

CERT.IS

SKÝ – 28. Október 2020

Óvissustig fjarskiptageirans í september 2020

TLP:WHITE

cert@cert.is

<https://www.cert.is>

<https://www.cert.is/rfc2350>

whoami



Kristján Valur er rafmagnsverkfræðingur og tölvunarfræðingur að mennt. Hann lauk doktorsprófi í tölvunarfræði með áherslu á upplýsingaöryggi frá KTH og HR árið 2012. Kristján hefur starfað við hugbúnaðargerð og verkefni tengd kerfishönnun um árabil, en unnið hjá CERT-IS sem netöryggissérfræðingur frá 2015, nú síðastliðið ár sem fagstjóri netöryggissveitar.

CERT.is

Þjóðar-CSIRT sem stuðlar að öryggi mikilvægra innviða

"Netöryggissveitinni er ætlað að fyrirbyggja, draga úr og bregðast við hættu vegna netárása eða hliðstæðra öryggisatvika eins og kostur er í þeim tölvukerfum sem falla innan netumdæmis hennar. Þetta gerir sveitin m.a. með því að stuðla að eflum forvörnum og viðbragðsstarfsemi, í samvinnu og samstarfi við þjónustuhóp sinn. Hluta hlutverk sveitarinnar er að styðja þjónustuhópinn við að takast á við ógnir og öryggisatvik. Sveitin leitast við að greina öryggisatvik sem ógna heildstæði og öryggi ómissandi upplýsingainnviða, takmarka útbreiðslu atvikanna og tjón af þeirra völdum. Við útbreidd og alvarleg öryggisatvik skal sveitin samhæfa viðbrögð og aðgerðir innan netumdæmisins." (reglugerð 475/2013)

Þjónustuhópur

- Skráð fjarskiptafyrirtæki (2013)
- Stjórnarráð Íslands („GovCERT“ 2018)
- Rekstraraðilar nauðsynlegrar þjónustu og stafrænir þjónustuveitendur (NIS - lög 78/2019) frá 1. september 2020

<https://www.cert.is>

RDOS – September 2020

- Tilkynning um DDoS árás og RDOS hótun í byrjun september
- Ógnarmat:
 - Hótað mjög stórri árás gegn mikilvægum innvið
 - Andstæðingur sem notaði sömu merki og aðferðafræði hafði fylgt hótun eftir
 - Önnur atvik og aðstæður síðustu vikur á undan hótuninni – þ.m.t. DDoS
- Viðbrögð:
 - Samráð við tilkynnanda
 - Rannsókn m.a. öflun upplýsinga frá erlendum samstarfsaðilum
 - Virkjun neyðarstjórnar fjarskiptageirans
 - Samráð við Almannavarnir og ráðuneyti
 - Miðlun upplýsinga til þjónustuhóps og annarra mikilvægra innviða
 - Upplýsingar til opinberrar birtingar

Viðbúnaðaráætlanir

- Áætlun fjarskiptageirans og CERT-IS frá 2017
- Áætlun AlmannaVARNA og CERT-IS frá 2019
- Skilgreining
 - Ferla
 - Stjórnkerfis
 - **Samskipta**



Innihald

1. Inngangur
2. Staðhættir
3. Skilgreiningar
 - Almennavarnastig
 - Umfang
 - Forgangur
 - Trúnaðarflokkun
 - Ómissandi upplýsingainnviðir
4. Boðun
5. Stjórnkerfi
 - SST / Stjórnstöð
 - Vettvangsstjórn
 - Fjölmiðlar
6. Starfssvæði
7. (sértækur kafli)
8. Verkefni viðbragðsaðila
9. Skipulag fjarskipta/samskiptalisti
10. Kort
11. Dreifingarlisti
12. Breytingasaga

Tilgangur

- Miðla réttum og nægilegum upplýsingum til hagsmunaaðila
 - Stjórnendur þ.m.t. stjórnvöld
 - Viðbragðsaðilar þ.m.t. Almannaþingin
 - Þeir sem þurfa að verjast – skilvirk miðlun á tæknilegum upplýsingum
- Stigskipt viðbrögð miðað við umfang og hættu sem er á ferðum
- Minnka óvissu
- Stuðla að samræmingu og skilvirkari vinnubrögðum
 - Verkaskipting og ábyrgðarsvið

