Leiðbeinandi tilmæli

vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila

Nr. 1/2019

Gefin út samkvæmt 2. mgr. 8. gr. laga nr. 87/1998 um opinbert eftirlit með fjármálastarfsemi

11. mars 2019

FJÁRMÁLAEFTIRLITIÐ
THE FINANCIAL SUPERVISORY AUTHORITY, ICELAND

Efnisyfirlit

Inngangur

Fjármálaeftirlitið hefur eftirlit með starfsháttum eftirlitsskyldra aðila á grundvelli laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, og sérlaga sem um starfsemi þeirra gilda. Liður í slíku eftirliti er að stuðla að því að eftirlitsskyldir aðilar fylgist með áhættu sem leiðir af rekstri upplýsingakerfa og lágmarki hana eftir því sem kostur er.

Þessum leiðbeinandi tilmælum er ætlað að setja fram og samræma hvaða viðmið liggja til grundvallar mati á hlítingu eftirlitsskyldra aðila við ákvæði í lögum og stjórnvaldsfyrirmælum varðandi rekstraráhættu með áherslu á rekstur upplýsingakerfa og notkun upplýsingatækni vegna hennar. Tekið skal fram að tilmælunum er ekki ætlað að koma í stað ákvæða í lögum og stjórnvaldsfyrirmælum varðandi vernd persónuupplýsinga, netöryggismál eða aðra þætti sem snerta rekstur upplýsingakerfa.

Lágmörkun áhættu við rekstur upplýsingakerfa er m.a. fólgin í því að gera ráðstafanir sem miða að því að stýra rekstraráhættu. Einnig ber að tryggja öryggi upplýsinga, það er að tryggja aðgengi aðeins þeirra sem hafa til þess heimild, þegar þeir þurfa slíkt aðgengi og að upplýsingarnar séu réttar og óspilltar.

Umfang aðgerða til að tryggja öryggi upplýsingakerfa þarf að vera í samræmi við umfang rekstrar eftirlitsskylds aðila og þá áhættu sem honum fylgir. Því gerir Fjármálaeftirlitið ríkari kröfur um eftirfylgni til eftirlitsskyldra aðila með umsvifamikla og fjölþætta starfsemi en minni aðila með einfalda starfsemi, sbr. 51. – 53. liði tilmælanna.

Tilmæli þessi hafa að geyma viðmið til nánari skýringar um þær kröfur sem lög og reglur kveða á um varðandi rekstraráhættu með áherslu á rekstur upplýsingakerfa. Fjármálaeftirlitið leggur viðmiðin til grundvallar við mat á því hvort farið sé að lögum og reglum, þ.m.t. heilbrigðum og eðlilegum viðskiptaháttum. Komist Fjármálaeftirlitið að þeirri niðurstöðu að um brot á lögum eða reglum sé að ræða gerir Fjármálaeftirlitið kröfu um úrbætur, sbr. 1. mgr. 10. gr. laga nr. 87/1998, og leggur mat á hvort tilefni sé til að beita öðrum úrræðum til að bregðast við broti.

1. Gildissvið

1. Þessi leiðbeinandi tilmæli taka til allra eftirlitskyldra aðila skv. 2. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998.
2. Tilmælin ná til reksturs þeirra upplýsingakerfa[1] eftirlitsskyldra aðila sem hafa þýðingu fyrir eða áhrif á starfsemi þeirra.
3. Þegar eftirlitsskyldur aðili er hluti af samstæðu þá eiga tilmælin við um rekstur upplýsingakerfa hjá félögum sem eru í samstæðunni með eftirlitsskylda aðilanum, ef þau hafa þýðingu fyrir eða hafa áhrif á starfsemi eftirlitsskylda aðilans.

2. Stjórnun og ábyrgð[2]

4. Stjórn eftirlitsskylds aðila ber ábyrgð á að rekstur upplýsingakerfa uppfylli þau viðmið sem koma fram í tilmælum þessum[3]. Stjórn eftirlitsskylds aðila ber að gera viðeigandi ráðstafanir til þess að öll upplýsingakerfi, sbr. 2. lið, sem hafa þýðingu fyrir eða áhrif á starfsemi fyrirtækisins séu starfrækt í samræmi við tilmælin.
5. Ábyrgð stjórnar skv. 4. lið á við hvort sem rekstri upplýsingakerfa er útvistað að hluta til eða í heild sinni. Ábyrgð á rekstri upplýsingakerfa og áhættustýring vegna útvistunar liggur ávallt hjá stjórn eftirlitsskylds aðila og verður henni ekki útvistað. Við framkvæmd útvistunar reksturs upplýsingakerfa, í heild eða að hluta, ber stjórn að hafa eftirlit með því að viðmið samkvæmt kafla 3 *Útvistun* í þessum tilmælum séu að fullu uppfyllt.
6. Það er á ábyrgð stjórnar eftirlitsskylds aðila að til staðar sé viðbúnaðarumgjörð, sbr. hluta 2.3 *Viðbúnaðarumgjörð* í þessum tilmælum.
7. Mikilvægt er að stjórn eftirlitsskylds aðila tryggi að rekstur upplýsingakerfa, þar með talið viðhald, sé stöðugur, í samræmi við stefnur, og þar sem það á við áætlanir, og fylgi skriflegum verkferlum, sbr. 9. lið. Stjórn ber að sjá til að fullnægjandi aðföng séu til staðar svo sem tæknibúnaður og mannauður, þar með talin nauðsynleg þekking og færni.

