FJÁRMÁLAEFTIRLITIÐ
THE FINANCIAL SUPERVISORY AUTHORITY, ICELAND

Umræðuskjal

nr. 3/2012

Drög að leiðbeinandi tilmælum um rekstur upplýsingakerfa eftirlitsskyldra aðila

Umræðuskjalið er sent umsagnaraðilum og þeim gefinn kostur á að koma á framfæri umsögn vegna umræðuskjalsins eigi síðar en mánudaginn 28. maí nk. Skjalið er einnig birt á vefsíðu Fjármalaeftirlitsins www.fme.is

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

4. maí 2012

Inngangur

Fjármálaeftirlitið hefur eftirlit með starfsháttum eftirlitsskyldra aðila, skv. lögum um opinbert eftirlit með fjármálastarfsemi nr. 87/1998 og að þeir starfi í samræmi við þau lög og reglur sem um starfsemi þeirra gilda. Það hefur samkvæmt 2. mgr. 8. gr. sömu lagaheimild til að gefa út og birta opinberlega almenn leiðbeinandi tilmæli um starfsemi eftirlitsskyldra aðila.

Með leiðbeinandi tilmælum þessum er stefnt að því að samræmdar kröfur verði gerðar til allra eftirlitsskyldra aðila varðandi rekstur upplýsingakerfa og notkun upplýsingatækni.

Megintilgangur tilmælanna er að lágmarka rekstraráhættu eftirlitsskyldra aðila og stuðla að eftirfylgni eftirlitsskyldra aðila við lög og reglur er lúta að rekstri upplýsingakerfa. Tekið skal fram að tilmælum þessum er á engan hátt ætlað að koma í stað ákvæða laga og reglugerða er lúta að vernd persónuupplýsinga.

Lágmörkun áhættu við rekstur upplýsingakerfa er m.a. fólgin í því að gera ráðstafanir sem miða að því að stýra rekstraráhættu, koma í veg fyrir hagsmunaárekstra og tryggja gagnsæi á markaði. Einnig ber að tryggja öryggi upplýsinga, þ.e. 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 á að vera í samræmi við umfang rekstur eftirlitsskylds aðila og þá áhættu sem honum fylgir. Tilmælin gilda um alla eftirlitsskylda aðila en eðli máls samkvæmt hefur Fjármálaeftirlitið ástæðu til að gera ríkari kröfur til eftirlitsskyldra aðila með umsvifamikla og fjölþætta starfsemi en minni aðila með einfalda starfsemi. Því er gert ráð fyrir að smærri aðilum[1] dugi einfalt utanumhald, þó þeim beri að hafa þau sjónarmið að leiðarljósi sem fram koma í tilmælunum.

Samkvæmt 1. mgr. 8. gr. laga nr. 87/1998 um opinbert eftirlit með fjármálastarfsemi ber eftirlitsskyldum aðilum að haga starfsemi sinni í samræmi við heilbrigða og eðlilega viðskiptahætti. Jafnframt má af 2. mgr. 10. gr. laganna leiða skyldu sömu aðila til þess að halda hag og rekstri sínum heilbrigðum. Fjármálaeftirlitið telur að í framangreindu felist m.a. að eftirlitsskyldir aðilar framkvæmi árlegt sjálfsmat á upplýsingatækniumhverfi sínu. Á grundvelli 2. málsl. 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi fer Fjármálaeftirlitið fram á að sjálfsmatið sé sent eftirlitinu, eigi síðar en í október ár hvert, ásamt upplýsingum um mat á umfangi rekstrar og flækjustigi viðskiptakerfa.

Alþjóðlegir staðlar gilda á þessu sviði og einnig er töluvert til af leiðbeiningum um rekstur upplýsingakerfa. Má þar nefna ÍST ISO/IEC 27001 um upplýsingaöryggi, ISO 9000 gæðastaðalinn og CobiT. Í mörgum öðrum Evrópuríkjum hafa verið sett fram sambærileg tilmæli eða reglur og er tekið mið af þeim í tilmælum þessum.[2]

[1] Stærð aðila er ákvörðuð út frá fjölda starfsmanna, uppsetningu á rekstri upplýsingatæknikerfa og flækjustigi viðskiptahugbúnaðar. Sjálfsmatseyðublað er aðgengilegt í Skýrsluskilakerfi Fjármálaeftirlitsins.

