FJÁRMÁLAEFTIRLITIÐ
THE FINANCIAL SUPERVISORY AUTHORITY, ICELAND

Samantekt umsagna vegna umræðuskjals nr. 3/2012

Umsagnir bárust frá eftirtöldum aðilum:

1. Íslandsbanka
2. Kortaþjónustunni hf.
3. Lánasjóður sveitarfélaga
4. Landsbankinn hf.
5. Landssamtök Lífeyrissjóða
6. Skipti hf.
7. T plús hf.
8. Kauphöll Íslands hf.
9. Reiknistofa bankanna
10. Verðbréfaskráningu Íslands hf.

Umsagnir aðila sem óska eftir trúnaði er ekki að finna í þessari samantekt. Umræðuskjal nr. 3/2012 varð að leiðbeinandi tilmælum nr. 1/2012 um upplýsingakerfi eftirlitsskyldra aðila.

Nr.	Nafn umsagnaraðila	Tilvísun	Umsögn
1	Íslandsbanki	2.3	í tölulið 2.3. segir: "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. " Áhættumat af þessu tagi er í eðli sínu viðkvæmt og óæskilegt að það sé sent úr húsi. Þótt slík gögn séu að sjálfsögðu aðgengileg Fjármálaeftirlitinu í vettvangsathugunum er hætt við að vitneskja um að það sé að staðaldri sent eftirlitsaðilum kunni að hafa neikvæð áhrif á sjálft áhættumatið, þar sem starfsmenn kynnu að vera tregari til að benda á veikleika og það vinni því á endanum gegn tilgangi áhættumatsins. Ekki verður í fljótu bragði séð að gildandi tilmæli norska fjármálaeftirlitsins, Finanstilsynet, geri ráð fyrir að áhættumatinu sé skilað inn, heldur aðeins að það sé fyrirliggjandi og reglulega yfirfarið.
2	Íslandsbanki	8.5	í tölulið 8.5. segir: "Með vísan till. 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. ,,Orðalagið ber með sér að tilkynna eigi hverskonar frávik til Fjármálaeftirlitsins. Telja verður að svo umfangmikil tilkynningarskylda geti reynst verulega íþyngjandi ogvandséð er að hún sé til þess fallin að styrkja opinbert eftirlit. Eðlilegt er að ef Fjármálaeftirlitið hyggst krefjast slíkra tilkynninga, þá verði sú tilkynningarskylda skýrt afmörkuð og bundin við alvarleg frávik. Norska fjármálaeftirlitið hefur sett fram leiðbeiningar um slíka skýrslugjöf á heimasíðu sinni.2 í 2. tölulið þeirra leiðbeininga er notað orðalagið "atburðir sem leiða til verulega minnkandi virkni" og það nánar útskýrt með dæmum.
3	Íslandsbanki	9.2.3. og 9.4.	í töluliðum 9.2.3. og 9.4. er talað um 5 ára geymslutíma, en í tölulið 9.9 er rætt um sjö ára geymslutíma. Þetta misræmi, sem í raun hlýst af mismunandi framsetningu í bókhaldslögum annarsvegar og verðbréfaviðskiptalögum hinsvegar, er óheppilegt og ekki til þess fallið að eyða óvissu um geymslutímakröfur.
4	Íslandsbanki	9.3	í tölulið 9.3. segir m.a.: "í ljósi ofangreinds telur Fjármálaeftirlitið enn fremur að eftirlitsskyldum aðilum beri að hljóðrita öll símtöl sem innihalda viðskiptaupplýsingar. " Þetta þýðir í reynd að hljóðrita þyrfti alla borðsíma, auk farsíma starfsmanna – enda líklegt að viðskiptaupplýsingar komi fram í símtölum í flesta síma. Hinsvegar hefur hingað til verið horft til þeirra eininga sem taka á móti viðskiptafyrirmælum þegar ákvarðað er hvernig staðið skuli að hljóðritunum. Verklagsreglur taka hinsvegar á því ef viðskiptafyrirmæli eru móttekin í síma sem ekki eru hljóðritaðir. Eðlilegt væri að tilmælin tækju mið af þeirri framkvæmd.
5	Íslandsbanki	9.5.5	í tölulið 9.5.5. er notað orðalagið "viðurkenndur staður" í "hæfilega öruggri fjarlægð". Æskilegt væri að Fjármálaeftirlitið skýrði nánar hvað átt er við með þessum hugtökum. Hvaða kröfur er í raun verið að gera?

6	Íslandsbanki	9.8	í tölulið 9.8. segir: *"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 efritað. "* Þetta orðalag er með þeim hætti að útvistun upplýsingakerfa verður með öllu óframkvæmanleg. Eðli máls samkvæmt mun eftirlitsskyldur aðili aldrei hafa fulla lögsögu og stjórn yfir kerfum sem úthýst eru og í flestum tilfellum er þjónustuaðila treyst fyrir fullnægjandi afritatöku. Eftirlitsskyldi aðilinn getur aðeins reynt að viðhafa eftirlit með því að eftirlitsferlar þjónustuaðilans virki eins og til er ætlast og gæðiþjónustunnar uppfylli þær væntingar sem gerðar eru til hennar. Einföld dæmi um þetta eru gagnaflutningar í gegnum þjónustu fjarskiptafyrirtækja, sem sjá þjónustuþegum fyrir margvíslegum tengileiðum. S.W.I.F.T. samskiptakerfið er annað dæmi um kerfi sem notendur hafa í raun enga stjórn á sjálfir, en er þrátt fyrir það lofað að ýmsum öryggiskröfum sé fullnægt. Hýsing búnaðar hjá þriðja aðila hlýtur ávallt að fela í sér að þjónustukaupi missi stjórn og lögsögu að einhverju marki, þótt ábyrgð hans á verkefninu sé áfram til staðar.
7	Íslandsbanki	9.9	í tölulið 9.9. er sérstaklega beint "tilmælum til eftirlitsskyldra aðila, sem einnig eru bókhaldsskyldir, að öryggisafrit séu tekin af þeim bókhaldsgögnum sem geyma ber. " Orðalagið hefur vakið spurningar um það hvort hér sé einnig átt við að pappírsgögn séu afrituð, þ.e. ljósrituð og/eða skönnuð, en slíkt gæti reynst verulega íþyngjandi og kallar á breytt verklag.
8	Íslandsbanki	11.4	í tölulið 11.4. " ... beinir Fjármálaeftirlitið þeim tilmælum til eftirlitsskyldra aðila að þeir keðjuútvisti ekki hýsingu á upplýsingakerfum og gögnum, hvorki að hluta né öllleyti. " Ljóst er að þetta ákvæði mun geta haft veruleg og íþyngjandi áhrif á fyrirkomulag útvistunar í dag. Jafnframt getur verið erfitt að tryggja framfylgd slíks ákvæðis í reynd.
9	Íslandsbanki	12.1	í tölulið 12.1. "fer Fjármálaeftirlitið fram á að eftirlitsskyldir aðilar skili til Fjármálaeftirlitsins upplýsingum um upplýsingatækniumhverfi og rekstur upplýsingakerfa samhliða mati á flækjustigi ... " Tíðni, umfang og form þessarar skilaskyldu er ekki ljóst og þarfnast nánari skýringa við. Ef upplýsingarnar eru of viðamiklar er ljóst að veiting þeirra felur í sér öryggisveikleika fyrir viðkomandi fjármálastofnun.
10	Íslandsbanki	12.2	í tölulið 12.2. segir: "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. " Hér er um nýmæli að ræða, sem virðist fela í sér að ráða þurfi ytri aðila til að framkvæma slíka yfirferð. Bent er á að slíkar kannanir eru á verksviði innri endurskoðunardeilda, sbr. tölulið 8.8. í leiðbeinandi tilmælum nr. 3/2008 um störf endurskoðunardeildar fjármálafyrirtækja. Hjá Innri endurskoðun íslandsbanka starfa tveir faggiltir tölvuendurskoðendur ("Certified Information

