# Innra eftirlit

RÍKISENDURSKOÐUN

2. útgáfa
október 2017

# Efnisyfirlit

# 1 Inngangur

Öflugt innra eftirlit er ein af forsendum árangursríkrar stjórnunar. Í þessu riti er fjallað um innra eftirlit, í hverju það er fólgið og hvernig staðið er að mati á því.

Ritið er fyrst og fremst skrifað með hliðsjón af þörfum stjórnenda þeirra stofnana og fyrirtækja ríkisins sem Ríkisendurskoðun ber lögum samkvæmt að endurskoða.

Þetta er önnur útgáfa ritsins. Fyrri útgáfa þess var gefin út á árinu 1998. Viðhorf til innra eftirlits hefur þróast nokkuð á undanförnum áratugum og var því tími til kominn að endurbæta ritið með tilliti til þess.

Þessi samantekt er í ritröð sem stofnunin hefur tekið saman um tilteknar fyrirbyggjandi aðgerðir sem flestar stofnanir og fyrirtæki ríkisins geta gripið til í því skyni að treysta eða efla ákveðna þætti í starfsemi sinni. Það er von Ríkisendurskoðunar að þetta rit komi stofnunum og fyrirtækjum ríkisins að góðu gagni.

Ríkisendurskoðun, október 2017.

# 2 Skilgreining á innra eftirliti

## 2.1 Hugtakið innra eftirlit

Í sinni víðustu merkingu felur hugtakið innra eftirlit í sér allt það ferli sem stuðlar að því að viðkomandi stofnun eða fyrirtæki nái settum markmiðum um árangur og skilvirkni í rekstri, áreiðanlega skýrslugerð og fylgni við lög og reglur. Í 65. gr. laga um opinber fjármál nr. 123/2015 er innra eftirlit skilgreint með sama hætti:

> „Forstöðumaður ríkisaðila í A-hluta, eða eftir atvikum stjórn, ber ábyrgð á framkvæmd innra eftirlits. Innra eftirlit felur í sér þær reglubundnu aðgerðir og ráðstafanir sem hlutaðeigandi aðili gerir til að stuðla að hagkvæmni rekstrar, öryggi fjármuna, áreiðanleika upplýsinga og almennt að því að markmiðum starfseminnar verði náð og fylgt sé lögum og reglum."

Í ritinu er byggt á skilgreiningu COSO[1] þar sem innra eftirlit er brotið niður í eftirfarandi 17 meginþætti:

**Eftirlitsumhverfi**

- ✓ Heilindi og siðferðilegt gildismat.
- ✓ Ráðuneyti/stjórn er óháð framkvæmdastjórn stofnunar.
- ✓ Völd og ábyrgð eru skilgreind í samþykktu skipulagi.
- ✓ Mannauður - Ráða, þjálfa og halda í hæft starfsfólk.
- ✓ Völd og ábyrgð á innra eftirliti fari saman.

**Áhættumat**

- ✓ Meginmarkmið starfseminnar eru skýrt skilgreind.
- ✓ Áhættuþættir eru auðkenndir og greindir.
- ✓ Sviksemisáhætta er metin.
- ✓ Breytingar sem kalla á breytt innra eftirlit eru auðkenndar og greindar.

**Eftirlitsaðgerðir**

- ✓ Eftirlitsaðgerðir eru valdar og þróaðar.
- ✓ Rafrænar eftirlitsaðgerðir með upplýsingatækni eru valdar og þróaðar.
- ✓ Verklagsreglur eru settar um eftirlitsaðgerðir.

**Upplýsingar og samskipti**

- ✓ Afla upplýsinga sem skipta máli.
- ✓ Innri samskipti.
- ✓ Ytri samskipti.

**Vöktun innra eftirlits**

- ✓ Sívirkar aðgerðir til þess að meta innra eftirlit.
- ✓ Upplýsingar um ágalla og veikleika metnar og komið á framfæri.

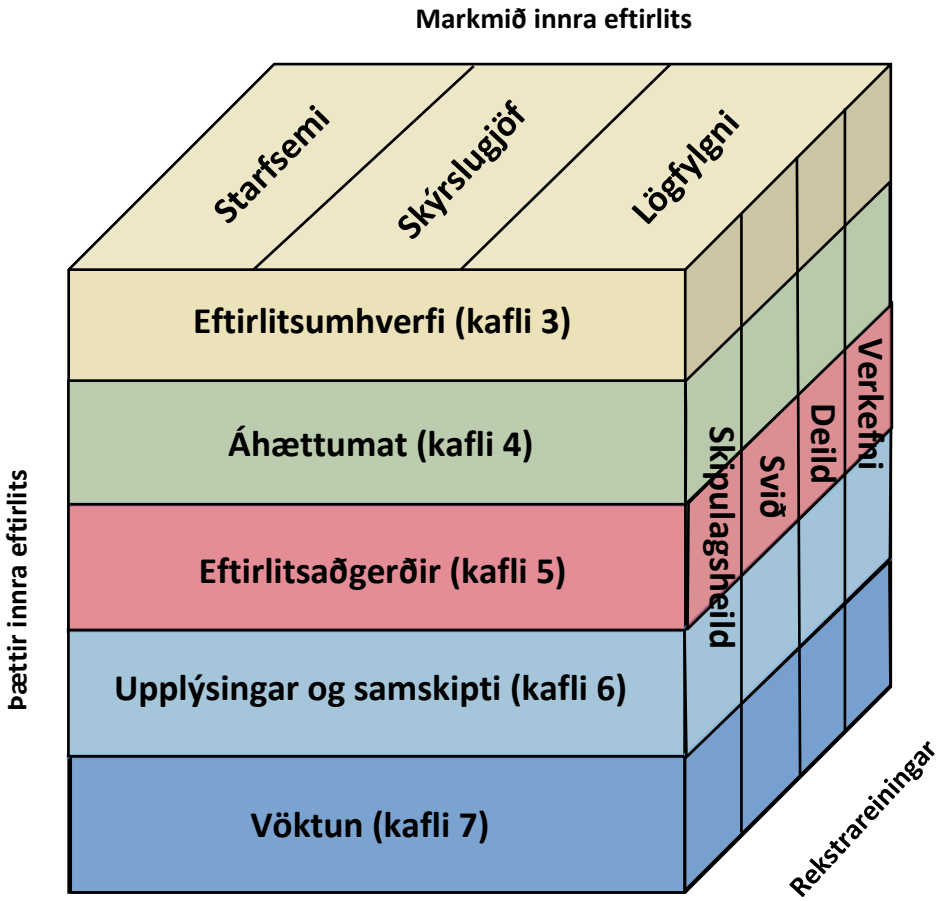
Í ritinu tekur efnisumfjöllun mið af áðurnefndum meginþáttum innra eftirlits.

[1] https://www.coso.org/Documents/COSO-ICIF-11x17-Cube-Graphic.pdf

Innra eftirlit eru ferlar sem hannaðir hafa verið með það fyrir augum að viðkomandi stofnun eða fyrirtæki nái markmiðum sínum. Mikilvægt er að innra eftirlit sé skjalað þannig að hægt sé að tryggja gæði þess og sameiginlegan skilning allra sem koma að eftirlitinu.

Eftirfarandi mynd er ætlað að sýna tengsl meginþátta innra eftirlits við markmið innra eftirlits og einstaka starfssvið viðkomandi stofnana og fyrirtækja.

Mynd 1. Innra eftirlit – COSO teningurinn




## 2.2 Markmið innra eftirlits

Öflugt innra eftirlit er nauðsynlegt í rekstri ríkisaðila. Innra eftirliti er ætlað að vera hluti af þeim aðgerðum sem stofnanir og fyrirtæki nota til þess að ná markmiðum sínum. Sameiginleg markmið allra stofnana og fyrirtækja ríkisins eru m.a. þau að:

- ✓ Reksturinn sé árangursríkur og skilvirkur, þar með talin ráðstöfun tíma og fjármuna.
- ✓ Semja áreiðanleg reikningsskil.
- ✓ Fylgja lögum og reglum sem gilda um starfsemina.
- ✓ Tryggja rekstraröryggi upplýsingakerfa, áreiðanleika og viðeigandi leynd gagna.

Á grundvelli framanritaðs má flokka markmið innra eftirlits með eftirfarandi hætti:

### 2.2.1 Starfsemi – rekstrartengd markmið

Að viðkomandi starfsemi sé hagkvæm og skilvirk. Starfsemin nái rekstrar- og fjárhagsmarkmiðum sínum og gætt sé að varðveislu eigna.

### 2.2.2 Skýrslugjöf – markmið um áreiðanlegar upplýsingar

Að innri og ytri skýrslugjöf sé áreiðanleg, tímanleg, gagnsæ og uppfylli önnur þau skilyrði sem kunna að vera sett til skýrslugjafar.

### 2.2.3 Lögfylgni – markmið um fylgni við lög og reglur

Að reynt sé að tryggja að starfsemin fylgi þeim lögum og reglum sem um hana gilda. Reglurnar kunna að vera eigin innri verklagsreglur sem stjórnendur viðkomandi starfsemi hafa sett eða reglur settar af ytri aðilum, s.s. í formi reglugerða.

