Marinó G. Njálsson

NETÖRYGGI

Samþættuð hlítingarstjórnun

ÁSKORANIR SKIPULAGSHEILDA

Kröfur koma úr ólíkum áttum og hafa mismunandi vægi

Hvaðan koma kröfur

- Öryggisstefna (og aðrar stefnur).
- Úr áhættumati.
- Lög, reglugerðir, stjórnvaldsfyrirmæli.
- Staðlar og öryggisfyrirmæli.

VIÐFANGSEFNIÐ

Greina kröfurnar.

- Bera kennsl á kröfur í ESB lögum, reglugerðum og tilskipunum.
- Varpa kröfum í staðal sem mikið er notaður, ISO/IEC 27001.
- Tengja minna notaða staðla við ISO/IEC 27001.

ALMENNT VERKLAG

Forvinna

- Tryggja að kröfur séu tilgreindar.
- Bera kennsl á ógnir og veilur
- Ákvarða stigmögnun út frá áhættu.
- Tengja við þekktar leiðbeiningar.

Innleiðing

- Velja úrræði.
- Draga úr áhættu.
- Uppfylla kröfur sem best er hægt.
- Skjalfesta niðurstöður.
- Hrinda í framkvæmd.
- Skjalfesta yfirlýsingu um nothæfi.