			Systems Auditor"), auk tölvunarfræðings með mastersgráðu í reikningshaldi, og er vandséð að ytri aðili sé betur í stakk búinn til að meta fylgni bankans við tilmælin. Hér er því um að ræða verulegan viðbótarkostnað við eftirlit án þess að því fylgi virðisauki umfram það eftirlit sem þegar er fyrir hendi. Eftir sem áður getur hver aðili um sig ákveðið að leita til ytri aðila varðandi sérhæfða aðstoð á þessu sviði ef hann hefur ekki yfir að ráða viðeigandi þekkingu. Meginreglan við innleiðingu eftirlitsþátta er að ávinningur af notkun þeirra sé mein en kostnaður sem af þeim hlýst. Það er því mikilvægt að Fjármálaeftirlitið gæti meðalhófs þegar nýjar kröfur eru settar varðandi upplýsingagjöf. Má í því sambandi einnig vísa til laga nr. 27/1999 um opinberar eftirlitsreglur, en þar segir í 3. gr.: "Þegar eftirlitsreglur eru samdar eða stofnað er tilopinbers eftirlits skal viðkomandi stjórnvald meta þörf fyrir eftirlit, gildi þess og kostnað þjóðfélagsins af því. Slíkt mat getur m.a. falist í áhættumati, mati á alþjóðlegum skuldbindingum um eftirlit, mati á kostnaði opinberra aðila, fyrirtækja og einstaklinga, mati á hvort ná megi sama árangri með hagkvæmari aðferðum eða mati á þjóðhagslegu gildi eftirlits. "
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
11	Kortaþjónustan hf.	Almenn athugasemd	í inngangskafla umræðuskjalsins kemur fram að umfang aðgerða til að tryggja öryggi upplýsingakerfa eigi að vera í samræmi við umfang rekstrar eftirlitsskylds aðila og þá áhættu er honum fylgi. Þótt tilmælin gildi um alla eftirlitsskylda aðila hafi Fjármálaeftirlitið ástæðu til að gera ríkari kröfur til eftirlitsskyldra aðila með umsvifamikla og fjölþætta starfsemi en minni aðila með einfalda starfsemi. Því sé gert ráð fyrir að smærri aðilum dugi einfalt utanumhald, þó þeim beri að hafa þau sjónarmið að leiðarljósi sem fram koma í tilmælunum. í þessu sambandi er vísað til sjálfsmatseyðublaðs sem sé aðgengilegt í Skýrsluskilakerfi Fjármálaeftirlitsins. Kortaþjónustan hf. er mjög hlynnt því að greint verði á milli aðila með framangreindum hætti en telur eigi að síður ýmislegt í umræðuskjalinu vera óljóst í þessum efnum. Þannig sé óljóst hvernig eftirlitsskyldur aðili eigi að notfæra sér tilmælin sem leiðbeinandi, þrátt fyrir að stærð hans samkvæmt sjálfmatseyðublaði og þeim viðmiðum sem tilgreind eru í því sambandi liggi fyrir. Erfitt er t.d. að átta sig á því hvað felst í því orðalagi að smærri aðilum dugi "einfalt utanumhald" enda er það orðalag afar matskennt. Breytir þar engu þótt í umræðuskjalinu sé tekið fram að smærri aðilum með einfalt utanumhald "beri að hafa þau sjónarmið að leiðarljósi sem fram koma í tilmælunum" enda er það orðalag að sama skapi einnig mjög matskennt. Hér þarf að hafa í huga að tilmælum Fjármálaeftirlistins er ætlað að vera leiðbeinandi og verður því að gera ríkar kröfur um skýrleika slíkra tilmæla þannig að eftirlitsskyldur aðili geti sem best nýtt sér þau og uppfyllt. Sem fyrr greinir er Kortaþjónustan hf. hlynnt tillögu umræðuskjalsins um að í tilmælunum verði greint milli stærri og smærri aðila en telur með vísan til framangreinds óskýrleika að heppilegra væri að í efnislegri skiptingu tilmælanna væri beinlínis greint milli þessara aðila og tilgreindar með mun nákvæmari

			hætti þær kröfur sem tilmælin gera til hvors hóps um sig. Með slíkri skiptingu gæti viðkomandi, að undangengnu sjálfsmati, betur áttað sig á þeim kröfum sem til hans eru gerðar samkvæmt tilmælunum í stað þess að veikjast í vafa um hvað felist í "einföldu utanumhaldi" og að hvaða leyti, ef hann samkvæmt sjálfsmati telst vera smærri aðili, honum beri einungis "að hafa þau sjónarmið að leiðarljósi sem fram koma í tilmælunum". Að þessu sögðu skal það tekið fram að Kortaþjónustan hf. telur einkum brýnt þegar greint er á milli stærri og smærri aðila í tilmælunum að sérstaklega verði litið til þeirra þátta sem teljast umfangsmiklir og kostnaðarsamir og því sér í lagi íþyngjandi fyrir smærri aðila, sbr. t.d. úttekt þriðja aðila og árleg skýrsla til Fjármálaeftirlitsins, sbr. 3. tölul. hér að neðan. Slakað verði á kröfum tilmælanna til smærri aðila vegna þessara þátta.
12	Kortaþjónustan hf.	9.3	í lokamálsl. greinar 9.3. kemur fram að Fjármálaeftirlitið telji að eftirlitsskyldum aðilum beri að hljóðrita öll símtöl sem innihalda viðskiptaupplýsingar. Af þessu tilefni vill Kortaþjónustan hf. nefna að þrátt fyrir að í eðli sínu sé einfalt að hljóðrita símtöl þá þyrfti hljóðritun sú sem hér um ræðir að gerast innan PCI (e. Payment Card Industry) umhverfis hins eftirlitsskylda aðila þar sem vera kann að tekið sé við kortaupplýsingum símieiðis. í slíkum tilvikum verður hljóðritun umtalsvert flóknari og íþyngjandi einkum fyrir minni rekstraraðila. Hljóðritun sem þessi gengur ennfremur gegn öryggisstaðli alþjóðlegu kortafyrirtækjanna Visa International og MasterCard International, eða svo kölluðum PCI DSS staðli (e. Payment Card Industry Data Security Standard) en þar er áskilið að einungis skuli varðveita kortaupplýsingar þegar rík ástæða kann að vera fyrir hendi. í þessu sambandi er einnig rétt að taka fram að Kortaþjónustan hf. tekur aldrei við viðskiptafyrirmælum símleiðis heldur þurfa slik fyrirmæli ávallt að berast með sannanlegum hætti, t.d. með tölvupósti eða á faxi. Öðru máli kann að gegna ef eftirlitsskyldur aðili tekur við fyrirmælum sem þessum símieiðis. Með framangreind sjónarmið í huga telur Kortaþjónustan hf. að í tilmælunum skuli, þegar kemur að hljóðritun símtala, greina milli þeirra aðila sem annars vegar taka á móti viðskiptafyrirmælum símleiðis og hinna sem gera það ekki. Þeir síðarnefndu skuli undanþegnir því að hljóðrita símtöl.
13	Kortaþjónustan hf.	12.2	í grein 12.2. beinir Fjármálaeftirlitið þeim tilmælum til eftirlitsskyldra aðila að þeir fái þriðja aðila til að taka út hjá sér öll þau atriði sem tilmælin tilgreina og jafnframt að skila í þessu sambandi árlegri skýrslu til eftirlitsins. Kortaþjónustan hf. telur áskilnað sem þennan afar íþyngjandi enda geti úttekt sem þessi reynst afar umfangsmikil og kostnaðarsöm, einkum fyrir smærri aðila. Því sé afar mikilvægt að undanþiggja smærri aðila þessari kröfu eftirlitsins. Með ti!liti til þeirra sjónarmiða sem rakin eru hér að framan undir 1. tölul. er auk þess óljóst hvaða atriði skuli lögð áhersla á í úttekt sem þessari eftir því hvort starfsemi eftirlitsskylds aðila telst umsvifamikil og fjölþætt eða smærri í sniðum þar sem dugi "einfalt utanumhald" og þar sem hafa beri "þau sjónarmið að leiðarljósi sem fram koma í tilmælunum".

