Fjarskiptastofa

Kynning á NIS

Unnur Kristín Sveinbjarnardóttir, sviðsstjóri stafræns öryggis
unnur@fjarskiptastofa.is
25. október 2023

Efni kynningar

Fjarskiptastofa

1. Netöryggislög nr. 78/2019 - *örstutt*
2. NIS-2
   - *Markmið – af hverju NIS-2?*
   - *Aðilar*
   - *Kröfur*
   - *Eftirlit*
3. Staða innleiðingar

Fjarskiptastofa

Netöryggislög

Netöryggislög *- markmið*

Fjarskiptastofa

Lög nr. 78/2019, um öryggi net- og upplýsingakerfa mikilvægra innviða tóku gildi 1. september 2020.

- Byggja á NIS-1 tilskipun ESB frá árinu 2016.

- Hefur það markmið *að bæta net- og upplýsingaöryggi rekstraraðila á mismunandi sviðum atvinnulífsins sem veita samfélagi okkar og atvinnulífi nauðsynlega þjónustu.*

- Í þessu felst að aðilar skulu:
  - Innleiða fyrirbyggjandi ráðstafanir um áhættustýringu og viðbúnað til að koma í veg fyrir atvik eða takmarka tjón af atvikum *(kröfur+eftirlit).*
  - byggja á gildandi alþjóðlega viðurkenndum stöðlum um bestu framkvæmd á sviði net- og upplýsingaöryggis.
  - **innleiða, viðhalda og bæta stöðugt stjórnunarkerfi upplýsingaöryggis.**

Reglugerðir nr. 866/2020 og 1255/2020

Netöryggislög *- gildissvið*

Fjarskiptastofa

- NIS-lögin gilda um mikilvæga innviði sem greinast í tvo flokka:
  1. *Rekstraraðila nauðsynlegrar þjónustu (RNÞ) á sviði fjármála, orku, samgangna, heilsu, neysluvatns og starfrænna grunnvirkja*
     - Eftirlitsstjórnvöld tilnefna RNÞ til ráðherra sem birtir skrá í B-hluta Stjórnartíðinda.
     - 53 aðilar skilgreindir sem RNÞ. (uppfærsla væntanleg)
  2. *Veitendur stafrænnar þjónustu á sviði netmarkaðar, leitarvélar á netinu og skýjavinnsluþjónustu.*
     - Ekki þarf tilnefningu fyrir veitendur stafrænnar þjónustu. (örfélög og stærri)
- Gilda um net- og upplýsingakerfi sem eru undirstaða fyrir veitingu þjónustu.
- Sex eftirlitsstjórnvöld sem framfylgja ákvæðum laganna á sínu sviði.

