STEFNA FJARSKIPTASTOFU

UM FYRIRKOMULAG OG FRAMKVÆMD EFTIRLITS MEÐ REKSTRARAÐILUM STAFRÆNNA GRUNNVIRKJA

OKTÓBER 2021

Fjarskiptastofa

Stefna Fjarskiptastofu um fyrirkomulag og framkvæmd eftirlits með rekstraraðilum stafrænna grunnvirkja

Fjarskiptastofa hefur mótað eftirfarandi stefnu um fyrirkomulagi og framkvæmd eftirlits með rekstraraðilum stafrænna grunnvirkja gagnvart NIS-löggjöfinni og afleiddri reglugerð. Fjarskiptastofa ber samkvæmt 2. mgr. 27.gr. reglugerðar nr. 866/2020 að setja sér stefnu um fyrirkomulag og framkvæmd eftirlits.

Það er stefna Fjarskiptastofu:

- Að eftirlit Fjarskiptastofu stuðli að auknu öryggi og viðnámsþrótti upplýsinga- og netkerfa rekstraraðila stafrænna grunnvirkja.
- Að hafa eftirlit með því að rekstraraðilar stafrænna grunnvirki hlíti NIS-löggjöfinni og afleiddri reglugerð.
- Að hafa yfirsýn yfir stöðu öryggis net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja.
- Að eftirlit með rekstraraðilum stafrænna grunnvirkja sé samræmt, skilvirkt og að rekstraraðilar njóti jafnræðis.
- Að úttektum Fjarskiptastofu sé forgangsraðað með tilliti til fyrirliggjandi áhættu.
- Að gefa bindandi fyrirmæli þegar frávik greinast.
- Að annað hvert ár verði kallað eftir sjálfsmati rekstraraðila á öryggisskipulagi þeirra.

Stefnan er rýnd og endurskoðuð eftir þörfum en að lágmarki á tveggja ára fresti og í kjölfar breytinga á NIS-löggjöfinni og afleiddum reglugerðum.

Fjarskiptastofa

1. Net- og upplýsingaöryggi

Íslenskt nútímasamfélag reiðir sig í æ ríkara mæli á stafræna tækni og er nú svo komið að hnökrar í rekstri net-og upplýsingakerfa geta haft víðtækar og alvarlegar afleiðingar í för með sér fyrir almenning og fyrirtæki og stafrænt öryggi leikur mikilvægt hlutverk í efnahagslegu og samfélagslegu tilliti. Með virkum og vönduðum öryggisráðstöfum er lágmörkuð sú áhætta sem steðjað getur að öryggi net- og upplýsingakerfa, þ.m.t. vegna fátíðra atburða sem geta valdið fjárhagslegum skaða, gagnatapi eða alvarlegum rekstrartruflunum eins og langtíma rekstrar- og þjónusturofi fyrirtækja.

Árið 2016 kom út tilskipun Evrópuþingsins og ráðsins varðandi ráðstafanir til að ná háu sameiginlegu öryggisstigi í net- og upplýsingakerfum í öllu Evrópusambandinu. Tilskipunin var innleidd á Íslandi með setningu laga nr. 78/2019 um öryggi net- og upplýsingakerfa mikilvægra innviða (almennt vísað til sem NIS). Á grundvelli laganna var sett reglugerð nr. 866/2020 um öryggi net- og upplýsingakerfa rekstraraðila nauðsynlegra þjónustu. Til að tryggja öryggi og ásættanlega vernd við rekstur net- og upplýsingakerfa ber rekstraraðilum stafrænna grunnvirkja að uppfylla þær lágmarkskröfur sem fram koma í reglugerðinni.

Í desember 2020 lagði framkvæmdastjórn Evrópusambandsins fram tillögu að nýrri tilskipun um samræmt stig netöryggis (hér eftir NIS2). Tillagan hefur það markmið að samræma enn frekar viðnámsþrótt fyrirtækja og opinbera aðila við atvikum á viði netöryggis. Í tillögunni má sjá að NIS2 mun ná til aðila sem í dag eru undanskildir gildissviði NIS. Má þar m.a. nefna gagnaver, traustþjónustuveitendur, ríkisstofnanir og rekendur jarðstöðva sem styðja við geimtengda þjónustu. Innleiðing NIS2 hér á landi mun hafa þau áhrif að þessir aðilar þurfa að ráðast í aðgerðir til að tryggja netöryggi í starfsemi sinni og mæta þeim kröfum sem regluverkið gerir. Jafnframt hefur innleiðing þau áhrif að umfang eftirlits Fjarskiptastofu mun aukast.