Nr.	Nafn umsagnaraðila	Tilvísun	Umsögn
14	Lánasjóður sveitarfélaga ohf.	Almenn athugsemd	í upphafi skal tekið fram að lánasjóðurinn telur það verðugt markmið að setja leiðbeinandi tilmæli um rekstur upplýsingakerfa til að lágmarka rekstraráhættu. Hins vegar verður við slíka vinnu að hafa í huga að tilmælin eru leiðbeinandi, að upplýsingakerfi bjóða upp á mismunandi lausnir og eftirlitsskyldir aðilar eru margir, misstórir, í ólíkum rekstri og með mismunandi þarfir. Setning leiðbeinandi tilmæla er stjórnsýslathöfn, sem lýtur óskráðum meginreglum stjórnsýsluréttar s.s. lögmætisreglu, rannsóknarreglu og meðalhófsreglu. Hér verður sérstaklega vikið að lögmætisreglu, en í umfjöllun um einstaka kafla má sjá að lánasjóðurinn telur ekki augljósa eða rökstudda þörf fyrir ýmsum ákvæðum tilmælanna, og telur að til viðbótar skorti að gætt sé meðalhófs. a) Lögmætisreglan Fjármálaeftirlitinu er heimilt að gefa út og birta opinberlega almenn leiðbeinandi tilmæli um starfsemi hóps eftirlitsskyldra aðila, sbr. 2. mgr. 8. gr. laga nr. 87/1998. Af lögskýringargögnum er ljóst að leiðbeinandi tilmælum var ekki ætlað að vera skuldbindandi eins og ákvæði reglugerða og reglna sem settar eru með sérstakri heimild í lögum.' Þetta sjónarmið var ítrekað í áliti Umboðsmanns Alþingis (mál nr. 581512009), en þar kom fram að tilmæli Fjármálaeftirlitsins á framangreindum grunni séu aðeins)eiðbeinandi". Athafnir stjórnvalda, s.s. stjórnvaldsfyrirmæli, verða ávallt að samrýmast lögmætisreglunni, auk annarra réttaröryggisreglna. Með leiðbeinandi tilmælum getur Fjármálaeftirlitið ekki sett "reglur", þar sem slík tilmæli geta ekki verið sjálfstæður grundvöllur réttarreglna. Einnig geta slík tilmæli geti ekki lagt íþyngjandi skyldur á eftirlitsskylda aðila eða verið skuldbindandi sem slík. Þannig er ljóst að efni leiðbeinandi tilmæla þurfa að vera í samræmi við efnisákvæði í lögum á starfssviði Fjármálaeftirlitsins. Þegar um íþyngjandi ákvæði er að ræða, verður að gera ríkar kröfur til þess að lagaheimildir séu skýrar og afdráttarlausar. Að mati lánasjóðsins eru "tilmælin" í raun reglur, án þess að skýr og afdráttarlaus lagaheimild sé fyrir mörgum efnisákvæðum þeirra. Jafnframt er óljóst hvernig tilmælin samrýmast ákvæðum laga um persónuvernd og meðferð persónuupplýsinga nr. 7712000 og reglna settra á grundvelli þeirra. b) Heilbrigðir og eðlilegir viðskiptahættir í inngangskafla . tilmælanna" er sérstaklega vísað till. mgr. 8. gr. og 2. mgr. 10. gr. laga nr. 87/1998, en hvorugt þessara ákvæða geta talist fullnægjandi lagaheimild. Annars vegar er um að ræða lagaákvæði sem snýr að verkefnum og skyldum Fjármálaeftirlitsins og hins vegar ákvæði sem snýr að valdheimildum eftirlitsins til að krefjast úrbóta. Hvorugt .ákvæðið samrýmist kröfum lögmætisreglunnar sem grundvöllur undir setningu íþyngjandi stjórnvaldsreglna. Ef litið er nánar á 2. mgr. 10. gr. laga nr. 87/1998, er ljóst að ákvæðinu verður einungis beitt gagnvart einstökum eftirlitsskyldum aðila í stjórnsýslumáli. Þannig segir í ákvæðinu að Fjármálaeftirlitið skuli gera athugasemdir, ef það telur hag eða rekstur eftirlitsskylds aðila að öðru leyti "óheilbrigðan" og "brjóta í bága" við eðlilega viðskiptahætti, og krefjast þess að úr sé bætt innan hæfilegs frests. Til viðbótar því að vera valdbeitingarheimild í

			sérstökum málum gagnvart einstökum aðilum, þá snýr andlag ákvæðisins að samskiptum eftirlitsskylds aðila og viðskiptavinar hans. Af lögskýringargögnum má sjá að ákvæðinu er ætlað að taka til neytendaverndar. Lykilhugtak í þessu samhengi eru "eðlilegir viðskiptahættir", en til þess að farið sé gegn ákvæðinu, þarf hagur og rekstur eftirlitsskylds aðila að vera óheilbrigður og þannig brjóta í bága við eðlilega viðskiptahætti. Sé gætt samræmisskýringar og litið til laga nr. 5712005 um eftirlit með viðskiptaháttum og markaðssetningu, má sjá að hugtakið viðskiptahættir ná yfir markaðssetningu fyrirtækja eða aðra athöfn, athafnaleysi eða hátterni sem tengist kynningu á vöru eða þjónustu og viðskiptum með vöru eða þjónustu. Ákvæði sérlega um einstaka eftirlitsskylda starfsemi og forsaga þeirra styðja einnig þessa niðurstöðu. Af framangreindu er ljóst að engin lagarök standa til þess að ákvæði 2. mgr. 10. gr. laga nr. 87/1998 feli í sér heimild til að setja almennar reglur, hvað þá verulega íþyngjandi reglur. e) Kostnaður Af tilmælunum er ljóst að kostnaðarvitund var ekki höfð að leiðarljósi við samningu þeirra. Framkvæmd tilmælanna mun kalla á verulegan kostnað, sem verður hlutfallslega hærri hjá smærri fyrirtækjum. Slíkur kostnaður mun verða tugir, jafnvel hundruð milljóna króna. Af inngangi tilmælanna og tilkynningu um þau verður ekki séð að Fjármálaeftirlitið hafi framkvæmt kostnaðarmat á áhrifum þeirra. Af þeim sökum er dregið í efa að fylgt hafi verið meginreglum stjórnsýsluréttar um rannsóknarskyldu og meðalhóf við gerð umræðuskjalsins. Jafnframt er dregið í efa að Fjármálaeftirlitið geti, án lagastoðar, krafist þess að eftirlitsskyldir aðilar leggi út í verulegan kostnað án þess að um sé að ræða beinar eftirlitsaðgerðir, í stjórnsýslumáli gagnvart tilteknum aðila eða þá með sérstakri ákvörðun að uppfylltum lagaskilyrðum, skv. 7. gr. laga nr. 87/1998. í umfjöllun um einstaka kafla verður vikið að kröfum sem líklegir eru til að valda umtalsverðum kostnaði. Varðandi inngang er sérstök ástæð til að gera athugasemdir við árlegt sjálfsmat. Ekki liggur fyrir hvaða þörf er á árlegu sjálfsmati eða á hvaða grunni (forskrift) slíkt mat á að byggja. d) Skyldur skv. lögum nr. 27/7999 ekki upp(vlltar Samkvæmt 3. gr. laga nr. 27/1999 um opinberar eftirlitsreglur, skal stjórnvald ,,þegar eftirlitsreglur eru samdar ..... meta þörf fyrir eftirlit gildi þess og kostnað þjóðfélagsins af því". Augljóst er að slíkt mat hefur ekki farið fram og því hafa ekki verið uppfylltar lögbundnar kröfur um mat á þörf og kostnaði við þau fyrirmæli sem í drögunum felast.

15	Lánasjóður sveitarfélaga ohf.	1 Kafli	í lið 1.1. segir að tilmælin taki til allra eftirlitsskyldra aðila skv. 2. gr. laga nr. 87/1998. Rétt er að vekja athygli á því að almennt hefur verið litið svo á að eftirlitsskyldir aðilar, í hefðbundnum skilningi, teldust þeir aðilar sem taldir eru upp í 1. mgr. 2. gr. laga nr. 87/1998. Þessir aðilar borga m.a. eftirlitsgjöld samkvæmt lögum nr. 99/1999. Miðað við framsetningu Fjármálaeftirlitsins má skilja ákvæðið þannig að t.d. aðilar skv. 3. mgr. 2. gr., s.s. innherjar hjá útgefendum fjármálagerninga sem teknir hafa verið til viðskipta á skipulegum markaði, falli undir tilmælin. Lánasjóðurinn dregur í efa að svo víðtækt gildissvið fái staðist. í lið 1.1. er gerð sú krafa að "öll upplýsingakerfi sem hafi þýðingu fyrir eða áhrif á starfsemi fyrirtækisins" skuli· starfrækt í samræmi við tilmælin. Þar sem öll upplýsingakerfi hafa einhver áhrif á starfsemina þá eru tilmælin, með þessu, látin ná til allra upplýsingakerfa fyrirtækja. Þegar við bætist ótrúlega víð skilgreining á upplýsingakerfum, er ljóst að fátt í starfsemi fyrirtækjanna fellur utan tilmælanna. Að mati lánasjóðsins er ekki gætt meðalhófs í framangreindri afmörkun og nægjanlegt væri að einungis þýðingarmikil upplýsingakerfi féllu undir tilmælin. í lið 1.2. eru upplýsingakerfi skilgreind sem "kerfi, vélræn og óvélræn sem koma að vinnslu upplýsinga ásamt öllum tengingum að, frá og milli þeirra". í þekkingarfyrirtækjum eins og fjármálafyrirtækjum er nánast öll starfsemi tengd vinnslu upplýsinga, m.a. samskipti fólks. Ef ætlast er til að "óvélræn" kerfi falli undir tilmælin þá þarf að afmarka um hvaða þætti (kerfi) í starfsemi fjármálafyrirtækja er að ræða, setja fram dæmi um slík kerfi, - auk þess sem rökstyðja ber þörf á því að öll ákvæði tilmælanna eigi við um slík "óvélræn kerfi", s.s. afritataka. Ekki er ljóst hvað er átt við með "utanaðkomandi aðgangur" í lið 1.4.
16	Lánasjóður sveitarfélaga ohf.	2 kafli	Lánasjóðurinn gerir ekki athugasemdir við tilmæli um að fyrirtæki geri áhættugreiningu á upplýsingakerfum. Hins vegar telur lánasjóðurinn að skortur á meðalhófi og kostnaðarvitund komi vel fram í 2. kafla. Samkvæmt drögunum er ætlast til þess a.m.k. einu sinni á ári láti eftirlitsskyldir aðilar fara fram í gegnum áhættugreiningu og skjalfestar niðurstöður hennar séu sendar til Fjármálaeftirlitsins. Ekki er ljóst hvað Fjármálaeftirlitið ætlar að gera með árleg afrit af áhættugreiningu allra eftirlitsskyldra aðila. Spyrja má, hvort stefnan sé að endurmeta og taka ábyrgð á öllum slíkum áhættugreiningum, og hvort það sé skilvirk framkvæmd? Jafnframt má spyrja, hvort að Fjármálaeftirlitið hafi áætlað kostnað vegna þessa og mögulega hækkun á eftirlitsgjöldum? Lánasjóðurinn telur að hér sé um óþarfa kvaðir og kostnað að ræða. Að mati lánsjóðsins er nægjanlegt, og í samræmi við rekstraröryggi, að eftirlitsskyldir aðilar láti framkvæma áhættugreiningu og uppfæri hana eftir þörfum. Slík greining væri tiltæk, eins og önnur gögn eftirlitsskyldra aðila, ef Fjármálaeftirlitið teldi ástæðu til að kalla eftir henni.
17	Lánasjóður sveitarfélaga ohf.	3. kafli	Lánasjóðurinn gerir ekki athugasemdir við að bera ábyrgð á rekstri upplýsingakerfa, enda er það hluti af starfsemi sjóðsins. Hann gerir hins vegar athugasemdir við þá skyldu, að honum beri að uppfylla "allar kröfur" sem gerðar séu í "leiðbeinandi tilmælum", einkum með hliðsjón af öðrum efnisákvæðum tilmælanna.