NIS-2 *(Tilskipun 2022/2555)*

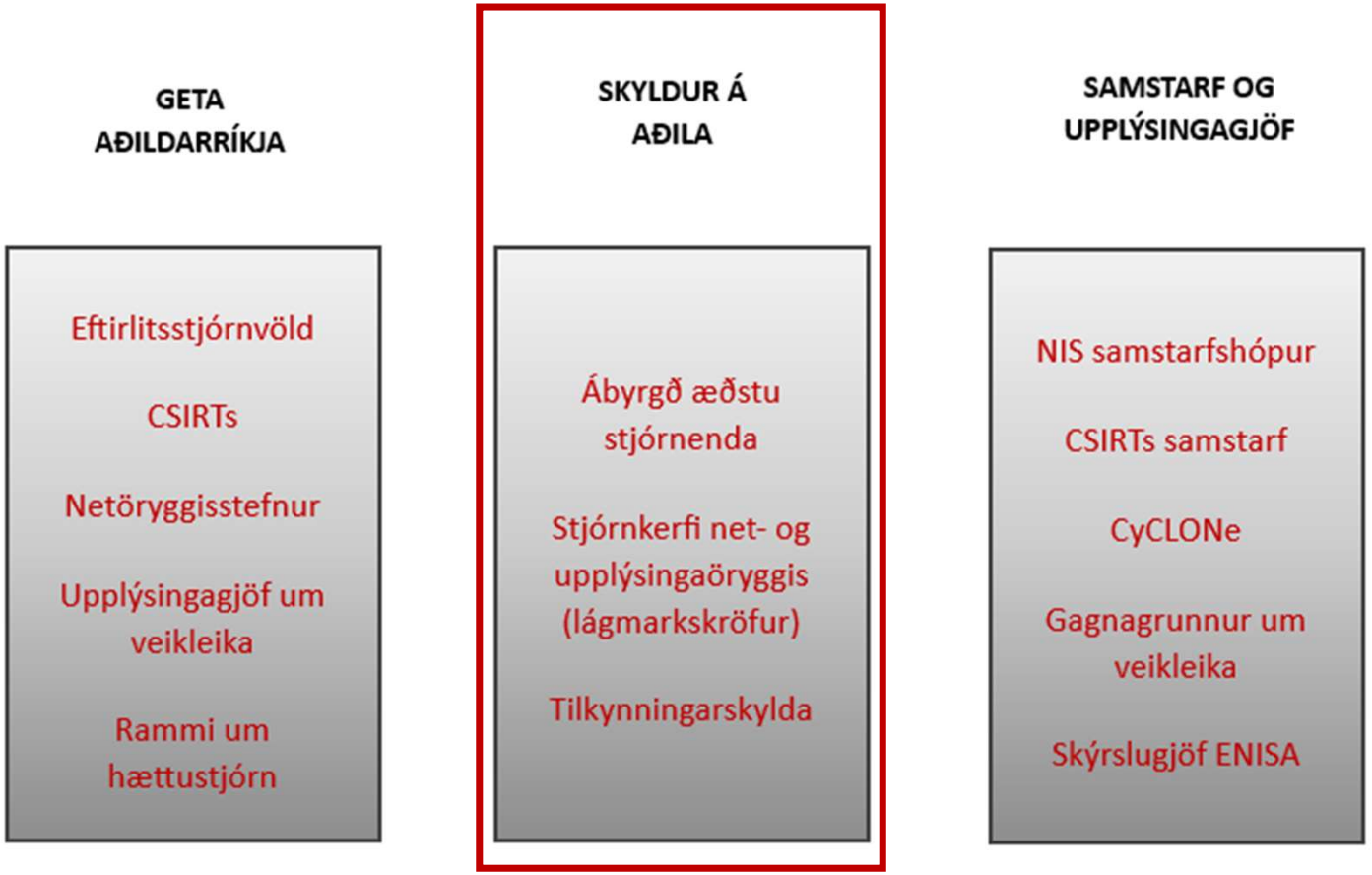
Fjarskiptastofa

Markmið - *Af hverju NIS-2?*

…markmið NIS-2 er að ná háu samræmdu stigi netöryggis innan ESB.

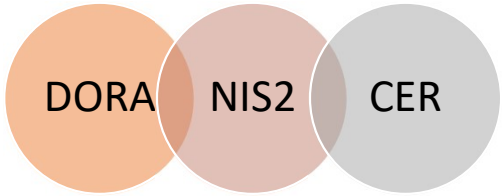
Ekki öll mikilvæg starfsemi innan gildissviðs	Ósamræmi í gildissviði milli aðildarríkja (RNÞ)	Mismunandi lágmarkskröfur netöryggis milli aðildarríkja
Mismunandi þröskuldar fyrir atvikatilkynningar	Ómarkvisst og takmarkað eftirlit	Ekki skyldubundin miðlun upplýsinga milli aðildarríkja og milli aðila