## 2.3 Einkenni innra eftirlits

### 2.3.1 Stöðugt eftirlit

Innra eftirlit er ekki ein sérstök tiltekin aðgerð heldur ýmsar aðgerðir sem stjórnendur og aðrir starfsmenn beita sífellt til þess að fylgjast með og tryggja starfsemina. Þessar aðgerðir eiga að vera eðlilegur hluti af starfi allra starfsmanna viðkomandi stofnunar eða fyrirtækis.

### 2.3.2 Byggir á starfsmönnum

Innra eftirlit stendur og fellur með starfsfólki viðkomandi stofnunar eða fyrirtækis. Endanleg ábyrgð á innra eftirliti er hjá forstöðumanni en allir starfsmenn hafa tilteknum skyldum að gegna og verða að sinna þeim ef það á að skila árangri.

### 2.3.3 Ýmsir þættir takmarka gæðin

Innra eftirlit er háð takmörkunum, t.d. vegna mistaka eða ásetnings stjórnenda og starfsfólks eða vegna ófyrirséðra atvika utan valdsviðs viðkomandi stofnunar eða fyrirtækis. Þá ætti kostnaður við innra eftirlit aldrei að vera meiri en ávinningurinn. Það getur því einungis veitt hæfilega vissu um að stofnun nái markmiðum sínum. Nánar er fjallað um takmörk innra eftirlits í 8. kafla.

# 3 Eftirlitsumhverfi

Eftirlitsumhverfið felur í sér stjórnarhætti og stjórnskipulag stofnunarinnar og viðhorf og aðgerðir stjórnenda vegna innra eftirlits og mikilvægi þess fyrir viðkomandi starfsemi.

Gæði innra eftirlits ráðast mjög af eftirlitsumhverfinu. Ólíklegt er að innri eftirlits-aðgerðir, sama hversu vel þær eru uppbyggðar, séu virkar ef eftirlitsumhverfið er andsnúið þeim. Það er undir stjórnendum og starfsmönnum komið að jákvætt viðhorf ríki í garð innra eftirlits. Auk jákvæðs viðhorfs eru verkaskipting, agi og fræðsla um tilgang innra eftirlits ein helsta forsenda fyrir góðum árangri.

Eftirfarandi fimm þættir eru taldir ráða mestu um árangur af innra eftirliti:

- ✓ Heilindi og siðferðilegt gildismat.
- ✓ Ráðuneyti/stjórn er óháð framkvæmdastjórn.
- ✓ Völd og ábyrgð eru skilgreind í samþykktu skipulagi.
- ✓ Mannauður - Ráða, þjálfa og halda í hæft starfsfólk.
- ✓ Völd og ábyrgð á innra eftirliti fara saman.

## 3.1 Heilindi og siðferðilegt gildismat

Heiðarleiki og siðferðileg gildi eru þættir sem skipta mjög miklu máli fyrir gæði innra eftirlits. Því er mikilvægt að stjórnendur séu heiðarlegir, sýni heilindi í starfi sínu og séu starfsfólki góð fyrirmynd í þeim efnum. Stjórnendur ættu að gera starfsfólki ljóst að slíkir kostir séu mikils metnir og mikilvægir fyrir viðkomandi starfsemi. Slík gildi eru oft sett fram í formlegum siðareglum og mannauðsstefnu.

Benda má á að í lögum nr. 70/1996 um réttindi og skyldur starfsmanna ríkisins er lögð sérstök áhersla á þessa eiginleika. Í 14. gr. segir m.a. að starfsmanni sé skylt að rækja starf sitt af alúð og samviskusemi í hvívetna. Hann skuli gæta kurteisi, lipurðar, réttsýni og forðast að hafast nokkuð það að í starfi sínu eða utan þess sem er honum til vanvirðu eða álitshnekkis eða varpað geti rýrð á það starf eða þá starfsgrein sem hann vinnur við.

## 3.2 Ráðuneyti/stjórn er óháð framkvæmdastjórn

Í 65. gr. laga um opinber fjármál nr. 123/2015 kemur fram að forstöðumaður ríkisaðila í A-hluta, eða eftir atvikum stjórn, ber ábyrgð á framkvæmd innra eftirlits. Samkvæmt lögunum hefur ráðherra hins vegar heimild til þess að skipa nefnd sem er honum til ráðgjafar um fyrirkomulag og framkvæmd innra eftirlits og innri endurskoðunar. Slíkar nefndir hafa ekki verið skipaðar þegar þetta er skrifað.

Forstöðumaður ber ábyrgð gagnvart þeim ráðherra sem hlutaðeigandi stofnun heyrir undir. Ráðherra ber síðan ábyrgð gagnvart Alþingi á að stofnanir sem undir hann heyra starfi skv. lögum.

Forstöðumaður stofnunar ber ábyrgð á innra eftirliti og þar með á vali aðgerða sem draga eiga úr tilteknum áhættuþáttum í viðkomandi rekstri. Stjórnendur stofnana geta þannig sett verklagsreglur sem gilda innan þeirra stofnana til þess að tryggja framgang innra eftirlits. Viðhorf stjórnanda til reikningsskila, gagnavinnslu og starfsfólks skiptir miklu máli við val aðgerða svo og hve öflugt ytra eftirlit er með rekstrinum.

Stjórnendur verða að sýna stuðning sinn við innra eftirlit með því að leggja áherslu á mikilvægi ytri og innri endurskoðunar og að bregðast fljótt og vel við athugasemdum þeirra.

## 3.3 Völd og ábyrgð skilgreind í samþykktu skipulagi

Öflugt innra eftirlit byggir meðal annars á því að í stjórnskipulagi sé skýrt afmarkað hvernig valdi og ábyrgð er úthlutað og hvernig boðleiðum er háttað. Stjórnskipulag stofnunar tekur mið af stærð og eðli viðkomandi starfsemi.

## 3.4 Hæft starfsfólk

Mikilvægt er að bæði stjórnendur og starfsfólks búi yfir nægilegri hæfni til þess að geta sinnt sínum störfum. Viðhalda þarf hæfni starfsfólks með endurmenntun og þjálfun vegna sérstakra verkefna þegar þörf krefur. Einnig skiptir máli að frammistaða starfsmanna sé metin reglulega.

Stofnanir og fyrirtæki ættu að móta stefnu í mannauðsmálum þar sem fram koma grundvallarreglur um ráðningu, þjálfun, frammistöðumat, starfsframa, agamál og stjórnun starfsfólks. Öll þessi atriði skipta miklu máli varðandi jákvætt viðhorf starfsmanna til stofnunar eða fyrirtækis og geta skipt sköpum varðandi viðhorf þeirra til innra eftirlits og framkvæmdar þess.

## 3.5 Völd og ábyrgð á innra eftirliti fari saman

Stjórnendur framselja tiltekið vald og ábyrgð á daglegum störfum og samskiptum í hendur undirmanna sinna. Mikilvægt er með tilliti til innra eftirlits að þetta framsal sé hæfilegt. Veigamikil forsenda framsalsins er að undirmenn séu háðir faglegri stjórnun og mikilvægt að því sé fylgt eftir að starfsmenn beri þá ábyrgð sem þeim hefur verið úthlutað í tengslum við innra eftirlit.

## 3.6 Atriði til athugunar

Hér eru tilgreindar nokkrar spurningar sem ætlað er að vekja stjórnendur til umhugsunar um eftirlitsumhverfi.

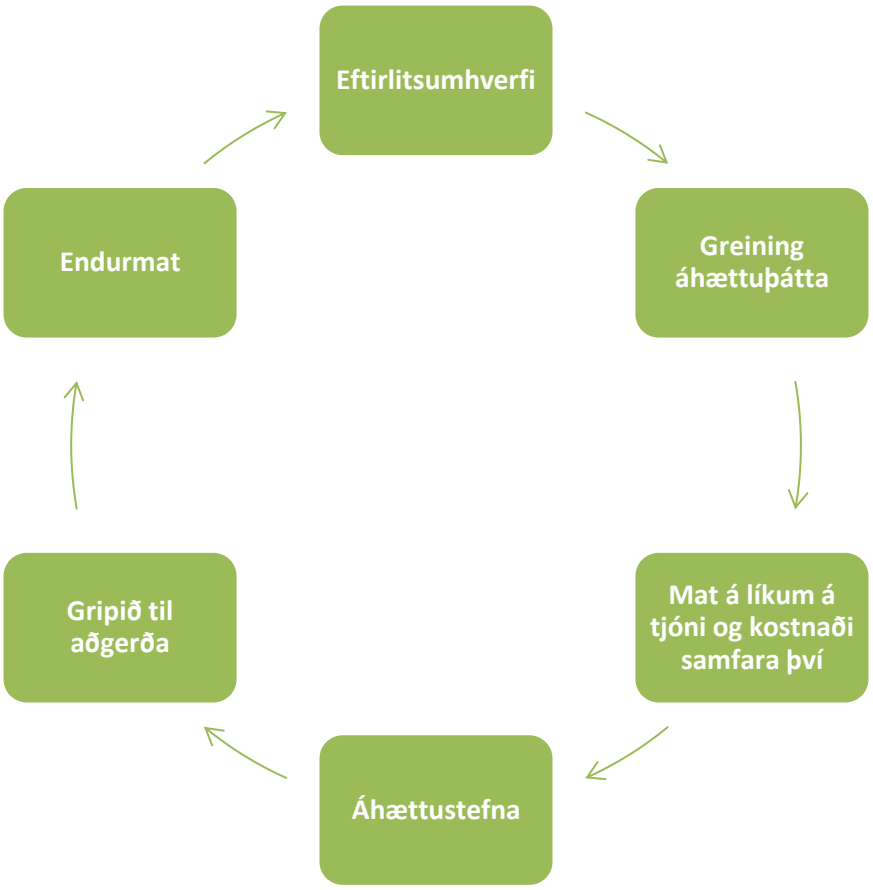
| | Eftirlitsumhverfi | Já | Nei | Ath. |
|---|---|---|---|---|
| 1. | Er lögð nægileg áhersla á kröfur um heiðarleika, heilindi og siðferðilegt gildismat í fyrirmælum stjórnenda? | | | |
| 2. | Liggja fyrir skriflegar reglur um hegðun á vinnustað og viðurlög vegna brota á þeim? | | | |
| 3. | Er verkaskipting í samræmi við hæfni, starfsreynslu og þjálfun starfsmanna? | | | |
| 4. | Er til stefna í mannauðsmálum? | | | |
| 5. | Er til stefna um þjálfun og endurmenntun starfsfólks? | | | |
| 6. | Er frammistaða starfsmanna metin reglulega? | | | |
| 7. | Er skipurit til staðar sem sýnir uppbygg-ingu og ábyrgðarsvið? | | | |