18	Lánasjóður sveitarfélaga ohf.	4. kafli	Kafli 4 hefur að geyma ýmis gagnleg ákvæði en hins vegar skaðast þau af kröfum umfram meðalhóf, sem munu einungis valda óþarfa kostnaði hjá eftirlitsskyldum aðilum. Þannig telur lánasjóðurinn óþarfa að til séu verklýsingar varðandi allt og nægjanlegt sé að hafa "fyrirliggjandi skriflegar lýsingar á mikilvægum verkferlum fyrir rekstur og öryggi upplýsingakerfa". Þetta er þó sagt með fyrirvara á umfangi skilgreiningar á hugtakinu "upplýsi ngakerfi". Varðandi grein 4.3. þá er ljóst að öll upplýsingakerfi hafa þýðingu fyrir rekstur eftirlitsskyldra aðila. Að mati lánasjóðsins ætti umrædd grein eingöngu að ná til "mikilvægra upplýsingakerfa", þó gerður sé fyrirvari við umfang skilgreiningar á hugtakinu "upplýsingakerfi". Að mati lánasjóðsins er grein 4.4. ofaukið. Telja verður að stefna og samningur um útvistun væri fullnægjandi, sbr. einnig athugasemdir við kafla 11. Að mati lánasjóðsins er óþarfi að mæla fyrir um "gæðamarkmið á einstökum sviðum upplýsingatækni" og hafa "skrifleg ferli til að fylgja eftir gæðamarkmiðunum og skrá frávik niður". Framangreind skylda er alltof víðtæk og mun valda verulegri skriffinnsku og kostnaði, án þess að ávinningur verði í nokkru samræmi við kostnað og fyrirhöfn. Ef eftirlitsskyldir aðilar vilja setja sér gæðamarkmið er það hluti af þeirra eigin þjónustu- eða gæðastefnu, en ekki liður í stjórnvaldskröfum.
19	Lánasjóður sveitarfélaga ohf.	5. kafli	Lánasjóðurinn telur rétt að vekja athygli á því að grein 5.1. mætti gjarnan vera fyrirmynd fleiri ákvæða, þ.e. þar sem áherslan er lögð á "mikilvæg" kerfi. Lánasjóðurinn gerir ekki athugasemdir við efnisinntak greinar 5.5. Hins vegar telur lánasjóðurinn ekki að tilvísun í upplýsingagjöf til Fjármálaeftirlitsins sé meginröksemdin heldur sú þagnarskylda sem hvílir á fjármálafyrirtækjum, sbr. 58. gr. laga um fjármálafyrirtæki nr. 161/2002.
20	Lánasjóður sveitarfélaga ohf.	6. kafli	Lánasjóðurinn telur eðlilegt stefnumið að mælast til þess að eftirlitsskyldir aðilar hafi almennan skriflegan verkferil um rekstur upplýsingakerfa (sem heild). Ef hins vegar markmið greinar 6.1. er að gera kröfu um sérstakan verkferil fyrir allar mögulegar tegundir upplýsingakerfa (vélræn og óvélræn) þá eru gerðar athugasemdir við slíkt með vísan til meðalhófs. í samræmi við sjónarmið sem áður hafa komið fram verður ekki talið að allt viðhald á öllum upplýsingakerfum þurfi að fara fram eftir skriflegum verkferlum, sbr. grein 6.3. Hér skortir afmörkun og meðalhóf.
21	Lánasjóður sveitarfélaga ohf.	7. kafli	í grein 7.1. kemur enn fyrir krafa um "verkferla" um hvert viðvik, án takmörkunar eða meðalhófs. Að mati lánasjóðsins er nægjanlegt að mælast til þess að "öflun, þróun og prófun" á upplýsingakerfum sé framkvæmd á forsvaranlegan hátt. Það ætti að vera hægt að treysta forsvarsmönnum fyrirtækja til að nota verkferla eða skrá upplýsingar, í slíkum tilfellum, þegar það á við. Sömu sjónarmið eiga við um grein 7.3. þar sem ætlast er til að settir séu "verkferlar" um "allar" breytingar sem geta haft áhrif á öll upplýsingakerfi (vélræn og óvélræn). í grein 7.2. er vísað til greinar 3.1 um "ábyrgðaraðila". Hins vegar er hlutverkið "ábyrgðaraðili" ekki skilgreint í grein 3.1, en einungis sagt að stjórn beri ábyrgð á rekstri upplýsingakerfa. Að mati lánasjóðsins er það

			verulega íþyngjandi ef stjórnum eftirlitsskyldra aðila er ætlað að samþykkja allar breytingar á öllum upplýsingakerfum (vélrænum og óvélrænum). Varðandi grein 7.4. er vísað til athugasemda við kafla 8 varðandi skráningu frávika og meðalhóf.
22	Lánasjóður sveitarfélaga ohf.	8. kafli	Skilgreina þarf hugtakið "frávik" sem er lykilhugtak við túlkun kaflans. Ef "frávik" eru öll möguleg tilvik þar sem upplýsingakerfi (vélræn og óvélræn) geta "hikstað", þá eru kröfur kaflans of víðtækar og ekki í samræmi við meðalhóf. Miðað við framangreinda (víða) skilgreiningu telur lánasjóðurinn að einungis eigi að skrá "umtalsverð frávik" eða frávik sem hafa neikvæða þýðingu fyrir starfsemina. Svipuð sjónarmið eru varðandi tilkynningaskyldu til Fjármálaeftirlitsins. Það er óraunhæft og óhagkvæmt að gera kröfu um það að öll smávægileg frávik, sem enga þýðingu hafa fyrir starfsemina, verði tilkynnt.
23	Lánasjóður sveitarfélaga ohf.	9. kafli	Lánasjóðurinn telur að ákvæði 9. gr. laga nr. 87/1998 feli í sér heimildir til að fara fram á upplýsingar sem eru fyrir hendi hjá eftirlitsskyldum aðilum. Ákvæðið felur hins vegar ekki í sér sjálfstæða heimild til að gera kröfur um tilhögun eða geymslu upplýsinga. í kaflanum er einnig settar fram kröfur, s.s. um hljóðritun símtala, sem geta hæglega rekist á við ákvæði laga nr. 77/2000. Lánasjóðurinn telur ákvæði greinar 9.3. vera svo íþyngjandi að sérstök lagaheimild þurfi að vera fyrir hendi, auk þess sem spurningar vakna um persónuvernd. Þessu til viðbótar efast lánasjóðurinn um að meðalhófs sé gætt og kallar eftir upplýsingum um þá rannsókn sem liggur að baki ákvæðinu. Að síðustu vakna ýmsar spurningar um tæknilegar lausnir og kostnað. Hér verða aðeins nefnd nokkur atriði sem lánsjóðurinn geldur varhug við varðandi efni þessarar greinar, en áskilinn er réttur til frekari athugasemda. í fyrsta lagi er ekki einungis átt við kerfi sem varða viðskipta-og fjárhagsupplýsingar heldur alla starfsemi fyrirtækja, enda "tengist" öll starfsemi viðskiptum. í öðru lagi er ætlast til að símar séu hljóðritaðir hjá öllum starfsmönnum í fyrirtækjum. Fyrir utan persónuverndarspurningar þá verður ekki séð hvert sé markmiðið með slíkum hlerunum og hvernig meðalhófs hefur verið gætt. Benda má á að hljóðritanir í verðbréfamiðlun (sem ekki byggir á fyrirmælum í lögum eða stjórnvaldsfyrirmælum) tíðkast sem liður í sönnun munnlegra samninga, sem eru almennt tíðkaðir í slíkum viðskiptum. í tilviki lánasjóðsins verður ekki séð hvaða þýðingu það hafi að t.d. væru tekin upp símtöl við sveitarstjórnarmenn um möguleg kjör og skilmála, sem síðan verða skriflegar ef af lánveitingu verður. í þriðja lagi liggur ekki fyrir hvernig og hvaða upplýsingar á að afla um föx, farsíma eða snarspjall. í fjórða lagi vaknar spurningar um afmörkun. Hvað með samskiptamáta s.s. .facebook", sem getur náð til lokaðra hópa, eða viðskiptahádegisverði. Lánsjóðurinn telur að flest ákvæði greina 9.4 til 9.9 séu skiljanleg, en þó einungis að því gefnu að umfang upplýsingasöfnunar verði endurskoðað, sbr. ofangreint. Lánasjóðurinn áskilur sér þó allan rétt til að koma með athugasemdir við einstök ákvæði síðar, einkum um ofuráherslu á "verkferla". Bent skal á pennaglöp

