Deloitte.

Innleiðing leiðbeinandi tilmæla FME nr. 2/2014

Frá sjónarhóli endurskoðunarnefnda

Sif Einarsdóttir
yfirmaður innri endurskoðunarþjónustu Deloitte
21. maí 2014

Umfjöllun

Leiðbeinandi tilmæli 2/2014
Innra eftirlit upplýsingakerfa

- Leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 2/2014 (áður nr. 1/2012) snúast um *innra eftirlit upplýsingakerfa* eftirlitsskyldra aðila
- Megintilgangur tilmælanna er að lágmarka rekstraráhættu eftirlitsskyldra aðila
- Umfang aðgerða til að tryggja öryggi upplýsingakerfa á að vera í samræmi við *umfang reksturs* eftirlitsskylds aðila og þá *áhættu* sem honum fylgir.

Innra eftirlit upplýsingakerfa

Ábyrgð og skyldur stjórnar, endurskoðunarnefnda og stjórnenda

Hvað segja íslensk lög?

Hlutafélög

„Félagsstjórn skal annast um að **nægilegt eftirlit** sé haft með bókhaldi og meðferð fjármuna félagsins. Framkvæmdastjóri skal sjá um að bókhald félagsins sé fært í samræmi við lög og venjur og meðferð eigna félagsins sé með tryggilegum hætti. „(68. gr. laga um hlutafélög nr. 2/1995)

Einingar tengdar almannahagsmunum

"Endurskoðunarnefnd skal meðal annars hafa eftirfarandi hlutverk án tillits til ábyrgðar stjórnar, stjórnenda eða annarra á þessu sviði:
1. Eftirlit með vinnuferli við gerð reikningsskila.
2. Eftirlit með **fyrirkomulagi og virkni innra eftirlits einingarinnar**, innri endurskoðun, ef við á, og áhættustýringu.
3. Eftirlit með endurskoðun ársreiknings og samstæðureiknings einingarinnar.
4. Mat á óhæði endurskoðanda eða endurskoðunarfyrirtækis og eftirlit með öðrum störfum endurskoðanda eða endurskoðunarfyrirtækis.
5. Setja fram tillögu til stjórnar um val á endurskoðanda eða endurskoðunarfyrirtæki.]" (108. Gr. b. Laga um ársreikninga nr. 3/2006)

Innra eftirlit upplýsingakerfa

Ábyrgð og skyldur stjórnar, endurskoðunarnefnda og stjórnenda, frh.

Fjármálafyrirtæki

Ábyrgð yfirstjórnar.
"Yfirstjórn fjármálafyrirtækis ber ábyrgð á að skyldur þess samkvæmt lögum og reglum séu uppfylltar.

Yfirstjórn skal reglulega meta og endurskoða skilvirkni stefnu, fyrirkomulags og verklags, sem komið hefur verið á til að uppfylla skyldur samkvæmt lögum og reglum og gera viðeigandi ráðstafanir til að ráða bót á hvers konar annmörkum.

(5. gr. Reglugerðar um fjárfestavernd og viðskiptahætti fjármálafyrirtækja.)

Lífeyrissjóðir

„Stjórn lífeyrissjóðs ber ábyrgð á starfsemi sjóðsins í samræmi við lög þessi, reglugerðir settar samkvæmt þeim og samþykktir sjóðsins. Stjórn lífeyrissjóðs skal einnig hafa með **höndum almennt eftirlit með rekstri, bókhaldi og ráðstöfun eigna sjóðsins**. Stjórnin setur sér starfsreglur og gerir tillögur til breytinga á samþykktum sjóðsins á ársfundi." (29.gr. l.nr. 129/1997 um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða)

Innra eftirlit upplýsingakerfa

Ábyrgð og skyldur stjórnar, endurskoðunarnefnda og stjórnenda, frh.

Lífeyrissjóðir (frh.)

„Stjórn lífeyrissjóðs annast m.a. eftirfarandi verkefni: „
…
„8. að móta **innra eftirlit lífeyrissjóðsins** og skjalfesta **eftirlitsferla**],
9. að **móta eftirlitskerfi** sem gerir sjóðnum kleift að greina, vakta, meta og stýra áhættu í starfsemi sjóðsins].“ (29. gr. l. nr. 129/1997 um skyldutryggingu lífeyrisréttinda og starfsemi lífeyrissjóða)

Vátryggingafélög

Stjórnin skal setja reglur, sem staðfestar skulu af Fjármálaeftirlitinu, **um innra eftirlit**, innri endurskoðun, fjárfestingarstarfsemi, lánveitingar og viðskipti við tengda aðila. Stjórnin ber ásamt framkvæmdastjóra ábyrgð á því að **skipulag félagsins og innra eftirlit sé fullnægjandi** og á því að félagið geti lagt fram upplýsingar sem þörf er á til eftirlits með því. (54.gr. l.nr. 56/2010)

Innra eftirlit upplýsingakerfa
Skilgreining á innra eftirliti

Innra eftirlit hefur verið skilgreint þannig (skilgreining COSO *):

Internal control is a process, effected by an entity‘s board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Lauslega þýtt:

Innra eftirlit er ferli sem mótast af stjórn fyrirtækis, stjórnendum þess og starfsmönnum. Tilgangur þess er að veita hæfilega vissu um að fyrirtækið nái markmiðum um árangur og skilvirkni í rekstri, áreiðanlega skýrslugerð og fylgni við lög og reglur.