# 4 Áhættumat

Stofnanir þurfa að geta brugðist við þeirri áhættu sem ógnað getur markmiðum þeirra. Greining og mat á þeim áhættuþáttum sem haft geta áhrif á viðkomandi starfsemi skapar grundvöll að viðeigandi viðbrögðum við þeim. Eftirfarandi fjórir þættir eru taldir ráða mestu um árangursríkt áhættumat í tengslum við innra eftirlit:

- ✓ Meginmarkmið starfseminnar eru skýrt skilgreind. Hægt er að greina og meta áhættu þess að markmið náist ekki á fullnægjandi hátt.
- ✓ Áhættuþættir eru auðkenndir og greindir. Hægt er að sporna við eða stjórna þeim áhættuþáttum sem gætu komið í veg fyrir að stofnun/fyrirtæki nái markmiðum sínum.
- ✓ Sviksemisáhætta er metin og hugað að hugsanlegum áhrifum sviksemi ef slík tilvik kæmu upp.
- ✓ Breytingar sem kalla á breytt innra eftirlit eru auðkenndar og greindar.

Mynd 2 hér á eftir sýnir hvernig áhættumat tengist öðrum þáttum.




Mynd 2. Ferli áhættumats

## 4.1 Greining áhættuþátta

Við greiningu á áhættuþáttum í tilteknum rekstri þurfa stjórnendur að horfa bæði til þátta innan og utan viðkomandi stofnunar eða fyrirtækis, þar á meðal samskipta við utanaðkomandi aðila.

Dæmi um innri áhættuþætti eru:

- ✓ Mikill vöxtur eða samdráttur í starfseminni.
- ✓ Breytingar á starfsháttum, t.d. hluti rekstrar fluttur í annan landshluta.
- ✓ Minnkandi miðstýring.
- ✓ Breytingar á ábyrgð stjórnenda.
- ✓ Mikil endurnýjun í hópi starfsfólks, t.d. nýir starfsmenn í lykilstörfum.
- ✓ Minni kröfur gerðar til hæfni starfsfólks og dregið úr þjálfun þess.
- ✓ Verktakar fengnir til þess að vinna helstu verkefni.
- ✓ Rekstrartruflanir í tölvukerfum.
- ✓ Ný eða breytt upplýsingakerfi.

Dæmi um ytri áhættuþætti eru:

- ✓ Tækniþróun.
- ✓ Breyttar þarfir viðskiptavina.
- ✓ Ný lög og/eða reglugerðir.
- ✓ Breytingar á fjárveitingum.
- ✓ Breytingar í efnahagslífi.
- ✓ Náttúruhamfarir.

Ef ríkisstofnun eða fyrirtæki nær ekki markmiðum sínum verða stjórnendur að huga sérstaklega að ástæðum þess við greiningu áhættuþátta.

## 4.2 Mat á líkum á tjóni og kostnaði vegna þess

Mat á áhættuþáttum felst annars vegar í því að meta hversu miklar líkur eru á því að tiltekin áhætta valdi tjóni og hins vegar því að meta hve mikið tjónið gæti orðið.

Ekki er til ein algild aðferð sem hægt er að nota við framangreint áhættumat og erfitt er að reikna nákvæmlega líkur á tjóni og kostnað vegna þess. Ástæðan er sú að sjaldnast liggja fyrir tæmandi gögn sem hægt er að styðjast við. Því er ekki mælt með að verja mikilli vinnu og kostnaði í nákvæma útreikninga. Betra er að meta áhættu og líklegt tjón út frá bestu fáanlegu upplýsingum og eigin reynslu.

Oft ræður eðli viðkomandi starfsemi því hvort tiltekinn áhættuþáttur er stór eða lítill. Áhættuþáttur sem talinn er vera stór hjá einum aðila kann að skipta litlu máli hjá öðrum. Rafmagnsleysi, þó ekki sé nema stutta stund, er t.d. gífurlega stór áhættuþáttur í rekstri sjúkrahúss en hefur ekki jafn alvarlegar afleiðingar hjá ýmsum öðrum stofnunum.

## 4.3 Áhættustefna

Þegar mat á áhættuþáttum í viðkomandi rekstri liggur fyrir þarf að setja markmið sem eftirlitsaðgerðum er ætlað að ná. Slík markmið eru sett fram í áhættustefnu

og skal hún vera skrifleg. Einn liður í henni er sérstök öryggisstefna fyrir upplýsingakerfi.

Við mótun áhættustefnu þarf m.a. að taka tillit til eftirfarandi þátta:

- ✓ **Áhættuvilji** (risk appetite) - Sú áhætta sem stjórnendur eru tilbúnir að taka til að ná settum markmiðum. Áhættuvilji endurspeglar viðhorf stjórnenda til áhættu, þ.e. hvort þeir eru áhættusæknir eða áhættufælnir, og hefur áhrif á starfsumhverfi og stjórnunarstíl. Rétt er að benda á að eitt af grunngildum í opinberum fjármálum er varfærni. [2]

- ✓ **Áhættuþol** (risk tolerance) - Ásættanleg frávik í rekstri með hliðsjón af settum markmiðum. Stjórnendur ákvarða áhættuþol með hliðsjón af mikilvægi tengdra markmiða og samræma áhættuþolið áhættuviljanum.

- ✓ **Áhættusafn** (risk portfolio) – Líta þarf heildstætt á alla áhættuþætti og meta mikilvægi hvers og eins í heildarmyndinni.

## 4.4 Endurmat áhættu

Mat á áhættu kann að breytast og áhættuþáttur sem áður taldist stór í viðkomandi rekstri kann að verða metinn óverulegur síðar. Stöðugt koma fram nýir áhættuþættir, t.d. vegna lagabreytinga eða tækniþróunar. Vegna breytilegra aðstæðna, bæði í innra og ytra rekstrarumhverfi stofnana og fyrirtækja ríkisins, er stöðug greining áhættuþátta ásamt mati á þeim og aðgerðum sem eiga að draga úr áhættu nauðsynleg.

## 4.5 Tengsl áhættumats og aðgerða

Tilgangur eftirlitsaðgerða er að halda áhættu innan þeirra marka sem stjórnendur telja skynsamlega. Kostnaður við aðgerðir skiptir að sjálfsögðu miklu máli þegar valið er á milli kosta.

Viðbrögð við áhættu geta verið:

- ✓ **Umbera áhættu** (tolerate) - Þegar ákveðið er að grípa ekki til neinna mótvægisaðgerða til þess að minnka áhættuna. Ástæðan getur verið sú að kostnaður við mótvægisaðgerð sé meiri heldur en hugsanlegt tjón.

- ✓ **Forðast áhættu** (Terminate) – Þegar ákveðið er að breyta verkþáttum til að útiloka ákveðna áhættu í viðkomandi ferli. Dæmi um þessa tegund viðbragða er þegar staðið er frammi fyrir snjóflóðahættu og brugðist er við henni með því að færa eignir af snjóflóðahættusvæðinu á annað svæði þar sem slík hætta er ekki fyrir hendi.

[2] https://www.stjornarradid.is/verkefni/efnahagsmal-og-opinber-fjarmal/log-um-opinber-fjarmal/grunngildi/

- ✓ **Deila áhættu** (Transfer) – Þegar ákveðið er að deila áhættunni með öðrum. Dæmi um þessa tegund viðbragða eru kaup á tryggingum eða samrekstur með öðrum aðilum í svipaðri aðstöðu.

- ✓ **Meðhöndla áhættu** (Treat) – Þegar ákveðið er að grípa til aðgerða til þess að minnka líkur á hættu eða minnka möguleg áhrif þess skaða sem áhættunni getur fylgt. Dæmi um þessa tegund viðbragða er þegar staðið er frammi fyrir snjóflóðahættu og brugðist er við henni með því að byggja snjóvarnargarða sem draga eiga úr líkum á tjóni.

