

Deloitte.

Innra eftirlit og stjórnun upplýsingakerfa

Tryggvi R. Jónsson
Deloitte – ERS
12. maí 2009



Áhættuþjónusta (ERS) Deloitte

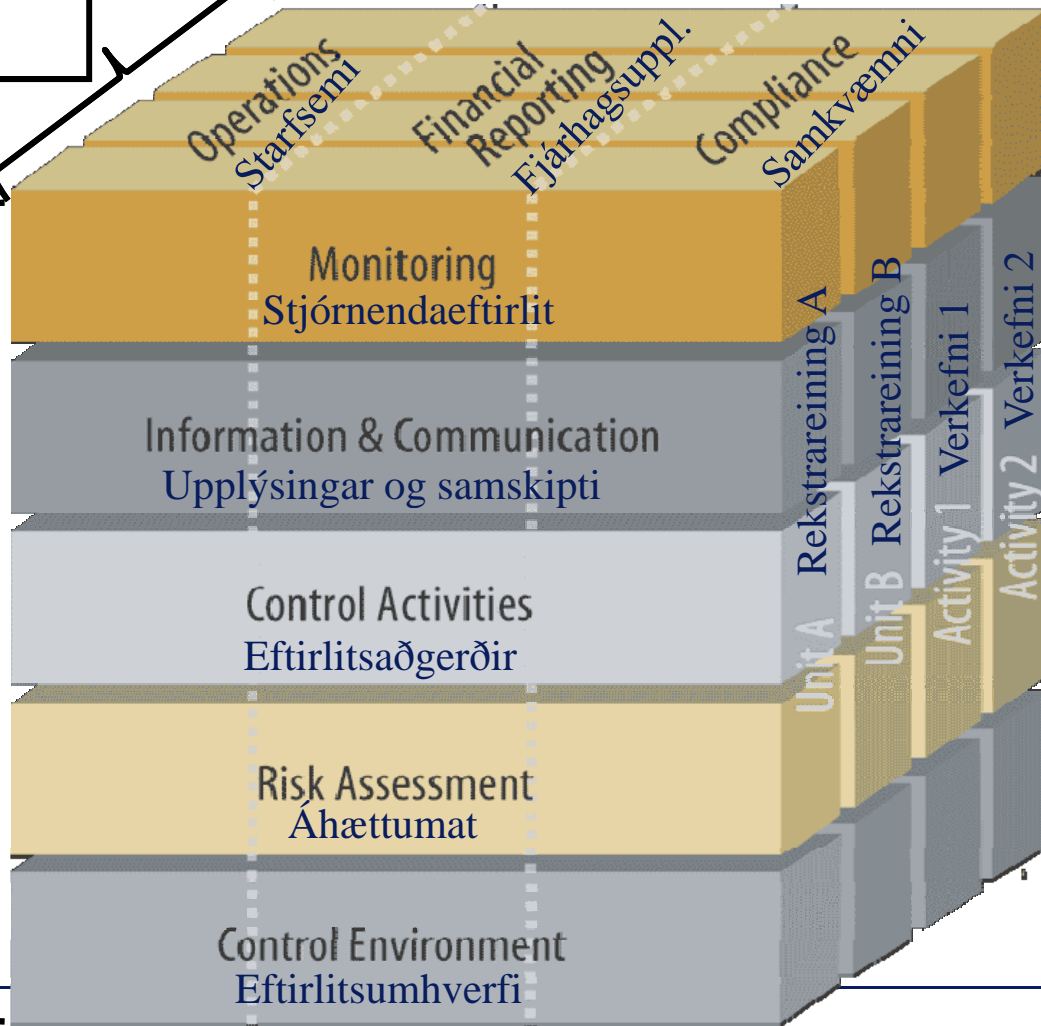
Áhættuþjónusta Deloitte (Enterprise Risk Services, ERS) miðar að því að veita þjónustu sem mætir vaxandi notkun á upplýsingatækni í starfsemi fyrirtækja.