2. Hlutverk Fjarskiptastofu

Fjarskiptastofa hefur eftirlit með framkvæmd NIS-laga gagnvart rekstraraðilum nauðsynlegrar þjónustu á sviði stafrænna grunnvirkja. Stafræn grunnvirki eru skilgreind í lögunum sem tengi- og skiptipunktar, þjónustuveitendur lénsheitakerfis og skráningarstofur höfuðléna. Það eru þó ekki allir aðilar sem reka framangreinda þjónustu sem falla innan gildissviðs laganna. Viðkomandi rekstraraðili þarf einnig að teljast vera mikilvægur í efnahagslegu og

samfélagslegu tilliti. Þannig eru settar ákveðnar kröfur í lögunum og framangreindri reglugerð sem uppfylla þarf svo aðili teljist rekstraraðili nauðsynlegrar þjónustu.

Samkvæmt lögunum ber þeim stjórnvöldum sem fara með eftirlitshlutverk á grundvelli laganna að tilnefna þá aðila sem að uppfylla skilyrði laganna um mikilvægi til samgöngu- og sveitarstjórnarráðuneytisins. Ráðherra birtir á grundvelli þeirra tilnefninga skrá í B deild Stjórnartíðinda. Í ársbyrjun 2021 voru 27 á skrá ráðherra yfir rekstraraðila nauðsynlegrar þjónustu og þar af sex sem skilgreindir eru sem rekstraraðilar stafrænna grunnvirkja og falla þar með undir eftirlit Fjarskiptastofu. Gera má ráð fyrir reglubundinni uppfærslu á skrá ráðherra geta aðilar orðið fleiri en nú eru á skrá ráðherra.

Fyrir þá rekstraraðila nauðsynlegrar þjónustu sem hlíta eftirliti stofnunarinnar þá hefur stofnunin heimild til að afla allra upplýsinga og gagna um skipulag net- og upplýsingaöryggis sem stofnunin telur nauðsynleg vegna framkvæmdar eftirlitsins. Stofnunin hefur heimild til að gera úttektir og prófanir á hve miklu leyti rekstraraðilarnir uppfylli kröfur NIS-laganna og reglugerða sem settar eru á grundvelli þeirra. Þá hefur stofnunin heimildir til að rannsaka þær áhættur og atvik sem upp koma í net- og upplýsingakerfum aðila til að kanna hvort kröfur laganna og afleiddra réttarheimilda hafi verið uppfylltar á þeim tímapunkti þegar áhætta var til staðar eða atvik varð.

Fjarskiptastofa fer með hlutverk samhæfingarstjórnvalds sem sinnir almennri stefnumörkun um eftirlit með lágmarkskröfum um öryggi net- og upplýsingakerfa mikilvægra innviða samkvæmt lögum nr. 78/2019 og reglugerð nr. 866/2020 með það að markmiði að stuðla sem best að samræmi og jafnræði við framkvæmd laganna.

Fjarskiptastofa hefur heimild til að biðja rekstraraðili nauðsynlegrar þjónustu að framkvæma sértækt áhættumat á einstökum hlutum net- og upplýsingakerfa, sérstakri áhættu sem getur sem getur steðjað að kerfunum sem og vegna útvistunar á rekstri þeirra.

3. Markmið

Meginmarkmið eftirlits Fjarskiptastofu er það stuðla að auknum öryggi og viðnámsþrótti net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja gagnvart net- og upplýsingaöryggisógnum. Það er markmið Fjarskiptastofu að í lok árs 2023 sé öryggisskipulag, áhættustýring og viðbúnaður rekstraaðila í samræmi við alþjóðleg bestu viðmið um framkvæmd á þessu sviði.