Í 5. kafla hér á eftir er fjallað um ýmsar tegundir eftirlitsaðgerða til þess að draga úr áhættu í rekstrinum.

## 4.6 Atriði til athugunar

Hér eru nokkrar spurningar sem ætlað er að vekja stjórnendur til umhugsunar um áhættumat.

| | Áhættumat | Já | Nei | Ath. |
|---|---|---|---|---|
| 1. | Er áhættumat hluti af starfi stjórnenda? | | | |
| 2. | Hafa áhættuþættir viðkomandi rekstrar verið skilgreindir? | | | |
| 3. | Hafa líkur á tjóni og hugsanlegur kostnaður vegna þess verið metinn? | | | |
| 4. | Hafa skilgreindir áhættuþættir verið flokkaðir eftir því hvort þeir teljast ásættanlegir eða ekki? | | | |
| 5. | Hafa markmið eftirlitsaðgerða verið skilgreind í stefnu? | | | |
| 6. | Er allt ferli áhættumatsins endurmetið reglulega? | | | |

# 5 Eftirlitsaðgerðir

Í kjölfar áhættumats þurfa stjórnendur að ákveða hvernig þeir ætla að bregðast við þeirri áhættu sem talin er fylgja viðkomandi rekstri. Ákvörðunum um að draga úr eða útiloka tiltekna áhættuþætti verður að fylgja eftir með viðeigandi aðgerðum innan stofnana og fyrirtækja.

Eftirfarandi þrír þættir eru taldir ráða mestu um árangur af eftirlitsaðgerðum innra eftirlits:

- ✓ Eftirlitsaðgerðir eru valdar og þróaðar í þeim tilgangi að draga úr áhættu á að markmið skipulagsheildarinnar náist ekki.

- ✓ Eftirlitsaðgerðir með upplýsingakerfum eru valdar og þróaðar þannig að þeim sé ætlað að auka líkur á að markmiðum skipulagsheildarinnar sé náð.

- ✓ Verklagsreglur eru settar um eftirlitsaðgerðir sem ætlað er að stuðla að því að stefna stofnunar/fyrirtækis nái fram að ganga.

Hugtakið innri eftirlitsaðgerð er í þessu riti notað í svo víðri merkingu að það nær til allra aðgerða sem auka líkur á því að rekstraraðili nái markmiðum sínum, hvort sem um er að ræða staðfestingu með áritun, verkaskiptingu, verklagsreglur, aðgangstakmarkanir, öryggisgæslu eða annað.

Eðli eftirlitsaðgerða geta verið mismunandi. Þær geta verið:

- ✓ **Leiðbeinandi** (Directive) – setja reglur eða leiðbeiningar til þess að hjálpa starfsmönnum að gera rétta hluti á réttan hátt.

- ✓ **Fyrirbyggjandi** (Preventive) – koma á forvörnum sem draga úr líkum á því að villur og frávik eigi sér stað.

- ✓ **Upplýsandi** (Detective) – upplýsa og aðvara um hættu áður en hún verður að umtalsverðu vandamáli eða upplýsa fljótt um atriði sem hafa farið úrskeiðis. Krafan um gagnsæi í starfsemi opinberra aðila er dæmi um þessa tegund eftirlitsaðgerða.

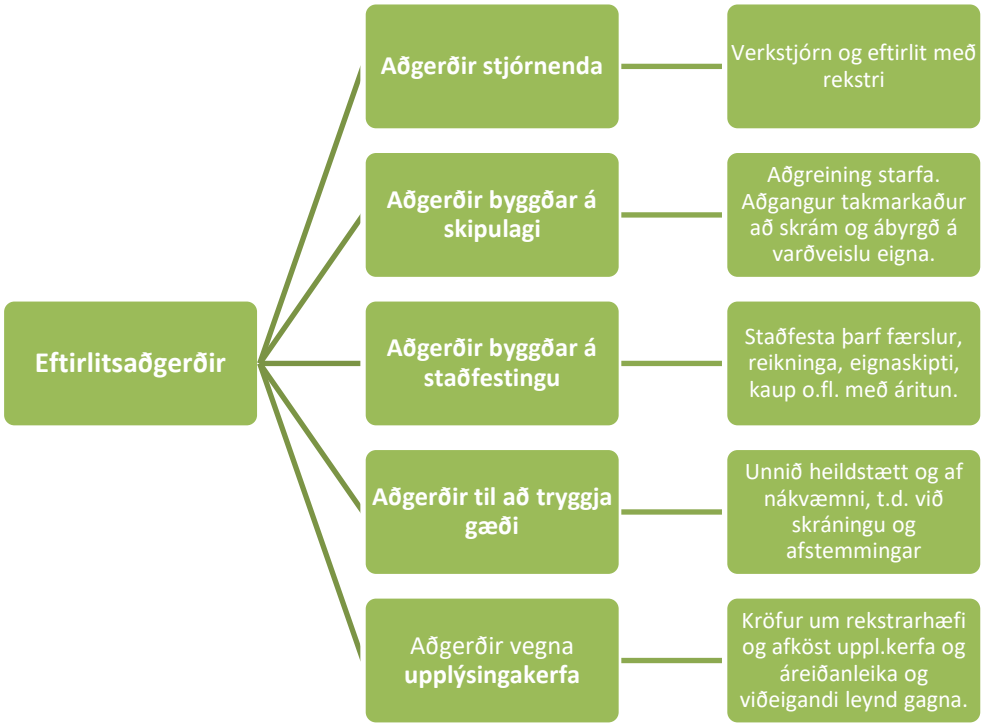
- ✓ **Leiðréttandi** (Corrective) – bregðast rétt við afleiðingum þess sem farið hefur úrskeiðis. Læra af reynslunni og endurbæta forvarnir til að draga úr líkum á að mistök endurtaki sig.

Því stærri sem tiltekinn áhættuþáttur er þeim mun viðameiri þurfa eftirlitsaðgerðir

vegna hans að vera. Ekki er raunhæft að líta svo á að hægt sé að útiloka alla áhættu sem steðja kann að nútíma rekstri með eftirlitsaðgerðum. Slíkt er ýmist of dýrt eða óframkvæmanlegt. Hins vegar má draga það mikið úr áhættuþáttum með viðeigandi aðgerðum að líkurnar á áföllum verði innan ásættanlegra marka.

Innri eftirlitsaðgerð á að vera eðlilegur þáttur hvers verkferlis. Hún þarf að vera árangursrík, hagkvæm og skilvirk og hana þarf að endurmeta reglulega. Slíkt endurmat kallar á að til sé skrifleg lýsing á aðgerðinni þar sem fram kemur hvað á gera, hvernig, hvenær og hvers vegna.

Eftirlitsaðgerð vegna sama áhættuþáttar kann að vera ólík frá einum aðila til annars. Ástæður þess geta t.d. verið ólíkt eðli og umfang rekstrar, mismunandi markmið, mat stjórnenda eða kröfur til upplýsingakerfa um rekstrarhæfi afköst eða áreiðanleika gagna.




Mynd 3. Eftirlitsaðgerðir

Í eftirfarandi undirköflum verður fjallað um einstaka þætti eftirlitsaðgerða sem koma fram á myndinni hér að ofan.

## 5.1 Aðgerðir stjórnenda

Stjórnendur þurfa reglulega að ganga úr skugga um að reksturinn skili þeim árangri sem að er stefnt. Í því skyni þurfa þeir að bera raunverulegan árangur saman við fjárlög, fyrri áætlanir og árangur.

Eftirlitsaðgerðir stjórnenda geta auðveldað þeim að fylgjast með hvernig viðkomandi stofnun eða fyrirtæki gengur að ná þeim markmiðum sem sett voru í formi árangursmælikvarða. Þessar aðgerðir geta falist í samanburði og mati á margskonar upplýsingum og geta leitt í ljós að úrbóta sé þörf á einhverjum sviðum.

Stjórnendur bera ábyrgð á verkstjórn og að verkefni séu unnin á fullnægjandi hátt.

## 5.2 Aðgerðir sem byggja á skipulagi

### 5.2.1 Aðgreining starfa

Rétt er að deila ábyrgð á lykilverkefnum niður á hæfilega marga starfsmenn til að draga úr hættu á mistökum eða misferli. Af þessu leiðir m.a. að aðgreina þarf ábyrgð á meðferð fjármuna og heimilda til útgjalda. Sami starfsmaðurinn á ekki að sjá um alla þætti tiltekins verkefnis. Ef ómögulegt er að komast hjá slíku ætti að skylda þá starfsmenn til þess að taka sumarfrí árlega og sjá til þess að aðrir sinni störfum þeirra á meðan.