[2] T.d. Noregur - http://www.finanstilsynet.no/en/,
Svíþjóð - http://www.fi.se/Folder-EN/Startpage/Regulations/,
Danmörk - http://www.finanstilsynet.dk/en.aspx,
Finnland - http://www.finanssivalvonta.fi/en/Regulation/Regulations/Financial_sector/Pages/Default.aspx og
England - http://fsahandbook.info/FSA/html/handbook/COBS/11/8

Efni leiðbeinandi tilmæla um rekstur upplýsingakerfa eftirlitsskyldra aðila

1. Gildissvið

1.1. Tilmælin taka til allra eftirlitskyldra aðila skv. 2. gr. laga nr. 87/1998 um opinbert eftirlit með fjármálastarfsemi. Í ofangreindu felst að þeir aðilar sem falla undir gildissvið tilmæla þessara geri viðeigandi ráðstafanir til þess að öll upplýsingakerfi sem hafa þýðingu fyrir eða áhrif á starfsemi fyrirtækisins séu starfrækt í samræmi við tilmælin.

1.2. Með upplýsingakerfi er átt við þau kerfi, vélræn og óvélræn, sem koma að vinnslu upplýsinga ásamt öllum tengingum að, frá og milli þeirra.

1.3. 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 áhrif á eða skipta máli fyrir rekstur eftirlitsskylda aðilans.

1.4. Ef veittur er utanaðkomandi aðgangur að upplýsingakerfum skal vera tryggt með skriflegum samningum að kröfur tilmælanna til öryggis og skjalfestingar séu uppfylltar.

2. Áhættugreining

2.1. Fjármálaeftirlitið beinir þeim tilmælum til eftirlitsskyldra aðila að þeir ákveði viðmið fyrir ásættanlega áhættu tengda notkun upplýsingatækni m.t.t. starfssviðs og flækjustigs viðkomandi aðila. Í því sambandi þarf jafnframt að endurskoða viðmiðin með reglubundnum hætti og greina áhættu af rekstri upplýsingakerfa.

2.2. Til þess að framangreint áhættugreiningarferli nái markmiði sínu telur Fjármálaeftirlitið að ábyrgð, m.a. að því er lýtur að eftirfylgni á ráðstöfunum sem grípa á til í kjölfar undangenginnar áhættugreiningar, þurfi að vera skilgreind með skýrum hætti. Jafnframt telur Fjármálaeftirlitið að eftirlitsskyldur aðili þurfi í því sambandi a.m.k. einu sinni á ári og auk þess í tengslum við breytingar sem skipta máli fyrir upplýsingaöryggi, fara í gegnum áhættugreiningu til þess að tryggja að áhættan sé innan viðmiða sem sett hafa verið fram sbr. 1 mgr. þessarar greinar.

2.3. Á grundvelli 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi fer Fjármálaeftirlitið fram á að niðurstaða áhættugreiningarinnar sé skjalfest og að henni verði skilað til Fjármálaeftirlitsins, eigi síðar en í október ár hvert.

3. Ábyrgð

3.1. Það er afstaða Fjármálaeftirlitsins að eftirlitsskyldur aðili beri ábyrgð á að rekstur upplýsingakerfa uppfylli allar kröfur sem til hans eru gerðar í tilmælum þessum. Þetta 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.

4. Skipulag og gæði

4.1. Mikilvægt er að eftirlitsskyldir aðilar setji sér stefnu þar sem ákveðin eru markmið og öryggiskröfur til reksturs upplýsingakerfa. Jafnframt, að fyrirliggjandi séu skriflegar lýsingar á öllum nauðsynlegum verkferlum fyrir rekstur og öryggi upplýsingakerfa.

4.2. Mikilvægt er að í slíkum lýsingum sé ábyrgðin á eftirfarandi atriðum, viðvíkjandi rekstri upplýsingatæknikerfa, ávalt tryggð:

4.2.1. Stjórnun
4.2.2. Öflun búnaðar
4.2.3. Þróun
4.2.4. Rekstri
4.2.5. Kerfisviðhaldi
4.2.6. Afritun
4.2.7. Öryggi upplýsinga
4.2.8. Innleiðingu
4.2.9. Niðurlagningu kerfa og búnaðar

4.3. Skjalfest og uppfærð lýsing á einstökum upplýsingakerfum sem hafa þýðingu fyrir starfsemi eftirlitsskylds aðila ætti ávalt að liggja fyrir.

