða innbrotsprófun skal stýrihópur sérhvers aðila á fjármálamarkaði framkvæma eigið áhættumat og koma á eigin áhættustýringarráðstöfunum.

2. Stýrihópur tilnefnda aðilans á fjármálamarkaði sem um getur í b-lið 3. mgr. 16. gr. þessarar reglugerðar eða aðilinn á fjármálamarkaði sem tilnefndur er í samræmi við 4. mgr. 26. gr. reglugerðar (ESB) 2022/2554 skal meta áhættuna í tengslum við þátttöku margra aðila á fjármálamarkaði í ógnamiðuðu innbrotsprófuninni. Stýrihópar þeirra aðila á fjármálamarkaði sem taka þátt skulu hafa samstarf við stýrihóp tilnefnda aðilans á fjármálamarkaði til að greina mögulega sameiginlega áhættu.

7. gr.

Val á veitendum ógnamiðaðrar innbrotsprófunar

1. Stýrihópurinn skal gera ráðstafanir til að stýra áhættu í tengslum við ógnamiðuðu innbrotsprófunina og einkum tryggja, að því er varðar sérhverja ógnamiðaða innbrotsprófun, að:

a) veitandi ógnagreiningargagna og ytri prófunaraðilar afhendi stýrihópnum ítarlega ferilskrá og afrit af vottorðum sem, samkvæmt viðurkenndum markaðsstöðlum, eru viðeigandi fyrir framkvæmd vinnu þeirra,

b) veitandi ógnagreiningargagna og ytri prófunaraðilar falli að öllu leyti og réttilega undir viðeigandi starfsábyrgðartryggingu, þ.m.t. vegna áhættu vegna misferlis og gáleysis,

c) veitandi ógnagreiningargagna leggi a.m.k. fram þrjár umsagnir frá fyrri verkefnum í tengslum við innbrotsprófanir og prófanir rauðs teymis,

d) ytri prófunaraðilar leggi a.m.k. fram fimm umsagnir frá fyrri verkefnum í tengslum við innbrotsprófanir og prófanir rauðs teymis,

e) starfsfólk veitanda ógnagreiningargagna sem er falið að gera ógnamiðaða innbrotsprófun:

   i. samanstandi af a.m.k. stjórnanda með að lágmarki fimm ára reynslu af ógnagreiningum og a.m.k. einum aðila til viðbótar með að lágmarki tveggja ára reynslu af ógnagreiningum,

   ii. búi yfir víðtækri og viðeigandi stigi fagþekkingar og færni, þ.m.t.:

      1) úrræðum, aðferðum og verklagi til söfnunar greiningargagna,

      2) landfræðipólitískri þekkingu, tækniþekkingu og þekkingu á geiranum,

      3) fullnægjandi samskiptahæfni til að geta með skýrum hætti sett fram og gefið skýrslu um niðurstöður verkefnisins,

   iii. hafi samtals tekið þátt í a.m.k. þremur fyrri verkefnum á sviði ógnagreininga í tengslum við innbrotsprófanir og prófanir rauðs teymis,

   iv. inni ekki á sama tíma af hendi verkefni blás teymis eða aðra þjónustu sem gæti haft í för með sér hagsmunaárekstra að því er tekur til aðilans á fjármálamarkaði, þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu sem tekur þátt í ógnamiðaðri innbrotsprófun sem þeim er falin,

   v. sé aðskilið frá og heyri ekki undir starfsfólk sama veitanda ógnamiðaðrar innbrotsprófunar og útvegar ytri prófunaraðila fyrir sömu ógnamiðuðu innbrotsprófun,

f) að því er varðar ytri prófunaraðila, skal rautt teymi sem er falið að gera ógnamiðaða innbrotsprófun:

i. skipað a.m.k. einum stjórnanda, sem hefur að lágmarki fimm ára reynslu á sviði innbrotsprófunar og prófana rauðs teymis, og a.m.k. tveimur viðbótarprófurum, sem hver hefur reynslu á sviði innbrotsprófana og prófana rauðs teymis sem spannar minnst tvö ár,

ii. búa yfir víðtækri og viðeigandi fagþekkingu og færni, þar á meðal þekkingu á starfsemi aðilans á fjármálamarkaði, könnun, áhættustýringu, þróun árásarleiða, raunlægum innbrotum, bragðvísi, veikleikagreiningu, auk fullnægjandi samskiptahæfni til að kynna og skýra frá niðurstöðum verkefnisins á skilmerkilegan hátt,

iii. hafi samtals tekið þátt í a.m.k. fimm fyrri verkefnum í tengslum við innbrotsprófanir og prófanir rauðs teymis,

iv. hvorki vera starfandi hjá, né veita þjónustu til, veitanda ógnagreiningargagna sem á sama tíma innir af hendi verkefni blás teymis fyrir annað hvort aðila á fjármálamarkaði, þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða þjónustuveitanda upplýsinga- og fjarskiptatækni innan samstæðu sem tekur þátt í ógnamiðuðu innbrotsprófuninni,

v. vera aðskilið frá öðru starfsfólki sama veitanda ógnamiðaðrar innbrotsprófunar sem á sama tíma veitir þjónustu á sviði ógnagreiningargagna fyrir sömu ógnamiðuðu innbrotsprófun,

g) prófunaraðilarnir og veitandi ógnagreiningargagna geri endurheimtarráðstafanir í lok prófunar, þ.m.t. framkvæmi örugga eyðingu upplýsinga er varða lykilorð, skírteini og aðra leynilega lykla sem voru vásettir við ógnamiðuðu innbrotsprófunina, tilkynni aðilum á fjármálamarkaði með öruggum hætti um vásetta reikninga, tryggi örugga söfnun, geymslu, stýringu og eyðingu annarra gagna sem safnað er við prófunina,

h) prófunaraðilar geri eftirfarandi endurheimtarráðstafanir, til viðbótar við þær ráðstafanir við lok prófunar sem um getur í g-lið:

i. afvirkjun skipana og stýringa,

ii. neyðarrofar sem byggjast á umfangi og dagsetningum,

iii. fjarlæging bakdyra og annarra spilliforrita,

iv. tilkynning um möguleg brot,

v. ferlar fyrir endurheimt afrita í framtíðinni sem kunna að varða spilliforrit eða verkfæri sem sett voru upp í prófuninni,

vi. vöktun á starfsemi bláa teymisins og upplýsingagjöf til stýrihópsins um að prófunaratvik hafi mögulega uppgötvast,

i) prófunaraðilar og veitandi ógnagreiningargagna stundi hvorki né taki þátt í neinni af eftirfarandi starfsemi:

i. óheimilli eyðileggingu búnaðar aðilans á fjármálamarkaði og þriðja aðila sem veitir honum upplýsinga- og fjarskiptatækniþjónustu, ef um það er að ræða,

ii. óstýrðri breytingu á upplýsingum og upplýsinga- og fjarskiptatæknieignum aðilans á fjármálamarkaði og þriðja aðila sem veitir honum upplýsinga- og fjarskiptatækniþjónustu, ef um það er að ræða,

iii. að tefla vísvitandi í tvísýnu samfellu nauðsynlegrar eða mikilvægrar starfsemi aðila á fjármálamarkaði,

iv. óheimilli inntöku kerfa sem eru utan umfangs,

v. óheimilli birtingu niðurstaðna úr prófunum.