Stoðir NIS-2

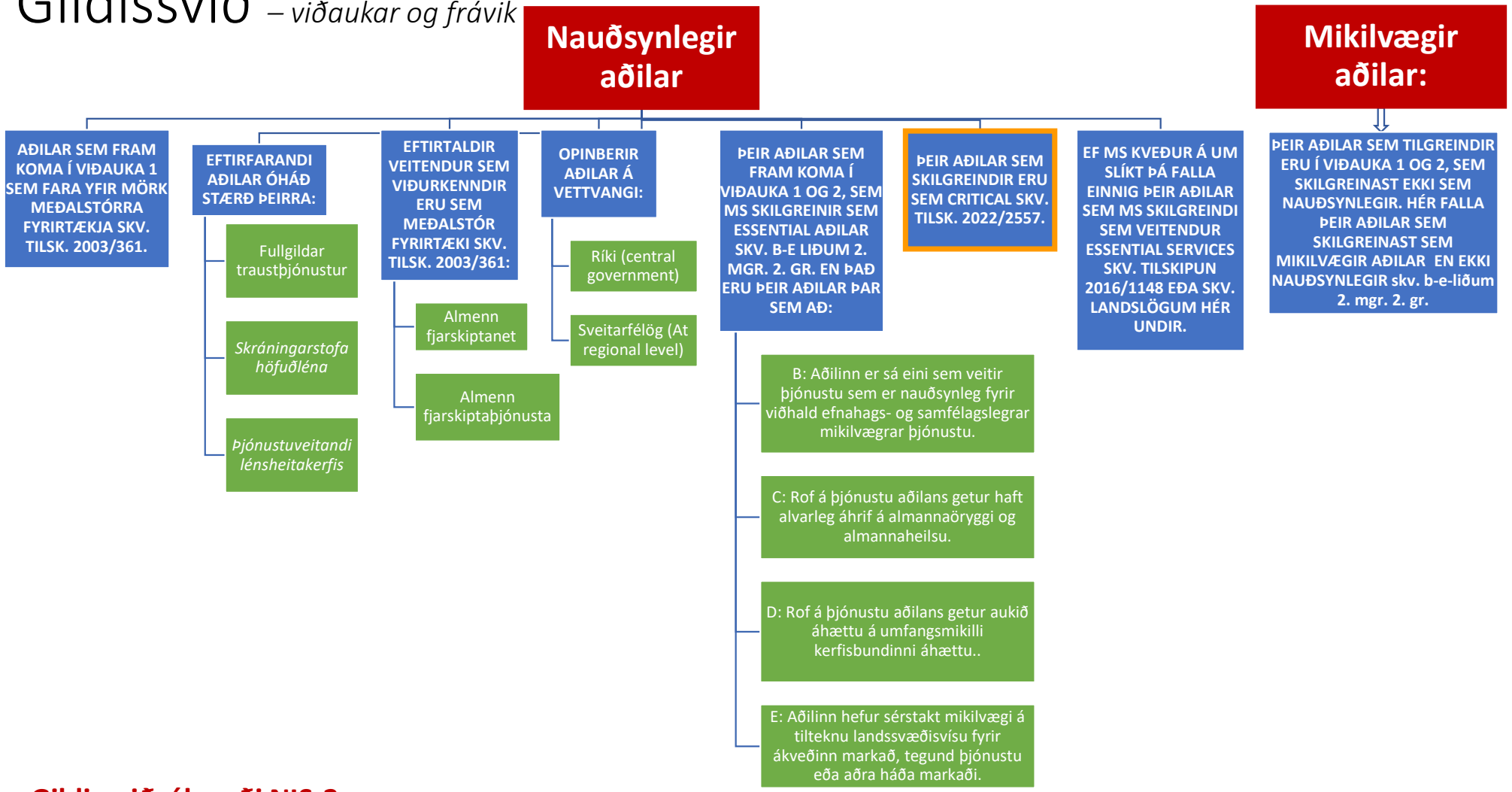

GETA AÐILDARRÍKJA
Eftirlitsstjórnvöld
CSIRTs
Netöryggisstefnur
Upplýsingagjöf um veikleika
Rammi um hættustjórn
SKYLDUR Á AÐILA
Ábyrgð æðstu stjórnenda
Stjórnkerfi net- og upplýsingaöryggis (lágmarkskröfur)
Tilkynningarskylda
SAMSTARF OG UPPLÝSINGAGJÖF
NIS samstarfshópur
CSIRTs samstarf
CyCLONe
Gagnagrunnur um veikleika
Skýrslugjöf ENISA