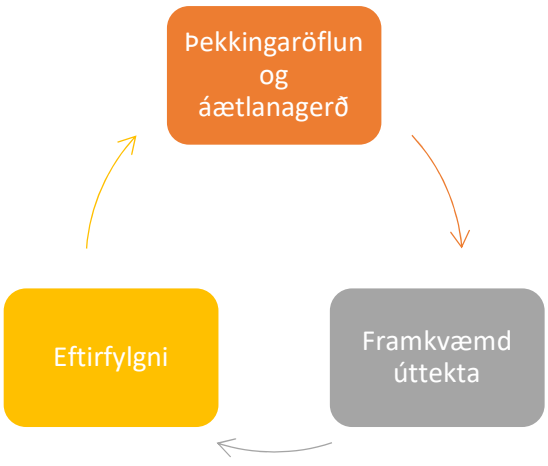
Fjarskiptastofa áréttar mikilvægi góðs samstarfs við rekstraraðila enda telur stofnunin að framkvæmd eftirlits með þeim hætti sé farsælast til þess að ná sameiginlegu markmiði aðila, þ.e. að tryggja öryggi og virkni þeirrar efnahagslegu og samfélagslegu mikilvægu þjónustu sem að viðkomandi rekstraraðili veitir.

Framkvæmd eftirlits verður á að stærstum hluta á höndum sérfræðinga Fjarskiptastofu þótt í ákveðnum afmörkuðum úttektar- og/eða prófunarverkefnum geti stofnunin leitað til utanaðkomandi sérfræðinga. Fjarskiptastofa leggur mikið upp úr trausti milli aðila og mun gæta að öryggi gagna í hvívetna. Fjarskiptastofa hefur hlotið ISO/IEC 27001 vottun sem og að lagakrafa er um að starfsfólk stofnunarinnar sem sinnir eftirliti á þessu sviði hafi hlotið öryggisvottun ríkislögreglustjóra.

Vert er að taka fram að eftirlit Fjarskiptastofu á grundvelli NIS-laga er lögum samkvæmt aðgreint frá starfsemi netöryggisveitarinnar, CERT-ÍS, og sinnir ekki meðhöndlun á áhættu eða atvikum þegar þau koma upp. Netöryggissveit er þó skylt að miðla upplýsingum til eftirlitstjórnvalda um áhættu og/eða atvik sem tilkynningarskyld eru skv. lögunum.

4. Eftirlit Fjarskiptastofu

Eftirlit Fjarskiptastofu hefur hvorki upphaf né enda heldur er er um að ræða sífellu verkefni með þremur fösum; 1) þekkingaröflun og áætlanagerð, 2) framkvæmd úttekta og 3) eftirfylgni.



Í fyrsta fasanum fer fram gagnaöflun þar sem safnað er upplýsingum um öryggi net- og upplýsingakerfa hjá

rekstraraðilum og byggt á þeim upplýsingum er úttektum og prófunum forgangsraðað í úttektaráætlun. Í öðrum fasa, framkvæmd úttekta, er unnið eftir úttektaráætlun og könnuð hlíting við lágmarkskröfur, lagt mat á hlítingu og niðurstöður teknar saman í skýrslu og ef við á gefin bindandi fyrirmæli. Þriðji fasinn er eftirfylgni, en í þeim fasa er vöktun á að unnið sé eftir bindandi fyrirmælum Fjarskiptastofu.

4.1. Þekkingaröflun og áætlanagerð

Fjarskiptastofnun hefur það hlutverk að gera úttektir og prófanir á því hvort rekstraraðilarnir uppfylli kröfur NIS laganna og reglugerða sem settar eru á grundvelli laganna. Það felst m.a. í að yfirfara fylgni rekstraraðila stafrænna grunnvirkja við lágmarkskröfur samkvæmt gildandi lögum og reglugerðum. Forgangsröðun eftirlits Fjarskiptastofu tekur mið af nokkrum atriðum, þar má nefna niðurstöður fyrri úttekta Fjarskiptastofu, sjálfsmöt rekstraraðila stafrænna grunnvirkja, atvika sem upp hafa komið, breytingar í umhverfi fyrirtækisins, ISO 27001:2017 vottun, niðurstöður ytri úttekta og ekki síst áhættumati.

Þekkingaröflun og sjálfsmat rekstraraðila

Annað hvert ár er kallað eftir sjálfsmati rekstraraðila á öryggisskipulagi þeirra. Í sjálfsmatinu eru lagðar fyrir rekstraraðila spurningar um fyrirkomulag öryggismála og áhættustýringarumgjörð en jafnframt viðbótarspurningar varðandi umfang og rekstur.

