Upplýsingaöryggi í áhættustjórnun fyrirtækja

Ágústa Berg

Október 2024

Umfjöllun mín

Hvað er áhætta

Líkur eða möguleiki á hættu, tapi, meiðslum eða öðrum óhagstæðum afleiðingum.

Oxford English Dictionary

Atburður eða ástand sem kemur í veg fyrir að fyrirtæki nái markmiðum sínum.

Skilgreining KPMG á Enterprise Risk

Möguleikinn á atburði sem mun hafa áhrif á stefnu og markmið félags.

COSO Enterprise Risk Management Framework

Áhætta er varðar upplýsingaöryggi

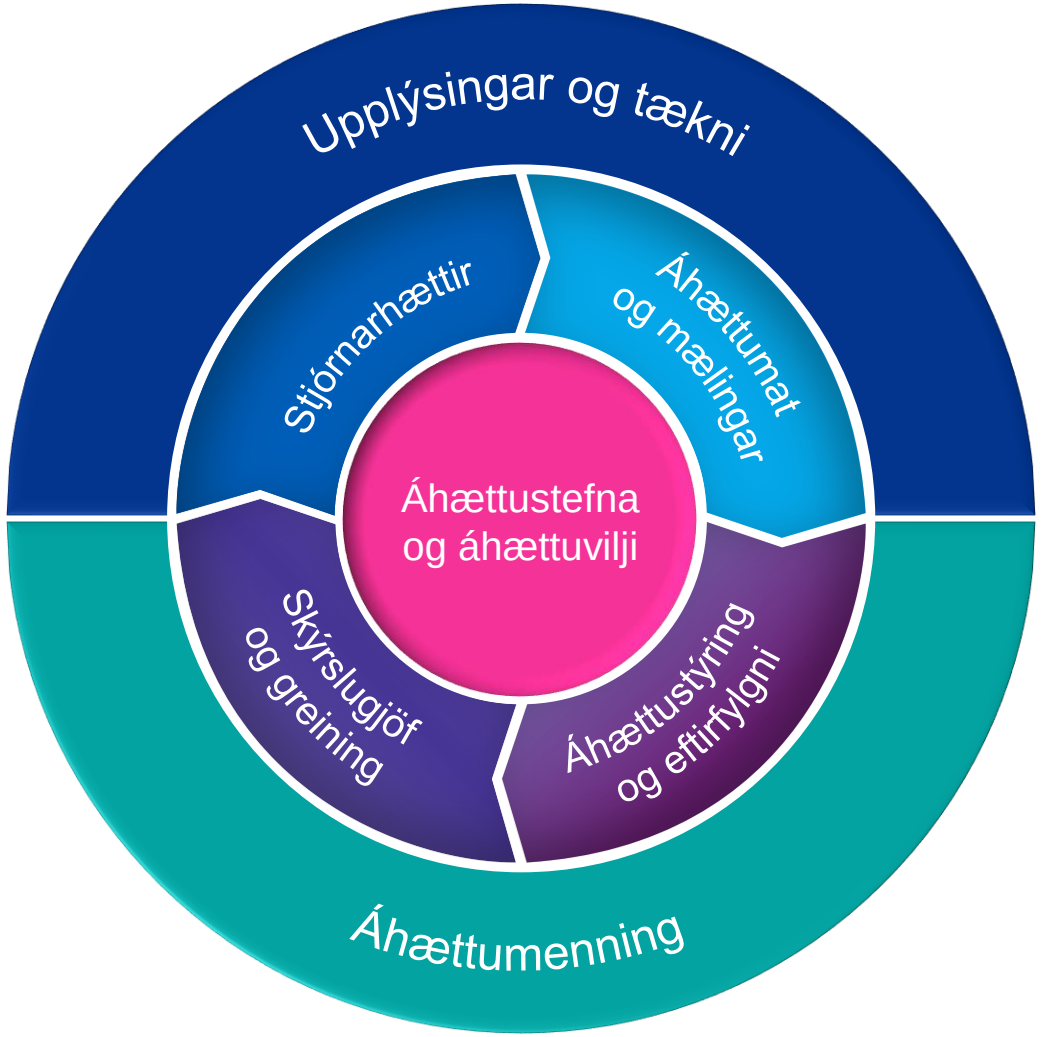
Loss of confidentiality, integrity or availability of data or information systems

NIST

Aðstæður eða atburður sem geta haft skaðleg áhrif á öryggi net- og upplýsingakerfa.

