Fylgiskjal 3.

FRAMSELD REGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2024/1774

frá 13. mars 2024

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

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) 2022/2554 frá 14. desember 2022 um stafrænan rekstrarlegan viðnámsþrótt fyrir fjármálageirann og um breytingu á reglugerðum (EB) nr. 1060/2009, (ESB) nr. 648/2012, (ESB) nr. 600/2014, (ESB) nr. 909/2014 og (ESB) 2016/1011 ([1]), einkum fjórðu undirgrein 15. gr. og fjórðu undirgrein 3. mgr. 16. gr.,

og að teknu tilliti til eftirfarandi:

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

([4]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 600/2014 frá 15. maí 2014 um markaði fyrir fjármálagerninga og um breytingu á reglugerð ráðsins (ESB) nr. 648/2012 (Stjtíð. ESB L 173, 12.6.2014, bls. 84, ELI: http://data.europa.eu/eli/reg/2014/600/oj).

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

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

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

SAMÞYKKT REGLUGERÐ ÞESSA:

I. BÁLKUR

ALMENNAR MEGINREGLUR

1. gr.

Heildaráhættusnið og flækjustig

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

a) dulritun og dulmáli,

b) rekstraröryggi upplýsinga- og fjarskiptatækni,

c) netöryggi,

([6]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1093/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska bankaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og niðurfellingu ákvörðunar framkvæmdastjórnarinnar 2009/78/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 12, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([7]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1094/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska vátrygginga- og lífeyrissjóðaeftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/79/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 48, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([8]) Reglugerð Evrópuþingsins og ráðsins (ESB) nr. 1095/2010 frá 24. nóvember 2010 um að koma á fót evrópskri eftirlitsstofnun (Evrópska verðbréfamarkaðseftirlitsstofnunin), um breytingu á ákvörðun nr. 716/2009/EB og um niðurfellingu á ákvörðun framkvæmdastjórnarinnar 2009/77/EB (Stjtíð. ESB L 331, 15.12.2010, bls. 84, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([9]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2016/679 frá 27. apríl 2016 um vernd einstaklinga í tengslum við vinnslu persónuupplýsinga og um frjálsa miðlun slíkra upplýsinga og niðurfellingu tilskipunar 95/46/EB (almenna persónuverndarreglugerðin) (Stjtíð. ESB L 119, 4.5.2016, bls. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([10]) Reglugerð Evrópuþingsins og ráðsins (ESB) 2018/1725 frá 23. október 2018 um vernd einstaklinga í tengslum við vinnslu meginstofnana, stofnana, skrifstofa og fagstofnana Sambandsins á persónuupplýsingum og um frjálsa miðlun slíkra upplýsinga og um niðurfellingu reglugerðar (EB) nr. 45/2001 og ákvörðunar nr. 1247/2002/EB (Stjtíð. ESB L 295, 21.11. 2018, bls. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

d) verkefnastjórnun og breytingastjórnun í upplýsinga- og fjarskiptatækni,

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

II. BÁLKUR

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

I. KAFLI

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

1. þáttur

2. gr.

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

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

a) tryggja öryggi netkerfa,

b) innihalda verndarráðstafanir gegn innbrotum og gagnamisnotkun,

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

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

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

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

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

c) innihaldi vísa og ráðstafanir til að:

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

   ii. skrá undantekningar frá innleiðingunni,

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

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

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

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

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

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

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

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

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

2. þáttur

3. gr.

Stýring upplýsinga- og fjarskiptatækniáhættu

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

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

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

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

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

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

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

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

   ii. úthlutun hlutverka og ábyrgðar varðandi:

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

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

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

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

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

      2) mat á tiltækum mótvægisráðstöfunum,

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

e) ákvæði um vöktun á:

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

   ii. innri og ytri veikleikum og ógnum:

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

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

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

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

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

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

3. þáttur

Eignastýring upplýsinga- og fjarskiptatækni

4. gr.

Eignastýringarstefna í upplýsinga- og fjarskiptatækni

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

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

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

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

   i. einkvæmt auðkenni sérhverrar upplýsinga- og fjarskiptatæknieignar,

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

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

   iv. auðkenni eigenda upplýsinga- og fjarskiptatæknieigna,

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

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

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

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

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

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

5. gr.

Verklagsreglur um stýringu upplýsinga- og fjarskiptatæknieigna

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

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

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

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

4. þáttur

Dulritun og dulmál

6. gr.

Dulritun og dulritunarstýringar

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

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

a) dulritun gagna í dvala og í flutningi,

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

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

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

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

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

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

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

7. gr.