Úrvinnsla og niðurstöður þessa sjálfsmats gefur Fjarskiptastofu yfirsýn á stöðu mála hjá rekstraraðilum og nýtist jafnframt sem mikilvægt innlegg fyrir afmörkun og forgangsröðun frekara eftirlits með rekstraraðilum í formi úttekta.

Samhliða sjálfsmati er eftir atvikum óskað eftir upplýsingum um hvernig brugðist hefur verið við áður greindum frávikum, atvikaskrám, niðurstöðum atvikagreininga og annað sem Fjarskiptastofa telur nauðsynlegt til sinna eftirliti með NIS- lögunum. Niðurstöður yfirferðar á framangreindum gögnum verða síðan nýttar til að ákveða afmörkun úttekta.

Áhættumat og áætlanagerð

Í kjölfar þekkingaröflunar og sjálfsmats liggur fyrir hvort ISO 27001:2017 vottun er til staðar hjá rekstraraðila og hvert umfang vottunar er. Fjarskiptastofa getur ákveðið að nýta sér þegar það á við tilvist vottunar að hluta til, í heild eða ákveðið eftir frekari yfirferð að vottun nýtist ekki við úttekt. Framkvæma þarf greiningu á umfanginu að teknu tilliti til þess hvaða kerfi eru

innan umfangs úttektar og hvar þau eru hýst. Staðfesta skal að til staðar séu stýringar sem uppfylla viðeigandi kröfur í ISO 27001 sem falla innan vottunnar rekstraraðila. Ef ákveðið er að styðjast við vottun að hluta þarf að yfirfara frávik og ábendingar sem kunna að hafa komið fram við síðustu úttekt á hlítingu við ISO 27001. Ef greining á umfangi vottunar nær yfir stóran hluta eftirlitsþátta laganna og reglugerðarinnar, og valið er að styðjast við ISO vottun með ákveðnum hætti, t.a.m. við forgangsröðun verkefna, þarf þó ávallt að framkvæma ákveðna skoðun á virkni stýringa sem eru innan umfangs vottunar til að staðfesta virkni og hlítni við ákvæði reglugerðarinnar.

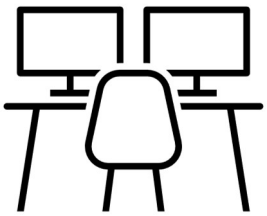
Í kjölfar niðurstaðna sjálfsmats og annarrar þekkingaröflunar vinnur Fjarskiptastofa áhættugreining og áhættumat á rekstraraðilum stafrænna grunnvirkja. Byggt á þeim niðurstöðum er sett fram áhættumiðuð úttektaráætlun og ákveðið að hvaða rekstraraðilum og skoðunarliðum kastljósinu verður beint hverju sinni. Umfang úttekta eru að auki valin með hliðsjón af fjármagni, mannafla og öðrum aðföngum. Úttektaráætlunin verður uppfærð eftir þörfum eða að lágmarki þegar verulegar breytingar verða áhættu, rekstraraðilum, Fjarskiptastofu og/eða lagaumhverfinu.

4.2. Framkvæmd úttekta

Fyrir hverja úttekt er ákvarðað markmið úttektarinnar, umfang, ásættanleg viðmið og hvaða aðferðafræði skuli beitt. Skilgreina hvaða gögn eru nauðsynleg til að afla upplýsinga frá hlutaðeigandi rekstraraðila. Leitast er við að aðferðafræðin sem valin er sé þess eðlis að markmiðum úttektar sé náð og að þær gefi fullnægjandi upplýsingar um virkni þeirra öryggisráðstafana sem til skoðunar eru.

Við framkvæmd eftirlits er hægt að styðjast við mismunandi matsaðferðir. Sem dæmi má nefna mat á skjölum og gögnum (skrifborðsúttektir) þar sem t.d. skjalfestar stefnur eru yfirfarnar. Þá er hægt að meta stöðu aðila í gegnum spurningalista og viðtöl við starfsmenn og/eða stjórnendur fyrirtækja. Eins er hægt að framkvæma vettvangsskoðun og athuga stöðu aðila með beinum hætti á virkni stýringa ásamt tæknilegum prófunum. Framkvæmd úttektar getur stuðst við eina tegund matsaðferðar, tvær eða fleiri, allt eftir umfangi úttektar.