- Endurskoðun innra eftirlits (Control Assurance) og önnur þjónusta á sviði innra eftirlits m.a. innra eftirlit upplýsingakerfa.
- Innri endurskoðun (Internal Audit).
- Ráðgjöf á sviði upplýsingaöryggis (Security and Privacy).



Innra eftirlit – COSO teningurinn

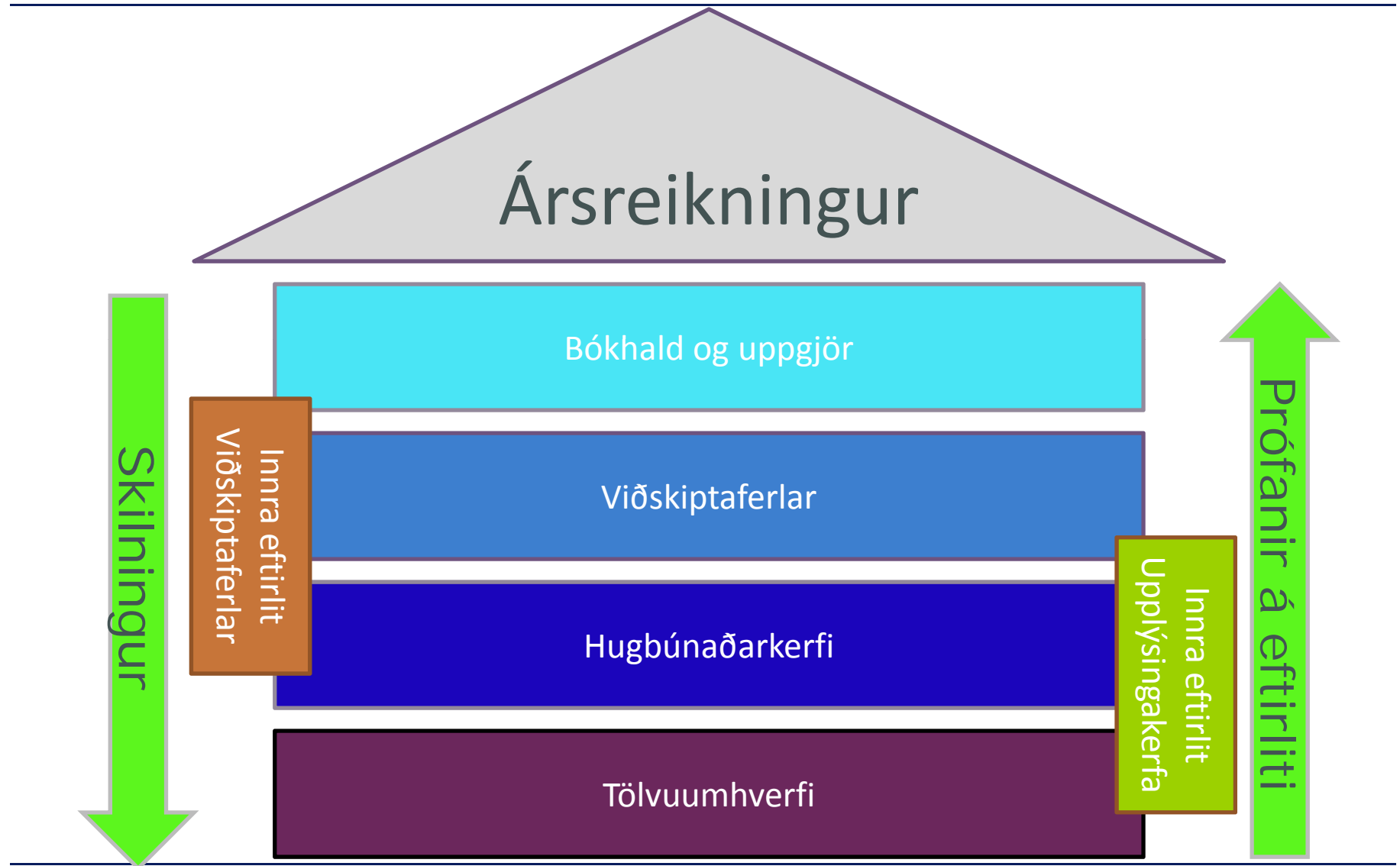
Ofan á teningnum eru þrjú markmið innra eftirlits.