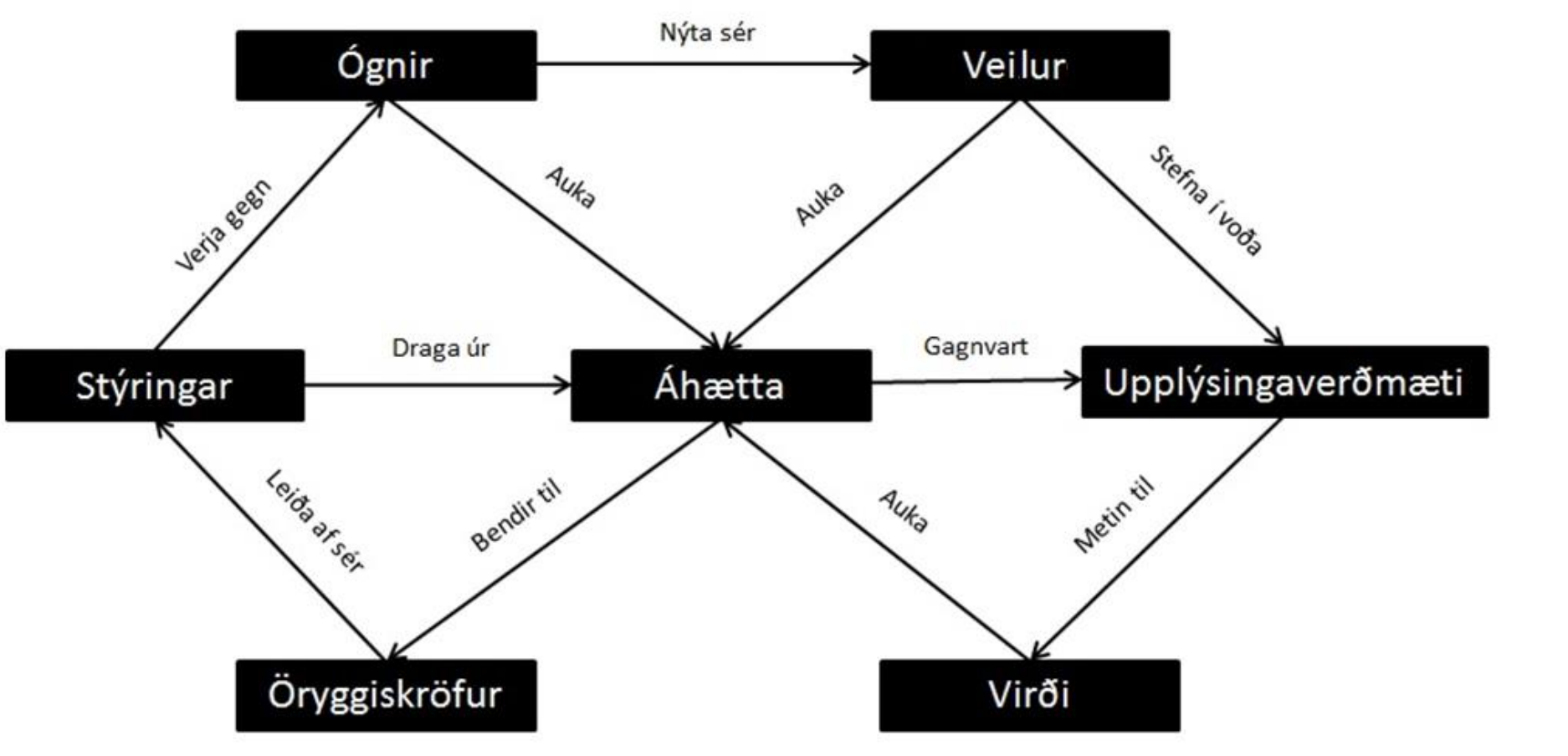
Úttektir

- Skoða varpanir milli krafna og niðurstaðna.
- Staðfesta virkni úrræða.
