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.