Á framhlið teningsins má sjá 5 þætti innra eftirlits.

Á hægri hlið teningsins eru starfssemisþættir fyrirtækisins.

Ytri endurskoðun – fjárhagsupplýsingar og ársreikningur



Upplýsingakerfin geta komið víða við

- Fjárhagsupplýsingar.
- Upplýsingar um viðskiptavini/skjólstæðinga, t.d. sjúkraskrár (leynd).
- Starfsemistengdar upplýsingar, t.d. um framleiðslu, rannsóknir, notkun.
- Aðgengi að kerfum getur skipt mestu (t.d. vefverslun, fjarskiptafyrirtæki).



Val eftirlitsþátta

- Ákveða þarf hvaða eftirlitsþætti þarf að innleiða.
- Hvernig skal byrja og velja eftirlitsþætti?
 - ISO 27xxx / 17799 / BS7799
 - COBIT
 - PCI DSS
 - ITIL
 - Ytri kröfur (FME, PV, endurskoðendur)
 - Algeng atvik (kannanir, vefsíður, o.fl.)
 - Eigið áhættumat
- 5.000 eftirlitsþættir !
- Deming hringurinn: Plan – Do – Check – Act



Hönnun og skjölun eftirlitsþátta

- Hver er tilgangurinn eða markmiðið með eftirlitsþætti í veg fyrir hvað er verið að koma, hvaða kröfur er verið að uppfylla eða hvaða áhættu er verið að vega á móti? (Design/Plan)
- Hvernig er eftirlitsþáttur útfærður, hvað erum við að gera til að ná tilganginum? (Implementation/Do)
- Hver ber ábyrgð á framkvæmdinni?
- Hver er tíðnin?
- Hvar er útfærslan skjöluð (SOP)?
- Hvar eru gögn um framkvæmdina geymd (audit trails)?
- Hvernig prófum við framkvæmdina? (Testing / Check)?
- Hvernig lagfærum við framkvæmdina (Act)?



Dæmi: Aðgangsvéitingar

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Aðgangur sé í samræmi við starfssvið viðkomandi starfsmanns og ekki umfram það sem þarf.	Yfirmenn heimila aðgang starfsmanna sinna við hverja aðgangsvéitingu með tölvupósti, sem tölvudeild varðveitir í sérstöku pósthólfi, áður en tölvudeild veitir aðgang í samræmi við starfssvið viðkomandi starfsmanns.	Innri endurskoðandi tekur út aðgangslista og ber undir rýni viðkomandi yfirmanna ársfjórðungslega.

Hvað með aðskilnað hlutverka? Innri endurskoðandi lagði höfðuðið í bleyti og fann í gamalli kennslubók matrixu yfir aðskilnað hlutverka.

Dæmi: Aðgangssveitingar – útgáfa 2

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Aðgangur sé í samræmi við starfssvið viðkomandi starfsmanns og ekki umfram það sem þarf.	Yfirmenn heimila aðgang starfsmanna sinna við hverja aðgangssveitingu með tölvupósti, sem tölvudeild varðveitir í sérstöku pósthólfi, áður en tölvudeild veitir aðgang í samræmi við starfssvið viðkomandi starfsmanns.	Innri endurskoðandi tekur út aðgangslista og ber undir rýni viðkomandi yfirmanna ársfjórðungslega. Innri endurskoðandi ber aðgangsheimildir saman við kröfur um aðskilnað hlutverka.

Í ljós kom að yfirmenn báðu almennt um “öll réttindi” og því aðskilnaður hlutverka ekki studdur af aðgangstakmörkunum kerfa. Tölvudeild fékk hugmynd að umbótum...