[1] Með *upplýsingakerfum* er átt við þau stafrænu kerfi sem koma að vinnslu upplýsinga ásamt öllum tengingum að, frá og milli þeirra.

[2] Við mat á hlítingu við 4. – 9. lið í þessum tilmælum, verður m.a. höfð hliðsjón af þeim viðmiðum sem Evrópska bankaeftirlitsstofnunin (EBA/GL/2017/05) hefur sett fram í viðmiðunarreglum sínum (e. guidelines) varðandi mat á áhættu vegna upplýsingakerfa. Sjá nánar hér: https://www.eba.europa.eu/regulation-and-policy/supervisory-review-and-evaluation-srep-and-pillar-2/guidelines-on-ict-risk-assessment-under-the-srep. Stuðst verður við liði 20 - 34 og þeir heimfærðir upp á eftirlitsskylda aðila í samræmi við starfsemi þeirra.

[3] Slíka ábyrgð leiðir af ýmsum ákvæðum sérlaga á fjármálamarkaði, sbr. 17. gr., 1. mgr. 54. gr. og 78. gr. g laga um fjármálafyrirtæki, nr. 161/2002, sbr. ennfremur 6. gr. laga um verðbréfaviðskipti, nr. 108/2007, sbr. 38., 39. og 5. mgr. 44. gr. laga um vátryggingastarfsemi, nr. 100/2016, sbr. ennfremur 4. – 6. gr. reglugerðar um vátryggingastarfsemi, nr. 585/2017, sbr. 1. mgr. 29. gr. og 36. gr. e laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, sbr. ennfremur 3. gr. og 2. mgr. 6. gr. reglugerðar um eftirlitskerfi með áhættu lífeyrissjóða, nr. 590/2017, sbr. 2.–5. tölul. 2. mgr. 10. gr. og 11. gr. laga um kauphallir, nr. 110/2007, sbr. 13. gr. laga um rafræna eignarskráningu verðbréfa, nr. 131/1997 og sbr. 3. tölul. 1. mgr. 17. gr. laga um verðbréfasjóði, fjárfestingarsjóði og fagfjárfestasjóði, nr. 128/2011, sbr. ennfremur 8. og 11. gr. reglugerðar um skipulagskröfur rekstrarfélaga verðbréfasjóða (þ.m.t. um hagsmunaárekstra, viðskiptahætti, áhættustýringu og inntak samkomulags milli vörslufyrirtækis og rekstrarfélags) nr. 471/2014.

2.1 Stefnur og verkferlar[4]

8. Stjórn eftirlitsskylds aðila setur stefnu, eða eftir atvikum stefnur, þar sem fram koma m.a. markmið með, og öryggiskröfur til, reksturs upplýsingakerfa. Slík stefna, eða eftir atvikum stefnur, þarf að taka til útvistunar, þ.e. hvaða þáttum í rekstri upplýsingakerfa megi útvista og hvert megi útvista þeim.
9. Til að lágmarka rekstraráhættu eftirlitsskyldra aðila þarf skjalfest verklag að liggja til grundvallar rekstri upplýsingakerfa, þar á meðal skriflegir verkferlar[5]. Hluti af slíku verklagi er að halda dagbók (e. log) um m.a. veitingu aðgangs að kerfum og breytingar á honum. Verkferlarnir þurfa m.a. að taka tillit til þeirra viðmiða sem sett eru fram í tilmælum þessum varðandi:
    - Áhættugreiningu og áhættumat, sbr. hluta 2.2
    - Viðbúnaðarumgjörð, sbr. hluta 2.3[6]
    - Breytingastjórnun, sbr. hluta 2.4[7]
    - Útvistun og skýjaþjónustu, sbr. kafla 3[8]
    - Öryggismál, þar með talið þjálfun og fræðslu, sbr. kafla 4
    - Frávikaskráningu og tilkynningar, sbr. hluta 5.1

2.2 Áhættugreining og áhættumat[9]

10. Sem hluta af mati og greiningu á rekstraráhættu þarf eftirlitsskyldur aðili að greina áhættu vegna upplýsingakerfa og meta hana. Eftirlitsskyldur aðili þarf því að búa yfir ferli til að vakta áhættuna og lágmarka líkurnar á að hún raungerist.
11. Stjórn eftirlitsskylds aðila ákveður viðmið fyrir ásættanlega áhættu tengda notkun upplýsingatækni með tilliti til starfsemi og umfangs viðkomandi aðila. Endurskoða þarf viðmiðin með reglubundnum hætti.
12. Stjórn eftirlitsskylds aðila skal tryggja að a.m.k. árlega, en oftar komi til breytingar sem áhrif hafa á upplýsingaöryggi, sé áhætta metin sem tengist notkun upplýsingatækni vegna starfsemi aðilans. Matið skal unnið til að tryggja að áhættan sé innan viðmiða sem stjórn