Gildissvið *- nálgun*

- Þeir aðilar sem að falla undir NIS-2 veita þjónustu sem tilgreind er í viðauka I og viðauka II við tilskipunina.
  - Í viðauka I eru nauðsynlegir innviðir (e. essential).
  - Í viðauka II eru mikilvægir innviðir (e. important).
- Viðaukar skilgreina markaði, undirmarkaði og aðila (e. entities).
- Umfangsmikið gildissviðsákvæði í tilskipuninni sjálfri auk ávæðis varðandi nauðsynlega og mikilvæga innviði.
  - Ákveðnar millitivísanir í önnur ákvæði og aðra löggjöf ESB.
  - Undantekningar frá meginreglu um stærð aðila í viðaukum I og II.
- Taka verður tillit til systurgerða NIS-2.



Gildissvið – *viðaukar og frávik*

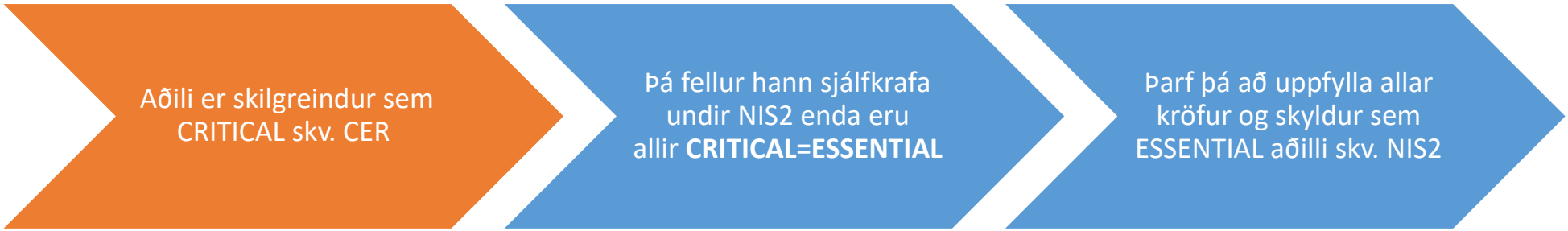


Gildissviðsákvæði NIS-2

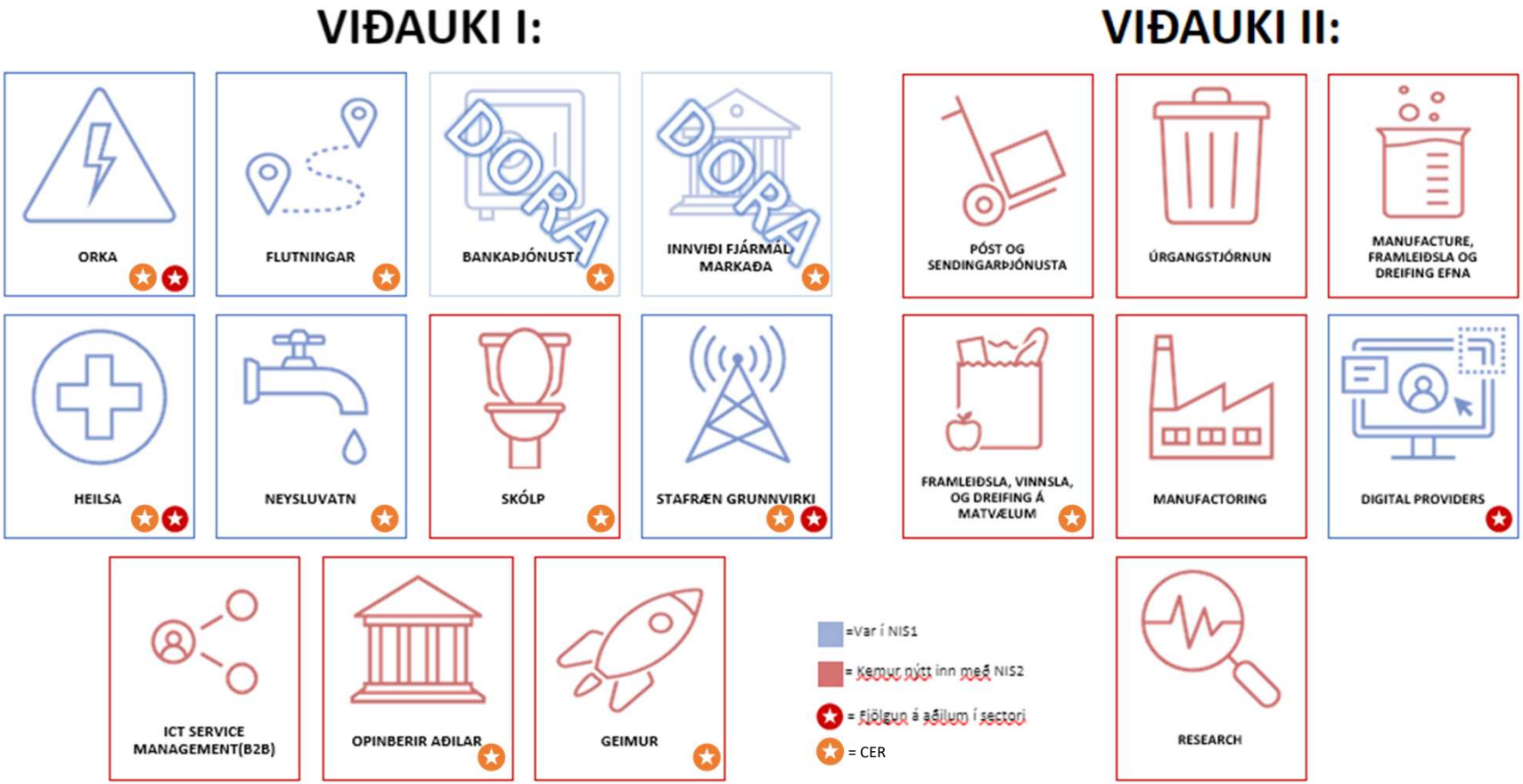
CER – *samspil við NIS-2*

Fjarskiptastofa

- Allir aðilar sem eru **CRITICAL** **skv. CER eru ESSENTIAL skv. NIS2.**
- Hvernig og hvort aðilar eru skilgreindir sem CRITICAL skv. CER hefur þar af leiðandi áhrif á umfang gildissviðs NIS-2.
- **CRITICAL** aðilar þurfa að uppfylla kröfur NIS og CER (heimild til framsals eftirlits)