2. Stýrihópurinn skal halda skrá yfir gögnin sem prófunaraðilarnir og veitendur ógnagreiningargagna leggja fram til að sýna fram á að farið sé að a- til f-lið 1. mgr.

Í undantekningartilvikum geta aðilar á fjármálamarkaði gert samninga við ytri prófunaraðila og veitendur ógnagreiningargagna sem uppfylla ekki eina eða fleiri af kröfunum sem settar eru fram í a- til f-lið 1. mgr., að því tilskildu að þessir aðilar á fjármálamarkaði grípi til viðeigandi ráðstafana til að draga úr áhættunni sem tengist því að þessum liðum sé ekki fylgt og skrái þær ráðstafanir.

8. gr.

Sértæki fyrir samsettar eða sameiginlegar ógnamiðaðar innbrotsprófanir

1. Ef margir aðilar á fjármálamarkaði, sem tilgreindir eru í samræmi við 2. eða 4. mgr. 16. gr., taka þátt í samsettri eða sameiginlegri ógnamiðaðri innbrotsprófun skal sérhver aðili á fjármálamarkaði fylgja öllum þeim skrefum sem sett eru fram í 9.–15. gr. nema leiðandi yfirvald ógnamiðaðrar innbrotsprófunar ákveði annað.

2. Nema kveðið sé á um annað í þessari reglugerð skal, þegar mörg yfirvöld ógnamiðaðrar innbrotsprófunar taka þátt í samsettri eða sameiginlegri ógnamiðaðri innbrotsprófun, eins og um getur í 3. mgr. 16. gr. eða 5. mgr. 16. gr., líta á tilvísanir í 9.–15. gr. í „yfirvald ógnamiðaðrar innbrotsprófunar“ sem vísanir í leiðandi yfirvald ógnamiðaðrar innbrotsprófunar að því er varðar slíka samsetta eða sameiginlega ógnamiðaða innbrotsprófun.

9. gr.

Undirbúningsfasi

1. Aðili á fjármálamarkaði sem tilgreindur er skv. þriðju undirgrein 8. mgr. 26. gr. reglugerðar (ESB) 2022/2554 skal hefja ógnamiðaða innbrotsprófun eftir tilkynningu frá yfirvaldi ógnamiðaðrar innbrotsprófunar þess efnis að framkvæma skuli ógnamiðaða innbrotsprófun.

2. Aðili á fjármálamarkaði skal, innan þriggja mánaða frá viðtöku tilkynningarinnar sem um getur í 1. mgr., leggja fram til prófunarstjóranna allar eftirfarandi upphafsupplýsingar um ógnamiðaða innbrotsprófun:

a) verkefnalýsingu, þ.m.t. samantekna verkefnisáætlun sem inniheldur upplýsingarnar sem settar eru fram í I. viðauka,

b) samskiptaupplýsingar hópstjóra stýrihópsins,

c) upplýsingar um fyrirhugaða notkun innri eða ytri prófunaraðila eða hvort tveggja, ef við á eins og fram kemur í 15. gr.,

d) upplýsingar um boðleiðir sem skal nota á meðan ógnamiðaða innbrotsprófunin fer fram,

e) dulnefni ógnamiðuðu innbrotsprófunarinnar.

3. Ef upplýsingarnar sem um getur í a- til e-lið 2. mgr. eru fullnægjandi og tryggja hentuga og skilvirka framkvæmd ógnamiðuðu innbrotsprófunarinnar skal yfirvald ógnamiðuðu innbrotsprófunarinnar staðfesta upphafsupplýsingar aðilans á fjármálamarkaði um ógnamiðuðu innbrotsprófunina og tilkynna aðilanum á fjármálamarkaði um það.

4. Í kjölfar fullgildingar yfirvalds ógnamiðuðu innbrotsprófunarinnar á upphafsupplýsingunum um ógnamiðuðu innbrotsprófunina skal aðilinn á fjármálamarkaði koma á stýrihópi sem styður hópstjóra stýrihópsins í verkefnum hans við að:

a) tilgreina boðleiðir og -ferla innan stýrihópsins, við prófunaraðilana og veitendur ógnagreiningargagna varðandi öll málefni í tengslum við ógnamiðaða innbrotsprófun,

b) upplýsa stjórn og/eða framkvæmdastjórn aðilans á fjármálamarkaði um framgang ógnamiðuðu innbrotsprófunarinnar og áhættu í tengslum við hana,

c) taka ákvarðanir á grundvelli sérþekkingar á efninu gegnum alla ógnamiðuðu innbrotsprófunina,

d) framkvæma ógnamiðuðu innbrotsprófunina í samræmi við þessa reglugerð,

e) velja veitanda ógnagreiningargagna fyrir ógnamiðuðu innbrotsprófunina,

f) velja ytri prófunaraðila, innri prófunaraðila eða hvort tveggja,

g) semja umfangsskilgreiningarskjal.

5. Ef yfirvald ógnamiðuðu innbrotsprófunarinnar telur að upphafleg skipan stýrihópsins og síðari breytingar á honum séu fullnægjandi til að inna af hendi verkefnin sem um getur í 4. mgr. skal yfirvald ógnamiðuðu innbrotsprófunarinnar staðfesta stýrihópinn og upplýsa hópstjóra hópsins um það.

6. Aðilinn á fjármálamarkaði skal leggja fram umfangsskilgreiningarskjal sem inniheldur allar upplýsingarnar sem um getur í II. viðauka til prófunarstjóra innan sex mánaða frá viðtöku tilkynningarinnar frá yfirvaldi ógnamiðuðu innbrotsprófunarinnar sem um getur í 1. mgr. Stjórn og/eða framkvæmdastjórn aðilans á fjármálamarkaði skal samþykkja umfangskilgreiningarskjalið.

7. Aðilar á fjármálamarkaði skulu hafa eftirfarandi viðmiðanir til hliðsjónar við ákvörðun á hvort nauðsynleg eða mikilvæg starfsemi skuli vera innan umfangs ógnamiðaðrar innbrotsprófunar:

a) nauðsyn eða mikilvægi starfseminnar og möguleg áhrif á fjármálageirann og fjármálastöðugleika á vettvangi Sambandsins og á landsvísu,

b) mikilvægi starfseminnar fyrir daglegan rekstur aðilans á fjármálamarkaði,

c) útskiptanleika starfseminnar,

d) samtengingu við aðra starfsemi,

e) landfræðilega staðsetningu starfseminnar,

f) geiratengt hæði annarra eininga við starfsemina,

g) ef þau eru tiltæk, ógnagreiningargögn um starfsemina.

8. Stýrihópurinn skal deila upphafsupplýsingunum um ógnamiðuðu innbrotsprófunina og umfangsskilgreiningarskjalinu með prófunaraðilunum og veitendum ógnagreiningargagna þegar gerður hefur verið samningur við þá. Stýrihópurinn skal upplýsa prófunaraðilana og veitendur ógnagreiningargagna um prófunarferlið sem ber að fylgja.

9. Aðilinn á fjármálamarkaði skal tryggja að útvegun eða tilnefning prófunaraðila og veitenda ógnagreiningargagna sé lokið fyrir upphaf prófunarfasans.

10. Áður en prófunarfasinn hefst skal stýrihópurinn hafa samráð við prófunarstjórana um áhættumat á ógnamiðuðu innbrotsprófuninni og um ráðstafanir varðandi áhættustýringu. Stýrihópurinn skal rýna áhættumatið eða ráðstafanirnar varðandi áhættustýringu ef yfirvald ógnamiðuðu innbrotsprófunarinnar telur að aðgerðirnar taki ekki á áhættunni sem felst í ógnamiðuðu innbrotsprófuninni með fullnægjandi hætti.