[4] Að því er varðar hlutverk stjórnar, setningu stefnu vegna reksturs upplýsingakerfa, gerð skriflegra verkferla og skyldur eftirlitsskyldra aðila vegna rekstraráhættu, vísast til sömu ákvæða í lögum og tengjast 4. lið þessara tilmæla.
[5] Í verkferlum eftirlitsskyldra aðila þarf að vera skýrt hverjir bera ábyrgð á einstökum verkþáttum. Skjalfesting ferlisins þarf jafnframt að vera dagsett vegna rekjanleika og texti þess skýr.
[6] Við mat á hlítingu við hluta 2.3 *Viðbúnaðarumgjörð* og kafla 4 *Öryggismál* í þessum tilmælum verður m.a. höfð hliðsjón af þeim viðmiðum sem Evrópska bankaeftirlitsstofnunin hefur sett fram í fyrrnefndum viðmiðunarreglum varðandi mat á áhættu vegna upplýsingakerfa. Könnuð verða viðmið sem tíunduð eru á bls. 25 – 27 og á bls. 29 í viðmiðunarreglunum.
[7] Við mat á hlítingu við hluta 2.4 *Breytingastjórnun* í þessum tilmælum, verður m.a. höfð hliðsjón af þeim viðmiðum sem Evrópska bankaeftirlitsstofnunin hefur sett fram í viðmiðunarreglunum varðandi mat á áhættu vegna upplýsingakerfa. Könnuð verða viðmið sem tíunduð eru á bls. 28 –29 í viðmiðunarreglunum.
[8] Við mat á hlítingu við kafla 3 *Útvistun og skýjaþjónusta* í þessum tilmælum verður m.a. höfð hliðsjón af þeim viðmiðum sem Evrópska bankaeftirlitsstofnunin hefur sett fram í viðmiðunarreglunum varðandi mat á áhættu vegna upplýsingakerfa. Könnuð verða viðmið sem tíunduð eru á bls. 29 – 30 í viðmiðunarreglunum.
[9] Við mat á hlítingu við hluta 2.2 í þessum tilmælum verður m.a. höfð hliðsjón af þeim viðmiðum sem Evrópska bankaeftirlitsstofnunin hefur sett fram í viðmiðunarreglum um mat á áhættu vegna upplýsingakerfa. Stuðst verður við liði 35 - 62 og þeir heimfærðir upp á eftirlitsskylda aðila í samræmi við starfsemi þeirra.

setur fram sbr. 11. lið. Framkvæmd og niðurstaða áhættumats skal vera skjalfest, ásamt i) tillögum til úrbóta þar sem þörf er á og ii) eftirfylgni vegna úrbóta, sbr. 13. lið.

13. Í kjölfar áhættumats þarf eftirlitsskyldur aðili að skilgreina með skýrum hætti aðgerðir sem grípa þarf til vegna áhættu sem greind hefur verið. Tryggja þarf að ábyrgð vegna úrbóta sé skýr og þeim fylgt eftir.

2.3 Viðbúnaðarumgjörð

14. Sem hluta af mildun eða lágmörkun rekstraráhættu er eftirlitsskyldum aðilum skylt að gera ráð fyrir mögulegum áföllum sem geta valdið því að afkastageta upplýsingakerfa skerðist. Í því skyni þurfa stjórnir eftirlitsskyldra aðila jafnframt að koma á heildstæðri viðbúnaðarumgjörð til að bregðast við slíkum áföllum þar sem skilgreind eru hlutverk, ábyrgð, verkefni og áhættuliðir.
15. Á grundvelli áhættumats, sbr. hluta 2.2, þarf eftirlitsskyldur aðili að skilgreina hvaða upplýsingakerfi eru mikilvæg fyrir starfsemi hans. Viðbúnaðarumgjörðinni er ætlað að taka til allra mikilvægra upplýsingakerfa.
16. Umgjörðin þarf m.a. að taka til eftirfarandi ráðstafana:
    - Viðbrögð við þeim atriðum sem samkvæmt áhættumati geta brugðist og ráðstafanir sem grípa skal til.
    - Upplýsingagjöf til stjórnar, starfsmanna, viðskiptamanna og annarra aðila sem vitneskju þurfa að hafa um rekstrarstöðvun.
    - Skýr viðmið um hvenær gripið skuli til varalausna.
    - Endurheimtuferlar.
17. Endurskoða og uppfæra þarf umgjörðina árlega, sbr. þó 53. lið.

2.3.1 Áætlun um samfelldan rekstur

18. Eftirlitskyldum aðilum sem ber að hafa áætlun um samfelldan rekstur, eða sambærilega áætlun[10], skulu skjalfesta viðbrögð við áföllum sem leitt geta til rekstrarstöðvunar upplýsingakerfa.
19. Áætlunin skal að mati Fjármálaeftirlitsins m.a. ná til eftirfarandi atriða:
    - Yfirsýnar yfir upplýsingakerfin sem áætlunin nær til.
    - Lýsingar á viðbrögðum við ólíkum sviðsmyndum áfalla.
    - Skýrra viðmiða um gangsetningu á viðbrögðum við áfalli.
    - Ásættanlegra tímamarka rekstrarstöðvunar áður en gripið er til viðbragða við áfalli.
    - Verkferla til að koma rekstri upplýsingakerfa aftur í gang.
    - Yfirsýnar yfir ábyrgðarsvið og gangsetningaferla viðbragða við áfalli.