- Kanna stöðu yfirlýsingar um nothæfi.
- Bera kennsl á göt.

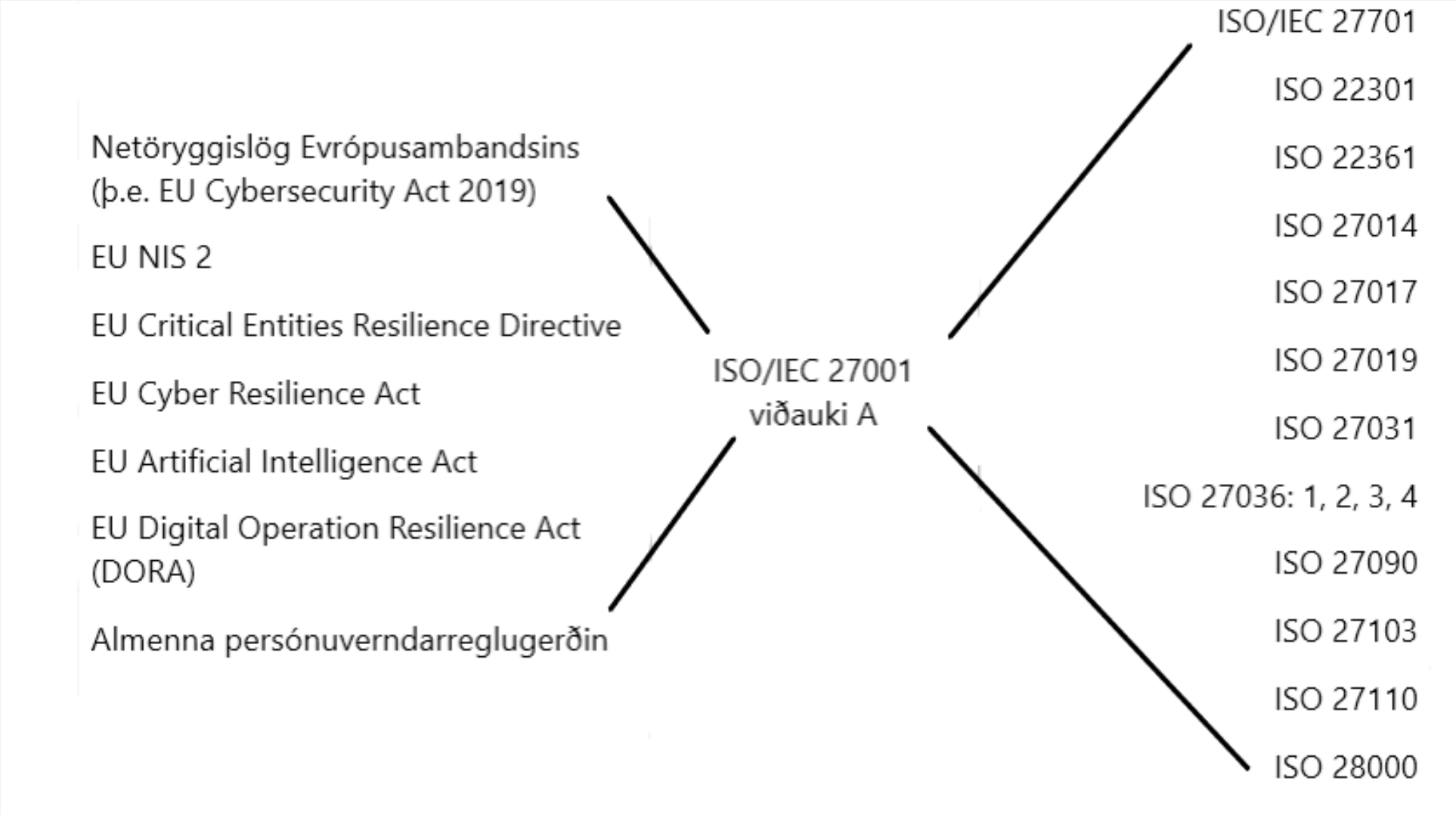
Krafa: Einfalda vinnu við innleiðingu og úttektir