Lög um öryggi net-og upplýsingakerfa mikilvægra innviða (Lög nr. 78/2019)

Skipulag áhættustjórnunar



Öll fyrirtæki búa við áhættu í rekstri

Með áhættustýringu er leitast við að gera fyrirtækjum kleift að taka áhættu með upplýstum hætti

Skilvirk áhættustýring gerir fyrirtækjum kleift að greina, stýra, miðla, vakta, staðfesta og tilkynna um áhættu sem getur haft áhrif á rekstur fyrirtækisins.

Áhættustýring felur í sér ferli við að greina áhættu, meta líkur á henni og afleiðingar

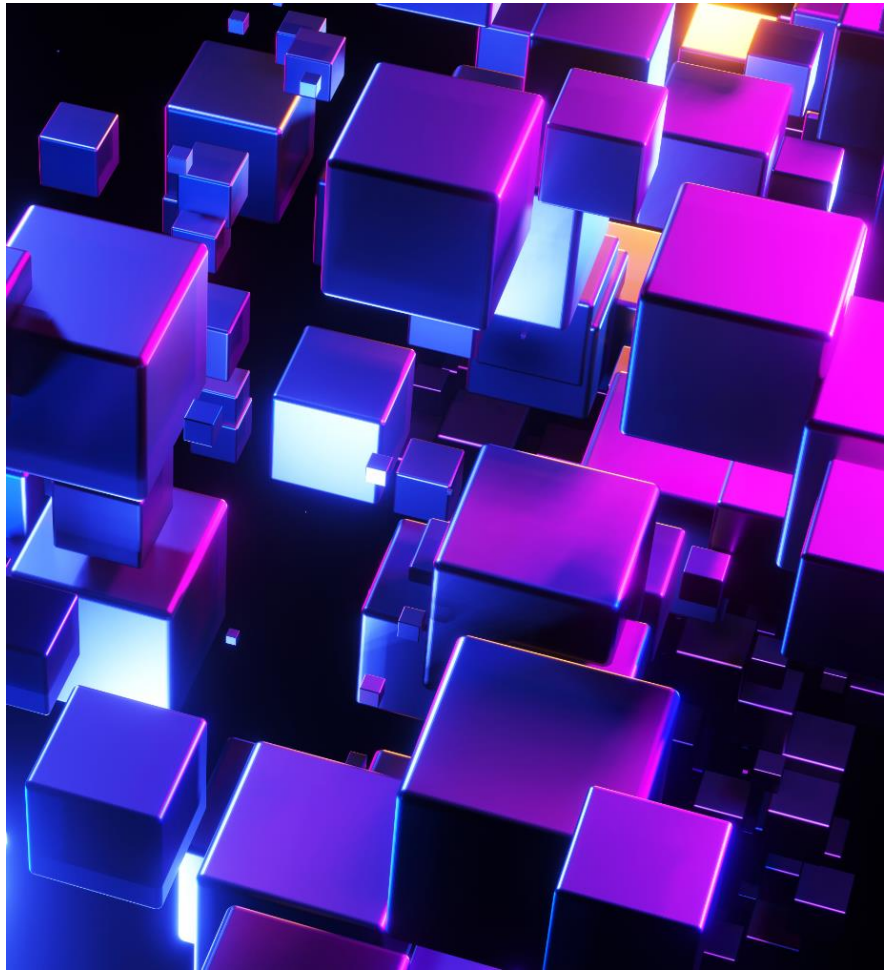
Áhættustýring er hluti af innra eftirliti