11. Stýrihópurinn skal meta reglufylgni veitenda ógnagreiningargagna og prófunaraðila sem hann íhugar að taki þátt í ógnamiðuðu innbrotsprófuninni við kröfurnar sem mælt er fyrir um í 27. gr. reglugerðar (ESB) 2022/2554 og við 1. mgr. 7. gr. þessarar reglugerðar og skjalfesta niðurstöður þess mats. Stýrihópurinn skal velja veitendur ógnagreiningargagna í samræmi við það mat og við áhættustýringaraðferðir þeirra. Áður en samningur er gerður við þá veitendur ógnagreiningargagna og ytri prófunaraðila sem urðu fyrir valinu skal stýrihópurinn leggja fyrir prófunarstjórana sönnun á að þessir veitendur ógnagreiningargagna og ytri prófunaraðilar uppfylli kröfurnar sem mælt er fyrir um í 27. gr. reglugerðar (ESB) 2022/2554 og við 1. mgr. 7. gr. þessarar reglugerðar. Stýrihópurinn skal ekki halda áfram með samningagerð við valda veitendur ógnagreiningargagna og ytri prófunaraðila ef yfirvald ógnamiðuðu innbrotsprófunarinnar telur að valdir veitendur ógnagreiningargagna og ytri prófunaraðilar uppfylli ekki kröfurnar sem mælt er fyrir um í 27. gr. reglugerðar (ESB) 2022/2554 eða að kröfunum sem mælt er fyrir um í 1. mgr. 7. gr. þessarar reglugerðar eða viðbótarkröfur sem leiða af löggjöf um þjóðaröryggi í samræmi við lög Sambandsins eða ef aðili á fjármálamarkaði fer ekki að fyrstu undirgrein 2. mgr. 7. gr. þessarar reglugerðar eða ef aðstæðurnar sem um getur í annarri undirgrein 2. mgr. 7. gr. þessarar reglugerð eru ekki fyrir hendi.

12. Ef umfangsskilgreiningarskjalið er fullklárað og tryggir framkvæmd viðeigandi og skilvirkrar ógnamiðaðrar innbrotsprófunar skal yfirvald ógnamiðuðu innbrotsprófunarinnar samþykkja það og upplýsa hópstjóra stýrihópsins um það.

10. gr.

Prófunarfasi: ógnagreiningargögn

1. Eftir að yfirvald ógnamiðuðu innbrotsprófunarinnar hefur samþykkt umfangsskilgreiningarskjalið skal veitandi ógnagreiningargagna greina almenn og geiratengd ógnagreiningargögn sem skipta máli fyrir aðilann á fjármálamarkaði. Ef yfirvald ógnamiðaðrar innbrotsprófunar hefur lagt fram almennt landslag netógna fyrir fjármálageirann í aðildarríki getur veitandi ógnagreiningargagna notað það landslag sem grundvöll fyrir landsbundið landslag netógna. Veitandi ógnagreiningargagna skal greina netógnir og núverandi eða mögulega veikleika að því er varðar aðilann á fjármálamarkaði. Þar að auki skal veitandi ógnagreiningargagna safna upplýsingum um og greina áþreifanleg, framkvæmanleg og samhengisbundin gögn um árásarmark og ógnagreiningar varðandi aðilann á fjármálamarkaði, þ.m.t. með því að hafa samráð við stýrihópinn og prófunarstjórana.

2. Veitandi ógnagreiningargagna skal setja fram viðkomandi ógnir og markvissar ógnagreiningar og leggja viðeigandi sviðsmyndir til við stýrihópinn, prófunaraðilana og prófunarstjórana. Fyrirhugaðar sviðsmyndir skulu vera ólíkar með tilliti til auðkenndra ógnaraðila og tengdra úrræða, aðferða og verklags og skulu beinast að hverri nauðsynlegri eða mikilvægri starfsemi innan umfangs ógnamiðuðu innbrotsprófunarinnar.

3. Hópstjóri stýrihópsins skal velja a.m.k. þrjár sviðsmyndir fyrir framkvæmd ógnamiðuðu innbrotsprófunarinnar á grundvelli eftirfarandi þátta:

a) ráðlegginga veitanda ógnagreiningargagna og ógnamiðaðs eðlis hverrar sviðsmyndar,

b) álits prófunarstjóranna,

c) fýsileika fyrirhugaðra sviðsmynda, m.t.t. framkvæmdar, á grundvelli sérfræðiálits prófaranna,

d) stærðar, flækjustigs og heildaráhættusniðs aðilans á fjármálamarkaði og eðlis, umfangs og flækjustigs þjónustu, starfsemi og reksturs hans.

4. Af völdum sviðsmyndum má aðeins ein ekki vera ógnamiðuð og má hún byggjast á framsýnni og hugsanlega tilbúinni ógn með mikið forspár-, fyrirhyggju-, tækifæris- eða framtíðargildi í ljósi fyrirséðrar þróunar á ógnarlandslagi aðilans á fjármálamarkaði.

Þegar um er að ræða samsetta ógnamiðaða innbrotsprófun skal að minnsta kosti ein sviðsmynd ná til viðeigandi undirliggjandi upplýsingatæknikerfa, ferla og tækni þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og styður við nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði sem prófunin nær til, án þess að hafa áhrif á sviðsmyndir sem beinast beint að nauðsynlegri eða mikilvægri starfsemi þeirra aðila á fjármálamarkaði sem taka þátt í prófuninni.

Þegar um er að ræða sameiginlega ógnamiðaða innbrotsprófun, sem tekur einnig til veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu, skal að minnsta kosti ein sviðsmynd ná til viðeigandi undirliggjandi upplýsingatæknikerfa, ferla og tækni aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu innan samstæðu og styður við nauðsynlega eða mikilvæga starfsemi aðila á fjármálamarkaði sem prófunin nær til, án þess að hafa áhrif á sviðsmyndir sem beinast beint að nauðsynlegri eða mikilvægri starfsemi þeirra aðila á fjármálamarkaði sem taka þátt í prófuninni.

5. Veitandi ógnagreiningargagna skal afhenda stýrihópnum skýrsluna um markviss ógnagreiningargögn, þ.m.t. sviðsmyndirnar sem valdar eru í samræmi við 3. og 4. mgr. Skýrslan um ógnagreiningargögn skal innihalda þær upplýsingar sem settar eru fram í III. viðauka.

6. Stýrihópurinn skal leggja fram skýrsluna um markviss ógnagreiningargögn til prófunarstjórans til samþykktar. Þegar skýrslan um markviss ógnagreiningargögn er fullkláruð og tryggir framkvæmd skilvirkrar ógnamiðaðrar innbrotsprófunar skal yfirvald ógnamiðuðu innbrotsprófunarinnar samþykkja skýrsluna og upplýsa hópstjóra stýrihópsins um það.

11. gr.

Prófunarfasi: prófun rauðs teymis

1. Eftir að yfirvald ógnamiðuðu innbrotsprófunarinnar hefur samþykkt skýrsluna um markviss ógnagreiningargögn skulu prófunaraðilarnir gera prófunaráætlun rauða teymisins sem skal innihalda upplýsingarnar sem settar eru fram í IV. viðauka. Prófunaraðilarnir skulu nota umfangsskilgreiningarskjalið og skýrsluna um markviss ógnagreiningargögn sem grundvöll fyrir gerð árásarsviðsmynda.