Dæmi: Aðgangssveitingar – útgáfa 3

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Aðgangur sé í samræmi við starfssvið viðkomandi starfsmanns og ekki umfram það sem þarf.	Yfirmenn óska eftir aðgangi í gegnum vefsíðu þar sem hægt er að velja fyrirfram ákveðin hlutverk (bókari, gjaldkeri, o.fl.) af fellilista sem er svo sent inn í verkbeiðnahólf tölvudeildar sem setur upp notanda samkvæmt viðkomandi aðgangsheimildum.	Innri endurskoðandi tekur út aðgangslista og ber undir rýni viðkomandi yfirmanna ársfjórðungslega. Innri endurskoðandi ber aðgangsheimildir saman við kröfur um aðskilnað hlutverka

Er ekki hægt að gera enn betur? Þarf þess? Fer eftir niðurstöðum prófana.

Dæmi: Breytingastjórnun

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Allar breytingar í raunumhverfi eru í samræmi við kröfur stjórnenda.	Beiðandi fyllir út breytingastjórnunarblað þar sem: a) Breytingu er lýst. b) Ábyrgðarmaður kerfis samþykkir fyrirhugaða breytingu. c) Forritari kvittar fyrir að breyting hafi verið prófuð í prófunarumhverfi.	Innri endurskoðandi fer yfir breytingabeirðnir og aðgætir hvort viðeigandi aðilar hafi fyllt út blaðið á viðeigandi hátt.

Í ljós kom að enginn athugaði hvort breytingar hafi verið í samræmi við upphaflega lýsingu eftir að þær voru settar inn í raunumhverfi.

Dæmi: Breytingastjórnun – útgáfa 2

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Allar breytingar í raunumhverfi eru í samræmi við kröfur stjórnenda.	Beiðandi fyllir út breytingastjórnunarblað þar sem: a) Breytingu er lýst. b) Ábyrgðarmaður kerfis samþykkir fyrirhugaða breytingu. c) Forritari kvittar fyrir að breyting hafi verið prófuð í prófunarumhverfi. d) Beiðandi yfirfer breytingu í prófunarumhverfi.	Innri endurskoðandi fer yfir breytingabeirðnir og aðgætir hvort viðeigandi aðilar hafi fyllt út blaðið á viðeigandi hátt.

Hvað með heild? Eru gerðar breytingar sem ekki er til breytingabeirðni fyrir? Svo reyndist vera m.v. atburðaskrá kerfisins (audit log).

Dæmi: Breytingastjórnun – útgáfa 3

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Allar breytingar í raunumhverfi eru í samræmi við kröfur stjórnenda.	Beiðandi fyllir út breytingastjórnunarblað þar sem: a) Breytingu er lýst. b) Ábyrgðarmaður kerfis samþykkir fyrirhugaða breytingu. c) Forritari kvittar fyrir að breyting hafi verið prófuð í prófunarumhverfi. d) Beiðandi yfirfer breytingu í prófunarumhverfi. e) Útgáfustjóri flytur breytingu milli umhverfa.	Innri endurskoðandi fer yfir breytingabeirðnir og aðgætir hvort viðeigandi aðilar hafi fyllt út blaðið á viðeigandi hátt.

Aðgangur forritara að raunumhverfi var fjarlægður og einn aðili gerður ábyrgur fyrir flutningi milli umhverfa (útgáfustjóri) sem færir eingöngu á milli umhverfa ef breytingastjórnunarblað er í lagi.

Dæmi: Öryggisstillingar

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Lykilorð séu endurnýjuð reglulega til að minnka líkur á misnotkun aðganga.	Kerfisstjóri sendir tölvupóst á alla starfsmenn og minnir á að skipta um lykilorð á 90 daga fresti.	Innri endurskoðandi fer yfir gögn úr tölvukerfi árlega sem segja til um hve langt er síðan lykilorði var breytt og heimsækir þá sem ekki hafa skipt um lykilorð á síðustu 90 dögum.