Viðaukar I og II - *Markaðir undir NIS-2*

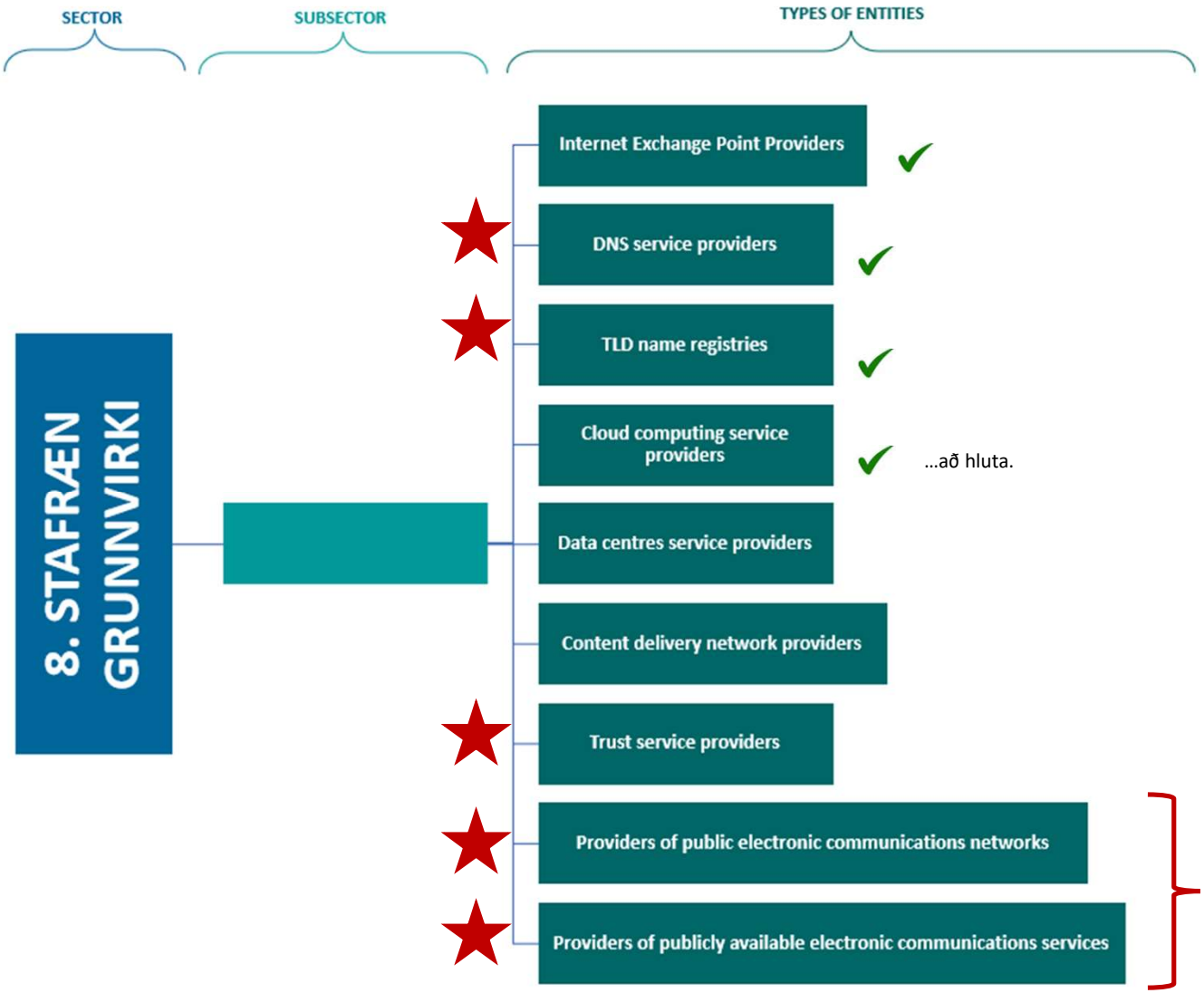


Gildissvið NIS-2 *– markaðir og undirmarkaðir*

Fjarskiptastofa

Viðauki I - Nauðsynleg þjónusta	**Viðauki II** - Mikilvæg þjónusta
Orka (rafmagn, svæðisbundin hitun, olía, gas og vetni)	Póst- og sendingarþjónusta
Samgöngur (loft, vatn vegir, lestir)	Úrgangsstjórnun
Bankastarfsemi (DORA)	Efni/Lyf (framleiðsla og dreifing)
Innviðir fjármálamarkaða (DORA)	Matvæli (framleiðsla, vinnsla og dreifing)
Heilbrigði (heilbr.þjónusta, rannsóknir og framleiðsla lyfja og lækningatækja)	Framleiðsla (lækningatæki, tölvur, fjarskiptavörur, rafmagnsvörur, vélar, bílar og flutningstæki)
Drykkjarvatn	Veitendur stafrænnar þjónustu (leitarvélar á netinu, netmarkaðir og "social networks")
Úrgangsvatn	Rannsóknir
Stafræn grunnvirki (IXP, DNS, TDL, skýjaþjónustur, gagnaver, dreifinet efnis, fjarskiptafyrirtæki, traustþjónustur)	
"ICT Service Management"	***Rautt = nýtt í NIS-2**
Geimur	
Opinberar stofnanir	