ÞETTA TENGIST ALLT

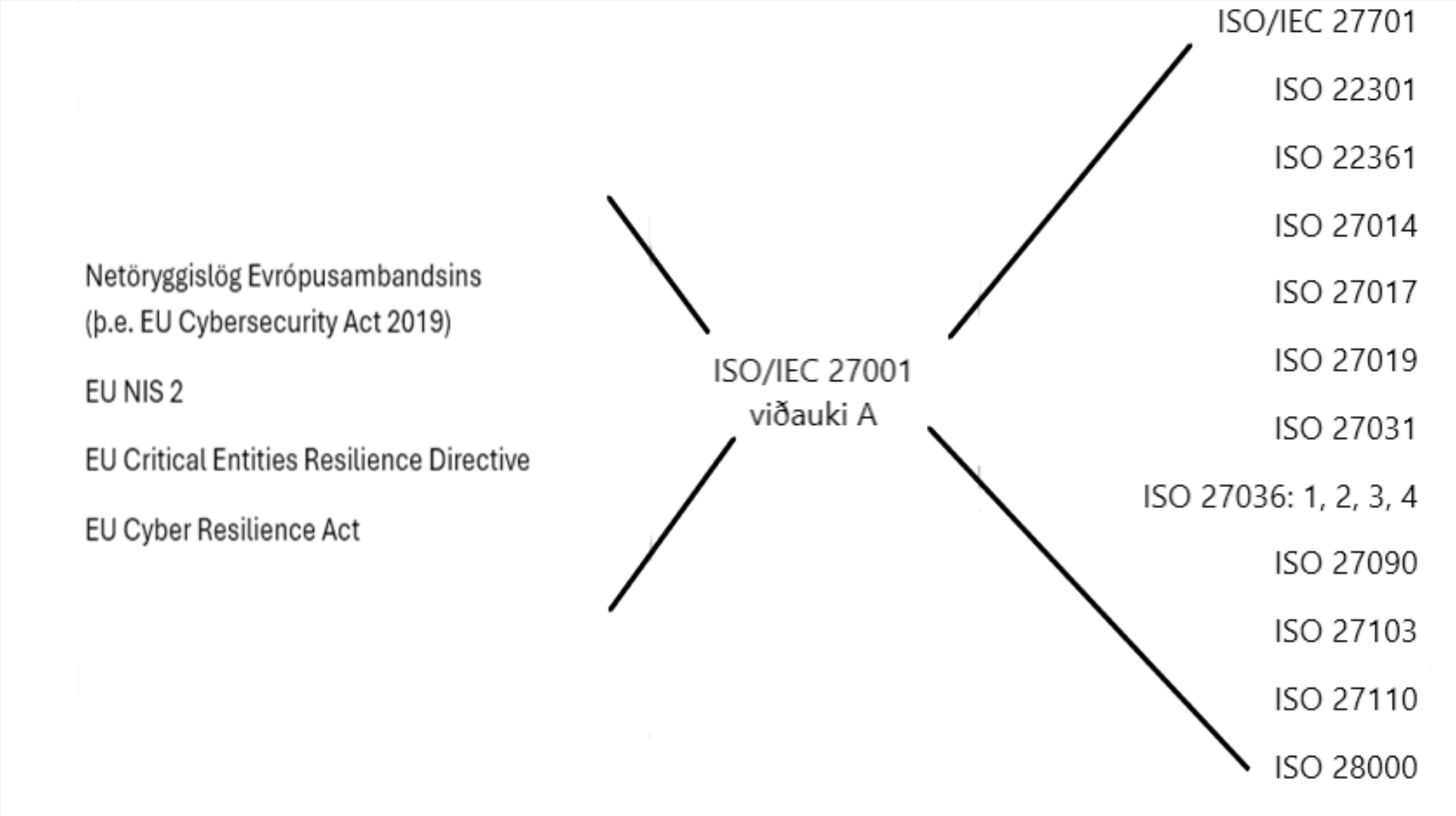
Hlítingastjórnun byggir á því að öll boxin séu skoðuð og þeim sinnt rétt