Í leiðbeinandi tilmælum Fjármálaeftirlitsins um innra eftirlit og áhættustýringu hjá fjármálafyrirtækjum nr. 1/2002 segir:

> „Virkt innra eftirlitskerfi felur í sér að fyrir hendi sé viðeigandi aðgreining starfa og að hagsmunir mismunandi verkefna sama starfsmanns stangist ekki á. Hættu á hagsmunaárekstrum þarf að greina og lágmarka og þau starfssvið þar sem slík hætta er til staðar þurfa að vera háð nákvæmu sérstöku eftirliti.“

Ekki er tilgreint nákvæmlega í umræddum reglum Fjármálaeftirlitsins hvaða starfsþættir valda hagsmunaárekstrum en í grófum dráttum er æskilegt að eftirfarandi störf séu aðgreind:

- ✓ Meðhöndlun eigna (t.d. gjaldkeri – fjárvarsla er meginstarf hans).
- ✓ Skráning (t.d. bókari beri ábyrgð á skráningu í bókhaldið).
- ✓ Yfirferð og afstemmingar (t.d. fjármálastjóri sem hefur yfirsýn og samþykkir færslur).
- ✓ Stýring aðgangs að upplýsingakerfum og umsjón með uppfærslum (t.d. kerfisstjóri sem kemur eingöngu að tölvutæknilegum þáttum en ekki að fjármálum).

Á ensku hefur stundum verið talað um “ABCs of Separation of Duties” um aðgreiningu starfa.

> **A**sset handling and disposition.
> **B**ooking, or recording, transactions to the general ledger, subledgers, and journals.
> **C**omparison or review of transactions or balances.

Mikilvægi upplýsingakerfa í fjármálaumsýslu fer enn fremur sífellt vaxandi þannig að huga þarf vel að innri eftirlitsþáttum í upplýsingakerfum, m.a. að aðgreina kerfisstjórn og veitingu aðgangsheimilda frá störfum í fjármáladeildum fyrirtækja.

Íslenskar ríkisstofnanir eru margar hverjar mjög litlar skipulagsheildir sem gerir það að verkum að erfitt getur verið að koma við fullkominni aðgreiningu starfa. Stjórnendur bera ábyrgð á rekstri stofnunar og það er þeirra að taka ákvarðanir um hvernig skuli taka á takmarkaðri aðgreiningu starfa. Þeir gætu tekið ákvörðun um að lágmarka áhættuna með því að hafa aðrar eftirlitsaðgerðir sem bæta upp veikleika í aðgreiningu starfa. Þeir geta ákveðið að gera ekki neitt og búa við áhættuna þar sem þeir telji áhættuna ekki vera mjög mikla eða þeir geta tekið ákvörðun um að breyta starfaskiptingu á milli þeirra starfsmanna sem í hlut eiga. Slík áhættugreining og ákvarðanataka stjórnenda ætti að vera skjalfest.

Einnig væri hægt að eyða áhættunni af ósamrýmanlegum störfum með því að útvista tilteknum starfsþáttum til annarra stofnana. Þetta á sérstaklega við þegar um litlar stofnanir eru að ræða. Til dæmis má færa starf gjaldkera frá ríkisstofnun til greiðsluþjónustu Fjársýslunnar. Hugsanlega mætti færa bæði gjaldkera og bókara út úr viðkomandi stofnun og nota þess í stað bókhalds- og greiðsluþjónustu Fjársýslu ríkisins og tryggja aðgreiningu starfa með þeim þætti. Meirihluti stofnana ríkisins leysir aðgreiningu þessara starfa með þessum hætti.

### 5.2.2 Ábyrgð og aðgangur að eignum og skrám

Ganga ber tryggilega frá tækjum, birgðum, skuldabréfum og öðrum eignum sem hætta er á að geti horfið eða verði notaðar í heimildarleysi. Ljóst þarf að vera hverjir hafa aðgang og heimildir til að sýsla með eignirnar. Fela ætti tilteknum starfsmönnum ábyrgð á varðveislu þeirra. Þörf fyrir að takmarka umgang og ábyrgð er mismikil eftir verðmæti eigna og því hve auðvelt er að flytja þær til og ráðstafa þeim. Endurmeta þarf reglulega heimildir starfsmanna til að umgangast tilteknar eignir eða bera ábyrgð á þeim.

Að jafnaði ætti að takmarka aðgang að upplýsingakerfum. Hve víðtæk takmörkun þarf að vera er mismunandi eftir því hve viðkvæmar upplýsingarnar eru fyrir heimildarlausum breytingum eða aðgangi utanaðkomandi aðila að þeim. Endurskoða þarf aðgangsheimildir með reglulegu millibili.

### 5.2.3 Skipulag og stjórnun bókhalds

Í 7. gr. laga um bókhald nr. 145/1994 kemur m.a. fram að skipulag og stjórnun bókhalds skuli miðuð við að tryggja vörslu bókhaldsgagna og eðlilegt innra eftirlit. Með innra eftirliti er m.a. átt við verklagsreglur þar sem kveðið er á um meðferð skjala, ábyrgð og verkaskiptingu. Markmiðið er að tryggja áreiðanlegt bókhald, örugga meðferð og vörslu fjármuna og að ekki hljótist tjón af villum, mistökum eða misnotkun.

## 5.3 Aðgerðir sem byggja á staðfestingum

Eftirlit sem byggir á að tilteknar ákvarðanir verði að staðfesta með áritun miðar að því að tryggja að ákvörðunum stjórnenda sé framfylgt. Þetta er sú aðferð sem notuð er til þess að tryggja að aðeins það sé framkvæmt sem samþykkt hefur

verið. Staðfesting með undirskrift eða rafrænni áritun er eftirlitsaðgerð sem er mjög mikið notuð innan stofnana og fyrirtækja ríkisins, sbr. kröfur um samþykkt reikninga, beiðna o.fl.

Stjórnendur þurfa að setja starfsmönnum sínum reglur um hvenær þörf er á staðfestingu ákvörðunar og hverjir hafi heimild til staðfestingar með áritun.

## 5.4 Aðgerðir sem tryggja eiga gæði

### 5.4.1 Skráning færslna

Bókhald skal fært reglulega. Færslur ber að merkja og skrá réttilega. Viðskipti þarf að skrá strax eftir að þau hafa átt sér stað og önnur atriði svo fljótt sem verða má í þeim tilgangi að upplýsingar um þau nýtist stjórnendum sem fyrst. Skráningin nær til alls ferlis færslunnar og felur í sér bæði uppruna hennar og samþykki.

Fjársýsla ríkisins hefur yfirumsjón með bókhaldi og reikningsskilum ríkisaðila. Hlutverk hennar er að sjá um að samræmi sé í færslu bókhalds og gerð reikningsskila þessara aðila. Fjársýsla ríkisins hefur í þessu skyni gefið út ýmsar leiðbeiningar og verklagsreglur sem ríkisaðilum ber að fylgja (sjá: www.fjs.is).

### 5.4.2 Skriflegar lýsingar

Gera verður þá kröfu að til séu skriflegar lýsingar á þeim innri eftirlitsaðgerðum sem beitt er innan hvers fyrirtækis eða stofnunar. Lýsa þarf viðkomandi aðgerð og tilganginum með henni eða m.ö.o. hvað þarf að gera, hvernig á að gera það, og hvers vegna. Benda má á að Ríkisendurskoðun hefur gefið út leiðbeiningar um skjalfestingu innra eftirlits fyrir stofnanir í A-hluta.[3]

Dæmi eru um kröfur í lögum um skriflegar lýsingar á tilteknu ferli og má í því sambandi vísa til 7. gr. laga um bókhald nr. 145/1994 en þar er gerð krafa um að skrifleg lýsing á skipulagi og uppbyggingu bókhalds liggi fyrir og skal m.a. veita upplýsingar um tölvukerfi og tölvubúnað, tengsl við aðrar tölvur og hlutverk þeirra. Ef sjálfvirkri tölvuúrvinnslu er beitt í bókhaldi skal á sama hátt liggja fyrir lýsing á henni á þann hátt að unnt sé án erfiðleika að fylgja eftir og hafa eftirlit með vinnslu hverrar færslu. Reikningar bókhaldsins skulu sérstaklega tilgreindir og notkun þeirra greinilega afmörkuð, svo og lýsing á tekjuskráningu.

## 5.5 Aðgerðir vegna upplýsingakerfa

Þó svo að einstakar innri eftirlitsaðgerðir séu útfærðar með öðrum hætti í upplýsingakerfum en í handvirkum kerfum, byggja þær allar á sömu grundvallaratriðunum. Nauðsynlegt er að skilgreina og nota öflugar innri eftirlitsaðgerðir í upplýsingakerfum. Á grundvelli slíkra eftirlitsaðgerða á að vera hægt að meta hvort gögn séu gild og hvort notandi hafi heimildir til þess að skrá, breyta eða nota ákveðin gögn í upplýsingakerfum.

Eftirlitsaðgerðir vegna upplýsingakerfa og gagna sem þau geyma eru annars vegar

[3] https://rikisendurskodun.is/wp-content/uploads/2016/01/Innra_eftirlit_i_stofnunum_A-hluta__nytt_skjal__09.05.2012.pdf

vegna rekstraröryggis kerfanna og hins vegar vegna áreiðanleika og vörslu gagnanna.

### 5.5.1 Rekstraröryggi upplýsingakerfa

Nú eru flestir ríkisaðilar svo háðir upplýsingakerfum sínum að ef þau eru ekki í rekstrarhæfu ástandi er starfsemi viðkomandi meira og minna lömuð. Aðaltilgangur eftirlitsaðgerða vegna upplýsingakerfa ætti því að vera sá að tryggja rekstrarhæfi kerfanna.