Stjórnun dulritunarlykils

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

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

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

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

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

5. þáttur

Rekstraröryggi upplýsinga- og fjarskiptatækni

8. gr.

Stefnur og verklagsreglur fyrir upplýsinga- og fjarskiptatæknirekstur

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

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

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

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

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

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

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

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

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

   iii. samskiptareglur fyrir gagnaferil og upplýsingar úr kerfisskrám,

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

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

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

   vii. kröfur um framkvæmd þróunar og prófunar í raunumhverfi,

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

i. verklagsreglur og samskiptareglur til að meðhöndla villur,

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

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

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

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

9. gr.

Getu- og frammistöðustjórnun

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

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

b) hámörkunar á nýtingu auðlinda,

c) vöktunarverklag fyrir viðhald og endurbætur á:

i. tiltækileika gagna og upplýsinga- og fjarskiptatæknikerfa,

ii. skilvirkni upplýsinga- og fjarskiptatæknikerfa,

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

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

10. gr.

Veikleika- og bótastjórnun

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

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

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

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

c) sannprófa hvort:

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

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

d) rekja notkun á:

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

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

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

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

g) vakta og sannprófa úrbætur á veikleikum,

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

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

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

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

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

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

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

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

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

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

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

11. gr.

Gagna- og kerfisöryggi

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

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

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

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

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

d) tilgreiningu öryggisráðstafana vegna spillikóða,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

12. gr.

Aðgerðaskráning

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

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

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

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

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

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

   ii. getustýringu,

   iii. breytingastjórnun,

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

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

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

e) ráðstafanir til að greina bilun í aðgerðaskráningarkerfum,

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

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

6. þáttur

Öryggi netkerfis

13. gr.

Öryggisstjórnun netkerfis

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

m) vegna netþjónustusamninga:

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

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

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

14. gr.

Öryggi upplýsinga í flutningi

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

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

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

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

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

7. þáttur

Verkefnastjórnun og breytingastjórnun í upplýsinga- og fjarskiptatækni

15. gr.

Verkefnastjórnun í upplýsinga- og fjarskiptatækni

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

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

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

a) markmið upplýsinga- og fjarskiptatækniverkefna,

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

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

d) áhættumat upplýsinga- og fjarskiptatækniverkefna,

e) viðkomandi áfanga,

f) kröfur um breytingastjórnun,

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

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

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

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

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

16. gr.

Kaup, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum

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

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

b) krefjast auðkenningar á:

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

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

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

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

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

a) stöðustofnunaraðila og viðskiptavini,

b) samvirkandi miðlæga mótaðila,

c) aðra hagsmunaaðila.

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

a) notendur,

b) veitendur nauðsynlegra nytjahluta og nauðsynlegrar þjónustu,

c) aðrar verðbréfamiðstöðvar,

d) aðra markaðsinnviði,

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

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

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

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

c) vakta innleiðingu aðgerðaáætlunarinnar.

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

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

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

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

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

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

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

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

17. gr.

Breytingastjórnun í upplýsinga- og fjarskiptatækni

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

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

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

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

   i. að breytingar séu skilgreindar og áætlaðar,

   ii. að hannað sé viðeigandi umbreytingarferli,

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

   iv. að gæðatrygging sé skilvirk,

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

   i. tilgangi og umfangi breytingar,

   ii. tímalínu fyrir innleiðingu breytingar,

   iii. væntanlegum niðurstöðum,

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

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

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

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

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

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

a) stöðustofnunaraðila og viðskiptavini,

b) samvirkandi miðlæga mótaðila,

c) aðra hagsmunaaðila.

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

a) notendur,

b) veitendur nauðsynlegra nytjahluta og nauðsynlegrar þjónustu,

c) aðrar verðbréfamiðstöðvar,

d) aðra markaðsinnviði,

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

8. þáttur

18. gr.

Raunlægt og umhverfislegt öryggi

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

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

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

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

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

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

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

   i. stefnu um hreint skrifborð af pappírum,

   ii. stefnu um hreinan skjá í upplýsingavinnslubúnaði.

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

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

II. KAFLI

Mannauðsstefna og aðgangsstýring

19. gr.

Mannauðsstefna

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

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

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

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

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

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

20. gr.

Stjórnun auðkenningar

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

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

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

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

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

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

21. gr.

Aðgangsstýring

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

III. KAFLI

Greining og viðbrögð við atvikum sem tengjast upplýsinga- og fjarskiptatækni

22. gr.

Atvikastjórnunarstefna sem tengist upplýsinga- og fjarskiptatækni

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

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

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

   i. greiningu og eftirlit með netógnum,

   ii. greiningu á óvenjulegum athöfnum,

   iii. veikleikastýringu,

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

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

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

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

23. gr.