2. Prófunaraðilarnir skulu hafa samráð við stýrihópinn, veitanda ógnagreiningargagnanna og prófunaraðilana um prófunaráætlun rauðs teymis, þ.m.t. fyrirkomulag samskipta-, starfshátta- og verkefnastjórnunar, undirbúning og notkunartilvik fyrir virkjun hjálparhandar, og samkomulag um skýrslugjöf til stýrihópsins og prófunarstjóranna.

3. Þegar prófunaráætlun rauðs teymis er fullkláruð og tryggir framkvæmd skilvirkrar ógnamiðaðrar innbrotsprófunar skal stýrihópurinn og yfirvald ógnamiðuðu innbrotsprófunarinnar samþykkja prófunaráætlun rauðs teymis og yfirvald ógnamiðuðu innbrotsprófunarinnar upplýsa hópstjóra stýrihópsins um það.

4. Þegar prófunaráætlun rauða teymisins hefur verið samþykkt í samræmi við 3. mgr. skulu prófunaraðilarnir framkvæma ógnamiðuðu innbrotsprófunina á meðan á prófunarfasa rauða teymisins stendur.

5. Tímalengd virks prófunarfasa rauðs teymis skal vera í réttu hlutfalli við umfang ógnamiðuðu innbrotsprófunarinnar, stærð, starfsemi, flækjustig og fjölda aðila á fjármálamarkaði og þriðju aðila sem veita upplýsinga- og fjarskiptatækniþjónustu eða veitendur upplýsinga- og fjarskiptatækniþjónustu innan samstæðu sem taka þátt í ógnamiðaðri innbrotsprófun og skal í öllu falli vara að lágmarki í 12 vikur. Árásarsviðsmyndir má framkvæma hverja á eftir annarri eða samtímis. Stýrihópurinn, veitandi ógnagreiningargagnanna, prófunaraðilarnir og prófunarstjórarnir skulu koma sér saman um lok virks prófunarfasa rauðs teymis.

6. Að því tilskildu að tryggt sé að prófunaráætlun rauða teymisins verði eftir sem áður fullgerð og geri kleift að framkvæma skilvirka ógnamiðaða innbrotsprófun skulu hópstjóri stýrihópsins og prófunarstjórar samþykkja breytingar á prófunaráætlun rauða teymisins eftir að hún hefur verið samþykkt, þar á meðal breytingar á tímalínu, umfangi, markkerfum eða flöggum.

7. Meðan á virkum prófunarfasa rauða teymisins stendur skulu prófunaraðilar veita skýrslugjöf um framvindu ógnamiðuðu innbrotsprófunarinnar til stýrihópsins og prófunarstjóranna a.m.k. vikulega og þá skal veitandi ógnagreiningargagna vera til taks fyrir samráð og frekari ógnagreiningu ef stýrihópurinn óskar eftir því.

8. Stýrihópurinn skal tímanlega veita hjálparhönd sem hönnuð er á grundvelli prófunaráætlunar rauða teymisins. Hjálparhönd má bæta við eða aðlaga að fengnu samþykki stýrihópsins og prófunarstjóranna.

9. Ef starfsmaður aðilans á fjármálamarkaði eða þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu eða veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu, eftir því sem við á, kemst á snoðir um prófunarstarfsemina skal stýrihópurinn, í samráði við prófunaraðilana og með fyrirvara um 10. mgr., leggja til og leggja fram ráðstafanir fyrir prófunarstjórana til staðfestingar sem gera það kleift að halda áfram með ógnamiðuðu innbrotsprófunina en tryggja jafnframt leynd hennar.

10. Við sérstakar aðstæður sem valda hættu á áhrifum á gögn, skemmdum á eignum og truflun á nauðsynlegri eða mikilvægri starfsemi, þjónustu eða rekstri aðilans á fjármálamarkaðinum sjálfum, þriðja aðila sem veitir honum upplýsinga- og fjarskiptatækniþjónustu eða veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu, eða truflunum á mótaðilum hennar eða fjármálageiranum, getur hópstjóri stýrihópsins stöðvað ógnamiðuðu innbrotsprófunina, eða, sem síðasta úrræði, þar sem ekki er unnt að halda ógnamiðuðu innbrotsprófuninni áfram með öðrum hætti og með fyrirvara um undangengið samþykki yfirvalds ógnamiðuðu innbrotsprófunarinnar, haldið ógnamiðuðu innbrotsprófuninni áfram með takmarkaðri fjólublárri teymisvinnu. Tímalengd takmarkaðrar fjólublárrar teymisvinnu skal teljast með í þeim 12 vikna lágmarkstíma sem virkur prófunarfasi rauða teymisins stendur yfir og vísað er til í 5. mgr.

12. gr.

Lokunarfasi

1. Þegar virkum prófunarfasa rauða teymisins er lokið skal hópstjóri stýrihópsins tilkynna bláa teyminu að ógnamiðuð innbrotsprófun hafi farið fram.

2. Innan fjögurra vikna frá lokum virks prófunarfasa rauðs teymis skulu prófunaraðilar leggja prófunarskýrslu rauða teymisins fyrir stýrihópinn sem inniheldur upplýsingarnar sem settar eru fram í V. viðauka.

3. Stýrihópurinn skal leggja fram prófunarskýrslu rauða teymisins til bláa teymisins og prófunarstjóra án ástæðulausrar tafar.

Að beiðni prófunarstjóra skal skýrslan sem um getur í fyrstu undirgrein ekki innihalda viðkvæmar upplýsingar.

4. Við viðtöku prófunarskýrslu rauða teymisins og innan tíu vikna frá lokum virks prófunarfasa rauðs teymis skal bláa teymið leggja fyrir stýrihópinn prófunarskýrslu bláa teymisins sem inniheldur upplýsingarnar sem settar eru fram í VI. viðauka. Stýrihópurinn skal leggja prófunarskýrslu bláa teymisins fyrir prófunaraðila og prófunarstjóra án ástæðulausrar tafar.

Að beiðni prófunarstjóra skal skýrslan sem um getur í fyrstu undirgrein ekki innihalda viðkvæmar upplýsingar.

5. Eigi síðar en tíu vikum eftir lok virks prófunarfasa rauða teymisins skal bláa teymið og prófunaraðilarnir endurtaka árásar- og varnaraðgerðir sem framkvæmdar voru við ógnamiðuðu innbrotsprófunina. Stýrihópurinn skal einnig stýra fjólublárri teymisvinnu í tengslum við efnisatriði sem bláa teymið og prófunaraðilarnir tilgreina í sameiningu, á grundvelli veikleika sem koma í ljós við prófunina og, ef við á, í tengslum við efnisatriði sem ekki var unnt að prófa í virkum prófunarfasa rauða teymisins.

6. Eftir að endurtekningunni og fjólubláu teymisvinnunni er lokið skulu stýrihópurinn, bláa teymið, prófunaraðilarnir og veitendur ógnagreiningargagna veita hver öðrum endurgjöf um ferli ógnamiðuðu innbrotsprófunarinnar. Prófunarstjórarnir mega veita endurgjöf.