Örar breytingar í regluverki

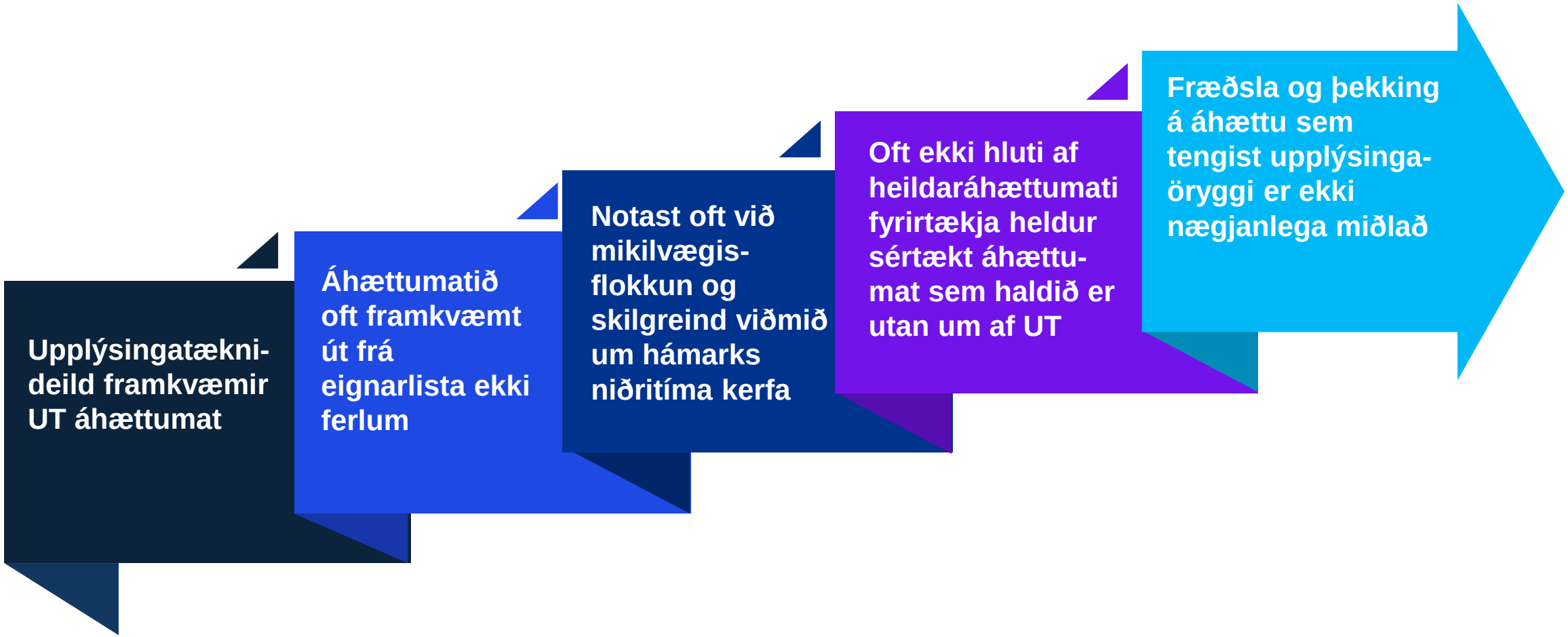
Upplýsingatæknideildir

„Stoðdeildir“

- Vinna oft og taka ákvarðanir í nokkurri „einangrun“ frá öðrum s.s. varðandi net- og upplýsingaöryggi
- Er ekki alltaf boðið að borðinu við mikilvægar rekstrarákvarðanir / breytingar jafnvel þó tengist upplýsingatækni
- Starfsfólk er oft „aðskilið“ frá öðru starfsfólki, sitja t.d. í öðru rými
- Samráð er ekki haft við starfsfólk varðandi áhættumat á öðrum deildum / ferlum, nema að takmörkuðu leiti