Rekstraröryggi upplýsingakerfa miðar að því að:

- ✓ Upplýsingakerfi séu aðgengileg.
- ✓ Upplýsingakerfi séu nothæf.

Almenn innri eftirlitsatriði vegna rekstraröryggis upplýsingakerfa eru í stórum dráttum þau sömu óháð því hvernig tölvurekstri er háttað. Þau felast m.a. í eftirliti með afritatöku og aðgangi, verkaskiptingu og aðgreiningu starfa við keyrslu forrita, gerð og prófun neyðaráætlana, kaupum, uppsetningu og viðhaldi á kerfishugbúnaði og þróun og viðhaldi á hugbúnaði.

### 5.5.2 Áreiðanleiki gagna

Það er grundvallaratriði að stofnanir og fyrirtæki gefi réttar upplýsingar eða afgreiði mál á réttum forsendum. Því eiga eftirlitsaðgerðir einnig að beinast að því að tryggja áreiðanleika gagna.

Áreiðanleiki gagna felst í því að:

- ✓ Gögn séu rétt færð inn.
- ✓ Gögn séu heildstæð, þ.e. öll gögn færð inn.
- ✓ Gögn séu gild en ekki úrelt.

Eftirlitsaðgerðir sem ætlað er að tryggja áreiðanleika gagna í upplýsingakerfum felast í því að ganga úr skugga um að gögn séu rétt færð inn, þau séu heildstæð og gild.

### 5.5.3 Viðeigandi gagnaleynd

Stofnanir og fyrirtæki vinna oft með upplýsingar sem almenningi er tryggður aðgangur að, t.d. samkvæmt upplýsingalögum nr. 140/2012, en frá þessu eru þó mikilvægar undantekningar sbr. lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000. Mikilvægt er að leynd gagna sé tryggð þegar hún á við. Gagnaleynd getur t.d. verið nauðsynleg vegna meðferðar viðkvæmra persónuupplýsinga eða eignaréttar-, höfundarréttar- og samkeppnissjónarmiða.

## 5.6 Atriði til athugunar

Hér eru nokkrar spurningar sem ætlað er að vekja stjórnendur til umhugsunar um æskilegar eftirlitsaðgerðir.

| | Eftirlitsaðgerðir | Já | Nei | Ath. |
|---|---|---|---|---|
| | **Aðgerðir stjórnenda** | | | |
| 1. | Er val eftirlitsaðgerða byggt á niður-stöðum formlegs áhættumats? | | | |
| 2. | Sýna stjórnendur í verki jákvætt viðhorf til eftirlitsaðgerða? | | | |
| 3. | Er verkstjórn sinnt með viðeigandi hætti? | | | |
| 4. | Er starfsfólki gerð skýr grein fyrir mikilvægi þess að farið sé eftir verklagsreglum í sambandi við eftirlitsaðgerðir? | | | |
| | **Aðgerðir byggðar á skipulagi** | | | |
| 5. | Er tryggt að enginn einn starfsmaður sjái í óeðlilega langan tíma um alla þætti tiltekins verkefnis? | | | |
| 6. | Er þess krafist að lykilstarfsmenn fari árlega í sumarfrí og að verkefni þeirra séu falin öðrum? | | | |
| 7. | Eru störf gjaldkera og bókara aðskilin? | | | |
| 8. | Er aðgangur að eignum og gögnum takmarkaður? | | | |
| 9. | Er einhver ábyrgur fyrir varðveislu eigna? | | | |
| | **Aðgerðir sem byggja á staðfestingu** | | | |
| 10. | Er krafist staðfestingar stjórnenda með áritun til að tryggja að eingöngu fari fram samþykkt viðskipti eða verkefni? | | | |
| | **Aðgerðir sem tryggja eiga gæði** | | | |
| 11. | Liggja fyrir skriflegar reglur um meðferð, skráningu og varðveislu gagna og skjala? | | | |
| 12. | Er eftirlitsaðgerðum beitt til að tryggja með raunhæfum hætti áreiðanleika gagna? | | | |
| 13. | Liggur fyrir skrifleg lýsing á skipulagi og uppbyggingu bókhalds? | | | |
| | **Aðgerðir vegna upplýsingakerfa** | | | |
| 14. | Er rekstraröryggi upplýsingakerfa byggt upp með þeim hætti að það tryggi að þau séu aðgengileg og nothæf þegar þörf krefur? | | | |
| 15. | Er viðeigandi gagnaleynd tryggð í upplýsingakerfum þegar unnið er með trúnaðarupplýsingar? | | | |

# 6 Upplýsingar og samskipti

Til þess að stjórnendur geti haft yfirsýn yfir reksturinn þurfa þeir að fá áreiðanlegar og viðeigandi upplýsingar um hann. Gögn þarf því að skrá og síðan að vinna úr þeim upplýsingar sem miðlað er tímanlega og í viðeigandi formi til stjórnenda og annarra innan stofnunar eða fyrirtækis sem þurfa á þeim að halda. Stjórnendur verða að vera meðvitaðir um að með auknum og greiðari aðgangi starfsmanna að ýmsum upplýsingum og upplýsingakerfum breytist allt flæði upplýsinga innan stofnunar eða fyrirtækis. Áður komu upplýsingar fyrst til stjórnenda sem síðan skiluðu þeim áfram til undirmanna. Nú geta undirmenn oft aflað sér upplýsinga beint auk þess sem samskipti þeirra við samstarfsmenn og aðra eru oft með öðrum hætti en áður vegna tæknibreytinga. Þetta gerir eftirlitshlutverk stjórnenda enn mikilvægara.

Stjórnendur þurfa að upplýsa starfsmenn um þá ábyrgð sem þeir bera á tilteknum þáttum í innra eftirliti. Mikilvægt er að samskipti á vinnustað séu með þeim hætti að starfsmenn geti komið upplýsingum um veikleika í innra eftirliti á framfæri við stjórnendur.

Eftirfarandi þrír þættir eru taldir ráða mestu um árangur í upplýsingagjöf og samskiptum í tengslum við innra eftirlit. Þessir þættir eru:

- ✓ Stofnunin/fyrirtækið aflar eða býr til og notar viðeigandi upplýsingar til að styðja við virkni annarra þátta innra eftirlits.

- ✓ Stofnunin/fyrirtækið miðlar upplýsingum innanhúss, þ.m.t. upplýsingum um markmið og hvernig ábyrgð stjórnenda og starfsmanna er háttað, til þess að styðja við virkni innra eftirlits.

- ✓ Stofnunin/fyrirtækið miðlar upplýsingum til aðila utan stofnunarinnar/ fyrirtækisins um atriði er varða virkni innra eftirlits.

## 6.1 Upplýsingar sem skipta máli

Ef stofnanir og fyrirtæki ríkisins eiga að ná markmiðum sínum er nauðsynlegt að góðar upplýsingar um alla þætti rekstrarins liggi fyrir.

Upplýsingakerfi eru í síauknum mæli hluti af vinnuumhverfi rekstraraðila. Bætt tækni við söfnun og greiningu upplýsinga hefur gert stjórnendum kleift að bregðast hraðar og á skilvirkari hátt við ýmsum vandamálum sem upp koma í rekstrinum. Upplýsingakerfi eru ómissandi við eftirlit með viðfangsefnum rekstraraðila því þau fylgjast með og skrá viðskipti um leið og til þeirra er stofnað, auk þess sem þau viðhalda og veita upplýsingar um fjárhagsleg málefni og önnur atriði sem tengjast rekstrinum.

Gæði þeirra upplýsinga sem safnað er, haldið er við og birtar eru í upplýsingakerfum, skipta miklu máli við ákvarðanatöku og geta því haft veruleg áhrif á frammistöðu þeirra sem stjórna rekstrinum. Mat á gæðum upplýsinga felst í að kanna hvort þær eru viðeigandi, tímanlegar, í gildi, nákvæmar og aðgengilegar. Gæði upplýsinga eru í réttu hlutfalli við styrkleika innra eftirlits.

## 6.2 Innri samskipti

Skilvirk samskipti innan viðkomandi stofnunar eða fyrirtækis eru mjög mikilvæg fyrir öflugt innra eftirlit. Til þess að tryggja skilvirk innri samskipti þarf að huga að eftirfarandi þáttum.

- ✓ Nauðsynlegt er að forstöðumenn upplýsi starfsmenn rækilega um mikilvægi ábyrgðar þeirra á innra eftirliti og að þeir sinni því af alúð.

- ✓ Starfsskyldur hvers starfsmanns þurfa að vera skýrar. Hver og einn verður að skilja til hlítar þátt innra eftirlits í starfi sínu. Þeim verður einnig að vera ljóst hvernig störf þeirra tengjast störfum annarra starfsmanna því það auðveldar mönnum að koma auga á vandamál, greina orsakir þeirra og grípa til viðeigandi aðgerða.

- ✓ Starfsfólki verður að vera ljóst að þegar óvænt atvik koma upp í starfi þeirra nægir ekki að bregðast eingöngu við þeim. Finna verður orsökina svo hægt sé að bæta við eða breyta eftirlitsaðgerðum og reyna þannig að koma í veg fyrir að sagan endurtaki sig.