7. Þegar yfirvald ógnamiðuðu innbrotsprófunarinnar hefur tilkynnt hópstjóra stýrihópsins að það hafi metið að prófunarskýrsla bláa teymisins og prófunarskýrsla rauða teymisins innihaldi upplýsingarnar sem settar eru fram í V. og VI. viðauka skal aðilinn á fjármálamarkaði, innan átta vikna, leggja fyrir yfirvald ógnamiðuðu innbrotsprófunarinnar skýrsluna með samantekt um viðeigandi niðurstöður ógnamiðuðu innbrotsprófunarinnar, eins og um getur í 6. mgr. 26. gr. reglugerðar (ESB) 2022/2554, sem inniheldur þá þætti sem settir eru fram í VII. viðauka, til samþykktar.

Að beiðni yfirvalds ógnamiðuðu innbrotsprófunarinnar skal skýrslan sem um getur í fyrstu undirgrein ekki innihalda viðkvæmar upplýsingar.

13. gr.

Úrbótaáætlun

1. Innan átta vikna frá tilkynningunni sem um getur í 7. mgr. 12. gr. þessarar reglugerðar skal aðilinn á fjármálamarkaði leggja fram úrbótaáætlanir og gögnin sem um getur í 6. mgr. 26. gr. reglugerðar (ESB) 2022/2554 fyrir yfirvald ógnamiðuðu innbrotsprófunarinnar og, ef um annað yfirvald er að ræða, fyrir lögbært yfirvald aðilans á fjármálamarkaði.

2. Úrbótaáætlunin sem um getur í 1. mgr. skal innihalda, fyrir hverja niðurstöðu innan ramma ógnamiðuðu innbrotsprófunarinnar:

a) lýsingu á þeim annmörkum sem komu í ljós,

b) lýsingu á fyrirhuguðum úrbótaráðstöfunum og forgangsröðun þeirra og vænt lok þeirra, þ.m.t., þar sem við á, ráðstafanir til að auka getu til að auðkenna, vernda, greina og bregðast við,

c) greiningu á frumorsök,

d) starfsfólk eða starfssvið aðilans á fjármálamarkaði sem ber ábyrgð á innleiðingu fyrirhugaðra ráðstafana eða úrbóta,

e) áhættuna sem fylgir því að grípa ekki til þeirra ráðstafana sem um getur í b-lið og, þar sem við á, áhættuna sem fylgir því að grípa til slíkra ráðstafana.

14. gr.

Staðfesting

1. Staðfestingin sem um getur í 7. mgr. 26. gr. reglugerðar (ESB) 2022/2554 skal innihalda upplýsingarnar sem settar eru fram í VIII. viðauka.

2. Ef mörg yfirvöld ógnamiðaðra innbrotsprófana voru þátttakendur í ógnamiðaðri innbrotsprófun skal leiðandi yfirvald ógnamiðaðrar innbrotsprófunar veita aðilunum á fjármálamarkaði sem voru prófaðir staðfestinguna sem um getur í 7. mgr. 26. gr. reglugerðar (ESB) 2022/2554.

15. gr.

Notkun innri prófunaraðila

1. Aðilar á fjármálamarkaði skulu koma á fót eftirfarandi fyrirkomulagi vegna notkunar á innri prófunaraðilum:

a) koma á og innleiða stefnu um stjórnun innri prófunaraðila í ógnamiðaðri innbrotsprófun,

b) ráðstöfunum til að tryggja að notkun innri prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun hafi ekki neikvæð áhrif á almenna varnar- eða viðnámsgetu aðilans á fjármálamarkaði gagnvart upplýsinga- og fjarskiptatæknitengdum atvikum eða hafi veruleg áhrif á aðgengi að tilföngum sem varið er til upplýsinga- og fjarskiptatæknitengdra verkefna meðan á ógnamiðaðri innbrotsprófun stendur,

c) ráðstafanir til að tryggja að innri prófunaraðilar hafi næg tilföng og getu til að framkvæma ógnamiðaða innbrotsprófun.

Stefnan sem um getur í a-lið skal:

a) innihalda viðmiðanir til að meta hentugleika, hæfni, mögulega hagsmunaárekstra innri prófunaraðila og tilgreina stjórnendaábyrgð í prófunarferlinu,

b) vera skjalfest og endurskoðuð reglulega,

c) kveða á um að innra prófunarteymið sé skipað teymisstjóra prófunar og a.m.k. tveimur aðilum til viðbótar,

d) krefjast þess að allir aðilar prófunarteymisins hafi verið starfsmenn aðilans á fjármálamarkaði eða veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu síðastliðna 12 mánuði,

e) innihaldi ákvæði um þjálfun innri prófunaraðila í því hvernig skuli framkvæma innbrotsprófun og prófun rauðs teymis.

2. Þegar yfirvald ógnamiðaðrar innbrotsprófunar samþykkir notkun innri prófunaraðila í samræmi við a-lið 2. mgr. 27. gr. reglugerðar (ESB) 2022/2554 skal yfirvald ógnamiðaðrar innbrotsprófunar taka tillit til krafnanna sem mælt er fyrir um í 1. mgr. 7. gr. þessarar reglugerðar.

3. Þegar innri prófunaraðilar eru notaðir skal aðilinn á fjármálamarkaði tryggja að slík notkun sé nefnd í eftirfarandi skjölum:

a) upphafsupplýsingunum um prófunina sem um getur í 9. gr.,

b) prófunarskýrslu rauðs teymis sem um getur í 2. mgr. 12. gr.,

c) skýrslunni með samanteknu niðurstöðunum úr ógnamiðuðu innbrotsprófuninni sem um getur í 6. mgr. 26. gr. reglugerðar (ESB) 2022/2554.

4. Prófunaraðilar sem eru starfandi hjá veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu teljast vera innri prófunaraðilar aðilans á fjármálamarkaði.

16. gr.

Samstarf og gagnkvæm viðurkenning

1. Í þeim tilgangi að gera ógnamiðaða innbrotsprófun í tengslum við aðila á fjármálamarkaði sem veitir þjónustu í fleiri en einu aðildarríki, þ.m.t. í gegnum útibú, skal yfirvald ógnamiðuðu innbrotsprófunarinnar:

a) ákvarða hvaða yfirvöld ógnamiðaðrar innbrotsprófunar í gistiaðildarríkjum skulu koma að málum, að teknu tilliti til þess hvort fleiri en ein nauðsynleg eða mikilvæg starfsemi fari fram eða sé dreift í gistiaðildarríkjum,

b) upplýsa yfirvöld ógnamiðaðrar innbrotsprófunar sem tilgreind eru í samræmi við a-lið um ákvörðun um að framkvæma ógnamiðaða innbrotsprófun á aðilanum á fjármálamarkaði,

c) nema yfirvöld ógnamiðaðrar innbrotsprófunar hafi komið sér saman um annað, skal yfirvald aðilans á fjármálamarkaði á sviði ógnamiðaðra innbrotsprófana leiða ógnamiðuðu innbrotsprófunina.

Yfirvöld ógnamiðaðrar innbrotsprófunar í gistiaðildarríkjunum geta, innan 20 virkra daga frá móttöku upplýsinga um framkvæmd ógnamiðaðrar innbrotsprófunar í framtíðinni, annaðhvort lýst yfir áhuga á að fylgjast með ógnamiðuðu innbrotsprófuninni sem áheyrnarfulltrúar eða tilnefnt prófunarstjóra til að taka þátt í ógnamiðuðu innbrotsprófuninni. Leiðandi yfirvald ógnamiðaðrar innbrotsprófunar skal láta öllum yfirvöldum ógnamiðaðrar innbrotsprófunar, sem koma fram sem áheyrnarfulltrúar, í té umfangskilgreiningarskjalið, yfirlitsskýrsluna um prófunina, úrbótaáætlunina og staðfestinguna.