24	Lánasjóður sveitarfélaga ohf.	11.kafli	Lánasjóðurinn telur það ekki í samræmi við meðalhóf að gerðar séu kröfur til þess að eftirlitsskyldir aðilar þurfi að hafa stefnu um hvaða upplýsingakerfi megi útvista og þá hvert - óháð því hvort einhverju er útvistað (grein 11.1). Slíkar kröfur um mögulega framtíðarútvistun kallar á aukavinnu og kostnað fyrir fyrirtæki, án nokkurrar sýnilegrar þarfar eða ávinnings. í ljósi þróunar í upplýsingatækni verður slík vinna fljótlega úrelt. Það hlýtur að teljast fullnægjandi fyrir markmiðið um að draga úr rekstraráhættu, að ákvörðun um útvistun byggi á vandaðri stefnumörkun og samningi, sbr. grein 11.6 í umræðuskjali. í lið 11.4 er mælst til þess að ekki sé um ,,keðjuútvistun" að ræða. Að mati lánasjóðsins kann að vera erfitt og óhagkvæmt fyrir fyrirtæki að fylgjast með og koma í veg fyrir að útvistunaraðilar nýti sér sjálfir útvistunaraðila við framkvæmd einhverrar tegundar þjónustu. Réttara væri að tilmælin mæltust til þess að útvistunarsamningar hefðu ákvæði um að ávallt lægi ljóst fyrir hvort að keðjuútvistun væri heimil, að upplýsingar um slíkt lægju fyrir og að ákvæði tilmælanna, s.s. um aðgang að gögnum, næðu til þeirrar útvistunar.
25	Lánasjóður sveitarfélaga ohf.	12. kafli	Lánasjóðurinn gerir ekki athugasemdir við að skila upplýsingum um upplýsingatækniumhverfi og rekstur upplýsingatæknikerfa, sbr. grein 12.1. Fyrirvari er þó gerður við athugasemdir við kafla 1. Varðandi lokamálslið greinarinnar, þá myndi lánasjóðurinn leggja til að ákvæðið tæki til "mikilvægra upplýsingakerfa", frekar en kerfa sem hefðu "þýðingu" fyrir starfsemina. Lánasjóðurinn gerir verulegar athugasemdir við þá skyldu sem "tilmælin" leggja á eftirlitsskylda aðila að fá þriðja aðila til að taka út "öll atriði" sem tilmælin tilgreina og skila árlegum skýrslum. Engin sjónarmið eru færð fram um nauðsyn svo ítarlegrar úttektar (öll atriði) né fyrir tíðni úttekta (árlega). Ljóst er að Fjármálaeftirlitið er að veita fyrirtækjum á sviði upplýsingatækni áskrift að verulegum tekjum á kostnað eftirlitsskyldra aðila. Enn sem fyrr virðist skorta að kostnaður sé íhugaður eða litið til meðalhófs.
26	Lánasjóður sveitarfélaga ohf.	Almenn umsögn	Af umsögn þessari má vera ljóst að lánasjóðurinn gerir verulegar athugasemdir við fyrirliggjandi umræðuskjal um rekstur upplýsingakerfa. Lánasjóðurinn telur að tilmælin séu í raun stjórnvaldsreglur, án þess að fullnægjandi lagastoð sé fyrir hendi. Jafnframt kunna tilmælin að gang í berhögg við ákvæði um persónuvernd. Efnislega fela tilmælin í sér verulega íþyngjandi kvaðir, án þess að fyrir liggi greining á þörfinni. Jafnframt er ekkert tillit tekið til meðalhófs og mismunandi stærðar og starfsemi eftirlitsskyldra aðila. Framangreint sést vel á því, að framkvæmd tilmælanna, að óbreyttu, myndi kosta lánasjóðinn tugi milljóna króna. Virðist sem höfundar tilmælanna hafi gleymt að taka tillit til innleiðingar- og viðvarandi kostnaðar við framkvæmd þeirra. Lánasjóðurinn leggur til að nýjar tillögur verði samdar í samstarfi SFF og Fjármálaeftirlitsins, en þar verði leitast við að greina þörf fyrir lágmarkskröfur til upplýsingakerfa. Síðan verði hugað að setningu tilmæla með hliðsjón af meðalhófi. Verði tilmælin sett óbreytt áskilur lánasjóðurinn sér rétt til þess að leita til Umboðsmanns Alþingis eða annarra úrlausnaraðila.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
27	Landsbankinn	2.3	í lið 2.3 er farið fram á að niðurstaða árlegrar áhættugreiningar tengda notkun upplýsingatækni og áhættugreiningu í tengslum við breytingar sem skipta máli fyrir

			upplýsingaöryggi sé skjalfest og skilað ár hvert. Hversu ítarleg er ætlast til þess að þess skýrslugjöf verði?
28	Landsbankinn	Kafli 6	Lagt er til að bætt verði við tilmælum í kafla 6. Rekstur kerfa sem fela í sér aðskilnað . milli þróunar-, prófunar- og rekstrarumhverfa (sbr. ISO 27001, gr. A.1 0.1.4) og aðskilnað skylduverka (sbr. ISO 27001, gr. A.1 0.1.3)
29	Landsbankinn	8.5	Samkvæmt drögunum í gr. 8.5 fela tilmælin í sér mjög víðtæka tilkynningaskyldu varðandi frávik í rekstri upplýsingakerfa. Tilgangur ákvæðisins ekki nægilega skýr að mati Landsbankans. Einnig er orðalagið í gr. 8.5 ekki nægilega skýrt. Sagt er um .brot á varðveislu, leynd, ...". Er hér átt við alvarleg frávik í rekstri upplýsingakerfa, brot einstaklinga af ásetningi eða hreinlega öll frávik? Á að tilkynna þessi frávik jafnóðum og þau eiga sér stað eða með skýrslugjöf árlega? Síðan er rætt um frávik sem valda því að "reksturinn stöðvist" sem þarf að skrá sérstaklega og tilkynna til Fjármálaeftirlitsins - væntanlega jafnóðum? Er hér átt við að allur rekstur bankans stöðvist eða hluti af honum t.d. afgreiðsla til viðskiptavina útibúum, greiðslumiðlun o.s.frv. og er hinum eftirlitsskylda aðila frjálst að meta það sjálfur?
30	Landsbankinn	9.2.1,9.2.3, 9.3 og 9.4	Sá skilningur sem Landsbankinn leggur í alla liði í kafla 9 er að þar sem fjallað er um upplýsingakerfi sé eingöngu átt við upplýsingakerfi sem innihalda skráningar og gögn er varða viðskipta- og fjárhagsupplýsingar auk upplýsinga- og samskiptakerfa er tengjast viðskiptum. Sumar greinar kaflans geta valdið ákveðnum misskilningi hvað þetta varðar. Lið 9.2.1 mætti til dæmis skilja sem svo að gerð séu öryggisafrit af öllum gögnum og upplýsingakerfum. Einnig mætti koma skýrar fram í síðustu setningu í lið 9.4 að þar sé átt við öryggisafrit gagna og upplýsingakerfa sem talin eru upp í lið 9.3 en ekki allra upplýsingakerfa hins eftirlitsskyldra aðila. Landsbankinn heimilar ekki að gefin séu viðskiptafyrirmæli í gegnum farsíma og því mun ekki reyna á þær kröfur í lið 9.3. Er setningin "í ljósi ofangreinds telur sem innhalda viðskiptaupplýsingar" í lið 9.3 rétt skrifuð eða er með viðskiptaupplýsingum átt við viðskiptafyrirmæli? Þetta getur skipt verulegu máli varðandi hversu mörg símtæki í bankanum þarf að hljóðrita. Leysa tilmælin í liðum 9.2.3 og 9.4 um að öryggisafrit séu ekki geymd skemur en í 5 ár bankann undan fyrri tilmælum um varðveislu allra gagna án tímamarka? Er í drögunum átt við gögn nýja bankans frá okt. 2008 eða gögn sem bankinn fékk í arf frá gamla bankanum?
31	Landsbankinn	9.6	í lið 9.6 segir: "Því þarf reglulega að framkvæmda endurheimt gagna af afriti til staðfestingar á virknj og tryggja að öll umrædd gögn og kerfi séu sannarlega afrituð".Landsbankinn leggur til að þessi grein verði felld út af þeirri ástæðu að það sé tæknilega illframkvæmanlegt vegna kostnaðar og umfangs að framkalla öll afrit þannig að tryggt sé að öll gögn séu sannarlega afrituð. Einnig ber að líta til þess að sum upplýsingakerfi sem hafa verið í afritun á síðustu 5 árum eru mögulega ekki í notkun lengur og því ekki hægt að endurheimta þau með reglulegum hætti. Sjá einnig kröfur í lið 9.2.3 þar sem fjallað er um sömu atriði og er því um tvítekningu að ræða.