- ✓ Starfsfólk þarf að geta miðlað upplýsingum um veikleika í innra eftirliti til yfirmanna. Mikilvægt er að brugðist sé við ábendingum starfsmanna á viðunandi hátt. Oft er hægt að koma í veg fyrir að veikleikar í innra eftirliti skapi vandamál í rekstrinum.

- ✓ Innan einstakra stofnana og fyrirtækja þarf að vera starfandi hópur sem hefur yfirsýn yfir starfsemina. T.d. er nauðsynlegt að yfirmenn haldi reglulega fundi þar sem fjallað er um frammistöðu, þróun, áhættuþætti, helstu nýjungar í starfseminni og önnur mikilvæg mál.

## 6.3 Ytri samskipti

Stofnanir og fyrirtæki eiga að jafnaði samskipti við ýmsa utanaðkomandi aðila sem geta haft áhrif á viðfangsefni, verkefni, rekstur og aðra þætti starfseminnar. Í stjórnsýslulögum nr. 37/1993 eru settar ýmsar kröfur til ríkisstofnana sem þær þurfa að fylgja í samskiptum við ytri aðila. Hér á eftir eru nefndir nokkrir þættir er snúa að innra eftirliti sem tengjast ytri samskiptum:

- ✓ Farvegur þarf að vera til staðar fyrir samskipti við utanaðkomandi aðila vegna þess að þeir geta miðlað mikilvægum upplýsingum, t.d. um gæði þjónustu viðkomandi stofnunar eða fyrirtækis og þar með um virkni innra

eftirlits. Ef t.d. er kvartað undan þjónustu tiltekins starfsmanns ætti starfsmaður óháður honum að sinna kvörtuninni.

- ✓ Þeim sem eiga í viðskiptum eða samskiptum við stofnanir og fyrirtæki skal gert ljóst að atferli eins og útgáfa óréttmætra reikninga eða móttaka óviðeigandi greiðslna er ekki liðið.

- ✓ Stjórnendur verða að tryggja að athugasemdir endurskoðenda séu teknar til alvarlegrar skoðunar og viðunandi úrbætur gerðar.

- ✓ Upplýsingagjöf til utanaðkomandi aðila á að vera í samræmi við þarfir þeirra.

## 6.4 Atriði til athugunar

Hér eru nokkrar spurningar sem ætlað er að vekja stjórnendur til umhugsunar um atriði sem snerta upplýsingar og samskipti.

| | Upplýsingar og samskipti | Já | Nei | Ath. |
|---|---|---|---|---|
| 1. | Skila upplýsingakerfi reglulega áreiðanlegum og viðeigandi upplýsingum sem nýtast við ákvarðanatöku? | | | |
| 2. | Eru rekstrarupplýsingar (bókhalds o.fl.) bornar saman við fyrri tímabil, markmið og fjárheimildir? | | | |
| 3. | Eru verklagsreglur, handbækur, lagafyrirmæli og samþykktir kynntar starfsfólki með virkum hætti? | | | |
| 4. | Eru gildandi verklagsreglur í samræmi við gildandi fyrirmæli laga og reglugerða? | | | |
| 5. | Eru starfsmenn upplýstir um starfskyldur sínar vegna innra eftirlits? | | | |
| 6. | Skilgreinir skipurit með skýrum hætti boðleiðir innan stofnunar eða fyrirtækis? | | | |
| 7. | Ef stjórn er til staðar er tryggt að rekstrarupplýsingar berist henni? | | | |
| 8. | Eru starfsmenn hvattir til að miðla upplýsingum um veikleika í innra eftirliti til stjórnenda? | | | |
| 9. | Fer óháður starfsmaður með kvartanir? | | | |
| 10. | Liggja fyrir skriflegar reglur um samskipti við viðskiptavini? | | | |
| 11. | Er reglulega farið yfir samninga við utanaðkomandi aðila? | | | |

# 7 Vöktun

Þar sem aðstæður breytast ört þurfa stjórnendur að fylgjast glöggt með innra eftirliti og meta hvort aðgerðir þess eigi við og geti tekist á við breytta eða nýja áhættu. Hugtakið vöktun er í þessu riti notað sem samheiti yfir hið stöðuga eftirlit sem á sér stað þegar fylgst er með framgangi innra eftirlitsins svo og þegar gerðar eru sérstakar úttektir á því.

Eftirfarandi tveir þættir eru taldir ráða mestu um árangur af vöktun í tengslum við innra eftirlit. Þessir þættir eru:

- ✓ Stofnunin/fyrirtækið velur, þróar og beitir viðvarandi vöktun og sérstökum prófunum til þess að meta hvort innra eftirlit sé til staðar og hvort það virki sem skyldi.

- ✓ Stofnunin/fyrirtækið metur frávik í innra eftirliti tímanlega og miðlar upplýsingum um það til viðeigandi ábyrgðaraðila svo þeir geti brugðist við, eins og viðeigandi þykir hverju sinni.

## 7.1 Stöðugt eftirlit

Því öflugra sem stöðuga eftirlitið er þeim mun minni þörf er á sérstökum úttektum. Stöðuga eftirlitið felst í raun í flestum daglegum störfum.

Þær aðferðir sem notaðar eru til að fylgjast með virkni innra eftirlits eru margar og mismunandi frá einum aðila til annars. Venjulega felast þær þó í reglulegum stjórnunarstörfum og verkstjórn, samanburði, samræmingu og öðrum hefðbundnum eftirlitsstörfum.

- ✓ Hluti af hefðbundnu starfi stjórnenda ætti að vera að afla upplýsinga um það hvort innra eftirlitið virki sem skyldi. Reglulega ætti að bera saman upplýsingar sem eiga sér ólíkan uppruna. Veruleg ónákvæmni eða frávik eru vísbendingar um hugsanlega veikleika í innra eftirliti.

- ✓ Upplýsingar frá utanaðkomandi aðilum ættu að vera samhljóða upplýsingum sem verða til innan stofnunar eða fyrirtækis. Ef svo er ekki er það vísbending um að huga þurfi að innra eftirliti. Viðskiptavinur sem greiðir reikning sinn möglunarlaust er í raun að staðfesta þær upplýsingar sem koma fram á honum. Kvarti viðskiptavinurinn á hinn bóginn getur falist í því vísbending um ófullnægjandi innra eftirlit.

- ✓ Skipurit rekstraraðila og viðeigandi verkstjórn ætti að veita yfirsýn yfir innri eftirlitsaðgerðir. Sjálfvirk villuboð og ábendingar við skráningu gagna í upplýsingakerfi, ásamt starfi þeirra sem vinna við kerfin, stuðla t.d. að því

að færslur séu réttar og færðar inn í heild sinni. Aðskilnaður starfa og dreifing ábyrgðar minnka möguleika á misferli.

- ✓ Bera ætti eignaskrá í upplýsingakerfum saman við talningu á eignum og kanna misræmi ef það kemur fram.

## 7.2 Sérstakar úttektir á innra eftirliti

Það er á ábyrgð stjórnenda að innra eftirlit virki sem skyldi hvort sem þeir fylgjast stöðugt með því eða sjá til þess að sérstakar úttektir á innra eftirliti séu gerðar. Dæmi um kröfur árlegra úttekta á innra eftirliti má finna í fyrirmælum opinberra aðila, sbr. reglur Fjármálaeftirlitsins nr. 577/2012 um endurskoðunardeildir og sjálfstætt starfandi eftirlitsaðila lífeyrissjóða.

Eftir því sem vöktun stjórnenda er meiri og virkari því minni þörf er fyrir sérstakar úttektir á innra eftirliti. Umfang og efnistök fara eftir áhættustigi starfseminnar og þörf fyrir að draga úr áhættu í rekstrinum. Sjaldnast er nauðsynlegt að sérstök úttekt nái til allra þátta innra eftirlits. Algengara er að hún nái aðeins til tiltekinna þátta þess. Þó kann að vera þörf á sérstakri úttekt í kjölfar skipulagsbreytinga, samdráttar í starfsemi eða breytinga í rekstri.

Þeir sem taka út innra eftirlit verða skilyrðislaust að þekkja eða hafa innsýn í starfsemi viðkomandi stofnunar/fyrirtækis og það verkferli sem þeir eru að skoða. Þeir verða einnig að gera sér grein fyrir því hvernig eftirlitið virkar í raun með því að prófa það og bera niðurstöður við það hvernig eftirlitinu var ætlað að virka. Sérstaklega þarf að huga að nýjum eða breyttum verkferlum og verkferlum sem hafa verið lagðir niður.

Ýmis efnistök eru möguleg. T.d. má nota gátlista, markmiðalista, flæðirit, mælingar og beinar prófanir til þess að athuga hve vel innri eftirlitsaðgerðir virka. Einnig má beita samanburði við aðrar stofnanir eða fyrirtæki ríkisins, önnur fyrirtæki eða almennar viðskiptavenjur. Beita ætti þeim efnistökum sem best eiga við hverju sinni miðað við aðstæður og tilgang úttektarinnar.