SKILJA TENGINGAR



SKILJA TENGINGAR



DÆMI UM VARPANIR MILLI NIS 2 OG ISO 27001

Tilskipun 2022/2055 (NIS 2)

- Grein 20 – Stjórnun
- Gerð eru kröfur um:
  - Að átta sig á stöðu sinni
  - Greina ákvæði laga og reglugerða
  - Stefnur og stefnumótun
  - Samskipti við yfirvöld
  - Viðbragðsáætlanir/neyðaráætlanir
  - Áhættumat
  - Deiling upplýsinga um ógnir
  - Atvikastjórnun
  - Stjórnun aðfangakeðju

ISO/IEC 27001:2022

- Býður upp á leiðsögn
- Eftirfarandi atriði tengjast við:
  - Grein 4.1
  - Stýring A 5.31
  - Grein 5.2
  - Stýring A 5.5
  - Stýringar A 5.26 og A 5.30
  - Grein 6.1
  - Stýring A 5.7
  - Stýringar A 5.24 til A 5.28
  - Stýringar A 5.19 til A 5.22

DÆMI UM STUÐNING STAÐLA VIÐ ISO 27001

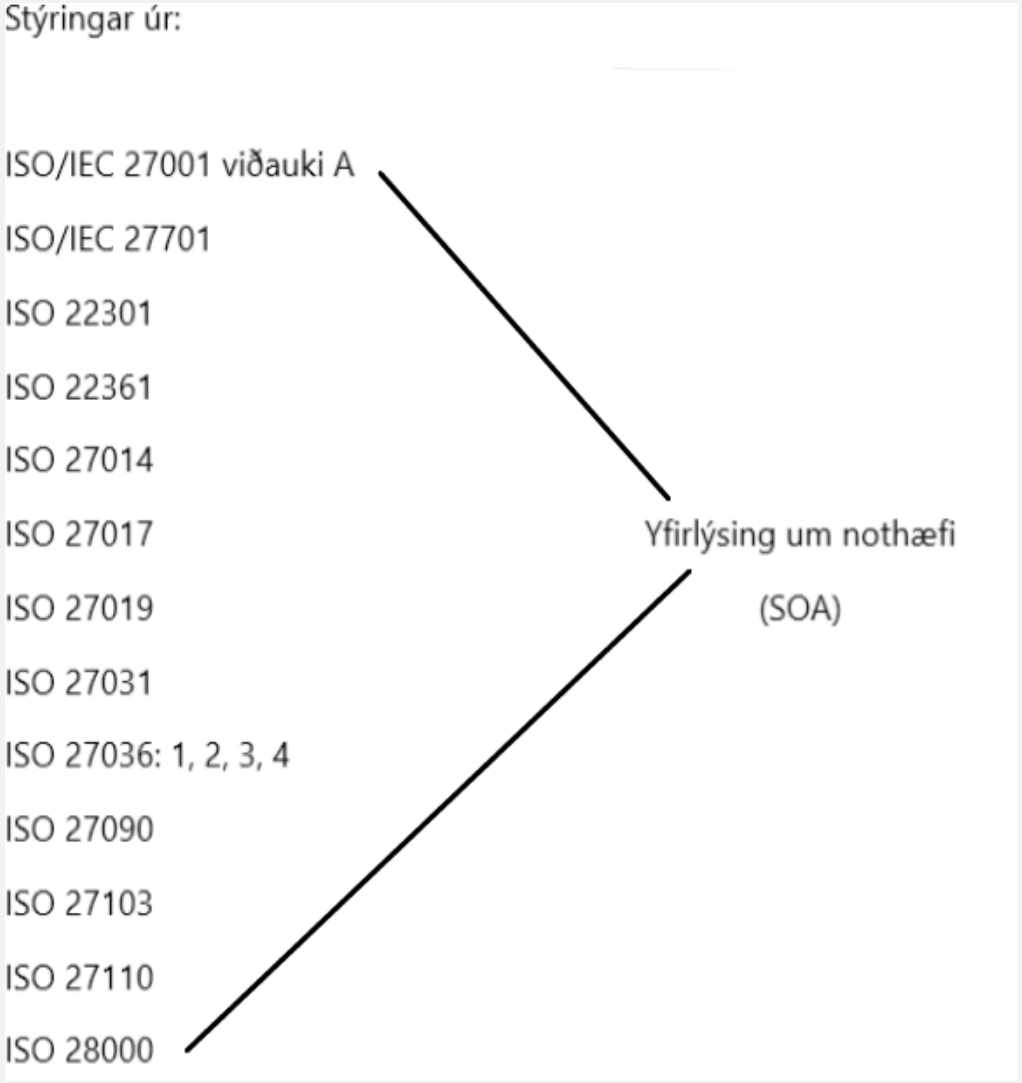
ISO/IEC 27001:2022

- Stýringar úr ISO/IEC 27001:
  - Grein 4.1
  - Stýringar A 5.26 og A 5.30
  - Stýringar A 5.19 til A 5.22
  - Stýringar A 5.24 til A 5.28

Aðrir ISO staðlar

- Leiðsögn úr:
  - ISO/IEC 27110 - Cybersecurity framework development guidelines
  - ISO 22301 - Security and resilience — Business continuity management systems
  - ISO 22313 - Security and resilience — Business continuity management systems
  - ISO 22361 - Security and resilience — Crisis management
  - ISO/IEC 27036-1:2021 - Cybersecurity — Supplier relationships- Part 1 - 4

TENGJA SAMAN STÝRINGAR



HVERJIR ERU ÁBYRGIR

Innanlands

- HVÍN
- ECCC
- NCC
- Fjarskiptastofa
- CERT-ÍS
- Seðlabankinn
- Skipulagsheildir
- Flugfélög
- Traustþjónustuveitendur

Alþjóðlega

- ESB/EES
- Framkvæmdastjórn ESB
- ENISA
- ESB CyCLONe
- Corporation Group
- Flugfélög
- Traustþjónustuveitendur

LOKAORÐ

- Stýringar í mörgum stöðlum eru frekar yfirborðskenndar og því er mikilvægt að nota leiðsögn um sambærilegar kröfur við tillögur að meðferð
- Fyrir hverja stýringu þarf að skjalfesta stigmagnandi viðbrögð
- Skipulagsheild starfandi á Íslandi gæti líka verið með starfsemi utanlands eða veitt þjónustu til aðila sem telst til mikilvægra innviða erlendis
- Skipulagsheild sem telst til mikilvægra innviða hér á landi gæti verið að nota þjónustu erlends aðila.
- Mikilvægt að nota eins og hægt er alþjóðleg viðmið, alþjóðlegar leiðbeiningar og alþjóðlega staðla