32	Landsbankinn	9.8	Varðandi gr. 9.8 vaknar sú spurning hvort markmið þessara tilmæla sé að útiloka eftirlitsskyldan aðila frá útvistun kerfa að hluta eða heild. Myndi notkun Landsbankans á viðskiptakerfum Reiknistofu bankanna vera í ósamræmi við þessi tilmæli? Myndi útvistun Lífeyrissjóðs tannlækna til Landsbankans (Lífeyrissjóðurinn hefur ekki lögsögu yfir upplýsingakerfum Landsbankans) vera í ósamræmi við þessi tilmæli? Ef svo er ekki þyrfti að umorða greinina og skýra betur við hvað er átt.
33	Landsbankinn	Kafli 11	Æskilegt er að FME endurskoði þá þætti í kafla 11 sem banna keðjuútvistun. í sumum tilfellum hefur bankinn og/eða dótturfélög hans gert samning um rekstur og hýsingu kerfis hjá þriðja aðila. Slíkur aðili gerir þá stundum samning við sérhæfðan aðila um hýsingu kerfisins í húsnæði annars aðila sem er sérhæfður aðili. Slík hýsing getur aukið öryggi viðkomandi reksturs sé hún vottuð t.d. samkvæmt ISO 27001. **Liður 11.2** í lið 11.2 er gerð krafa um óhindrað aðgengi Fjármálaeftirlitsins að gögnum sem hýst eru hjá þriðja aðila. í þessu tilfelli má velta upp hvort að þetta sé heppilegt orðalag og hvort ekki sé réttar að gera kröfu um að Fjármálaeftirlitið geti ávallt leitað eftir upplýsingum sem eru hýstar hjá þriðja aðila með sama hætti og ef eftirlitið væri að leita eftir gögnum hýstum hjá bankanum sjálfum. Mikilvægt er að þess sé ávallt gætt að beiðnir Fjármálaeftirlitsins um upplýsingar fari eftir formlegum leiðum, hvar svo sem viðkomandi upplýsingar eru hýstar. **Liður 12.1** í lið 12.1 eru gerðar nýjar kröfur um upplýsingar sem afhenda skal Fjármálaeftirlitinu. Það er skoðun Landsbankans að best færi á því að Fjármálaeftirlitið byggi til spurningalista, gátlista eða leiðbeiningar um framkvæmd mats á flækjustigi og hvaða upplýsingum um upplýsingatækniumhverfi og rekstur upplýsingakerfa óskað er eftir. Með því móti mætti auðvelda eftirlitsskyldum aðilum upplýsingagjöf og tryggja að þeir afhendi Fjármálaeftirlitinu þær upplýsingar sem til er ætlast á samræmdan hátt. Sé það ekki gert er hætta á að framsetning upplýsinga verði svo ólík að þær nýtist Fjármálaeftirlitinu ekki sem skyldi. Þá leggur Landsbankinn til að hægt verði að nota úttektir endurskoðenda á tölvuöryggi við að uppfylla kröfur um upplýsingagjöf vegna tækniumhverfis og reksturs upplýsingakerfa samhliða mati á flækjustigi. Staðlaður spurningalisti eða aðrar leiðbeiningar frá Fjármálaeftirlitinu myndi auðvelda slíka vinnu endurskoðenda. Má líta svo á að mat á umfangi rekstrar og flækjustigi viðskiptakerfa sé hluti af árlegu sjálfsmati á upplýsingatækniumhverfi og um raun sé um sömu skýrslu að ræða, sbr. Inngangur? **Liður 12.2** Má líta svo á að með vottun samkvæmt íST ISOllEe 27001 staðli um upplýsingaöryggi sé kröfum í lið 12.2 fullnægt? Sé það raunin myndi þá ekki nægja að afhenda úttektarskýrslu viðurkennds úttektaraðila um fylgni eftirlitsskylds aðila við staðalinn til þess að fullnægja kröfu um skýrslugjöf vegna úttekta þriðja aðila? Séu reglulegar viðhalds- og endurvottunarúttektir ekki taldar

			fullnægjandi staðfesting á að kröfur í tilmælunum séu uppfylltar er í raun verið að letja eftirlitsskylda aðila til þess að fá vottun samkvæmt íST ISO/lEC 27001staðli þar sem að vegna tilmælanna yrði að leggja út í að tvöfalda vinnu við úttektir við það sem fyrir er með tilheyrandi kostnaði.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
34	Landssamtök Lífeyrissjóða	Almenn umsögn	Fjármálaeftirlitið (FME) kynnti til umsagnar með dreifibréfi dags. 7. maí 2012 drög að uppfærslu leiðbeinandi tilmæla nr. 1/2005, um rekstur upplýsingatæknikerfa. II fagnar endurskoðun tilmælanna og telur að margt sem fram komi í hinum nýju drögum sé mjög til bóta og geti aukið öryggi reksturs viðkvæmra og viðamikilla kerfa. Þar sem drögin eru umfangsmikil og um er að ræða nokkrar breytingar frá fyrri útgáfu, er lagt til að stofnuð verði sérstök samráðsnefnd, þar sem hagsmunaaðilar sem bera ábyrgð á rekstri eftirlitsskyldra kerfa, geti átt fulltrúa. Samráðnefndinni væri ætlað að fara yfir drögin og leggja til endurbætur og lagfæringar eftir atvikum. Hvað drögin varðar, þá eru nokkur atriði sem llieggur til að verði skoðuð nánar. Sér í lagi er talið að sú aðferðafræði sem tilmælin leggja til við þróun og viðhald kerfa geti í sumum tilvikum verið óþarflega ítarleg og leggjum því til að gefinn sé kostur á útfærslu verkagsreglna er heimila einfaldari uppfærslu kerfis m.t.t. neyðarsjónamiða og/eða mjög smávægilegra breytinga (sjá kafla 7, t.d. grein 7.2). í 8. grein mætti skýra betur hvort fullnægjandi sé að tilkynningar um minniháttar rekstrarstöðvanir sem vara í skamman tíma eða utan hefðbundins þjónustutíma, berist árlega. Hvað varðar grein 9.3, þá má íhuga hvort tilmæli um hljóðritun símtala er innihalda viðskiptaupplýsingar, eigi heima í tilmælum um rekstur upplýsingatæknikerfa. Jafnframt telur II æskilegt að endurskoða þá þætti í drögunum þar sem mælst er til að eftirlitsskyldir aðilar, keðjuútvisti ekki rekstri eða rekstrarþáttum (sjá kafla ll, t.d. greinar 11.4 og 11.5). í sumum tilvikum hafa aðilar gert samning um rekstur og hýsingu kerfis hjá þriðja aðila og heimilað þeim aðila að hýsa kerfis sjálft í vélarsal og/eða húsnæði annars aðila sem sérhæfir sig í slíkum rekstri. Oft er um að ræða aðila sem eru vottaðir m.t.t. staðla sem FME vísar í, t.d. ISO 27001 og færa má rök að því að slík hýsing geti aukið öryggi rekstursins í heild sinni. Bent er á að í staðlinum íST 321, sem margir aðilar visa í þegar verksamningar á sviði UT eru gerðir, er gert ráð fyrir undirverktöku, svo fremi sem verkkaupi staðfestir og heimili slíkar aðgerðir. í ljósi ofangreinds, telur LL að það geti verið góður kostur að fela öflugum samráðshópi að fara nánar yfir fyrrnefnd drög og skila hugmyndum að breytingum. Slíkt geti leitt til betri verklagsreglna og ennþá betri reksturs þessara mikilvægu kerfa.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
35	Skipti	Almenn umsögn	Vísað er til bréfs Fjármálaeftirlitsins (FME) dags. 7. maí sl. vegna umræðuskjals nr. 3/2012 vegna draga að tilmælum um rekstur upplýsingatæknikerfa. Óskaði FME eftir