4.4. Ef hluta upplýsingatækniverkefna eða þeim öllum er útvistað, ætti eftirlitsskyldur aðili að hafa eigin stefnumið sem tryggja afhendingu þjónustunnar, svo sem væri ef þjónustunni væri ekki útvistað. Í því sambandi er mikilvægt að tilnefndur sé ábyrgðaraðili fyrir ólíka þætti upplýsingatækniverkefna. Þó liggur endanleg ábyrgð ávalt hjá eftirlitsskyldum aðila.

4.5. Eftirlitsskyldur aðili ætti einnig að setja sér gæðamarkmið á einstökum sviðum upplýsingatækni og hafa til staðar skrifleg ferli til að fylgja eftir gæðamarkmiðunum og skrá frávik niður.

5. Öryggi

5.1. Fjármálaeftirlitið beinir þeim tilmælum til eftirlitsskyldra aðila að þeir komi áverkferlum sem tryggja vernd búnaðar, lagna, kerfa og upplýsinga sem eru mikilvæg rekstri aðilans, sbr. lið 1.2., fyrir:

5.1.1. Áföllum
5.1.2. Misnotkun
5.1.3. Óheimilum aðgangi
5.1.4. Óheimilum breytingum og skemmdarverkum.

5.2. Verkferlar vegna ofangreinds skulu að mati Fjármálaeftirlitsins taka til stjórnunar, úthlutunar, endurskoðunar og afturköllunar aðgangsheimilda að upplýsingakerfum, þ.m.t. færanlegum miðlum og upplýsingavinnslubúnaði. Kröfur til upplýsingaöryggis og reksturs kerfa skulu að mati Fjármálaeftirlitsins vera mælanlegar og frávik skráð. Tryggja þarf að framkvæmd sé rekjanleg. Eftirlitsskyldur aðili skal að mati Fjármálaeftirlitsins tryggja að starfsfólk hljóti fullnægjandi þjálfun og fræðslu varðandi upplýsingaöryggi og ábyrgð þeirra hvað varðar upplýsingaöryggi sé komið á framfæri með skipulögðum hætti.

5.3. Eftirlitsskyldur aðili þarf að mati Fjármálaeftirlitsins að tryggja fullnægjandi stjórn og stýringar séu til staðar fyrir netkerfi til að tryggja vernd fyrir ógnum og halda uppi öryggi fyrir þau kerfi og hugbúnað sem notar netið, þ.á m. upplýsingar í flutningi. Í því sambandi telur Fjármálaeftirlitið að koma þurfi á stýringum fyrir almenningsnet og þráðlaus net til þess að vernda kerfi og notendahugbúnað.

5.4. Mikilvægt er að eftirlitsskyldur aðili skal tryggi öryggi sitt gagnvart óværum og spillikóða (e. Malicious Code) með viðeigandi vörnum og eftirlitskerfum.

5.5. Til þess að markmið 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi náist, sbr. umfjöllun þar að lútandi í lið 9.1, telur Fjármálaeftirlitið að eftirlitsskyldur aðili skuli koma á verkferlum til þess að vernda skjöl, gögn og gagnamiðla gegn óheimilli uppljóstrun, breytingum, brottflutningi og eyðileggingu. Meðal færanlegra miðla eru m.a. snjallsímar, spjald- og fartölvur, segulbönd, seguldiskar, minnislyklar, minniskort, færanleg harðdisksdrif, geisladiskar, stafrænir mynddiskar, innbyggðar minniseiningar tækjabúnaðar og aðrir sambærilegir miðlar.

6. Rekstur kerfa

6.1. Fjármálaeftirlitið beinir þeim tilmælum til eftirlitsskyldra aðila að skriflegir verkferlar liggi til grundvallar rekstri upplýsingakerfa.

6.2. Verkferlarnir skulu tryggja fullnægjandi og rétta gagnavinnslu, meðhöndlun og geymslu á gögnum ásamt aðgengi að upplýsingakerfum, sbr. 9 lið tilmæla þessara um vörslu og meðhöndlun gagna.

