Innleiðing PCI DSS, vandamál og lausnir

SKÝRR

Velkomin

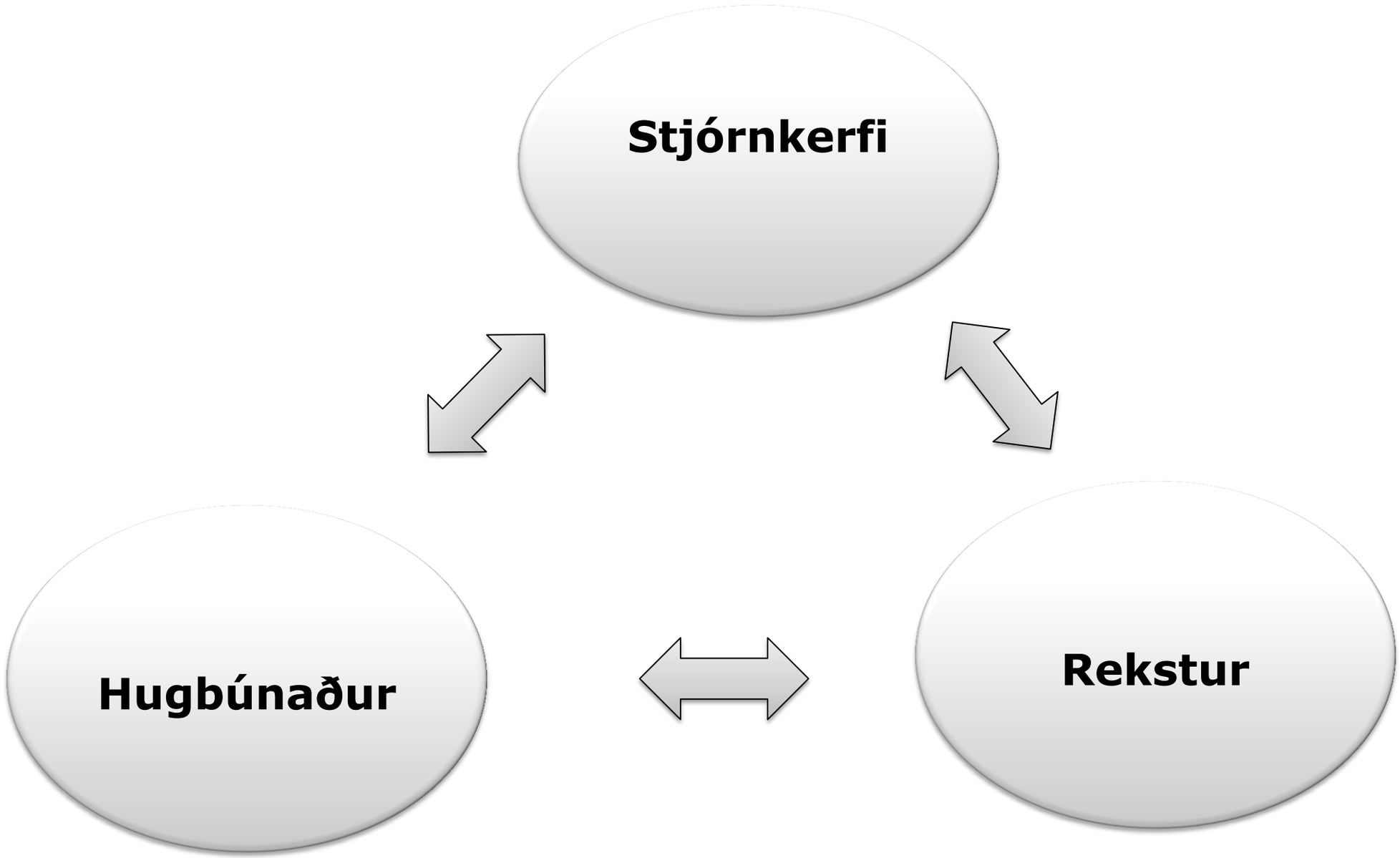
Einar Ragnar Sigurðsson

Af hverju PCI DSS?

- Enginn ótilneyddur
- Umfangsmikill tölvurekstur hjá Skýrr
  - Eitt lítið kerfi, Cardnet með kortagögn
- Krafa kreditkortafyrirtækjanna

- Afmörkun mikilvæg
  - “Skyrr doing business as Cardnet”
  - Skilgreint sem “fyrirtæki” innan Skýrr