Gildissvið NIS-2 *- starfseininar*



Gildissvið NIS-2 *- starfseiningar*

NIS-2 *– samanburður viðauka I og II*

Fjarskiptastofa

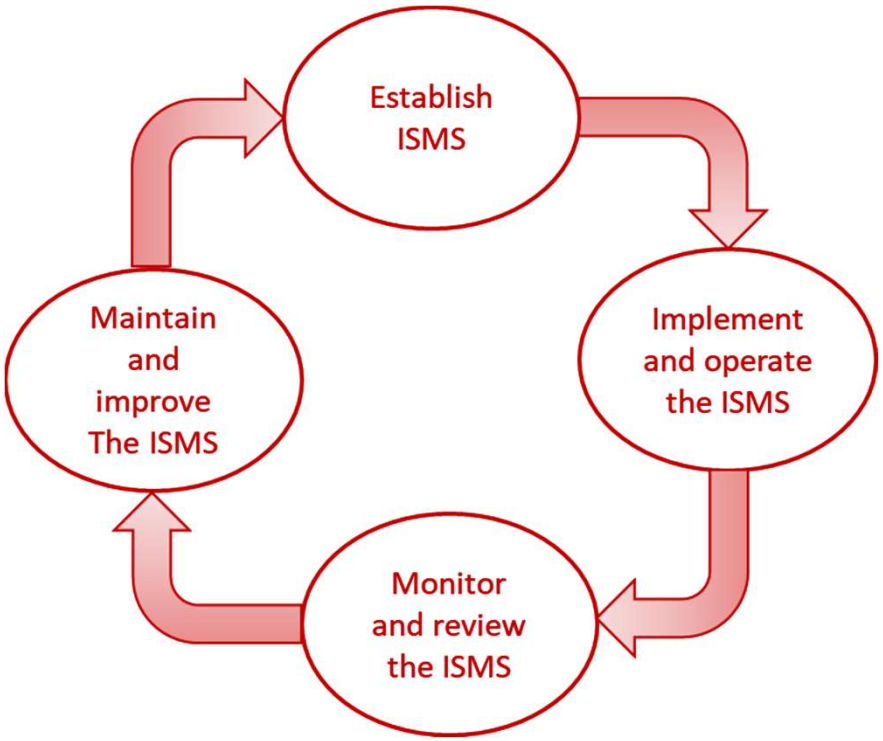
	Nauðsynlega þjónusta	Mikilvæg þjónusta
Öryggiskröfur	Kröfur um áhættumiðaða nálgun stjórnskipan netöryggis, þ.m.t. ábyrgð æðstu stjórnenda	
Tilkynningarskylda	Alvarleg atvik	
Eftirlit	Ex-ante og ex-post	Ex-post
Sektir	Eftirlitsviðurlög, þ.m.t. stjórnvaldssektir. Hvað varðar nauðsynlega þjónustu má grípa til afturköllun starfsheimilda	
Lögsaga	Almenn regla: Í aðildarríki þar sem aðili á stofnsettur. Undanþágur varðandi fjarskiptafyrirtæki - þar sem þau veita þjónustu. Ákveðin stafræn grunnvirki og stafræn þjónusta - Aðalskrifstofa innan ESB	

NIS-2 *- Samræmdar lágmarkskröfur*

Fjarskiptastofa

Stjórnskipan netöryggis

- Áhættumiðuð nálgun.
- „All-hazards“ nálgun.
- Innleiða viðeigandi tæknilegar, rekstrarlegar og stjórnskipulegar ráðstafanir til að stýra áhættu. (ISMS)
- „State of Art“ kröfur.
- Lágmarkskröfur settar fram í tilskipun.