6.3. Mikilvægt er að eftirlitsskyldur aðili tryggi viðhald og umsjón upplýsingakerfa þannig að rekstur þeirra sé stöðugur og í samræmi við áætlanir.Viðhald þarf að vera unnið eftir skriflegum verkferlum sem hafa í för með sér traustan, skipulagðan og fyrirsjáanlegan rekstur upplýsingakerfa.

7. Þróun og viðhald kerfa

7.1. Mikilvægt er að eftirlitsskyldur aðili hafi skriflega verkferla fyrir öflun, þróun og prófanir á upplýsingakerfum.

7.2. Ábyrgðaraðili upplýsingatæknikerfis skv. lið 3.1 skal þarf að gefa samþykki sitt fyrir notkun og/eða fyrir innleiðingu breytinga á kerfinu áður en það er tekið í notkun eða breyting er framkvæmd.

7.3. Verkferlar sem fjalla um breytingar þurfa að taka til allra breytinga sem geta haft áhrif á upplýsingakerfi og þurfa að tryggja viðeigandi, formlega meðhöndlun ásamt skráningu. Jafnframt þurfa verkferlar að taka á úthlutun og afturköllun aðgangsheimilda að þeim tölvuumhverfum er innihalda raungögn sem notuð eru fyrir þróun eða í prófanir.

7.4. Skrá þarf öll þau frávik sem að upp koma þegar kerfi eru tekin í notkun eða breytingar framkvæmdar í raunumhverfi sbr. lið 8.4.

8. Frávik

8.1. Mikilvægt er að eftirlitsskyldur aðili skal fylgi skriflegum ferlum sem taka til meðhöndlunar frávika.

8.2. Ferlarnir þurfa að taka til frávika sem verða í rekstri upplýsingakerfa.

8.3. Markmið meðhöndlunar frávikanna skal vera að koma aftur á eðlilegu rekstrarástandi, finna orsakir frávika og koma í veg fyrir að þau endurtaki sig.

8.4. Mikilvægt er að eftirlitsskyldur aðili viðhafi rafræna skráningu frávika.

8.5. Með vísan til 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi nr. Tilkynna þarf öll frávik sem tilheyra broti á varðveislu, leynd, réttleika gagna og tiltækileika upplýsingakerfa og gagna til Fjármálaeftirlitsins. Komi upp tilfelli þar sem að reksturinn stöðvast vegna frávika skal skrá þau sérstaklega og tilkynna til Fjármálaeftirlitsins.

9. Varðveisla og meðhöndlun gagna

9.1. Í 1. mgr. 9. gr. laga nr. 87/1998 um opinbert eftirlit með fjármálastarfsemi er kveðið á um að Fjármálaeftirlitið skuli athuga rekstur eftirlitsskyldra aðila svo oft sem þurfa þykir. Þeim er skylt að veita eftirlitinu aðgang að öllu bókhaldi sínu, fundargerðum, skjölum og öðrum gögnum í vörslu þeirra er varða starfsemina sem FME telur nauðsynlegan. Jafnframt getur Fjármálaeftirlitið skv. ákvæðinu óskað upplýsinga á þann hátt og svo oft sem það telur þörf á.

9.2. Til þess að markmið áðurgreinds ákvæðis um aðgang Fjármálaeftirlitsins að gögnum eftirlitsskyldra aðila náist er mikilvægt að öll þau gögn sem eftirlitið kann að óska eftir séu til staðar þá og þegar krafa um upplýsingar er sett fram. Þar af leiðandi telur Fjármálaeftirlitið að varðveisla og meðhöndlun gagna af hálfu eftirlitsskyldra aðila þurfi að uppfylla eftirfarandi skilyrði:

9.2.1. Gerð séu öryggisafrit af gögnum og upplýsingakerfum.
9.2.2. Fyrirkomulag og verklag afritunar sé með viðurkenndum og skipulegum hætti, skjalfest og innihaldi m.a. lýsingu á geymslutíma og staðsetningu afrita.
9.2.3. Afrit af upplýsingakerfum sem innihalda viðskiptaupplýsingar, og samskipti þeim tengdum, séu tiltæk á afritum að lágmarki 5 ár frá uppruna skráningar, þ.m.t. afritunarkerfi sem þarf til að endurheimta gögnin.