Yfirferð á gögnum (skrifborðsúttekt)

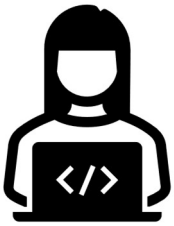


Almennt eru skrifborðsúttektir, þar sem farið er yfir skjöl og gögn frá aðilum, nauðsynlegur hluti allra úttekta. Gögn frá aðilum geta t.d. verið öryggisstefnur, áhættumat og valdar öryggisráðstafanir, neyðaráætlanir, einstaka hlutverk aðila og ábyrgðadreifing, verklagsreglur og verklýsingar, lýsingar á hönnun og uppbyggingu kerfa sem niðurstöður innri prófana og úttektir ytri aðila.

Viðtöl

Mat í formi viðtala er vel þekkt og getur það verið framkvæmt hvort sem er sjálfstætt eða til viðbótar við yfirferð gagna með skrifborðsúttekt en hægt er að afla mikilla huglægra en gagnlegra upplýsinga í gegnum viðtöl við starfsmenn viðkomandi aðila. Fjöldi viðmælenda getur verið mismunandi eftir stærð fyrirtækisins og dreifingu ábyrgðar á net- og upplýsingakerfum.

Vettvangsskoðun og tæknilegar prófanir



Mat í formi beinnar skoðunar á virkni stýringa og tæknilegar prófanir á öryggisráðstöfun er ítarlegasta tegund mats. Hér er t.d. um að ræða hefðbundnar vettvangsathuganir þar sem farið er á viðkomandi stað og athugað hvort t.a.m. viðkomandi öryggisráðstöfun sé til staðar og virkni staðfest með skoðun. Hérna getur þó jafnframt verið um að ræða úttektir sem framkvæmdar eru af starfsmanni stofnunarinnar og/eða ytri aðila á vegum hennar.

Mat á fylgni

Mikilvægur liður við samræmda nálgun eftirlits er samræmi í mati á fylgni við lágmarkskröfur um áhættustýringu og viðbúnað. Í mati sínu mun Fjarskiptastofu yfirfara 16 skoðunarliði (sjá mynd hér að neðan), sem byggja á reglugerð 866/2020 og stöðlunum ÍST ISO/IEC 27001 Stjórnunarkerfi um upplýsingaöryggi, ÍST ISO/IEC 27002 Starfsvenjur fyrir upplýsingaöryggisstýringar og ISO/IEC 27005 Áhættustýring upplýsingaöryggis. Fyrir hvern skoðunarlið er rekstraraðila gefin einkunn á bilinu 0-3. Samræmd matsaðferð og

einkunnargjöf gerir Fjarskiptastofu betur kleift að bera saman stöðu rekstraraðila og þar með öðlast yfirsýn yfir öryggi net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja.

Í töflunni hér á eftir eru forsendur þeirra viðmiða sem tölulegar einkunnir byggja á. Um er að ræða fjórar einkunnir, frá 0-3, ásamt litakóðum til að auðvelda úrvinnslu og yfirsýn.

	Einkunn 3 – Ekkert frávik, skoðunarliðir í lagi, stjórnkerfi hefur verið komið á og er samræmi við lágmarkskröfur reglugerðar. Ekki þörf á viðbrögðum.
	Einkunn 2 - Tækifæri til úrbóta. Ráðstafanir og skjalfesting er til staðar og innleiddar en úrbótaatriði komu upp við skoðun. Niðurstaða kallar á viðbrögð fyrir næstu úttekt.
	Einkunn 1 - Frávik kom upp við skoðun. Ráðstöfun og/eða skjalfesting er til staðar en eru ekki að fullu innleiddar. Niðurstöður kalla á viðbrögð innan sex mánaða.
	Einkunn 0 - Alvarlegt frávik kom upp við skoðun. Ekki hægt að staðfesta að ráðstöfun sé til staðar. Niðurstöður kalla á viðbrögð innan þriggja mánaða.

Við mat á heildarstöðu rekstraraðila er tekið tillit til þess hversu ítarleg úttekt fór fram, hvort úttektin náði til yfirferðar á skjalfestingu á stefnu og verklagsreglum, hvort dýpri rýni var framkvæmd með skoðun á innleiðingu og virkni með framkvæmd úrtaka, og eins ef úttekt var framkvæmd fyrir alla skoðunarliði eða takmörkuð við ákveðna liði.