Núverandi áhættustjórnun og upplýsingaöryggi



Upplýsingatæknideildir – hvert viljum við stefna

- **Flest, ef ekki öll fyrirtæki, eru í raun „tæknifyrirtæki“**
- **Mikilvægi upplýsingatæknis þarf að endurspeglast í hvernig við staðsetjum og tölum um hana**
  - Rekstrardeild vs. stoðdeild
  - Staðsetning í skipuriti
  - Vel upplýstir og ráðgefandi, t.d. varðandi breytingar / rekstrarákvarðanir
- **Stjórnandi upplýsingatækni ætti að vera hluti af framkvæmdastjórn**
- **Tryggja samþættingu starfsfólks með öðru starfsfólki**
- **Tryggja þekkingar og upplýsingaflæði, m.a. er varða upplýsingaöryggi, áhættu og stýringar**

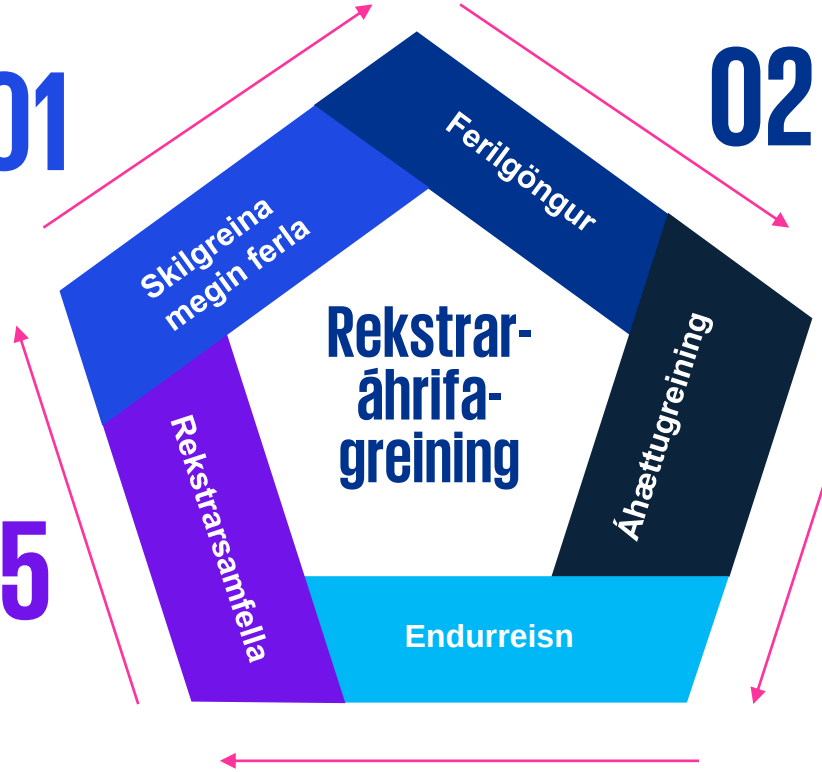
Áhættustjórnun og upplýsingaöryggi - hvert viljum við stefna

- **Mikilvægt að hugsa um áhrif upplýsingaöryggis heildstætt**
- **Færa sig frá því að áhættumeta út frá eignalista yfir í viðskipta- og stuðningsferla**
- **Efla fræðslu og þekkingu starfsfólks**
  - Helstu áhættur tengdar upplýsingaöryggi
  - Stýringar sem til staðar eru
  - Mikilvægi starfsfólks í því að tryggja að áhættur raungerist ekki
- **Huga að upplýsingatækniáhættum í öllum áhættumati, einnig sértækum áhættumötum s.s. vegna verkefna / breytingar**
- **Hafa heildarskrá yfir áhættur fyrirtækisins, þ.m.t. upplýsingatækni-áhættur**