Leiðandi yfirvald ógnamiðaðrar innbrotsprófunar skal samræma öll yfirvöld ógnamiðuðu innbrotsprófunarinnar sem koma að prófuninni á meðan á henni stendur og taka allar ákvarðanir sem þörf er á til að framkvæma ógnamiðuðu innbrotsprófunina á viðeigandi og skilvirkan hátt. Leiðandi yfirvald ógnamiðaðrar innbrotsprófunar getur ákvarðað hámarksfjölda yfirvalda ógnamiðaðrar innbrotsprófunar sem geta tekið þátt, ef skilvirkri framkvæmd ógnamiðuðu innbrotsprófunarinnar væri annars stefnt í hættu.

2. Þegar aðili á fjármálamarkaði notar sama veitanda upplýsinga- og fjarskiptatækniþjónustu innan samstæðu og aðilar á fjármálamarkaði með staðfestu í öðrum aðildarríkjum, eða tilheyrir samstæðu og deilir upplýsinga- og fjarskiptatæknikerfum með aðilum á fjármálamarkaði innan sömu samstæðu með staðfestu í öðrum aðildarríkjum, skal yfirvald ógnamiðaðrar innbrotsprófunar fyrir þann aðila á fjármálamarkaði hafa samband við yfirvöld ógnamiðaðrar innbrotsprófunar hinna aðilanna á fjármálamarkaði sem nota sama upplýsinga- og fjarskiptatæknikerfi innan samstæðu eða deila upplýsinga- og fjarskiptatæknikerfum sem hluti af samstæðunni og meta með þeim hagkvæmni og hentugleika þess að framkvæma sameiginlega ógnamiðaða innbrotsprófun að þeirra mati. Sameiginlegri ógnamiðaðri innbrotsprófun skal gefinn forgangur fram yfir einstaka ógnamiðaða innbrotsprófun þar sem það getur leitt til lækkunar á kostnaði og minni notkunar úrræða fyrir aðila á fjármálamarkaði og yfirvöld ógnamiðaðrar innbrotsprófunar, að því tilskildu að það hafi ekki áhrif á áreiðanleika og skilvirkni prófunarinnar.

3. Í þeim tilgangi að framkvæma sameiginlega ógnamiðaða innbrotsprófun:

a) skulu yfirvöld aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar koma sér saman um hvaða aðila á fjármálamarkaði skal tilnefna til að framkvæma ógnamiðuðu innbrotsprófunina, með tilliti til uppbyggingar samstæðunnar og skilvirkni prófunarinnar,

b) yfirvald aðilans á fjármálamarkaði á sviði ógnamiðaðar innbrotsprófunar, sem tilnefndur er í samræmi við a-lið, skal leiða ógnamiðuðu innbrotsprófunina, nema yfirvöld þeirra aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar sem taka þátt í sameiginlegu ógnamiðuðu innbrotsprófuninni komi sér saman um annað,

c) yfirvöld annarra aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar en þess aðila á fjármálamarkaði sem tilnefndur var til að leiða sameiginlegu ógnamiðuðu innbrotsprófunina, geta annaðhvort lýst yfir áhuga sínum á því að fylgjast með ógnamiðuðu innbrotsprófuninni sem áheyrnarfulltrúar eða tilnefnt prófunarstjóra fyrir þá ógnamiðuðu innbrotsprófun.

Leiðandi yfirvald ógnamiðaðrar innbrotsprófunar skal samræma öll yfirvöld ógnamiðuðu innbrotsprófunarinnar sem koma að sameiginlegu prófuninni og taka allar ákvarðanir sem þörf er á til að framkvæma sameiginlegu ógnamiðuðu innbrotsprófunina á traustan og skilvirkan hátt.

4. Þegar aðili á fjármálamarkaði hyggst framkvæma samsetta ógnamiðaða innbrotsprófun eins og um getur í 4. mgr. 26. gr. reglugerðar (ESB) 2022/2554, sem kann að ná til aðila á fjármálamarkaði með staðfestu í öðrum aðildarríkjum, skal yfirvald aðilans á sviði ógnamiðaðrar innbrotsprófunar hafa samband við yfirvöld hinna aðilanna á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar og meta með þeim hagkvæmni og hentugleika þess að framkvæma samsetta ógnamiðaða innbrotsprófun fyrir þá í samræmi við 4. mgr. 26. gr. reglugerðar (ESB) 2022/2554.

5. Í þeim tilgangi að framkvæma samsetta ógnamiðaða innbrotsprófun eins og um getur í 4. mgr. 26. gr. reglugerðar (ESB) nr. 2022/2554:

a) skulu yfirvöld aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar koma sér saman um hvaða aðila á fjármálamarkaði skuli tilnefna til að framkvæma samsettu ógnamiðuðu innbrotsprófunina, með tilliti til þeirrar upplýsinga- og fjarskiptatækniþjónustu sem veitt er aðilunum á fjármálamarkaði af þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu og skilvirkni prófunarinnar,

b) yfirvald aðilans á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar, sem tilnefndur er í samræmi við a-lið, skal leiða ógnamiðuðu innbrotsprófunina, nema yfirvöld þess aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar sem taka þátt í samsettu ógnamiðuðu innbrotsprófuninni komi sér saman um annað,

c) yfirvöld annarra aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar en tilnefnda aðilans á fjármálamarkaði sem leiðir samsetta ógnamiðaða innbrotsprófun geta annaðhvort lýst yfir áhuga sínum á því að fylgjast með ógnamiðuðu innbrotsprófuninni sem áheyrnarfulltrúar eða tilnefnt prófunarstjóra fyrir þá ógnamiðuðu innbrotsprófun.

Leiðandi yfirvald ógnamiðaðrar innbrotsprófunar skal samræma öll yfirvöld ógnamiðuðu innbrotsprófunarinnar sem koma að samsettu prófuninni og taka allar ákvarðanir sem þörf er á til að framkvæma samsettu ógnamiðuðu innbrotsprófunina á traustan og skilvirkan hátt.

6. Þegar yfirvald aðila á fjármálamarkaði á sviði ógnamiðaðrar innbrotsprófunar sem þarf að framkvæma ógnamiðaða innbrotsprófun er annað en lögbært yfirvald hans, eins og um getur í 46. gr. reglugerðar (ESB) 2022/2554, skulu þessi yfirvöld deila öllum viðeigandi upplýsingum um öll mál sem tengjast ógnamiðuðum innbrotsprófunum í þeim tilgangi að framkvæma ógnamiðaða innbrotsprófun eða sinna skyldum sínum í samræmi við þá reglugerð.

17. gr.

Gildistaka

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í Stjórnartíðindum Evrópusambandsins.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 13. febrúar 2025.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.

I. VIÐAUKI

Inntak verkefnisáætlunar (a-liður 2. mgr. 9. gr.)