			athugasemdum eigi síðar en 4. júní 2012. Tilmælunum er beint til allra eftirlitsskyldra aðila skv. 2. gr. laga nr. 87/1998 um opinbert eftirlit með fjármálastarfsemi. Skipti hf., sem handhafi innheimtuleyfis, telja rétt að koma á framfæri ákveðnum athugasemdum sem tilefni er til að setja fram. Að mati Skipta eru tilmælin miklu frekur miðuð að fjármálafyrirtækjum og félögum í verðbréfaviðskiptum heldur en inniheimtufyrirtækjum. Því er óvíst í hve miklum mæli þörf sé á því að fyrirtæki sem sinna eingöngu innheimtu uppfylli allar þær kröfur sem þarna koma fram. Athugasemdir Skipta lúta einkum að fjórum megin atriðum sem eru eftirfarandi. Í fyrsta lagi telja Skipti að það þurfi að taka skýrari afstöðu til þeirrar staðreyndar að starfsemi þeirra aðila sem eru eftirlitsskyldir er um margt ósambærileg. Þannig er starfsemi innheimtufyrirtækja annars vegar og fjármálafyrirtæki sem starfrækja viðskiptabankastarfsemi og fjárfestingabankastarfsemi hins vegar, ekki með nokkru móti sambærileg. Það er því vart unnt að réttlæta sambærilegar kröfur til slíkra aðila. Telja Skipti að það verði því að gera skýrari grein fyrir því hvers vegna tilmælin eigi að gilda jafnt fyrir alla. Það er ekki unnt að gera sömu kröfur til allra eftirlitsskyldra aðila. Í öðru lagi telja Skipti að það séu ákveðin vandkvæði falin í því að skýra tilmælin með hliðsjón af lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga. Sem dæmi má nefna að samkvæmt reglum nr. 837/2006 um rafræna vöktun og meðferð persónuupplýsinga sem verða til við rafræna vöktun þá ber að eyða persónugreinanlegum gögnum sem falla undir reglurnar eftir 90 daga. Samkvæmt fjarskiptalögum nr. 81/2003 er óheimilt að geyma persónugreinanlegar upplýsingar um jarskiptaumferð lengur en í sex mánuði. Í tilmælunum er gert ráð fyrir því að geymsla á samskiptum um viðskiptaupplýsingar eigi að geyma eigi skemur en í fimm ár. Í tilmælunum er síðan vísað till0. gr. laga um verðbréfaviðskipti nr. 108/2007. Slíkt ákvæði er ekki að finna í innheimtulögum nr. 95/2008. Til þess að skyldan um varðveislu gagna geti gilt gagnvart innheimtufyrirtækjum þá þyrfti það að koma fram í lögum nr. 95/2008 með sama hætti og í lögum nr. 108/2007. Skipti hf. I Ármúli 25 108 Reykjavík Sími 550 6000 Í þriðja lagi telja Skipti rétt að vekja athygli á því að í núgildandi tilmælum er tekið fram að þau fyrirtæki sem uppfylla staðla sem gilda um rekstur upplýsingatæknikerfa teljast uppfylla tilmælin. Að mati Skipta er æskilegt að sambærileg ákvæði komi skýrt fram í væntanlegum tilmælum enda er hætt við að nokkur vandkvæði geti orðið af því ef tilmælin og staðlar stangast á. Jafnvel mætti draga úr hættu á árekstrum með því að láta nægja að vísa í viðeigandi staðla og tilmælin verði einskorðuð við þau atriði sem eru til viðbótar viðeigandi stöðlum. Þá dregur það verulega úr flækjustigi að vísa eingöngu í staðlana í stað þess að eftirlitsskyld fyrirtæki og þau fyrirtæki sem taka að sér verkefni fyrir eftirlitsskyld fyrirtæki verða að greina sjálf hvort tilmælunum sé eingöngu ætlað að endurspegla staðla eða að bæta einhverjum kröfum við. Eru Skipti reiðubúin að gera nánar grein fyrir þessu atriði ef þess er óskað af hálfu FME en í öllu falli mætti leysa þetta vandamál með þeim hætti sem nú er gert, þ.e. að taka það fram að fyrirtæki sem uppfylli ákveðna staðla, uppfylli tilmælin þá þegar með því. Þá verður einnig að taka fram í tilmælunum að þeir aðilar sem taka að sér verkefni fyrir eftirlitsskyldan aðila geti aldrei afhent gögn til FME nema að eigandi gagnanna, þ.e. hinn eftirlitsskyldi aðili, sé upplýstur um beiðnina. Skipti telja að það brjóti gegn

			grundvallarréttindum aðila ef FME aflar eða óskar eftir gögnum án vitneskju viðkomandi. Slíkt leiðir til þess að með afhendingu er komið í veg fyrir að hinn eftirlitsskyldi aðili geti leitað til dómstóla, leiki vafi á lagaheimild til gagnaöflunar. Í fjórða lagi telja Skipti að það þurfi að gera skýrari grein fyrir þeim lagaheimildum sem tilmælin byggja á og hvaða réttaráhrif þau eigi að hafa. Þannig geta þau ekki vikið til hliðar lögum eða reglum sem önnur stjórnvöld hafa sett og eru rétthærri. Tilmælin eru eins og efni þeirra gefur til kynna, eingöngu tilmæli. Er ekki skýrt hvaða þýðingu tilmælin eiga að hafa þar sem þau fela í sér að einhverju leyti ríkari kröfur til eftirlitsskyldra aðila en gert er samkvæmt lögum. Er hér einkum átt við um innheimtufyrirtæki. Skipti eru reiðubúinn að gera frekari grein fyrir athugasemdum sínum en leggja áherslu á að ekki er að fullu leyti ljóst ástæður þess að jafn víðtækar kröfur séu lagðar á innheimtufyrirtæki sem reka starfsemi sem er í grundvallaratriðum ósambærileg við t.d. rekstur verðbréfasjóða. Telur félagið því að FME verði að aðlaga tilmælin að þeim hagsmunum sem þau eiga að vernda en ekki að gera rekstur smærri fyrirtækja erfiðari og kostnaðarsamari en nauðsynlegt er. Skipti áskilja sér allan rétt til þess að gera frekari athugasemdir en hér er gert og er ekkert sem túlka má í bréfi þessu með þeim hætti að félagið samþykki eða geri ekki athugasemdir við einstök atriði í tilmælunum.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
36	T-plús	9.3	Í grein 9.3 er fjallað um hljóðritun símtala er innihalda viðskiptaupplýsingar. T Plús hf. rekur vörslu- og uppgjörsþjónustu. Fyrirtækið á ekki í viðskiptum enda er starfsleyfið takmarkað við að framkvæma fyrirmæli fyrir hönd viðskiptavina (ganga frá kaupum og sölu fjármálagerninga) og til að veita vörsluþjónustu, sbr. b-liður. 1. tölu. 1. mgr. 25. gr. laga nr. 161/2001 og a-liður 2. tölul. 1. mgr. 25. gr. laga nr. 161/2002. Viðskiptavinir T Plús eru eftirlitsskyldir aðilar og eiga í viðskiptum í Kauphöllum. T Plús vill gjarnan að orðalag gr. 9.3 í tilmælunum verði skýrt þannig að þar sé tekið fram undir hvaða starfsleyfi tilmælin falli.
37	T-plús	11	Í grein 11.4 og 11.5 er fjallað um keðjuútvistun. Eins og áður segir starfar T Plús fyrir önnur fjármálafyrirtæki. Mikilvægur liður í þeim rekstri er starfræksla verðbréfakerfa fyrir viðskiptavini T Plús. Þessi kerfi eru í öllum tilvikum hýst hjá viðurkenndum aðilum s.s. Símanum, Nýherja o.þ.h. T Plús hefur, í samráði við sína viðskiptavini, opnað gátt (e.g. "tunnel") í kerfi þeirra og vinnur í þeim utanfrá. Mikilvægt er að þessháttar tenging verði ekki skilgreind sem keðjuútvistun, enda er hér ekki um breytingu á hýsingu að ræða heldur aðeins um tengingu á milli hýsingaraðila og rekstraraðila að ræða.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
38	Kauphöll Íslands hf.	Almenn umsögn	NASDAQ OMX Iceland hf. ("Kauphöllin") hefur fengið til umsagnar umræðuskjal frá Fjármálaeftirlitinu ("FME") nr. 3/2012, sem inniheldur drög að leiðbeinandi tilmælum um rekstur upplýsingakerfa eftirlitsskyldra aðila. Vill Kauphöllin koma á framfæri athugasemdum við drögin.