[10] Sbr. 2. mgr. 78. gr. g laga um fjármálafyrirtæki, nr. 161/2002, og einnig 5. mgr. 39. gr. laga um vátryggingastarfsemi, nr. 100/2016.

- Upplýsingagjafar til stjórnar, starfsmanna, birgja, viðskiptavina, opinberra stjórnvalda og fjölmiðla.

20. Mikilvægt er að áætluninni sé framfylgt, eftir því sem við á, með þjálfun, æfingum og prófunum á varalausnum sem tryggja að þær virki eins og til er ætlast. Jafnframt ættu prófanir og niðurstöður þeirra að vera skjalfestar þannig að hægt sé að leggja mat á framkvæmd og árangur.

2.4 Breytingastjórnun

21. Sá aðili, eða eftir atvikum aðilar, sem hefur umboð til að taka mikilvægar ákvarðanir varðandi rekstur upplýsingakerfis, ætti að gefa samþykki sitt fyrir breytingum og/eða innleiðingu breytinga á viðkomandi upplýsingakerfi áður en þær eru framkvæmdar.
22. Eftirlitsskyldur aðili þarf að hafa skriflega verkferla, sbr. 9. lið, fyrir öflun, þróun, innleiðingu, viðhald og prófanir á upplýsingakerfum. Verkferlarnir ættu að taka til áhættu sem tengist þróun, prófunum og samþykktarferli breytinga á upplýsingakerfum, þ.m.t. þróun eða breytingu á hugbúnaði áður en hann fer í notkun.
23. Í verkferlum skv. 22. lið þarf að kveða á um aðskilnað þróunar- og prófunarumhverfis frá raunumhverfi. Jafnframt þarf í slíkum verkferlum að skjalfesta úthlutun og afturköllun aðgangsheimilda að þeim tölvuumhverfum er innihalda raungögn séu þau notuð fyrir þróun eða í prófanir.
24. Skrá þarf öll þau frávik sem upp koma þegar kerfi eru tekin í notkun eða breytingar framkvæmdar í raunumhverfi, sbr. 46. og 47. lið.

3. Útvistun[11]

25. Ef þriðji aðili[12] er fenginn til að sinna verkefnum vegna upplýsingakerfis eftirlitsskylds aðila, skal tryggja að hann sé upplýstur um efni tilmælanna og framfylgi þeim í umboði eftirlitsskylds aðila. Útvistun[13] vegna upplýsingakerfa ætti alltaf að fara fram á grundvelli skriflegs samnings milli eftirlitsskylds aðila og þriðja aðila, eða með sambærilegu fyrirkomulagi sem tryggir að samskipti þeirra séu skjalfest og að verkefnum útvistunaraðila sé lýst.
26. Til að lágmarka rekstraráhættu hjá eftirlitsskyldum aðilum skulu í skriflegum samningi við útvistunaraðila, eða með sambærilegu fyrirkomulagi sbr. 25. lið, m.a. koma fyrir eftirtalin ákvæði:

---

[11] Skyldu eftirlitsskyldra aðila vegna útvistunar leiðir af ákvæðum um rekstraráhættu og útvistun í sérlögum á fjármálamarkaði, sbr. 1. mgr. 54. gr., 78. gr. g laga um fjármálafyrirtæki, nr. 161/2002, sbr. ennfremur 7. gr. laga um verðbréfaviðskipti, nr. 108/2007, sbr. 33. og 49. gr. laga um vátryggingastarfsemi, nr. 100/2016, sbr. ennfremur 21. gr. reglugerðar um vátryggingastarfsemi, nr. 585/2017, sbr. 39. gr. a laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, sbr. ennfremur 4. gr. reglugerðar um eftirlitskerfi með áhættu lífeyrissjóða, nr. 590/2017, sbr. 2.–5. tölul. 2. mgr. 10. gr. laga um kauphallir, nr. 110/2007, sbr. 13. gr. laga um rafræna eignarskráningu verðbréfa, nr. 131/1997 og sbr. 18. gr. laga um verðbréfasjóði, fjárfestingarsjóði og fagfjárfestasjóði, nr. 128/2011.

[12] Með þriðja aðila er átt við aðila sem sinnir útvistun og er ekki starfsmaður eftirlitsskylda aðilans.

[13] Með útvistun er átt við fyrirkomulag milli eftirlitsskylds aðila og þjónustuveitanda þar sem þjónustuveitandi annast eða framkvæmir verkefni, þjónustu eða aðgerðir, í heild sinni eða að hluta, sem annars væru í höndum viðkomandi eftirlitsskylds aðila.