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

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

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

a) safna, vakta og greina allt eftirfarandi:

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

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

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

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

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

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

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

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

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

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

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

b) greina dagsetningu og tíma þegar óvenjuleg athöfn greinist,

c) greina tegund óvenjulegrar athafnar.

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

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

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

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

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

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

IV. KAFLI

Stjórnun rekstrarsamfellu í upplýsinga- og fjarskiptatækni

24. gr.

Efnisþættir stefnu um rekstrarsamfellu í upplýsinga- og fjarskiptatækni

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

a) lýsingu á:

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

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

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

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

b) ákvæði um:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25. gr.

Prófun áætlana um rekstrarsamfellu í upplýsinga- og fjarskiptatækni

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

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

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

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

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

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

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

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

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

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

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

a) stöðustofnunaraðila,

b) utanaðkomandi þjónustuveitendur,

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

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

a) notendur verðbréfamiðstöðva,

b) veitendur nauðsynlegra nytjahluta og nauðsynlegrar þjónustu,

c) aðrar verðbréfamiðstöðvar,

d) aðra markaðsinnviði,

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

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

26. gr.

Viðbragðs- og endurreisnaráætlanir í upplýsinga- og fjarskiptatækni

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

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

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

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

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

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

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

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

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

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

b) sviðsmynda þar sem gæði í veitingu nauðsynlegrar eða mikilvægrar starfsemi minnka niður að óviðunandi marki eða bregðast og taka tilhlýðilegt tillit til hugsanlegra áhrifa af ógjaldfærni eða öðrum misbrestum viðkomandi þriðja aðila sem veitir upplýsinga- og fjarskiptatækniþjónustu,

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

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

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

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

g) árás frá innherja,

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

i) víðtæks rafmagnsleysis.

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

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

V. KAFLI

Skýrsla um úttekt á áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni

27. gr.

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

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

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

a) inngangskafla sem:

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

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

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

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

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

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

d) upphafs- og lokadagsetningar úttektartímabils,

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

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

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

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

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

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

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

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

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

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

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

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

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

   i. lista yfir fyrri úttektir hingað til,

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

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

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

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

   ii. niðurstöður úr mati á hlítni,

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

   iv. utanaðkomandi veitur.

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

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

III. BÁLKUR

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

I. KAFLI

Einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni

28. gr.

Stjórnunarhættir og skipulag

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

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

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

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

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

d) samþykki, hafi eftirlit með og skoði reglulega:

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

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

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

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

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

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

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

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

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

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

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

29. gr.

Upplýsingaöryggisstefna og -ráðstafanir

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

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

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

30. gr.

Flokkun upplýsingaeigna og upplýsinga- og fjarskiptatæknieigna

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

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

31. gr.

Stýring upplýsinga- og fjarskiptatækniáhættu

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

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

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

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

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

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

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

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

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

32. gr.

Raunlægt og umhverfislegt öryggi

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

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

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

II. KAFLI

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

33. gr.

Aðgangsstýring

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

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

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

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

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

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

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

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

34. gr.

Rekstraröryggi upplýsinga- og fjarskiptatækni

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

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

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

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

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

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

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

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

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

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

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

35. gr.

Öryggi gagna, kerfa og netkerfa

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

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

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

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

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

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

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

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

36. gr.

Öryggisprófun á upplýsinga- og fjarskiptatækni

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

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

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

37. gr.

Kaup, þróun og viðhald á upplýsinga- og fjarskiptatæknikerfum

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

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

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

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

38. gr.

Verkefnastjórnun og breytingastjórnun í upplýsinga- og fjarskiptatækni

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

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

III. KAFLI

Stjórnun rekstrarsamfellu í upplýsinga- og fjarskiptatækni

39. gr.

Efnisþættir áætlunar um rekstrarsamfellu í upplýsinga- og fjarskiptatækni

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

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

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

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

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

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

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

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

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

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

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

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

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

40. gr.

Prófun áætlana um rekstrarsamfellu

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

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

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

IV. KAFLI

Skýrsla um úttekt á einfölduðum áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni

41. gr.

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

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

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

a) inngangskafla sem veitir:

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

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

   iii. upplýsingar um það svið sem skýrslan fjallar um,

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

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

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

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

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

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

d) upphafs- og lokadagsetning úttektartímabils,

e) aðilann sem ber ábyrgð á úttektinni,

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

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

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

IV. BÁLKUR

LOKAÁKVÆÐI

42. gr.

Gildistaka

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

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

Gjört í Brussel 13. mars 2024.

Fyrir hönd framkvæmdastjórnarinnar,

Ursula VON DER LEYEN

forseti.