„Skyrr as a Cardnet“

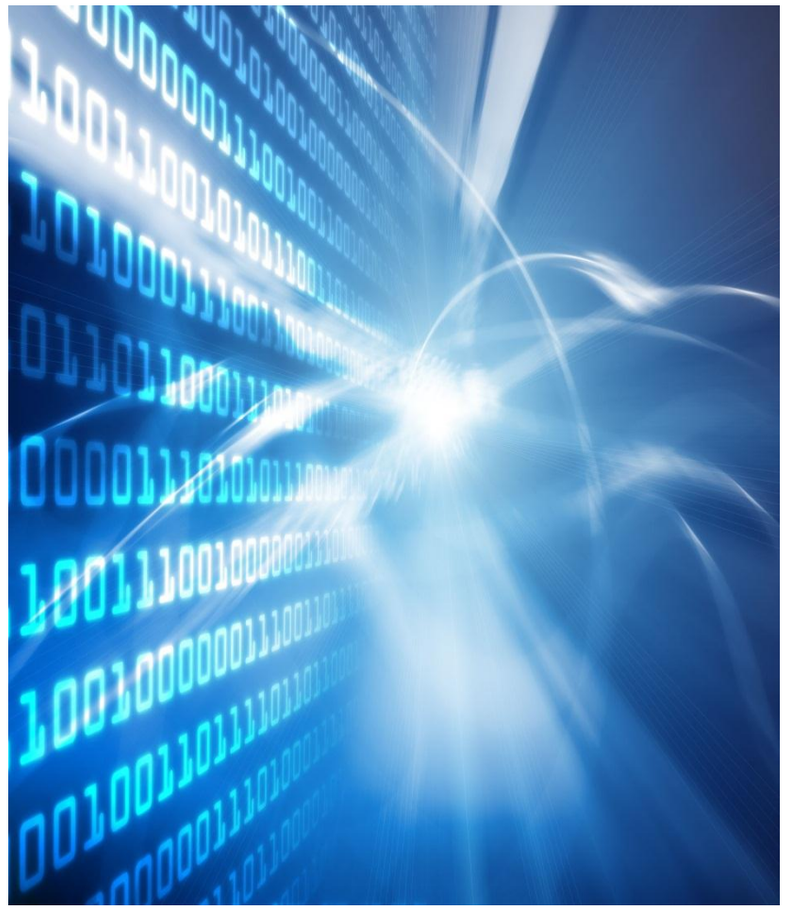


Stjórnkerfið

- Stýrinefnd
  - Eins konar framkvæmdastjórn fyrir „Skyrr doing business as Cardnet“
- Öryggisstefna
- Formleg samþykkt högunar, kerfiseininga og breytinga
- Skilgreining hlutverka
- Mjög formleg úthlutun ábyrgðar
- Starfsmenn og vitunarvakning
- Verkefnastjórn

Hugbúnaðargerðin

- Fylgja forritunarreglum
- Formlegar prófanir
- Rýni kóða
- Rekjanleiki í forritun
  - Útgáfustýring og breytingastjórnun
- Allt mikilvægir þættir
  - En það sem er val og útfærsla hvers og eins í ISO 27001 er krafa í PCI



Rekstur

- Að eingangra kortagögnin
  - Aðskilið með sérstökum eldvegg
  - Sértakir miðlarar
  - Sérstakt rými
- Formlegar verklagsreglur
  - Prófanir
  - Afturköllun breytinga
  - Ýtarleg skjölun og skrá ástæður allra breytinga
- Halda miðlurum dagréttum
- Raunlægt öryggi
- Viðbragðsáætlanir
  - Vöktun kerfa og rýni atburða
  - Nota viðurkennd tól
  - Vita hvernig á að bregðast við

Fjórþætt verkefni

- Uppsetning á CDE tækniumhverfi samkvæmt kröfum PCI staðalsins
- Tryggja að allur hugbúnaður uppfylli kröfur PCI staðalsins
- Stjórnunarleg umgjörð sé til staðar. Vitund starfsmanna og bakgrunnsathuganir
- Tryggja að regluverk fyrirtækisins styðji kröfur PCI staðalsins

Verkefnið hjá Skýrr

- Upphaf í október 2008
- Ááætluð lok um haust 2009
  - Varð umfangsmeira
- Skjalaúttekt í janúar 2010
- Tækniúttekt um vorið 2010
- Forvinna mikilvæg
  - Greining á öllum kröfum
- Styrk verkefnastjórnun er afar mikilvæg
  - Verkefnastjóraskipti höfðu áhrif á verkefnið

Vandamál og lausnir

- ISO 27001 ekki eins og PCI DSS
  - Ákveddu sjálfur eða gerðu það sem búið er að ákveða fyrir þig
- Greina allar kröfur staðalsins
  - Ath. úttektarviðmið sem koma fram í staðlinum
- Ákveða hvernig allar kröfur verða uppfylltar
- Byggja á fyrirliggjandi gæða- og öryggistjórnunarkerfi
- Einangra verkefnið eins og mögulegt er
  - Þráðlaus net aðskilin
  - Ekkert beint aðgengi að interneti
  - Sérstakt net útstöðva

Úttektin

- Úttektaraðili: Cybercom
- Frábrugðið „hefðbundinni ISO úttekt
  - Validation for compliance en ekki vottun (certification)
- Mikil samvinna við úttektarmanninn
  - Hlutverk úttektarmanns: Að hjálpa fyrirtækinu að verja kortagögnin sín
  - Mjög ítarleg skýrsla úttektarmanns staðfest af kortafyrirtækjum

Þegar upp er staðið

- Erfitt en gekk í heildina vel
- Mikilvægur undirbúningur hjá Skýrr
  - ISO 27001 vottun
    Ýmsar kröfur um stjórnunarhætti þær sömu
  - VeriSign kröfur vegna húsnæðis
- Vanmátum verkefnið
- Markviss verkefnastjórnun lykilatriði
- Mikilvægt að oftúlka ekki
  - Það sem stendur ekki í staðlinum,
    það er ekki í staðlinum
  - Ekki er hægt að leysa öll vandamál í einu