Upplýsingaliður	Upplýsingar sem krafist er
Aðili sem ber ábyrgð á verkefnisáætluninni, þ.e. hópstjóri stýrihópsins	Heiti Samskiptaupplýsingar
Prófunaraðilar	☐ innri ☐ ytri ☐ hvort tveggja
Boðleiðir sem valdar eru í samræmi við d-lið 2. mgr. 9. gr. og a-lið 4. mgr. 9. gr., þ.m.t.: a) dulritun tölvupósts sem skal nota b) nettengd gagnaherbergi sem skal nota c) snarskilaboðakerfi sem skal nota	
Dulnefni ógnamiðuðu innbrotsprófunarinnar	
Ef um slíkt er að ræða, nauðsynleg eða mikilvæg starfsemi aðila á fjármálamarkaði sem hann starfrækir í öðrum aðildarríkjum	1. skrá yfir nauðsynlega eða mikilvæga starfsemi sem starfrækt er í öðru aðildarríki 2. fyrir hverja nauðsynlega eða mikilvæga starfsemi, tilgreiningu á aðildarríki eða aðildarríkjum þar sem hún er starfrækt
Ef um slíkt er að ræða, nauðsynleg eða mikilvæg starfsemi sem nýtur stuðnings þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu	3. skrá yfir nauðsynlega eða mikilvæga starfsemi sem nýtur stuðnings þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu 4. fyrir hverja starfsemi, tilgreining á þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu
Væntanlegir frestir til að ljúka:	
1) Undirbúningsfasi, í samræmi við 9. gr.	áááá-mm-dd
2) Prófunarfasi, í samræmi við 10. og 11. gr.	áááá-mm-dd
3) Lokunarfasi, í samræmi við 12. gr.	áááá-mm-dd
4) Úrbótaáætlun í samræmi við 13. gr.	áááá-mm-dd

II. VIÐAUKI

Inntak umfangsskilgreiningarskjals (6. mgr. 9. gr.)

1. Umfangsskilgreiningarskjalið skal innihalda skrá yfir alla nauðsynlega eða mikilvæga starfsemi sem aðilinn á fjármálamarkaði hefur tilgreint.

2. Eftirfarandi upplýsingar skulu hafðar með fyrir hverja tilgreinda nauðsynlega eða mikilvæga starfsemi:

   a) ef nauðsynlega eða mikilvæga starfsemin er ekki innan umfangs ógnamiðuðu innbrotsprófunarinnar, útskýringu á því hvers vegna hún er ekki tekin með,

   b) ef nauðsynlega eða mikilvæga starfsemin er innan umfangs ógnamiðuðu innbrotsprófunarinnar:

      i. skýringu á því hvers vegna hún er tekin með,

      ii. tilgreinda upplýsinga- og fjarskiptatæknikerfið eða -kerfin sem styður eða styðja við þá nauðsynlegu eða mikilvægu starfsemi,

      iii. fyrir hvert tilgreint upplýsinga- og fjarskiptatæknikerfi:

         1. hvort um útvistun sé að ræða og ef svo er, heiti þriðja aðilans sem veitir upplýsinga- og fjarskiptatækniþjónustu,

         2. lögsögurnar þar sem upplýsinga- og fjarskiptatæknikerfið er notað,

         3. ítarlega lýsingu á bráðabirgðaflaggi eða -flöggum, sem tilgreinir hvaða öryggisþáttur leyndar, réttleika, ósvikni eða tiltækileika fellur undir hvert flagg.

———

III. VIÐAUKI

Inntak skýrslu um markviss ógnagreiningargögn (5. mgr. 10. gr.)

Skýrslan um markviss ógnagreiningargögn skal innihalda upplýsingar um allt eftirfarandi:

1. Heildarumfang rannsókna á greiningargögnum, þ.m.t. að lágmarki eftirfarandi:
   a) nauðsynleg eða mikilvæg starfsemi sem fellur innan umfangsins,
   b) landfræðileg staðsetning þeirra,
   c) opinbert tungumál ESB sem er notað,
   d) viðkomandi þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu,
   e) tímabilið þegar rannsóknargagna er aflað.
2. Heildarmat á því hvaða áþreifanlegu nýtanlegu greiningargögn er að finna um aðilann á fjármálamarkaði, þ.m.t.:
   a) notendanöfn og aðgangsorð starfsfólks,
   b) útlitslega svipuð lén sem hægt er að rugla saman við opinber lén aðilans á fjármálamarkaði,
   c) tæknikönnun: viðkvæmur eða misnotanlegur hugbúnaður, kerfi og tækni,
   d) upplýsingar sem starfsmenn hafa birt á netinu, sem tengjast aðilanum á fjármálamarkaði og gætu verið notaðar í árásarskyni,
   e) upplýsingar sem eru til sölu á huliðsnetinu,
   f) allar aðrar viðeigandi upplýsingar sem eru aðgengilegar á netinu eða almenningsneti,
   g) ef við á, upplýsingar um efnisleg árásarmörk, þ.m.t. leiðir til að fá aðgang að athafnasvæði aðilans á fjármálamarkaði.
3. Greining á ógnagreiningargögnum þar sem tekið er tillit til almenns ógnarlandslags og sérstakra aðstæðna aðilans á fjármálamarkaði, þar á meðal að lágmarki:
   a) landfræðipólitísks umhverfis,
   b) efnahagsumhverfis,
   c) tækniþróunar og annarrar þróunar í tengslum við starfsemina í fjármálaþjónustugeiranum.
4. Ógnarsnið aðila með illan ásetning (tiltekins einstaklings/hóps eða almenns flokks) sem kunna að beinast að aðilanum á fjármálamarkaði, þar á meðal þau kerfi aðilans á fjármálamarkaði sem líklegast er að aðilar með illan ásetning brjótist inn í eða beini spjótum sínum að, hugsanlegar ástæður, ásetning og rök fyrir hugsanlegri árás og hugsanleg aðferð árásaraðilanna.
5. Ógnasviðsmyndir: a.m.k. þrjár heildstæðar ógnasviðsmyndir fyrir þau ógnasnið sem tilgreind eru í samræmi við 4. lið sem hafa hæsta ógnarstigið. Ógnasviðsmyndirnar skulu lýsa heildstæðri árásarleið og innihalda, að lágmarki:
   a) eina sviðsmynd sem felur í sér, en takmarkast ekki við, að tiltækileiki þjónustu er vásettur,
   b) eina sviðsmynd sem felur í sér, en takmarkast ekki við, að heilleiki gagna er vásettur,
   c) eina sviðsmynd sem felur í sér, en takmarkast ekki við, að leynd upplýsinga er vásett.
6. Ef við á, lýsingu á sviðsmyndinni sem ekki er ógnamiðuð sem um getur í 4. mgr. 10. gr.

———

IV. VIÐAUKI

Inntak prófunaráætlunar rauðs teymis (1. mgr. 11. gr.)