Innri endurskoðandi og kerfisstjóri kvörtuðu yfir að ofangreint tæki of mikinn tíma og væri óáreiðanlegt vegna mikillar handavinnu og mannlegra inngripa.

Dæmi: Öryggisstillingar – útgáfa 2

Markmið (D)	Innleiðing / Framkvæmd (I)	Prófun (T)
Lykilorð séu endurnýjuð reglulega til að minnka líkur á misnotkun aðganga.	Netkerfi er stillt með þeim hætti að krefjast þess að lykilorð séu endurnýjuð á 90 daga fresti (Windows Active Directory Password Policy).	Innri endurskoðandi óskar eftir skjámynd af viðkomandi stillingum frá kerfisstjóra einu sinni á ári.

Má gera betur?

Helstu ábendingar vegna UT kerfa ... 2007 Global Survey

- Réttindi umfram þarfir (excessive access rights)
- Aðgreining starfa (Segregation of duties)
- Skortur á skráningu atburðaskráa og eftirlitsgagna (audit trails)
- Uppsöfnun réttinda við tilfærslu í starfi
- Aðgangsveitingar ekki samkvæmt verklagsreglum
- Eftirlitsþættir ekki skjalaðir
- Forritarar með aðgang að raungögnum og kerfum
- Eftirlitsgögn ekki rýnd
- Uppsetning netþjóna og kerfa ekki "hert"
- Viðbragðsáætlanir ekki prófaðar
- Ekki verið að vinna í öryggisvitund starfsmanna
- Raungögn notuð í prófunarumhverfum
- Veik lykilorð

Helstu ábendingar vegna UT kerfa ... 2008 Global Survey

- Réttindi umfram þarfir (excessive access rights)
- Aðgreining starfa (Segregation of duties)
- Aðgangssveitingar ekki samkvæmt verklagsreglum
- Skortur á skráningu atburðaskráa og eftirlitsgagna (audit trails)
- Eftirlitsþættir ekki skjalaðir
- Forritarar með aðgang að raungögnum og kerfum
- Eftirlitsgögn ekki rýnd
- Uppsöfnun réttinda við tilfærslu í starfi
- Raungögn notuð í prófunarumhverfum
- Viðbragðsáætlanir ekki prófaðar
- Uppsetning netþjóna og kerfa ekki "hert"
- Ekki verið að vinna í öryggisvitund starfsmanna
- Veik lykilorð

Móral sögunnar ...

- Velja mikilvægustu eftirlitsþættina (key controls) og innleiða þá fyrst.
- Muna eftir öllum markmiðunum (starfsemi, fjárhagsupplýsingar og samkvæmni).
- Sníða stakk eftir vexti og rekstri félagsins.
- Endurbætur og viðbætur (Plan-Do-Check-Act).
- Innra eftirlit upplýsingakerfa er ekki einkamál tölvudeilda.
- Ef það ætti að gera eitthvað strax ... (Quick Win)
 - aðgangsheimildir (ábyrgð, veiting, rýni)
 - notendaaðgangar (nýir og hættir starfsmenn, tilfærslur)
 - prófa afrit reglulega
 - aðskilja breytingar frá keyrsluumhverfi og raungögnum

Annað efni

SANS Top 20 öryggishættur: <http://www.sans.org/top20/>

Global Security Survey: Protecting what matters.

<http://tinyurl.com/dtt-oryggiskonnun>

PCI DSS (greiðslukortaöryggi): <https://www.pcisecuritystandards.org/>

ISACA: <http://www.isaca.org/>

ISO 27001 er hægt að fá hjá BSI á Íslandi: <http://www.bsiaislandi.is/>

Faghópar um öryggismál hjá Skýrslutæknifélaginu og Stjórnvísi:

<http://tinyurl.com/sky-oryggishopur>

<http://tinyurl.com/stjornvisi-oryggishopur>

Með kveðju

Tryggvi R. Jónsson, tjonsson@deloitte.is

GSM: 860-3177

Deloitte.