NIS-2 *– Tilgreindar lágmarkskröfur*

Fjarskiptastofa

Til viðbótar við almennt stjórnskipulag eru lágmarkskröfur um:

1. Stefnur um áhættumat og net- og upplýsingakerfi.
2. Atvikameðhöndlun.
3. Rekstrarsamfellu, endurreisnaráætlun og hættustjórn.
4. Öryggi birgjakeðju, þ.m.t. öryggistengda þætti sem varða tengsl við birgja og þjónustuveitendur.
5. Öryggi net- og upplýsingakerfa m.t.t. innleiðingu kerfa, þróun og viðhalda, þ.m.t. veikleikagreiningu og upplýsingagjöf.
6. Stefnur og ferla til að meta virkni stjórnskipulags og öryggisráðstafana.
7. Lágmarksaðferðir hvað varðar þjálfun.
8. Stefnur varðandi dulkóðun.
9. Öryggisráðstafanir varðandi starfsfólk, aðgangsstýringar og fleira.
10. Notkun fjölþátta auðkenningarleiða, örugg tal-, mynd- og textasamskipti og örugg neyðarsamskipti innan fyrirtækis.

NIS-2 *– Kröfur á stjórnendur*

Fjarskiptastofa

Samþykkja umgjörð áhættustýringar fyrir netöryggi og ráðstafanir sem gerðar eru.

Hafa umsjón með innleiðingu rástafana.

Hljóta þjálfun til að öðlast nægilega þekkingu og færni til að greina áhættu og meta áhættu á sviði netöryggis og áhrif þeirra á þjónustuna sem aðili veitir.

Bjóða starfsmönnum fyrirtækisins/stofnunarinnar sambærilega þjálfun.

Bera ábyrgð ef skortur er á hlítni við ákvæði tilskipunarinnar.

NIS-2 *- eftirlit*

Það eru ítarleg ákvæði um eftirlit í NIS-2:

- Rík krafa um áhættumiðað eftirlit.
- Sett er mun ítarlegri ákvæði um framkvæmd eftirlits t.a.m.:
  - Framkvæmd úttekta
  - Öryggisprófana
  - Rannsókn atvika
  - Kröfu um tímasettar úrbætur
  - Álagningu sekta sem og afturköllun starfsleyfam (nauðsynleg)
  - Perónuleg ábyrgð stjórnenda
  - O.fl.

- Áfram gerður greinarmunur á eftirliti milli nauðsynlegra aðila (ex-ante + ex-post) og mikilvægra aðila (ex-post).

Innleiðing

Innleiðing NIS-2 tilskipunar

Fjarskiptastofa

Staða á NIS-1

- Innleidd í EES-samninginn í febrúar 2023. Var ekki skyldubundin fyrir EFTA-ríki en þó tekin upp í EES-samninginn.
- Ísland (2019) og Liechtenstein (2023) hafa innleitt í landsrétt. Noregur hefur ekki innleitt NIS-1 (frumvarp komið).

Staðan á NIS-2

- Tilskipunin er EES-tæk (ólíkt NIS-1).
- EFTA skrifstofa í Brussel og vinnuhópar þar vinna að innleiðingu.
- Óvíst hvenær innleiðingardagsetning verður m.t.t. ESS/EFTA ríkja.
- Ráðuneyti háskóla, iðnaðar og nýsköpunar fer með forræði á innleiðingu tilskipunarinnar hér á landi.
  - Er á aðgerðaráætlun fyrir netöryggisstefnu stjórnvalda.

Tímalínur ESB

- Ár til stefnu fyrir aðildarríki + viðbótar innbyggðar tímalínur varðandi aðila.

Fjarskiptastofa