Áhættumat út frá rekstraráhrifagreining

01 Skilgreina megin viðskipta- og stoðferla

02 Framkvæma ferilgöngur



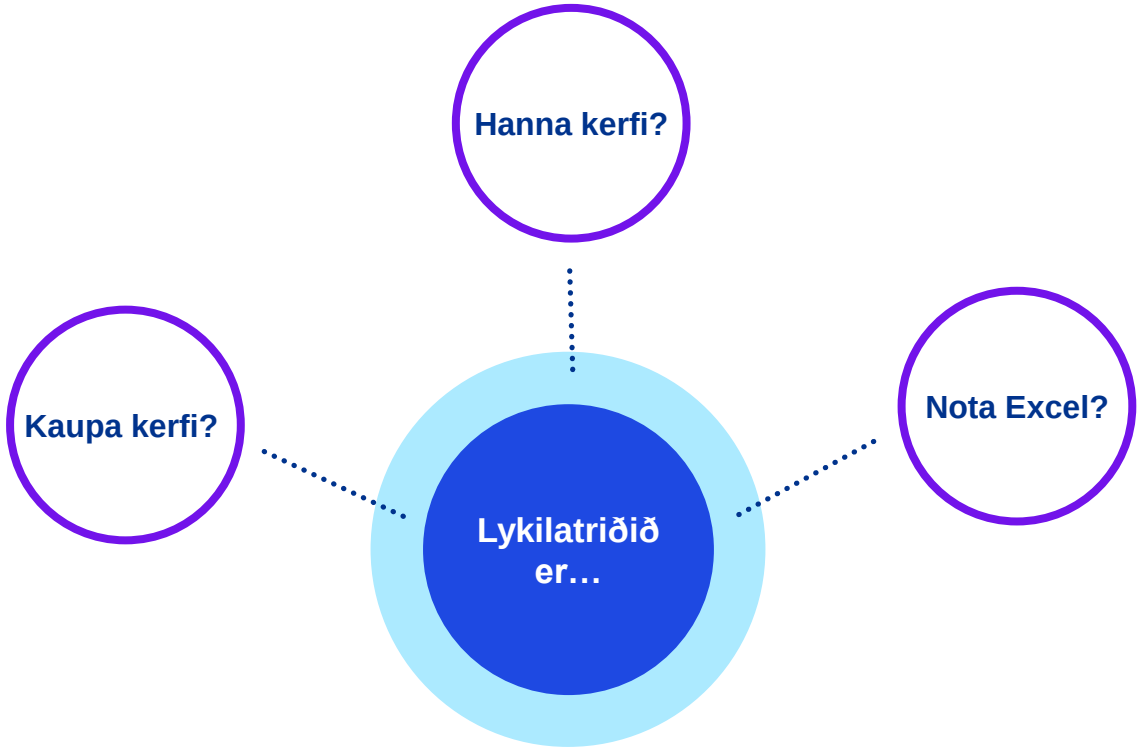
03 Áhættugreining og skilgreining stýringar

04 Endurreisnaráætlun og sviðsmyndir

05 Tengja áhættumatið við rekstrarsamfellu

Utanumhald áhættustjórnunar

Á að:

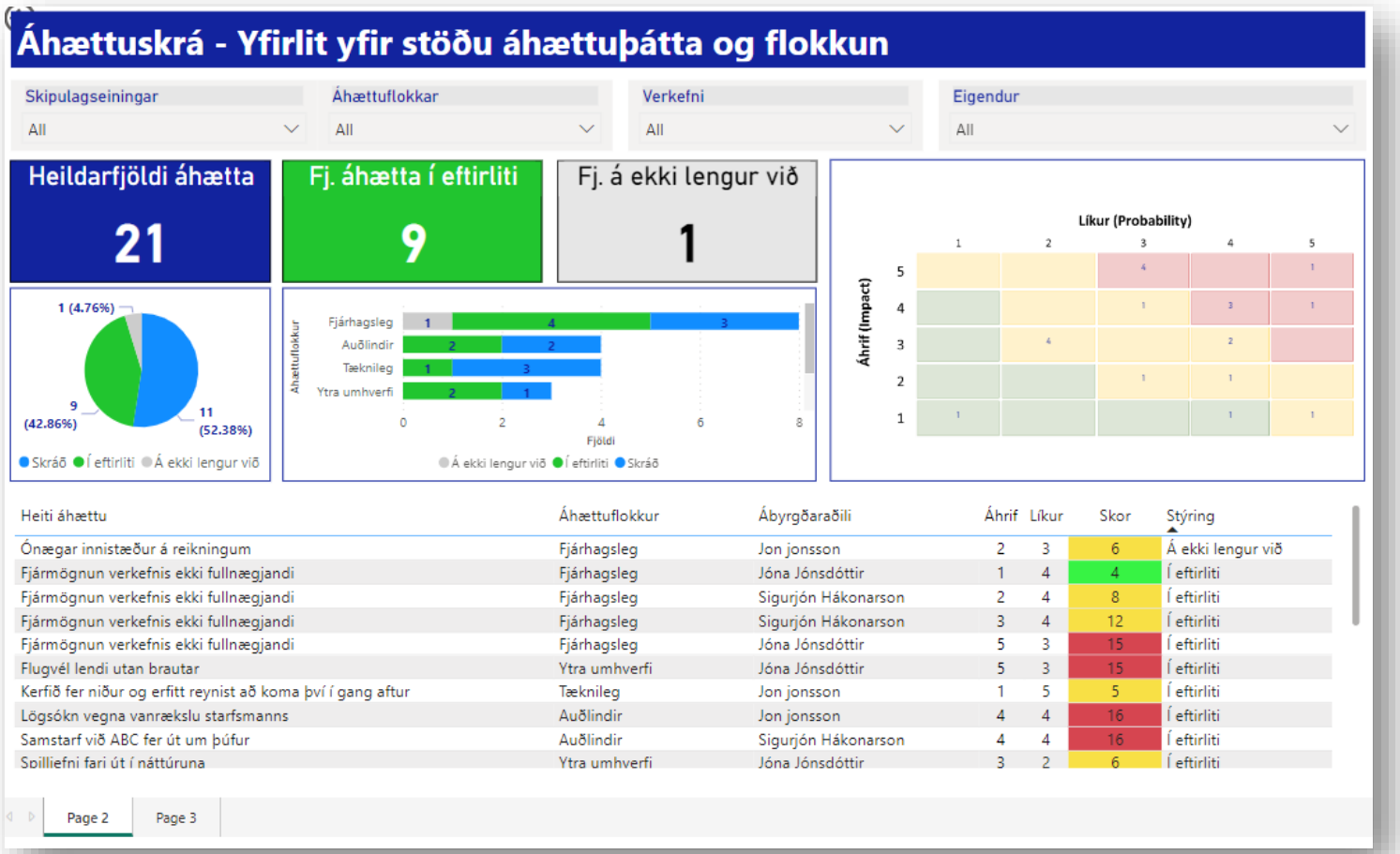


Utanumhald áhættustjórnunar

... það kerfi sem notað er fyrir áhættustjórnun sé:

- **Sveigjanlegt**
- **Innihaldi mælaborð**
- **Hægt sé að útdeila á starfsfólk**
- **Rekjanleiki**
- **Áminningar**
- **Verklagsreglur og áhættustefna áhættustjórnunar verða hluti af lausninni**

Sýnidæmi - mælaborð



Mælaborð í Power BI.

Mælaborðið hér er gagnvirkt og hægt að sía og bora sig niður til að fá frekari upplýsingar um stöður og mat.