			Umrædd leiðbeinandi tilmæli FME eru sett á grundvelli lagaheimildar skv. 2. mgr. 8. gr. laga um eftirlit með fjármálastarfsemi nr. 87/1998. Fram kemur í inngangi með tilmælunum að með þeim sé stefnt að því að samræmdar kröfur verði gerðar til allra eftirlitsskyldra aðila varðandi rekstur upplýsingakerfa og notkun upplýsingatækni. Einnig kemur fram að umfang aðgerða til að tryggja öryggi upplýsingakerfa eigi að vera í samræmi við umfang rekstrar eftirlitsskylds aðila og þá áhættu sem honum fylgi. Loks segir að tilmælin gildi um alla eftirlitsskylda aðila en eðli máls samkvæmt hafi FME ástæðu til að gera ríkari kröfur til eftirlitsskyldra aðila með umsvifamikla og fjölþætta starfsemi en minni aðila með einfalda starfsemi. Því sé gert ráð fyrir að smærri aðilum dugi einfalt utanumhald, þó þeim beri að hafa þau sjónarmið að leiðarljósi sem fram koma í tilmælunum. Hvað varðar rekstur upplýsingakerfa hjá Kauphöllinni þá er rík ástæða til að koma því á framfæri að í þessum efnum nýtur Kauphöllin hagræðis af því að vera hluti af samstæðu NASDAQ OMX á Norðurlöndunum. Innan samstæðunnar eru starfræktar kauphallir í Helsinki, Kaupmannahöfn og Stokkhólmi og hefur rekstur upplýsingakerfa að öllu leyti verið samræmdur á milli kauphallanna á Norðurlöndunum. Kauphöllin hefur því innleitt sömu viðmið og notast við sömu tæknilegu kerfi og aðrar kauphallir NASDAQ OMX á Norðurlöndunum. Enn fremur skal tekið fram að þrátt fyrir að hver kauphöll fyrir sig sé undir eftirliti fjármálaeftirlits í viðkomandi landi þá hafa kauphallimar ásamt danska, finnska, íslenska og sænska fjármálaeftirlitinu sammælst um að auka samræmingu í eftirliti og skýrslugjöf. Til marks um þetta þá framkvæmdu danska, finnska og sænska fjármálaeftirlitið sameiginlega úttekt á rekstri upplýsingakerfa innan NASDAQ OMX samstæðunnar á Norðurlöndunum haustið 2011. ÞÓ svo að íslenska fjármálaeftirlitið hafi ekki verið beinn þátttakandi í úttektinni þá var það að fullu upplýst um framkvæmdina og fékk aðgang að öllum tilheyrandi gögnum. Niðurstaða fjármálaeftirlitanna var jákvæð og einungis smávægilegar athugasemdir voru gerðar við rekstur upplýsingakerfa innan samstæðunnar. Niðurstaðan varðaði allar kauphallir NASDAQ OMX á Norðurlöndunum, þ.m.t. Kauphöllina og hafa kauphallimar brugðist við niðurstöðunni með samræmdum hætti. Kauphöllin telur nauðsynlegt, í samræmi við það sem fram kemur í inngangi með tilmælunum, að ákvæði tilmælanna séu skýrð í ljósi umsvifa eftirlitsskyldra aðila og að teknu tilliti til þess hvers konar eftirlitsskylda starfsemi um er að ræða. Hvað varðar Kauphöllina þá er um að ræða starfsemi utan um rekstur skipulegs verðbréfamarkaðar skv. lögum um kauphallir nr. 110/2007. Þar er því um að ræða rekstur sem er í grundvallaratriðum ólíkur rekstri annarra eftirlitsskyldra aðila sem einnig falla undir tilmælin, s.s. fjármálafyrirtæki, tryggingafélög, lífeyrissjóðir o.fl. Má þar helst nefna að Kauphöllin veitir ekki beina þjónustu til einstaklinga eða almennra fjárfesta. Enn fremur kemur Kauphöllin ekki með beinum hætti að framkvæmd viðskipta með fjármálagerninga, líkt og fjármálafyrirtæki. Að því virtu má sem dæmi nefna að sömu hagsmunir búa ekki að baki sjónarmiðum um vistun gagna er varða viðskiptaupplýsingar og samskipti þeim tengdum þegar um er að ræða kauphöll annars vegar og fjármálafyrirtæki hins vegar. Í ljósi framangreinds og að teknu tilliti til þess að aukin áhersla er á að samræma eftirlit og skýrslugjöf milli fjármálaeftirlitanna á Norðurlöndunum og NASDAQ OMX kauphallanna, þá er ástæða til að vekja athygli á því að þau

			tilmæli sem FME hefur lagt fram til umræðu gera í mörgum tilfellum mun ríkari kröfur til reksturs upplýsingakerfa og varðveislu gagna heldur en ástæða hefurverið talin til á hinum Norðurlöndunum. Svo virðist sem svo ítarleg tilmæli, sem ætlað er að taka með sama hætti til allra eftirlitsskyldra aðila, hafi ekki verið sett fram af öðrum fjármálaeftirlitum á Norðurlöndunum. Að því virtu er ástæða til að horfa til þess að umsvif rekstrar Kauphallarinnar eru mjög afmörkuð og einungis 18 starfsmenn starfa innan fyrirtækisins. Kauphöllin gæti því hæglega fallið undir það að teljast til "smærri aðila" sem fjallað er um í inngangi með tilmælum FME. Það er því mikið hagræði og gríðarlegur ábati sem fylgir því að eiga undir sömu viðmið og njóta sömu þjónustu varðandi rekstur upplýsingakerfa og aðrar kauphallir innan samstæðu NASDAQ OMX á Norðurlöndunum. Sé ætlunin sú að gera kröfu um að Kauphöllin fari að öllu leyti eftir ákvæðum tilmælanna, eins og þau eru sett fram, þá myndi slíkt hafa gríðarlegt óhagræði í för með sér og gæti það haft afgerandi áhrif á rekstur Kauphallarinnar. Kauphöllin fer því þess á leit að hugað sé að hinu samræmda umhverfi sem kauphallir á Norðurlöndunum starfa innan og að ekki séu gerðar ríkari kröfur til reksturs upplýsingakerfa hjá Kauphöllinni. Enn fremur vill Kauphöllin óska eftir því að FME leitist við að vera í auknu mæli aðili að hinu samræmda eftirliti sem norrænu fjármálaeftirlitin hafa með NASDAQ OMX kauphöllunum og samþykki samræmda skýrslugjöf í þeim tilfellum sem því verður komið við.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**
39	Reiknistofa bankanna	Almenn umsögn	Reiknistofa bankanna þakkar fyrir að vera gefinn kostur á að koma á framfæri athugasemdum við drögin. í ljósi þess að um er að ræða rekstur upplýsingakerfa eftirlitsskyldra aðila og ábyrgð á útvistun til upplýsingatæknifyrirtækja á borð við Reiknistofu bankanna hf liggur hjá hinum eftirlitsskyldu aðilum þykir Reiknistofunni rétt að þeir hinir sömu geri sínar athugasemdir til Fjármálaeftirlitsins. Reiknistofan bendir þó á víðtækt orðalag í 1 mgr. greinar 9.2 11" •• að öll þau gögn sem eftirlitið kann að óska eftir séu til staðar þá og þegar krafa um upplýsingar er sett fram." Að mati Reiknistofunnar þarf verklag að taka mið af mikilvægi upplýsingakerfa og forgangsröðun að teknu tilliti til þess kostnaðar sem af leiðir, eigi sú krafa við alla upptalningu í greinum 9. kafla um varðveislu og meðhöndlun gagna eftirlitsskyldra aðila. Kostnaðurinn við slíka uppsetningu verður allt of mikill Einnig er rétt að benda á að ákvæði um keðjuútvistun (grein 11.4-11.5) mun kalla á umtalsverðar breytingar í rekstri margra grunnkerfa á fjármálamarkaðnum. í dag kaupa fjármálafyrirtæki þjónustu frá Greiðsluveitunni vegna greiðslumiðlunarkerfa, sem aftur eru í rekstri og þróun hjá Reiknistofunni. Tæknilega séð verður ekki hægt uppfylla þetta skilyrði nema með mjög miklum tilkostnaði. Að mati Reiknistofunnar væri það óæskileg þróun. Reiknistofa bankanna er tilbúin til að koma að vinnu að breytingum á 9. kafla og 11.4 þannig að hægt væri að uppfylla kröfur FME án þess að það leiði til kostnaðaraukningar fyrir fjármálamarkaðinn.
Nr.	**Nafn umsagnaraðila**	**Tilvísun**	**Umsögn**

40	Verðbréfaskráning Íslands hf.	Almenn Umsögn	VS telur eðlilegt að almennt veðri horft til þess að tilmælin nái yfir breiðan hóp eftirlitsskyldra aðila og að VS hefur einungis á að skipa 7 starfsmönnum og starfsemin mjög afmörkuð. Um starfsemi VS gilda sérlög og er hún mjög eðlisólk starfsemi langflestra skipulagssskyldra aðila sem lúta lögum um fjárma´lafyrirtæki svo sem banka og verðbréfafyrirtækja og trygginafélaga. Til ða mynda verður ekki séð af hverju þörf sé á að taka upp öll símtöl sem eiga sér stað vegna starfseminnar. Engin viðskipti verða til fyrir milligöngu VS. Þau annast reikningsstofnanir, bankar og verðbre´fafyrirtæki í samræmi við fyrirmæli laga um rafræna eignarskra´ningu verðbréfa nr. 131/1997 og reglugerðar settri á grundvelli þeirra. Þá vill VS koma því á framfæri að þær kröfu sem gerðar eru um aukin skýrsluskrif eru mjög íþyngjandi fyrir féalg með rekstur í svo föstum skorðum. VS er enn fremur óheimilt að stunda aðrar starfsemi en lögin beinlínis kveða á um og hvers kyns breytingar á starfseminni krefjast tilkynningar til Fjármálaeftirlitsins og Seðlabankans. það er því ósk Verðbréfaskráningar að sá rammi sem henni verður ætlar í þesu samhengi taki tillit til framangreindra sjónarmiða.