- Ákvæði um hvaða þjónustu útvistunaraðili skal inna af hendi.
- Ákvæði um rétt eftirlitsskylds aðila til eftirlits með þeirri starfsemi útvistunaraðilans sem samningurinn tekur til, þar með talið aðgang ytri og innri endurskoðanda eftirlitsskylds aðila.
- Ákvæði um þagnarskyldu útvistunaraðila og starfsmanna hans til samræmis við þagnarskyldu þá sem hvílir á hinum eftirlitsskylda aðila.
- Ákvæði um heimild Fjármálaeftirlitsins til aðgangs að gögnum og upplýsingum eftirlitsskylda aðilans hjá útvistunaraðila.
- Ákvæði um að athuganir, sem Fjármálaeftirlitið telur vera nauðsynlegan lið í eftirliti með eftirlitsskylda aðilanum, geti farið fram á vinnustöð útvistunaraðila.
- Ákvæði um hvort keðjuútvistun sé heimil og þá að hvaða leyti og hvaða takmarkanir eftirlitsskyldur aðili setur útvistunaraðila til keðjuútvistunar.
- Ákvæði um hvernig þessi tilmæli verða uppfyllt, þ. á m. um varðveislu og meðhöndlun gagna og frávikatilkynningar.
- Ákvæði um reglulega endurskoðun samningsins. Yfirferð í tengslum við endurskoðun ætti að fara fram að minnsta kosti á tveggja ára fresti, sbr. þó 53. lið.
- Ákvæði um útgönguáætlun (e. exit strategy) eftirlitsskylda aðilans.

27. Mikilvægt er að í þjónustusamningi við útvistunaraðila sé tilnefndur ábyrgðaraðili hjá eftirlitsskylda aðilanum sem ber ábyrgð á að ákvæði skv. 26. lið séu uppfyllt. Jafnframt fylgist ábyrgðaraðilinn með að útvistunaraðili uppfylli þær kröfur sem gerðar eru til hans í þjónustusamningi og metur áhættu vegna útvistunar. Að mati Fjármálaeftirlitsins er æskilegt að tilgreina ábyrgðaraðila með vísan til starfstitils eða stöðu starfsmanns innan viðkomandi aðila, þ.e. að ekki sé um nafngreindan einstakling að ræða.
28. Sé hýsingu gagna útvistað þarf eftirlitsskyldur aðili að tryggja að Fjármálaeftirlitið geti nálgast gögn og upplýsingar til þriðja aðila með sama hætti og ef eftirlitið væri að leita eftir gögnum hjá eftirlitsskylda aðilanum sjálfum.
29. Fjármálaeftirlitið fer fram á að vera upplýst fyrirfram um útvistun, hvort sem þriðji aðili hefur staðfestu hér á landi eða erlendis, ásamt því að fá upplýsingar um hvert eftirlitið geti sótt gögn ef þörf krefur. Nauðsynlegar upplýsingar í þessu sambandi eru t.d. upplýsingar um útvistunaraðila, heimilisfang og varnarþing, hvar gögnin verða vistuð, upplýsingar um tengiliði hjá útvistunaraðila og staðfesting á því að útvistunaraðili sé upplýstur um að Fjármálaeftirlitinu sé heimill aðgangur að þeim gögnum sem um ræðir, sbr. 31. lið.
30. Með vísan til markmiðs 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, sbr. einnig umfjöllun í 35. lið telur Fjármálaeftirlitið æskilegt að eftirlitsskyldir aðilar keðjuútvisti ekki hýsingu á upplýsingakerfum og gögnum lengra en til fjórða aðila[14], hvorki að hluta né öllu leyti. Fjármálaeftirlitið beinir til eftirlitsskyldra aðila að keðjuútvista almennt ekki út fyrir Evrópska efnahagssvæðið og þá aðeins að því tilskildu að lagaumhverfi í því ríki sem keðjuútvistað er til standi ekki í vegi fyrir aðgengi Fjármálaeftirlitsins að gögnum.

[14] Með keðjuútvistun til fjórða aðila er átt við að eftirlitsskyldur aðili útvisti til þriðja aðila og að sá aðili útvisti til fjórða aðila. Fjármálaeftirlitið gerir ekki athugasemdir við slíka útvistun en telur að keðjur ættu ekki að ná til fimmta aðila eða lengra. Það telst ekki keðjuútvistun þegar um er að ræða útvistun innan samstæðu.

3.1 Skýjaþjónusta[15]

31. Eftirlitsskyldur aðili sem hyggst innleiða skýjalausn þarf að meta hvort útvistunin standist viðmið sem koma fram í þessum tilmælum með tilliti til þeirra krafna sem gerðar eru til rekstraráhættu í lögum og stjórnvaldsfyrirmælum. Slíkt mat felur m.a. í sér að fylla út gátlista[16] og skila honum til Fjármálaeftirlitsins eigi síðar en 30 dögum áður en fyrirhugað er að taka skýjalausnina í notkun.

32. Eftirlitsskyldur aðili þarf að meta áhættu sem hlýst af skýjalausnum, m.a. með hliðsjón af gátlista skv. 31. lið. Jafnframt þarf hann að sjá til þess að til staðar séu fullnægjandi öryggisráðstafanir vegna útvistunar.

4. Öryggismál

33. Til að gæta öryggis við rekstur upplýsingakerfa telur Fjármálaeftirlitið að eftirlitsskyldur aðili þurfi að koma á og viðhalda skriflegum verkferlum, sbr. 9. lið, sem er ætlað að veita upplýsingum, skjölum, gögnum og gagnamiðlum[17] vernd gegn óheimilli uppljóstrun, breytingum og eyðileggingu. Skjalfest verklag skal liggja til grundvallar viðhöfðum öryggisvörnum. Jafnframt skal skjala verklag vegna úthlutunar, endurskoðunar og afturköllunar aðgangsheimilda að kerfum eftirlitsskyldra aðila.