9.3. Undir ofangreind kerfi falla öll þau upplýsingakerfi eftirlitsskylds aðila sem innihalda skráningar og gögn er varða viðskipta- og fjárhagsupplýsingar. Ennfremur er hér átt við öll upplýsinga- og samskiptakerfi er tengjast viðskiptum, s.s. tölvupóstur, símkerfi, farsímar, föx, snarspjall eða annarskonar samskiptakerfi, auk annarra gagna sem innihalda viðskiptafyrirmæli. Í ljósi ofangreinds telur Fjármálaeftirlitið enn fremur að eftirlitsskyldum aðilum beri að hljóðrita öll símtöl sem innihalda viðskiptaupplýsingar.

9.4. Ofangreind afrit geta verið nauðsynleg Fjármálaeftirlitinu til 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 sem og eftirlitsákvæðum einstakra sérlaga. Í ljósi alls þess sem að ofan greinir og vegna þess að ekki er víst að fyrir liggi, þegar afrit eru gerð,

hvort eða hvenær Fjármálaeftirlitið muni óska eftir tilteknum gögnum er mikilvægt að gögnin séu geymd um tiltekin tíma. Fjármálaeftirlitið telur í þessu sambandi að öryggisafrit skuli ekki geymd skemur en fimm ár.[3]

9.5. Til þess að tryggja öryggi og trúverðugleika þeirra gagna sem í öryggisafritum eru geymd er mikilvægt að öryggisafrit séu þannig úr garði gerð að:

9.5.1. Notendur geti ekki endanlega eytt skjölum, færslum, skilaboðum eða samskiptasögu úr viðkomandi upplýsingakerfum. Afrit sem tekin eru innihaldi allar færslur viðskiptakerfa, skjöl, símtöl, tölvupóst, skilaboð, eða sambærileg gögn, í samfelldri og rekjanlegri tímaröð.
9.5.2. Afrit séu ritvarin með þeim hætti að ekki sé mögulegt að eyða eða breyta þeim fyrir mistök á nokkurn hátt.
9.5.3. Aðgengi að afritum sé takmarkað við samþykkta aðila.
9.5.4. Tryggt sé að þau séu læsileg til loka geymslutímans.
9.5.5. Afrit séu vistuð á viðurkenndum stað í hæfilega öruggri fjarlægð frá frumgögnum.

9.6. Afrit séu tiltæk eftirlitsaðilum með skömmum fyrirvara og aðgengi að tilteknum gögnum sé vera fyrirhafnarlítið.Fyrirkomulag og verklag afritunar þarf að mati Fjármálaeftirlitsins að innihalda reglubundið eftirlit með því að afrit séu samkvæmt skjalfestu verklagi, nothæf og aðgengileg. Því þarf reglulega að framkvæma endurheimt gagna af afriti til staðfestingar á virkni og tryggja að öll umrædd gögn og kerfi séu sannarlega afrituð.

9.7. Til þess að eftirlitsskyldur aðili geti sýnt fram á að ofangreint verklag sé viðhaft þarf framkvæmdin að vera skjalfest og staðfest með formlegum hætti. Jafnframt þarf skjölun að innihalda markmið, lýsingu á framkvæmd og með hvaða hætti nothæfi gagna var staðfest.

9.8. Til þess að eftirlitsskyldur aðili geti uppfyllt þau tilmæli sem nefnd eru í liðum 9.1-9.8 hér á undan er nauðsynlegt að einungis séu notuð þau upplýsingakerfi til skráningar viðskipta, eða til samskipta vegna viðskipta sem eftirlitsskyldur aðili hefur fulla lögsögu og stjórn yfir og getur afritað.

9.9. Samkvæmt 19. og 20. gr. laga nr. 145/1994 um bókhald er bókhaldsskyldum aðilum skylt að geyma með skipulögðum hætti ýmis bókhaldsgögn sem þýðingu hafa í rekstri hans í a.m.k. sjö ár frá lokum viðkomandi reikningsárs. Til þess að markmið ákvæðisins um aðgang að upplýsingum í bókhaldsgögnum sé tryggt beinir Fjármálaeftirlitið þeim tilmælum til eftirlitsskyldra aðila, sem einnig eru bókhaldsskyldir, að öryggisafrit séu tekin af þeim bókhaldsgögnum sem geyma ber.