** Heimild: COSO Internal control-Integrated Framework, www.coso.org.*

Innra eftirlit upplýsingakerfa

Af hverju opinberar kröfur um innra eftirlit?

Meiri kröfur til sumra fyrirtækja en annarra:

Eftirlitsskyldir aðilar Fjármálaeftirlitsins - eða - ekki eftirlitsskyldir aðilar

Einingar tengdar almannahagsmunum - eða - almenn fyrirtæki ekki tengd almannahagsmunum

Innra eftirlit upplýsingakerfa

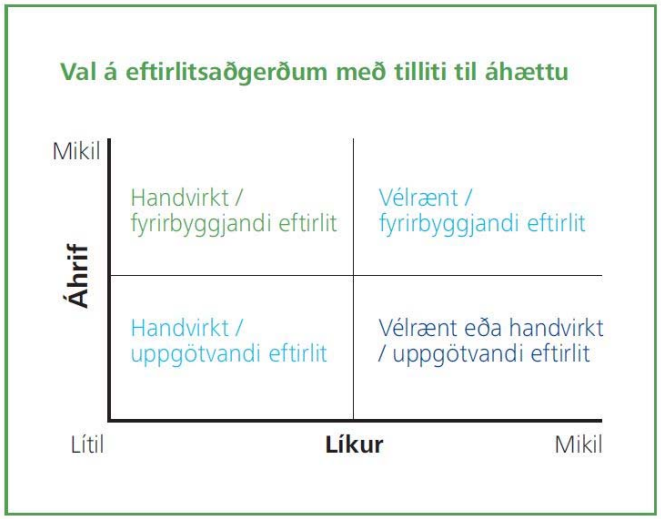
Eftirlitsskyldir aðilar eru *flokkaðir* eftir því hvort þeir teljast vera með umfangsmikla og fjölþætta starfsemi eða einfalda starfsemi, sjá gr. 1.5. í tilmælum.

Innra eftirlit upplýsingakerfa

Af hverju opinberar kröfur um innra eftirlit, frh.

Innra eftirliti er m.a. ætlað að:

- Koma í veg fyrir að mistök verði sem veldur fyrirtækinu tjóni.
- Verja eignir fyrirtækisins fyrir tjóni.
- Koma í veg fyrir að fyrirtækið verði fyrir tjóni af völdum sviksemi.

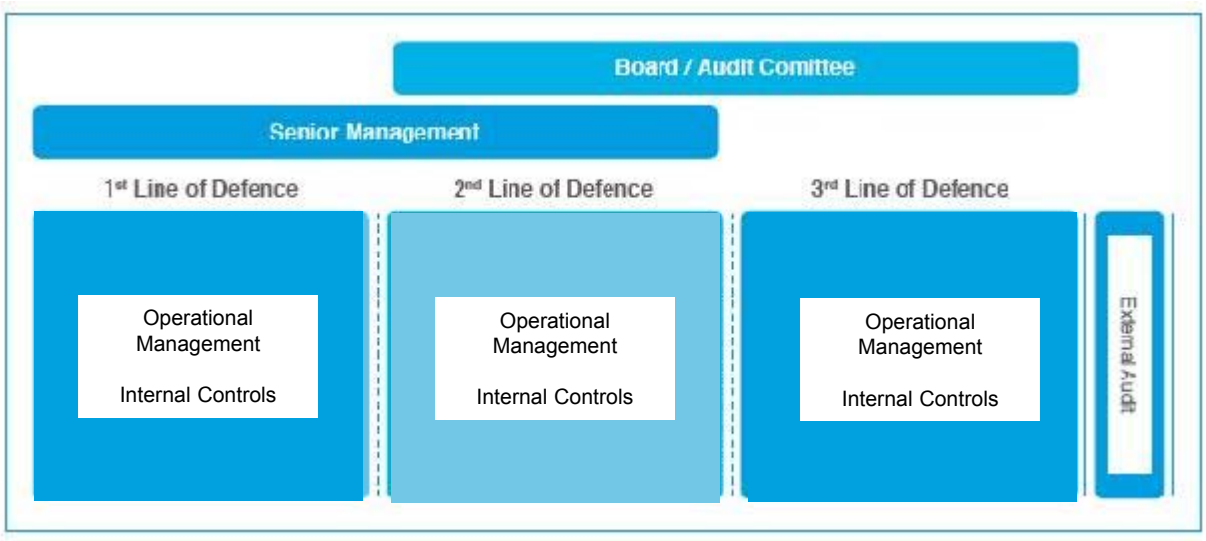


- *Innra eftirlit* er hluti af eðlilegri starfsemi fyrirtækja.
- *Innra eftirlit* er ekki bara íþyngjandi formkröfur eftirlitsaðila.
- *Innra eftirliti er ætlað að gera fyrirtækinu gagn.*

Ávinningurinn af innra eftirliti á að vera meiri af kostnaðurinn sem af eftirlitinu hlýst

Innra eftirlit upplýsingakerfa

Þrjár varnarlínur innra eftirlits



Fyrsta varnarlínan eru allir stjórnendur og starfsmenn sem fara með daglegt innra eftirlit í fyrirtækinu, hér er meginábyrgð á skipulagi og virkni innra eftirlitsaðgerða.