4.1 Varðveisla og meðhöndlun gagna

34. Í ferlum skv. 33. lið skal m.a. koma fram að notendur upplýsingakerfis eftirlitsskyldra aðila geti ekki endanlega eytt skjölum, færslum, skilaboðum eða samskiptasögu úr viðkomandi upplýsingakerfum á því tímabili sem um ræðir í 36. lið.

35. Samkvæmt 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, er eftirlitsskyldum aðila skylt að veita Fjármálaeftirlitinu aðgang að öllu bókhaldi sínu, fundargerðum, skjölum og öðrum gögnum í vörslu hans er varða starfsemina, sem Fjármálaeftirlitið telur nauðsynlegan. Til þess að markmið ákvæðisins náist er mikilvægt að þau gögn sem eftirlitið kann að óska eftir séu fyrir hendi þá og þegar krafa um aðgengi að þeim eða upplýsingum sem þau fela í sér er sett fram. Þar af leiðandi og að teknu tilliti til megintilgangs tilmæla þessara um lágmörkun rekstraráhættu telur Fjármálaeftirlitið að varðveisla og meðhöndlun gagna af hálfu eftirlitsskyldra aðila skuli fela í sér að gerð séu öryggisafrit af gögnum og upplýsingakerfum.[18] Afrit eru Fjármálaeftirlitinu nauðsynleg til

[15] Við mat á hlítingu við hluta 3.1 í þessum tilmælum, verður m.a. höfð hliðsjón af þeim viðmiðum sem Evrópska bankaeftirlitsstofnunin (EBA) hefur sett fram í tilmælum sínum (e. recommendation) um notkun skýjaþjónustu. Sjá nánar hér: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers. Stuðst verður við tilmælin og þau heimfærð upp á eftirlitsskylda aðila í samræmi við starfsemi þeirra.

[16] Gátlistinn er aðgengilegur á vef Fjármálaeftirlitsins, sjá nánar hér: https://www.fme.is/media/gatlistar/Gatlisti-vegna-innleidingar-skyjalausna-hja-eftirlitsskyldum-adilum-2019.pdf.

[17] Til gagnamiðla teljast m.a. snjallsímar, spjald- og fartölvur, segulbönd, seguldiskar, minnislyklar, minniskort, færanleg harðdisksdrif, geisladiskar, stafrænir mynddiskar, innbyggðar minniseiningar tækjabúnaðar og aðrir sambærilegir miðlar.

[18] Undir slík kerfi falla öll þau upplýsingakerfi eftirlitsskylds aðila sem innihalda skráningar og gögn er varða viðskiptaupplýsingar og/eða viðskiptafyrirmæli hvort sem að þau eru vistuð hjá eftirlitsskylda aðilanum sjálfum eða valið er að útvista. Hér er því átt við öll upplýsinga- og samskiptakerfi er tengjast viðskiptum, s.s. tölvupóst, símkerfi,

að endurgera sérhvert mikilvægt stig í ferli tiltekinna viðskipta. Slík endurgerð er mikilvægur liður í eftirlitshlutverki Fjármálaeftirlitsins, jafnt skv. 1. mgr. 8. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, sem og eftirlitsákvæðum einstakra sérlaga.

36. Öryggisafrit þurfa að uppfylla eftirfarandi skilyrði:

- Fyrirkomulag og verklag afritunar þarf að mati Fjármálaeftirlitsins að vera með skipulögðum hætti og innihalda virkt eftirlit með því að afritun sé unnin í samræmi við skjalfesta verkferla. Verkferlarnir ættu m.a. að fjalla um vistunartíma afrita, hvar þau eru vistuð og þann búnað sem nauðsynlegur er til endurheimtar.
- Afrit upplýsingakerfa sem innihalda viðskiptaupplýsingar[19] séu tiltæk að lágmarki í tvö ár frá uppruna skráningar.
- Afrit upplýsingakerfa sem geyma samskipti sem innihalda viðskiptafyrirmæli[20] séu tiltæk að lágmarki í fimm ár frá uppruna skráningar.
- Afrit af bókhaldskerfum séu tiltæk að lágmarki í sjö ár frá uppruna skráningar, samkvæmt 19. og 20. gr. laga nr. 145/1994 um bókhald, þ.m.t. sá búnaður og kerfi sem þarf til að endurheimta gögnin.
- Afrit séu tiltæk eftirlitsaðilum með skömmum fyrirvara og aðgengi að tilteknum gögnum sé fyrirhafnarlítið.

37. Til þess að tryggja öryggi og trúverðugleika þeirra viðskiptaupplýsinga og viðskiptafyrirmæla sem geymd eru í öryggisafritum er mikilvægt að:

- Afrit sem tekin eru innihaldi allar færslur viðskiptakerfa, skjöl, skrá yfir símtöl, tölvupóst, skilaboð, eða sambærileg gögn, í samfelldri og rekjanlegri tímaröð, enda innihaldi framangreind gögn viðskiptaupplýsingar og/eða viðskiptafyrirmæli.
- Vernda þarf afrit og upplýsingar sem í þeim felast með þeim hætti að ekki sé mögulegt að eyða þeim, eða breyta þeim fyrir mistök, á nokkurn hátt. Jafnframt þarf að vernda afrit og afritunarbúnað á hæfilegan hátt fyrir hættu af hnjaski og hættu frá umhverfinu.
- Aðgengi að afritum ætti að takmarka eins og kostur er.
- Tryggt sé að afrit séu læsileg til loka geymslutímans.