Prófunaráætlun rauðs teymis skal innihalda upplýsingar um allt eftirfarandi:

a) boðleiðir og verklagsreglur,

b) úrræði, aðferðir og verklag sem heimilt er að nota og sem ekki er heimilt að nota við árásina, þ.m.t. siðferðisleg mörk bragðvísi,

c) áhættustýringarráðstafanir sem prófunaraðilar skulu fylgja,

d) lýsingu á hverri sviðsmynd, þ.m.t.:

   i. ógnvaldurinn sem líkt er eftir,

   ii. tilgangur þeirra, ástæða og markmið,

   iii. markstarfsemin og upplýsinga- og fjarskiptatæknikerfið eða -kerfin sem styðja starfsemina,

   iv. þættir varðandi leynd, réttleika, tiltækileika og ósvikni sem stefnt er á,

   v. flögg,

e) nákvæm lýsing á hverri væntanlegri árásarleið, þar á meðal forkröfum og mögulegri hjálparhönd sem stýrihópurinn veitir, ásamt tímafresti fyrir afhendingu og hugsanlega notkun,

f) tímasetningu aðgerða rauðs teymis, þar á meðal tímaáætlun fyrir framkvæmd hverrar sviðsmyndar, sem skiptist að lágmarki í þrjá fasa sem prófunaraðili fer í gegnum í prófunarfasanum, þ.e. að komast inn í upplýsinga- og fjarskiptatæknikerfi aðila á fjármálamarkaði, að ferðast um upplýsinga- og fjarskiptatæknikerfin og síðan framkvæma aðgerðir á árásarmörkum og að lokum að hverfa á braut úr upplýsinga- og fjarskiptatæknikerfunum (inn-, gegnum- og útfasar),

g) upplýsingar um sérkenni innviða aðilans á fjármálamarkaði sem skal hafa í huga við prófunina,

h) ef um þær er að ræða, viðbótarupplýsingar eða önnur tilföng sem prófunaraðilar þurfa á að halda til að framkvæma sviðsmyndir.

V. VIÐAUKI

Inntak prófunarskýrslu rauðs teymis (2. mgr. 12. gr.)

Prófunarskýrsla rauðs teymis skal a.m.k. innihalda upplýsingar um allt eftirfarandi:

a) upplýsingar um árásina sem var framkvæmd, þ.m.t.:
   i. nauðsynlega eða mikilvæga starfsemi sem ráðist var á og tilgreinda upplýsinga- og fjarskiptatæknikerfi, -ferla og -tækni sem styðja við nauðsynlega eða mikilvæga starfsemi, eins og tilgreint var í prófunaráætlun rauða teymisins,
   ii. samantekt um hverja sviðsmynd,
   iii. flögg sem náðust og flögg sem náðust ekki,
   iv. árásarleiðir sem báru árangur og árásarleiðir sem voru árangurslausar,
   v. úrræði, aðferðir og verklag sem beitt var með árangri og sem var beitt árangurslaust,
   vi. frávik frá prófunaráætlun rauðs teymis, ef um slíkt var að ræða,
   vii. hjálparhendur, ef þær voru veittar,
b) allar aðgerðir sem prófunaraðilar vita að bláa teymið framkvæmdi til að endurgera árásina og draga úr áhrifum hennar,
c) veikleika sem uppgötvuðust og aðrar niðurstöður, þ.m.t.:
   i. lýsingu á veikleikum og öðrum niðurstöðum, þ.m.t. alvarleika þeirra,
   ii. greiningu á frumorsök árangursríkra árása,
   iii. ráðleggingar um úrbætur, þ.m.t. tilgreining á forgangsröðun úrbóta.

———

VI. VIÐAUKI

Inntak prófunarskýrslu blás teymis (4. mgr. 12. gr.)

Prófunarskýrsla blás teymis skal a.m.k. innihalda upplýsingar um allt eftirfarandi:

1. fyrir hvert stig árásarinnar sem prófunaraðilar lýsa í prófunarskýrslu rauðs teymis:
   a) lista yfir árásaraðgerðir sem uppgötvuðust,
   b) færslur í aðgerðaskrá sem eiga við þessar uppgötvanir,
2. mat á niðurstöðum og ráðleggingum prófunaraðilanna,
3. sönnunargögn um árás prófunaraðilanna sem blátt teymi hefur safnað,
4. greining blás teymis á frumorsök árangursríkra árása prófunaraðila,
5. listi yfir lærdóm sem dreginn var af prófuninni og möguleikar til úrbóta auðkenndir,
6. listi yfir efnisatriði sem taka skal fyrir í fjólubláu teymisvinnunni.

———

VII. VIÐAUKI

Nánari upplýsingar í skýrslunni með samanteknu niðurstöðunum úr ógnamiðuðu innbrotsprófuninni sem um getur í 6. mgr. 26. gr. reglugerðar (ESB) 2022/2554

Yfirlitsskýrslan um prófunina skal a.m.k. innihalda upplýsingar um allt eftirfarandi:

a) aðilana sem hlut eiga að máli,

b) verkefnaáætlunina,

c) samþykkt umfang, þ.m.t. rök fyrir því að hafa með eða hafa ekki með nauðsynlega eða mikilvæga starfsemi og tilgreind upplýsinga- og fjarskiptatæknikerfi, -ferla og -tækniþekkingu sem styður við nauðsynlega eða mikilvæga starfsemi sem fellur undir ógnamiðaða innbrotsprófun,

d) valdar sviðsmyndir og öll veruleg frávik frá skýrslu um markviss ógnagreiningargögn,

e) framkvæmdar árásarleiðir og úrræðin, aðferðirnar og verklagið sem var beitt,

f) flögg sem náðust og flögg sem náðust ekki,

g) frávik frá prófunaráætlun rauðs teymis, ef um slíkt var að ræða,

h) greiningar blás teymis, ef um þær er að ræða,

i) fjólublåa teymisvinnu í prófunarfasa, ef hún fór fram, og tengd skilyrði,

j) hjálparhendur, ef þær voru veittar,

k) áhættustýringarráðstafanir sem gerðar voru,

l) veikleika sem borið var kennsl á og aðrar niðurstöður, þ.m.t. alvarleiki þeirra,

m) greiningu á frumorsök árangursríkra árása,

n) samantekna áætlun um úrbætur, sem tengir veikleika og aðrar niðurstöður, frumorsakir þeirra og forgangsröðun úrbóta,

o) lærdóm sem dreginn var af fenginni endurgjöf.

———

VIII. VIÐAUKI

Upplýsingar um staðfestinguna á ógnamiðaðri innbrotsprófun sem um getur í 7. mgr. 26. gr. reglugerðar (ESB) 2022/2554

Í staðfestingunni skulu a.m.k. koma fram eftirfarandi upplýsingar:

a) um ógnamiðuðu innbrotsprófunina sem er framkvæmd:

   i. upphafs- og lokadagsetningar ógnamiðuðu innbrotsprófunarinnar,

   ii. nauðsynlega eða mikilvæga starfsemin sem er innan umfangs ógnamiðuðu innbrotsprófunarinnar,

   iii. ef við á, upplýsingar um nauðsynlega eða mikilvæga starfsemi sem fellur undir umfang ógnamiðuðu innbrotsprófunarinnar en var ekki prófuð,

   iv. ef við á, aðrir aðilar á fjármálamarkaði sem tóku þátt í ógnamiðuðu innbrotsprófuninni,

   v. ef við á, þriðju aðilar sem veita upplýsinga- og fjarskiptatækniþjónustu sem tóku þátt í ógnamiðuðu innbrotsprófuninni,

   vi. að því er varðar prófunaraðila:

      1. hvort innri prófunaraðilar voru notaðir,

      2. hvort aðilinn á fjármálamarkaði hafi beitt annarri undirgrein 3. mgr. 5. gr.,

   vii. tímalengd virks prófunarfasa rauða teymisins í almanaksdögum,

b) ef mörg yfirvöld ógnamiðaðrar innbrotsprófunar tóku þátt í ógnamiðuðu innbrotsprófuninni, hin yfirvöldin á sviði ógnamiðaðrar innbrotsprófunar og að hvaða marki þau tóku þátt,

c) lista yfir skjöl sem yfirvald ógnamiðuðu innbrotsprófunar skoðaði í tilgangi staðfestingarinnar.