Önnur varnarlínan er regluvarsla – fer yfir fylgni við lög og reglur, og áhættustýring – mælir áhættur og ber saman við viðmið.

Þriðja varnarlínan er innri endurskoðun, óháð stjórnendum, sem gerir sjálfstæðar kannanir á 1.-2. varnarlínu og gefur skýrslu til stjórnar og endurskoðunarnefndar.

Innra eftirlit upplýsingakerfa
Hvernig getur innri endurskoðun hjálpað?

Skilgreining á innri endurskoðun:

- “Innri endurskoðun er starfsemi sem veitir óháða og hlutlæga staðfestingu og ráðgjöf sem ætlað er að vera virðisaukandi og bæta rekstur fyrirtækja og stofnana. Innri endurskoðun leggur mat á og bætir virkni áhættustýringar, *eftirlitsaðferða* og stjórnarhátta með kerfisbundnum og öguðum vinnubrögðum og styður þannig viðkomandi fyrirtæki eða stofnun í því að ná markmiðum sínum. Innri endurskoðandi starfar sjálfstætt og tekur ekki ákvarðanir sem tengjast daglegri starfsemi. “

Heimild: “Hvað er innri endurskoðun?” Útgefið af FIE

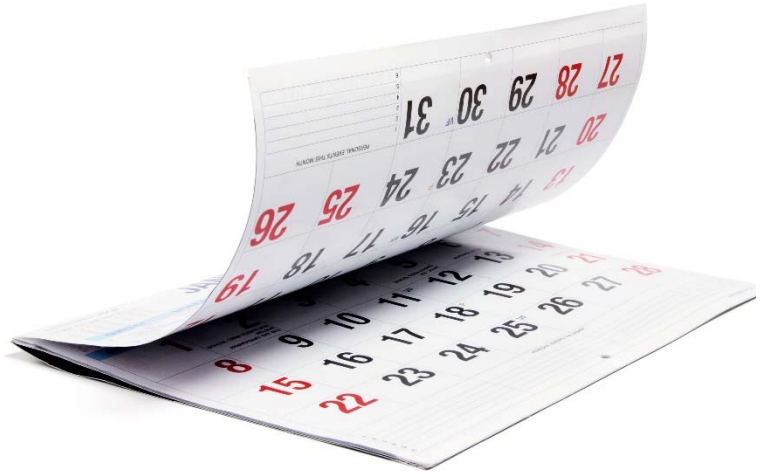
Innri endurskoðun er hluti af stjórnendaeftirliti fyrirtækja, innri endurskoðun heyrir undir stjórn og gefur skýrslur til endurskoðunarnefndar og stjórnar.

Innri endurskoðun á að skoða á viðeigandi hátt *atriði sem tengjast upplýsingatækni* í sinni yfirferð, samkvæmt alþjóðlegum innri endurskoðunarstöðlum.

Frá sjónarhóli úttektaraðila

Staða eftir úttektir ársins 2013

- Fylgni við leiðbeinandi tilmæli nr. 2/2014 er mismunandi eftir stærð og gerð eftirlitsskyldra aðila.
- Smærri fyrirtækin virðast eiga lengra í land en þau stærri.
- Smærri fyrirtæki:
  - Áhættumat ekki til staðar
  - Skortur á verklagsreglum
- Stærri fyrirtæki:
  - Áhættumat ekki uppfært nýlega
  - Útvistunarstefna ófullnægjandi
- Stór og smá fyrirtæki:
  - Útvistunarsamningar ófullnægjandi (gamlir)



Frá sjónarhóli úttektaraðila

Næstu skref

Eftirlitsskyldir aðilar þurfa að ljúka við að breyta því og bæta sem úttektaraðili gerði athugasemdir við vegna ársins 2013, m.a.:

- Formleg og skjalfest öryggis- og gæðastefna um rekstur upplýsingakerfa.
- Formleg og kerfisbundin áhættugreining/áhættumat.
- Skriflegir verkferlar og verklagsreglur um rekstur upplýsingakerfa, m.a. hvernig tryggja á upplýsingaöryggi, gagnaöryggi, afritun o.fl.
- Sérstaklega þarf að taka á meðhöndlun frávika, samfelldur rekstur, neyðaráætlun.
- Flokkun gagna eftir því hvort þau innihaldi viðskiptafyrirmæli.
- Útvistunarstefna, þjónustusamningar, aðgangur FME að gögnum.

Nálgun við ofangreint þarf að miðast við eðli og flækjustig viðkomandi fyrirtækis.

Deloitte.