4.2 Netöryggi (e. Cyber security)

38. Við framkvæmd áhættumats, sbr. hluta 2.2, og vegna viðbúnaðarumgjarðar, sbr. hluta 2.3, þarf eftirlitsskyldur aðili að huga sérstaklega að netöryggi svo hægt verði að lágmarka tjón vegna netárása.

farsíma, faxtæki, snarspjall eða annars konar samskiptakerfi, auk annarra kerfa sem geta innihaldið gögn með viðskiptafyrirmælum.

[19] Með viðskiptaupplýsingum er átt við allar upplýsingar og gögn um viðskiptavin og stöðu hans gagnvart viðkomandi eftirlitsskyldum aðila.

[20] Með viðskiptafyrirmælum er átt við samskipti sem fela í sér bindandi ákvarðanir á milli aðila, svo sem fyrirmæli um framkvæmd ákveðinna viðskipta, staðfestingu á samningum, o.s.frv.

39. Mikilvægt er að eftirlitsskyldur aðili verndi kerfi og upplýsingar gegn netógnum og sviksemi, svo sem óheimiluðum aðgangi, gagnastuldi, óværum og spillikóða (e. malicious code), með viðeigandi vöktun, netvörnum og öryggisfræðslu (sbr. 40. lið).

4.3 Öryggisþjálfun og -fræðsla

40. Eftirlitskyldur aðili þarf að efla og viðhalda þekkingu starfsmanna á bestu venjum í tengslum við upplýsingaöryggi og viðbrögð við aðsteðjandi ógnum. Liður í því er að auka þekkingu starfsmanna um netógnir og sviksemistilraunir. Slíkar hættur geta til að mynda beinst að eftirlitsskyldum aðila með tölvupóstum, á samskiptamiðlum og með smáskilaboðum.
41. Mikilvægt er að hafa til staðar fræðsluáætlun vegna öryggismála (þar með talið varðandi netöryggi), kynna hana reglulega og uppfæra kerfisbundið. Mikilvægur liður í öryggisþjálfun- og fræðslu hjá eftirlitsskyldum aðila er að æfa viðbúnað, sbr. hluta 2.3.

5. Innra eftirlit og frávik

42. Eftirlitsskyldum aðilum ber, sbr. 4., 8. og 10. lið, að viðhafa skilvirkt innra eftirlit sem nær m.a. til könnunar á fylgni við viðmið þessara tilmæla. Liður í slíku innra eftirliti eru úttektir á fylgni við tilmæli sbr. 43. lið, auk þess sem frávik ber að meðhöndla og tilkynna til Fjármálaeftirlitsins, sbr. hluta 5.2.

5.1 Úttekt á fylgni við tilmælin

43. Fjármálaeftirlitið beinir því til eftirlitsskyldra aðila að fela innri endurskoðanda eða óháðum aðila að gera úttekt á fylgni við þessi tilmæli. Mikilvægt er að framkvæmd úttektaraðila sé með skipulögðum og markvissum hætti og fylgi almennt þekktri og viðurkenndri aðferðafræði.
44. Úttekt skv. 43. lið skal framkvæma árlega, sbr. þó 53. lið.
45. Með vísan til 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi, nr. 87/1998, fer Fjármálaeftirlitið fram á að framkvæmd og niðurstaða úttektar skv. 43. lið, ásamt tillögum til úrbóta þar sem þörf er á, sé skjalfest og að henni verði skilað til Fjármálaeftirlitsins árlega í samræmi við fyrirmæli í þjónustugátt Fjármálaeftirlitsins.

5.2 Frávikatilkynningar og framvinduskýrslur[21]

46. Eftirlitsskyldir aðilar þurfa að hafa til staðar skriflega verkferla sem taka til meðhöndlunar á frávikum í rekstri upplýsingakerfa, þar með talið tilkynninga um frávik til

[21] Vegna frávikatilkynninga og framvinduskýrslna mun Fjármálaeftirlitið styðjast við nýja flokkun frávika, til samræmis við viðmiðunarreglur Evrópsku bankaeftirlitsstofnunarinnar (EBA/REC/2017/03) varðandi frávikaskýrslur (e. incidents reporting). Sjá nánar hér: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2. Stuðst verður við viðmiðunarreglurnar og þær heimfærðar upp á eftirlitsskylda aðila í samræmi við starfsemi þeirra.

Fjármálaeftirlitsins sbr. 48. og 49. lið. Meðhöndla skal frávik[22] með því að finna orsakir þeirra, koma aftur á eðlilegu rekstrarástandi og koma í veg fyrir að frávikin endurtaki sig.

47. Mikilvægt er að eftirlitsskyldur aðili viðhafi rafræna skráningu frávika, að þau séu rekjanleg og mælanleg.

48. Fjármálaeftirlitið fer fram á að öll frávik í rekstri upplýsingakerfa séu tilkynnt til stofnunarinnar svo fljótt sem verða má, þó eigi síðar en 4 tímum eftir að frávik uppgötvast. Frávikatilkynningum ber að skila í samræmi við leiðbeiningar sem fylgja eyðublaði í þjónustugátt Fjármálaeftirlitsins. Umfang tilkynningar ræðst af starfsemi eftirlitsskyldra aðila.