Áður hefur komið fram að æskilegt er að fyrir liggi skrifleg lýsing á innra eftirliti. Þrátt fyrir þetta getur óformlegri og óskjalfestri innri eftirlitsaðgerð verið beitt. Prófa ætti slíkar aðgerðir og ef þær reynast vel ætti að skjalfesta þær. Jafnframt er eðlilegt að mælst sé til þess við stjórnendur að þeir staðfesti þessar viðbótaraðgerðir með formlegum hætti. Góðar skriflegar lýsingar á innra eftirliti auðvelda úttekt á því auk þess sem lýsingin nýtist starfsfólki til skilnings á uppbyggingu innra eftirlits og hlutverki þeirra sjálfra í því. Viðeigandi lýsing er og nauðsynleg ef aðrir þurfa að fræðast um virkni innra eftirlits eða niðurstöður úttektar.

## 7.3 Viðbrögð við frávikum og veikleikum í innra eftirliti

Veikleikar í innra eftirliti geta komið í ljós við vöktun á eftirliti, í sérstökum úttektum eða með ábendingum utanaðkomandi aðila. Slíkir veikleikar geta valdið tjóni eða skapað erfiðleika.

Upplýsa þarf um veikleika þegar þeir finnast. Það er háð eðli þeirra og afleiðingum hverjum þarf að greina frá þeim en hægt er að setja um það tilteknar viðmiðunarreglur. Gera ætti forstöðumanni grein fyrir öllum alvarlegum veikleikum, villum, vandamálum eða brotum á stefnu eða verklagsreglum vegna innra eftirlits. Jafnframt ætti tilkynning að berast þeim starfsmanni sem ber ábyrgð á því verkferli sem veikleikinn tengist.

Að sjálfsögðu nægir ekki að greint sé frá veikleika í innra eftirliti. Nauðsynlegt er að viðkomandi eftirlitsaðgerð sé endurmetin og lagfærð ef þess er þörf.

## 7.4 Atriði til athugunar

Hér eru nokkrar spurningar sem ætlað er að vekja stjórnendur til umhugsunar um samtímaeftirlit.

| | Samtímaeftirlit | Já | Nei | Ath. |
|---|---|---|---|---|
| 1. | Eru stjórnendur vakandi yfir því að gera þurfi breytingar á innra eftirliti vegna breyttra aðstæðna eða nýrrar áhættu? | | | |
| 2. | Fylgist stjórn með því að brugðist sé við mikilvægum vandamálum sem upp koma í rekstrinum? | | | |
| 3. | Eru gerðar sérstakar úttektir á innra eftirliti í kjölfar mikilla skipulagsbreytinga, samdráttar í starfsemi og annarra meiriháttar breytinga á rekstri | | | |
| 4. | Eru niðurstöður úr eigin upplýsingakerfum bornar saman við upplýsingar frá utanaðkomandi aðilum? | | | |
| 5. | Gera þeir sem vinna við bókhald og gagnavinnslu afstemmingar reglulega? | | | |
| 6. | Eru allir veikleikar í innra eftirliti tilkynntir þeim starfsmönnum sem ábyrgð bera á þeim? | | | |

# 8 Takmörk innra eftirlits

Það er sama hversu öflugt innra eftirlit er, það getur aldrei tryggt að stofnanir og fyrirtæki nái markmiðum sínum. Ástæðan er sú að á eftirlitinu geta verið ýmsir annmarkar sem draga úr gæðum þess, svo sem mannleg mistök, kæruleysi, þreyta, möguleikar stjórnenda á því að ýta reglum innra eftirlitsins til hliðar og hugsanleg sammæli einstaklinga um að brjóta reglur þess. Þá ætti kostnaður við innra eftirlitið aldrei að vera meiri en ávinningur af því. Auk þessa geta atvik eða aðstæður utan valdsviðs viðkomandi stundum valdið því að markmið stofnunar eða fyrirtækis nást ekki.

## 8.1 Mannleg mistök

Innra eftirlit girðir ekki fyrir óskynsamlegar eða ófullnægjandi ákvarðanir stjórnenda. Oft þurfa þeir jafnvel að taka ákvarðanir í tímaþröng eða undir þrýstingi án þess að hafa aflað nauðsynlegra upplýsinga. Í slíkum tilvikum reynir mest á dómgreind, reynslu og þekkingu þess sem ákvörðun tekur.

Innra eftirlit getur orðið einskis nýtt vegna mistaka starfsmanna, t.d. þegar þeir misskilja leiðbeiningar eða gera mistök vegna kæruleysis, hugsunarleysis eða þreytu. Mistök af þessu tagi kunna að eiga sér stað vegna ónógrar verkstjórnar, þjálfunar eða leiðbeininga.

## 8.2 Stjórnendur geta ýtt reglum til hliðar

Stjórnendur geta í skjóli valds síns ýtt reglum innra eftirlits til hliðar með því að sniðganga fyrirfram skilgreind stefnumið, verklagsreglur og aðrar eftirlitsaðgerðir hvort sem er í eigin þágu eða í þágu viðkomandi stofnunar eða fyrirtækis.

Stjórnandi getur ýtt reglum innra eftirlits til hliðar, t.d. til þess að hagnast sjálfur fjárhagslega, láta líta út fyrir að fjárhagsstaðan sé betri en hún er í raun eða til að láta líta út fyrir að lögum og reglum sé fylgt þegar svo er ekki. Stjórnandi getur í þessu skyni bæði falsað gögn og notað villandi framsetningu við ráðuneyti, starfsmenn, endurskoðendur eða viðskiptavini.

Stjórnandi getur einnig í krafti valds síns ýtt reglum innra eftirlits til hliðar við óvenjulegar aðstæður vegna þess að hann telur það vera réttlætanlegt í þágu stofnunar sinnar eða fyrirtækis. Skjalfesta ætti slík tilvik og upplýsa þá sem málið varðar um þau.

## 8.3 Sammæli um að brjóta reglur um innra eftirlit

Ef einstaklingar sammælast um að brjóta reglur innra eftirlits og leyna því getur það leitt til þess að gefnar eru rangar upplýsingar um fjárhag eða önnur mikilvæg málefni. Þetta veikir að sjálfsögðu innra eftirlit og því þarf að hafa vakandi auga með slíku.

## 8.4 Kostnaður ætti ekki að vera meiri en ávinningur

Þegar draga á úr tiltekinni áhættu eða koma í veg fyrir hana er annars vegar valin viðeigandi eftirlitsaðgerð á grundvelli mats á líkum á tjóni og hve mikið það yrði og hins vegar á mati á kostnaði við mismunandi eftirlitsaðgerðir. Kostnaður við aðgerð ætti ekki að vera meiri en ávinningurinn af henni.

Yfirleitt er auðveldara að áætla kostnað við að taka tiltekinn eftirlitsþátt í notkun en að meta ávinninginn af honum. Almennt má segja að of viðamikið eftirlit sé dýrt og virki hamlandi en of lítið eftirlit auki áhættu í rekstri. Það er stjórnenda að viðhalda virku innra eftirliti, þar á meðal að vega og meta kostnað og ávinning af því.

## 8.5 Treyst á innra eftirlit annarra aðila

Með aukinni notkun og samtengingu upplýsingakerfa eru stofnanir og fyrirtæki ríkisins í auknum mæli að byggja á og treysta gögnum sem verða til í upplýsinga-kerfum annarra aðila, bæði einkaaðila og ríkisaðila. Notkun og traust á innra eftirliti annarra aðila getur skilað mikilli hagkvæmni og skilvirkni fyrir alla svo lengi sem innra eftirlit og gæði gagnanna er í lagi. Hins vegar gæti ríkisaðili þurft að fá einhverja staðfestingu á því að innra eftirlit sé fullnægjandi hjá þeim ytri aðila sem vinnur mikilvæg gögn sem byggt er á.

# Helstu heimildir


Alþjóðasamtök ríkisendurskoðunarstofnana (INTOSAI). (2004). **Guidelines for Internal Control Standards for the Public Sector** (INTOSAI GOV 9100). Sótt af http://www.issai.org/en_us/site-issai/issai-framework/intosai-gov.htm

Alþjóðasamtök ríkisendurskoðunarstofnana (INTOSAI). (2004). **Internal Control: Providing a Foundation for Accountability in Government** (INTOSAI GOV 9120). Sótt af http://www.issai.org/en_us/site-issai/issai-framework/intosai-gov.htm

Australian National Audit Office. (1998). **Framework for Effective Control**.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). **Internal Control — Integrated Framework**. Sótt af http://www.coso.org/IC.htm

Committee of Sponsoring Organizations of the Treadway Commission. (2009). **Guidance on Monitoring Internal Control Systems: Introduction**.

Ernst & Young. (1997). **Reporting on Internal Financial Control.**

Information Systems Audit and Control Foundation. (2016). **COBIT**. Sótt af http://www.isaca.org/COBIT/Pages/default.aspx

PWC – Ísland. (2017). I**nnra eftirlit – Mikilvægur þáttur í stjórnarháttum fyrirtækja**.

United States Government Accountability Office. (2014). **Standards for Internal Control in The Federal Government**. Sótt af http://www.gao.gov/products/GAO-14-704G

Ríkisendurskoðun – Bríetartúni 7
Pósthólf 5350 – 125 Reykjavík
Sími 569-7100
postur@rikisendurskodun.is – www.rikisendurskodun.is