10. Viðbúnaðarumgjörð

10.1. Fjármálaeftirlitið telur það lið í eðlilegum viðskiptaháttum og heilbrigðum rekstri, sbr. 1. mgr. 8. gr. og 2. mgr. 10. gr. laga um opinbert eftirlit með fjármálastarfsemi að eftirlitskyldur aðili geri ráð fyrir mögulegum áföllum sem geta valdið rekstrarstöðvun með þeim afleiðingum að rekstur upplýsingakerfa geti ekki haldið áfram. Þar af leiðandi telur Fjármálaeftirlitið að eftirlitsskyldur aðili skuli koma á

[3] Sjá til hliðsjónar 2. mgr. 10. gr. laga um verðbréfaviðskipti nr. 108/2007, sbr. einnig 50. gr. reglugerðar um fjárfestavernd og viðskiptahætti fjármálafyrirtækja nr. 995/2007.

heildstæðri umgjörð um stjórnun varðandi samfelldan rekstur þar sem skilgreind eru hlutverk, ábyrgð, verkefni og áhættur.

10.2. Á grundvelli áhættugreiningar, sbr. lið 2, telur FME mikilvægt að skilgreind séu þau upplýsingakerfi sem eru mikilvæg starfsemi aðilans og umgjörðin skal taka til.

10.3. Umgjörðin skal að mati Fjármálaeftirlitsins m.a. taka til eftirfarandi atriða:

10.3.1. Greiningu og mats á þá einstöku þætti sem geta brugðist og til hvaða viðeigandi ráðstafana skuli grípa.
10.3.2. Skýr viðmið skulu sett um hvenær grípa skuli til varalausna.
10.3.3. Endurheimtuferla.
10.3.4. Upplýsingagjöf til stjórnar, starfsmanna, viðskiptamanna og annarra aðila sem vitneskju þurfa að hafa um rekstrarstöðvun.

10.4. Mikilvægt er að umgjörðin sé í samræmi við stærð og umfang eftirlitsaðilans.

10.5. Endurskoða og uppfæra þarf umgjörðina reglulega.

10.6. Mikilvægt er að eftirlitskyldur aðili hafi skjalfesta viðbúnaðaráætlunin eða neyðaráætlun, sem skal grípa til í kjölfar áfalls sem veldur rekstrarstöðvun upplýsingakerfa. Áföll teljast þeir atburðir sem valda því að afkastageta upplýsingakerfa sé skert.

10.7. Áætlunin skal að mati Fjármálaeftirlitsins m.a. innihalda eftirfarandi atriði:

10.7.1. Yfirsýn yfir upplýsingakerfin sem tilheyra áætluninni.
10.7.2. Lýsingu á áfallalausnum.
10.7.3. Skýr viðmið um gangsetningu á áfallalausnum.
10.7.4. Ásættanleg tímamörk rekstrarstöðvunar áður en gripið er til áfallalausna.
10.7.5. Verkferlum til að koma rekstri upplýsingakerfa aftur í gang.
10.7.6. Yfirsýn yfir ábyrgðarsvið og gangsetningaferla áfallalausna.
10.7.7. Upplýsingagjöf til stjórnar, starfsmanna, birgja, viðskiptavina, opinberra stjórnvalda og fjölmiðla.

10.8. Mikilvægt er að áætluninni sé framfylgt með kennslu, æfingum og prófunum á varalausnum sem tryggja að þær virki eins og til er ætlast, eftir því sem við á. Jafnframt er mikilvægt að prófanir séu skjalfestar þannig að hægt sé að leggja mat á framkvæmd og árangur.

11. Útvistun

11.1. Fjármálaeftirlitið beinir þeim tilmælum til eftirlitsskyldra aðila að hafa stefnu varðandi útvistun sem tekur á hvaða þáttum í rekstri upplýsingatæknikerfa megi útvista og hvert megi útvista þeim.

11.2. Sé valið að útvista hýsingu gagna til þriðja aðila beinir Fjármálaeftirlitið þeim tilmælum til eftirlitsskyldra aðila að þeir gæti þess ávalt tryggja að Fjármálaeftirlitið hafi óhindrað aðgengi að þeim gögnum.

11.3. Kjósi eftirlitsskyldur aðili að útvista til erlends aðila fer Fjármálaeftirlitið fram á að vera upplýst fyrirfram um slíka útvistun ásamt því að veita nauðsynlegar upplýsingar um hvert eftirlitið geti sótt viðkomandi gögn ef þörf krefur.