49. Eftirlitsskyldum aðilum ber að skila framvinduskýrslum vegna frávika skv. 48. lið í samræmi við leiðbeiningar sem fylgja eyðublaði í þjónustugátt Fjármálaeftirlitsins. Framvinduskýrslum ber að skila svo fljótt sem verða má, þó eigi síðar en 3 dögum eftir að frávik uppgötvast. Umfang framvinduskýrslna ræðst af tegund frávika.

6. Hlutfallsregla og viðurlög

50. Í þessum kafla tilmælanna er fjallað um hvernig hlutfallsreglu (e. principle of proportionality) verður beitt við framkvæmd eftirlits. Þá er vikið að sambandinu milli ákvæða um viðurlög í sérlögum og þeirra viðmiða um mat á rekstraráhættu sem fram koma í tilmælunum.

6.1 Hlutfallsregla við eftirlitsframkvæmd

51. Við framkvæmd eftirlits vegna þessara leiðbeinandi tilmæla tekur Fjármálaeftirlitið tillit til stærðar, eðlis og umfangs reksturs upplýsingakerfa eftirlitsskylds aðila og þess hversu margþætt starfsemi þeirra er, sbr. 52. og 53. lið.

52. Eftirtöldum eftirlitsskyldum aðilum ber, án undantekninga, að fylgja þeim viðmiðum sem fram koma í þessum leiðbeinandi tilmælum:

    - Greiðsluþjónustuveitendur, sbr. 8. gr. laga um greiðsluþjónustu nr. 120/2011.
    - Samstæður vátryggingafélaga, sbr. 3. gr. laga um vátryggingasamstæður nr. 60/2017.
    - Kauphallir og aðrir skipulegir verðbréfamarkaðir, sbr. 1. og 2. gr. laga um kauphallir, nr. 110/2007.
    - Verðbréfamiðstöðvar, sbr. 2. gr. laga um rafræna eignarskráningu verðbréfa, nr. 131/1997.
    - Lífeyrissjóðir, sbr. 1. mgr. 1. gr. laga um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða, nr. 129/1997, þar sem hrein eign til greiðslu lífeyris er hærri en 100 milljarðar króna og virkir iðgjaldagreiðendur og lífeyrisþegar eru samanlagt fleiri en 10 þúsund.

[22] Með frávikum (e. incidents) er átt við þá ófyrirséðu atburði (e. events) sem upp koma í rekstri upplýsingakerfa sem skerða þjónustu eftirlitsskylds aðila umfram skilgreind markmið eða áhrif hafa á leynd (e. confidentiality), réttleika (e. integrity) eða tiltækileika (e. availability) upplýsingakerfa.

- Rekstrarfélög verðbréfasjóða, sbr. 7. tölul. 1. mgr. 4. gr. laga um fjármálafyrirtæki, nr. 161/2002, með samanlagðar eignir í stýringu yfir 100 milljarða króna.

53. Eftirlitsskyldum aðilum, öðrum en þeim sem nefndir eru í 52. lið, ber að uppfylla viðmið vegna þessara leiðbeinandi tilmæla með sama hætti og aðilum sem nefndir eru í 52. lið, en með aðlögunum varðandi eftirfarandi þætti:
    - Áhættumat skv. hluta 2.2 skal framkvæma reglulega og að lágmarki á þriggja ára fresti.
    - Viðbúnaðarumgjörð skv. hluta 2.3 skal uppfæra reglulega og að lágmarki á þriggja ára fresti.
    - Endurskoðun útvistunarsamninga skv. 26. lið skal framkvæma reglulega og að lágmarki á fjögurra ára fresti.
    - Úttekt óháðs aðila skv. 43. lið skal framkvæma reglulega og að lágmarki á þriggja ára fresti.
    - Frávikatilkynningar og framvinduskýrslur skv. hluta 5.2 taka mið af starfsemi eftirlitsskyldra aðila.

6.2 Viðurlög

54. Tilmæli þessi hafa að geyma viðmið sem Fjármálaeftirlitið setur fram og styðst við vegna eftirlits með rekstraráhættu, með áherslu á rekstur upplýsingakerfa. Viðmiðin eru sett fram til nánari skýringar á þeim kröfum sem lög og stjórnvaldsfyrirmæli kveða á um varðandi rekstraráhættu hjá eftirlitsskyldum aðilum. Kröfurnar og viðmiðin liggja til grundvallar mati Fjármálaeftirlitsins á hlítingu við ákvæði um rekstraráhættu í sérlögum um starfsemi eftirlitsskyldra aðila. Fjármálaeftirlitið metur viðurlög við brotum á ákvæðum um rekstraráhættu í samræmi við viðurlagahluta hverra sérlaga fyrir sig.

7. Gildistaka

55. Þessi leiðbeinandi tilmæli öðlast gildi við birtingu og falla þá jafnframt úr gildi leiðbeinandi tilmæli um upplýsingakerfi eftirlitsskyldra aðila, nr. 2/2014. Tilkynningar vegna frávika, sbr. hluta 5.2, verða þó ekki sendar á uppfærðu formi fyrr en eftir 1. janúar 2020.