Við ákvörðun um beitingu bindandi fyrirmæla er tekið mið af niðurstöðum úttekta og einkunnum fyrir skoðunaratriði. Tímamörk á viðbrögð rekstraraðila, dagsektir eða önnur stjórnsýsluviðurlög taka mið af einkunnunum skoðunarliða. Ljóst er þó að ávallt verður leitast við að gefa fyrst út bindandi fyrirmæli og tryggja eftirfylgni við þau, áður en meira íþyngjandi úrræðum verður beitt.

Niðurstöður úttektar

Að lokinni upplýsingaöflun, framkvæmd matsaðferða og mati á fylgni eru niðurstöður skjalfestar í drögum að skýrslu sem send er viðkomandi rekstraraðila stafræns grunnvirkis til yfirlestrar. Yfirlesturinn er hluti af rannsókn málsins og er til þess fallinn að gæta að því að málið sé nægilega upplýst áður en ákvörðun er tekin og andmælaréttur virtur. Í yfirlestrarferlinu er rekstraraðilum stafrænna grunnvirkja gefinn kostur á að kynna sér niðurstöðurnar, leiðrétta misskilning og miðla frekari upplýsingum til stofnunarinnar ef þörf er á.

Ef niðurstaða úttektar leiðir í ljós að rekstraraðilar fylgja ekki einhverjum þeim kröfum sem settar eru fram í NIS-lögunum eða reglugerð um öryggi net- og upplýsingakerfi mun Fjarskiptastofa krefjast þess að úr verði bætt með því að gefa út bindandi fyrirmæli. Hlutaðeigandi aðili fær þá hæfilegan frest til úrbóta sem tekur mið af niðurstöðum úttektar og einkunnagjöf.

4.3. Eftirfylgni

Í þeim tilvikum þar sem gefin eru út bindandi fyrirmæli fylgir Fjarskiptastofa þeim eftir til að gæta þess að úrbætur rekstraraðilans séu fullnægjandi. Viðhafa þarf það verklag að reglulega á úrbótatíma sendir viðkomandi rekstraraðili upplýsingar til Fjarskiptastofu um framgang úrbóta. Að loknum tímafresti bindandi fyrirmæla er kallað eftir upplýsingum um stöðu úrbóta og Fjarskiptastofa leggur sjálfstætt mat á hvort úrbætur séu fullnægjandi. Getur slíkt verið í formi vettvangsskoðunar og/eða tæknilegra prófana. Komi í ljós að viðkomandi rekstraraðili hafi vanrækt að fara að fyrirmælum Fjarskiptastofu um úrbætur getur stofnunin ákveðið að láta þriðja aðila vinna verkið á kostnað hlutaðeigandi sem og lagt á dagsektir þar til fyrirmælum hefur verið fullnægt að mati stofnunarinnar.

5. Eftirlitsáætlun Fjarskiptastofu 2021-2023

Áætlun Fjarskiptastofu nær frá október 2021 til desember 2023 en á þessum tíma er ráðgert að rekstraraðilarnir svari tvisvar sjálfsmati, Fjarskiptastofa framkvæmi áhættumat og áætlanagerð tvisvar, að unnar séu sjö úttektir hjá stafrænum grunnvirkjum. Að auki mun fara fram eftir þörfum eftirfylgni með bindandi fyrirmælum, rannsóknir á atvikum og kallað eftir áhættumötum rekstraraðila á sértökum þáttum.