Nauðsynlegar upplýsingar í þessu sambandi eru t.d. upplýsingar um útvistunaraðila, land hans og heimilisfang, upplýsingar um hvar gögnin verða vistuð, upplýsingum um tengiliði hjá útvistunaraðila og staðfesting á því að útvistunaraðili sé upplýstur um að Fjármálaeftirlitinu sé heimill aðgangur að þeim gögnum sem um ræðir.

11.4. Með vísan til markmiðs 1. mgr. 9. gr. laga um opinbert eftirlit með Fjármálastarfsemi, sbr. einnig umfjöllun í lið 9.1 hér á undan beinir Fjármálaeftirlitið þeim tilmælum til eftirlitsskyldra aðila að þeir keðjuútvisti ekki hýsingu á upplýsingakerfum og gögnum, hvorki að hluta né öllu leyti.

11.5. Með keðjuútvistun í lið 11.4 er átt við þegar útvistun á upplýsingatæknikerfum eftirlitsskylds aðila til hýsingaraðila er áfram útvistað frá hýsingaraðila til þriðja aðila. Það telst ekki keðjuútvistun þegar um er að ræða útvistun innan samstæðu.

11.6. Skriflegur samningur við útvistunaraðila skal að mati Fjármálaeftirlitsins innihalda að lágmarki:

11.6.1. Ákvæði um hvaða þjónustu vistunaraðili skal inna af hendi (Service Level Agreement).
11.6.2. Ákvæði um rétt eftirlitsskylds aðila til eftirlits með þeirri starfsemi vistunaraðilans sem samningurinn tekur til.
11.6.3. Ákvæði um þagnarskyldu vistunaraðila og starfsmanna hans til samræmis við þagnarskyldu þá sem hvílir á hinum eftirlitsskylda aðila.
11.6.4. Ákvæði um heimild Fjármálaeftirlitsins til aðgangs að gögnum og upplýsingum eftirlitsskylda aðilans hjá vistunaraðila
11.6.5. Ákvæði um að að athuganir, sem Fjármálaeftirlitið telur vera nauðsynlegan lið í eftirliti með eftirlitsskylda aðilanum, geti farið fram á vinnustöð vistunaraðila.

11.7. Í tengslum við síðastgreind ákvæði liðar 11 telur Fjármálaeftirlitið mikilvægt að eftirlitsskyldur aðili gæti þess, með eigin aðgerðum eða formlegu samstarfi við aðra aðila en vistunaraðilann, að hann búi yfir nægilegri þekkingu (tæknilegri og lagalegri) til að gera útvistunarsamninginn.

11.8. Mikilvægt er að eftirlitsskyldur aðili tilnefni ábyrgðaraðila á kröfum þeim sem til hans eru gerðar skv. liðum 11.1 – 11.5.

11.9. Það er afstaða Fjármálaeftirlitsins að útvistun á ábyrgð á að framkvæmd sé í samræmi við efni laga og reglna sem um starfsemina gilda, þ.m.t. efni þessara leiðbeinandi tilmæla, sé útvistað

11.10. Stjórnunarlegri ábyrgð verður að mati Fjármálaeftirlitsins ekki útvistað.

12. Skráning

12.1. Á grundvelli 1. mgr. 9. gr. laga um opinbert eftirlit með fjármálastarfsemi fer Fjármálaeftirlitið fram á að eftirlitsskyldir aðilar skili til Fjármálaeftirlitsins upplýsingum um upplýsingatækniumhverfi og rekstur upplýsingakerfa samhliða mati á flækjustigi, sbr. lið 1. Skjalfest, uppfærð lýsing á einstökum upplýsingakerfum, sem hafa þýðingu fyrir starfsemi eftirlitsskylds aðila skal jafnframt liggja fyrir.

12.2. Fjármálaeftirlitið beinir þeim tilmælum til eftirlitsskyldra aðila að þeir fái þriðja aðila til að taka út hjá sér öll þau atriði sem að tilmæli þessi tilgreina og skila inn skýrslu til Fjármálaeftirlitsins árlega. Mikilvægt er að framkvæmd úttektar þriðja aðila skv. lið 12.1 sé með skipulögðum og markvissum hætti og fylgi almennt þekktri og viðurkenndri aðferðafræði.