Október 2021	**Fyrsta sjálfsmat rekstraraðila og þekkingaröflun** Í byrjun fjórða ársfjórðungs er öllum stafrænum grunnvirkjum sent sjálfsmat til útfyllingar ásamt upplýsingabeiðni.
Desember 2021	**Áhættumat og áætlanagerð** Samhliða því að upplýsingaöflun og úrvinnsla er að klárast hefst vinna við forgangaröðun úttekta með áætlanagerð. Áætlanagerðin byggir á áhættugreiningu áhættumati.
Febrúar 2022	**Úttektartímabil 1** Frá febrúar 2022 til ágúst 2022 mun Fjarskiptastofa vinna að tveimur úttektum hjá tveimur stafrænum grunnvirkjum. Umfang og skoðunaratriði er háð áhættumati, áætlanagerð og auðlindum.
September 2022	**Uppfærsla áhættumats og áætlanagerðar**
Október 2022	**Úttektatímabil 2** Frá október 2022 til ágúst 2023 mun Fjarskiptastofa vinna að fimm úttektum hjá fimm stafrænum grunnvirkjum. Umfang og skoðunaratriði er háð áhættumati, áætlanagerð og auðlindum.
September 2023	**Annað sjálfsmat rekstraraðila og þekkingaröflun** Í byrjun fjórða ársfjórðungs er öllum stafrænum grunnvirkjum sent sjálfsmat til útfyllingar ásamt upplýsingabeiðni.
Desember 2023	**Uppfærsla stefnu Fjarskiptastofu** Stefna Fjarskiptastofu um fyrirkomulag og framkvæmd eftirlits með rekstraraðilum stafrænna grunnvirkja yfirfarin og uppfærð.

Til stafræna grunnvirkja teljast nú sex aðilar og mun þeim að öllum líkindum fjölga í næstu uppfærslu listans um þrjá. Í fyrsta tveggja ára hring mun því líklega ekki nást að fara í úttektir á öllum stafrænum grunnvirkjum en stefnt er að því að á fimm árum náist að taka út hlítingu allra stafræna grunnvirkja við hluta af lágmarkskröfum. Að auki mun Fjarskiptastofa fylgja eftir bindandi fyrirmælum, rannsaka atvik og kalla eftir sértökum áhættumötum þegar þörf er á.

6. Lokaorð

Í þessu skjali hefur Fjarskiptastofa sett fram sýn sína og áætlun er varðar eftirlit með net- og upplýsingaöryggi stafræna grunnvirkja. Í upphafi skjalsins er að finna stefnuna sjálfa, því næst er almenn umfjöllun um net- og upplýsingaöryggi og NIS-löggjöfina. Í kafla tvö er í stuttu máli farið yfirlit hlutverk Fjarskiptastofu og þar á eftir markmið eftirlitsins.

Meginmarkmið eftirlits Fjarskiptastofu er það stuðla að auknum öryggi og viðnámsþrótti net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja gagnvart áhættum sem steðjað geta að þeim.

Í kafla fjögur er umfjöllun um högun eftirlits Fjarskiptastofu og aðferðafræði, en eftirlitinu má í meginþáttum skipta í þrjá fasa, þ.e. 1) þekkingaröflun og áætlanagerð, 2) framkvæmd úttekta og 3) eftirfylgni.

Í síðasta kaflanum er að finna eftirlitsáætlun Fjarskiptastofu fyrir tímabilið október 2021 – desember 2023, en á en á þessum tíma er ráðgert að rekstraraðilarnir svari tvisvar sjálfsmati, Fjarskiptastofa framkvæmi áhættumat og áætlanagerð tvisvar, að unnar séu sjö úttektir stafrænum grunnvirkjum.

Stofnunin áréttar sem fram hefur komið í skjali þessu að markmið stofnunarinnar hlýtur að fara saman með markmiðum rekstraraðila stafrænna grunnvirkja á þessu sviði, þ.e. stuðla að auknu öryggi og viðnámsþrótti net- og upplýsingakerfa rekstraraðila stafrænna grunnvirkja gagnvart áhættum og atvikum sem steðja að kerfunum þeirra og tryggja með sem bestum hætti virkni umræddrar þjónustu. Óskar stofnunin því eftir farsælu samstarfi við rekstraraðila stafrænna grunnvirki til að ná þessum markmiðum.

Að mati stofnunarinnar er mikilvægt að sjónarmið hagsmunaaðila á þessa sýn stofnunarinnar komi fram. Í október 2021 óskaði Fjarskiptastofa eftir sjónarmiðum og athugasemdum frá hagsmunaaðilum hvað varðar efni þessara stefnudraga með því að setja drögin í opið samráð á heimasíðu stofnunnar og útsendingu tilkynningar á póstlista stofnunar og tengiliði Stafræns öryggis. Fjarskiptastofu bárust þrjár umsagnir en ekki var um að ræða efnislegar athugasemdir frá hagsmunaaðilum. Stefna er því óbreytt frá drögunum.