Stig og umfang ástands

Stig

- Eðlilegt ástand
- Óvissustig
- Hættustig
- Neyðarstig



Umfang

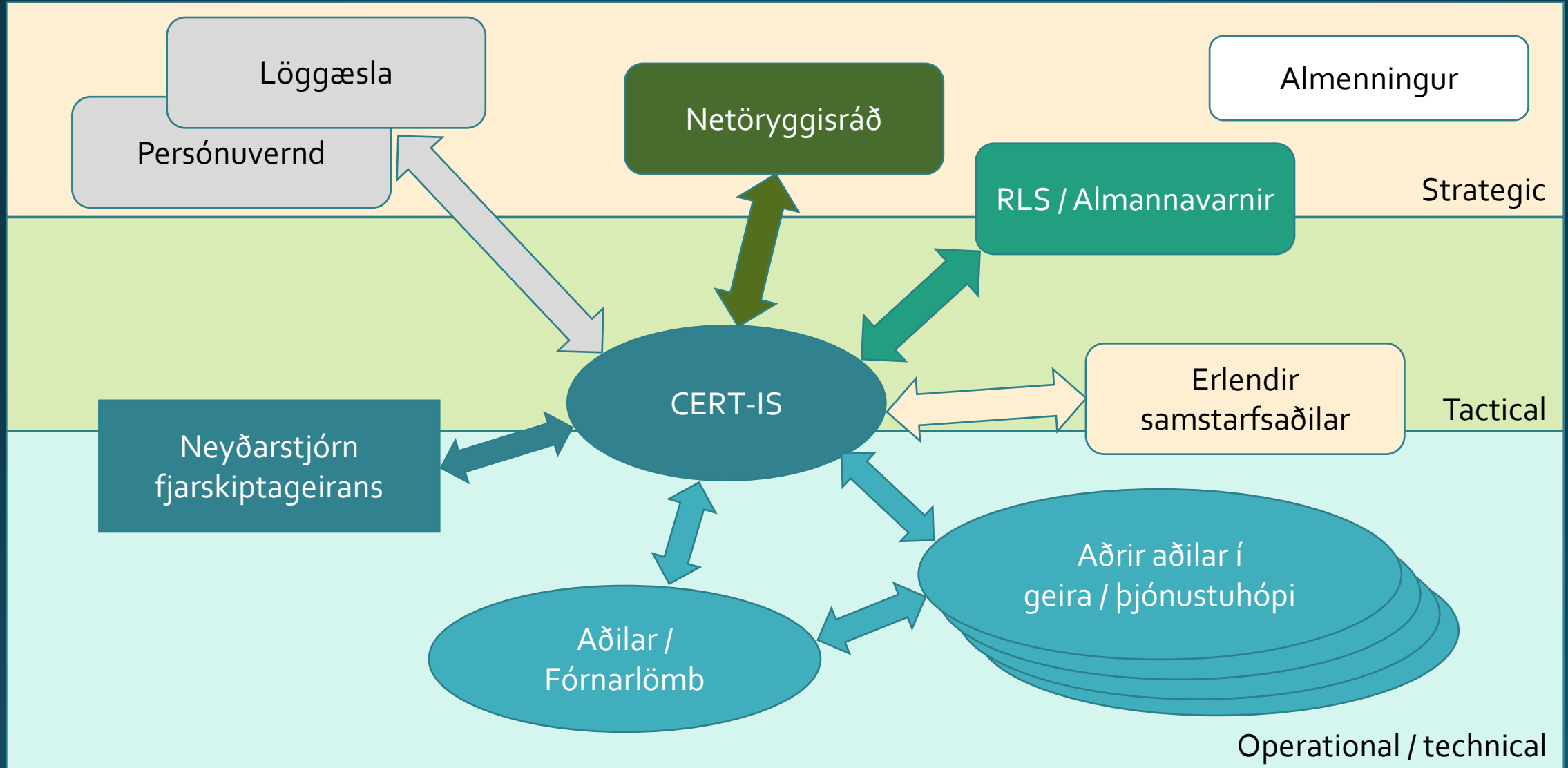
Grænt

Gult

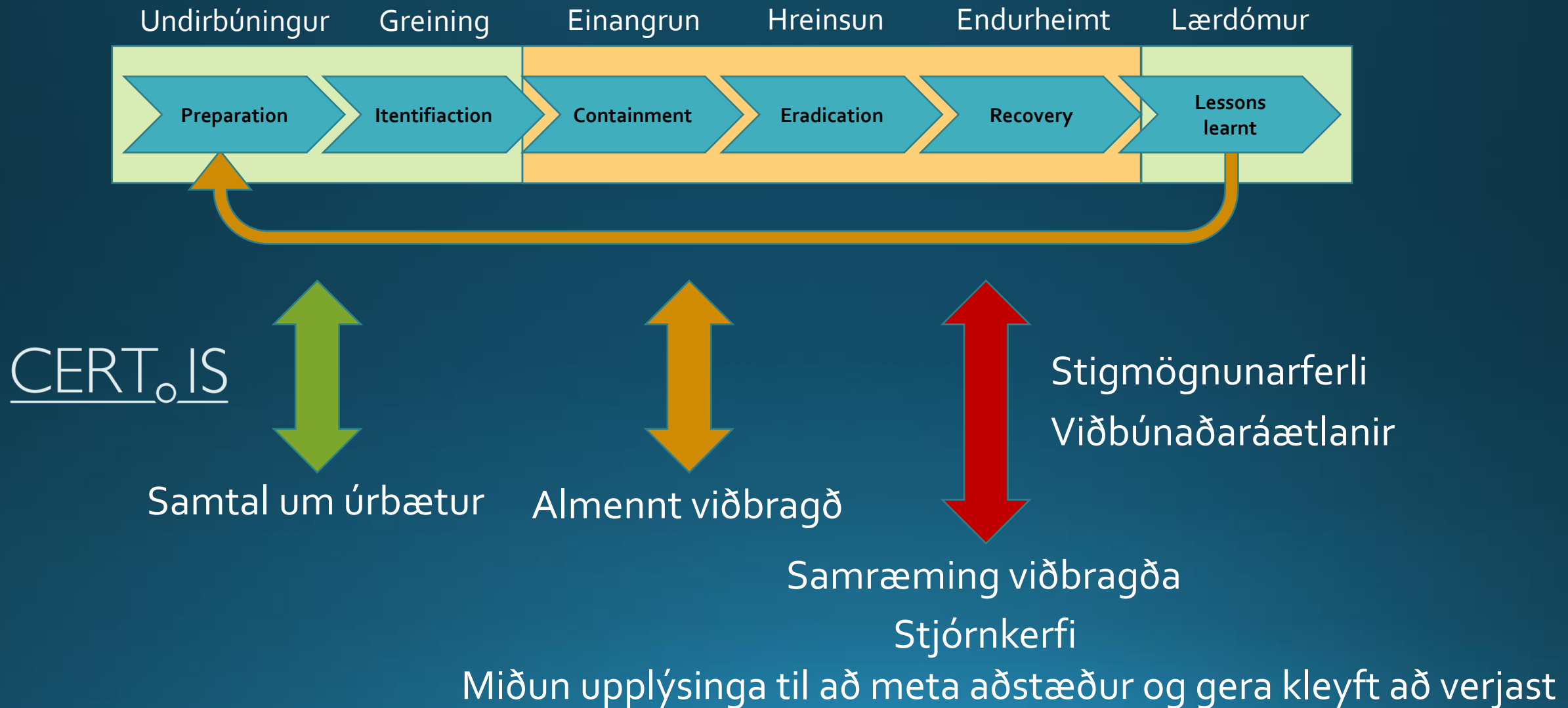
Rautt

Svart

Persónur og leikendur



Samskipti og ferlar



Öryggisskipulag

- Fyrir atvik
 - Reyna að sjá fyrir aðstæður
 - Búa til aðgerðalista og áætlanir
 - Æfa
- Meðan á atviki stendur
 - „Dont panic“
 - Nota ferla, skipuleggja
 - Nákvæm samskipti
 - Rýna upplýsingar og móta viðbrögð
 - Bókhalð yfir allt ferlið
- Eftir atvik
 - Læra og endurbæta



Viðbúnaðaráætlun



Viðbúnaðaráætlun



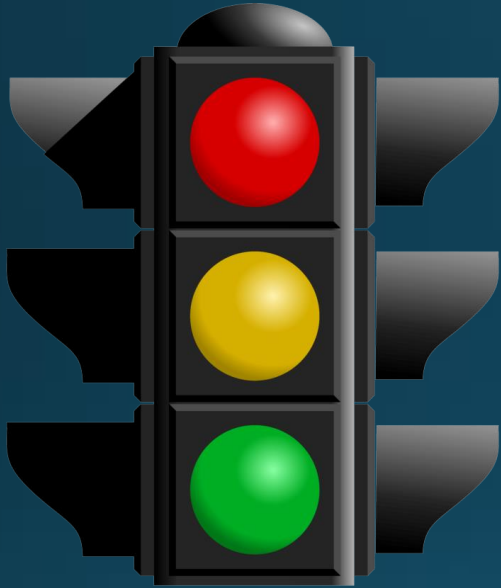
Viðbúnaðaráætlun

Miðlun

- „Sharing er caring“ --- en ...
 - Erum við að segja nóg – eða of mikið?
 - Skýr ábyrgð á samskiptum - framlína
- Tilgangur miðlunar
 - Til að minnka óvissu – góðar upplýsingar um mál sem eru í umræðu
 - Til að minnka áhættu – miðla upplýsingum um áhættu til að geta varist
- Markhópur, miðlar og trúnaður
 - Mjög þröngur – sími, dulkóðaður tölvupóstur, ..
 - Þröngur – dulkóðaður tölvupóstur, ...
 - Frekar opin – tölvupóstur, teams, ...
 - Opinber miðlun – tölvupóstur, fjölmiðlar, www



Trúnaður - TLP



- **TLP:WHITE** – Til opinberrar birtingar
- **TLP:GREEN** – Til þeirra sem málið varðar en opinber birting ekki heimiluð
- **TLP:AMBER** – Takmörkuð miðlun til þeirra sem á þurfa að halda til að stuðla að úrlausn öryggisatvika
- **TLP:RED** – Miðlun óheimil umfram upphafleg upplýsingaskipti

Miðlun til þeirra sem á þurfa að halda en í samræmi við óskir eigenda

<https://www.first.org/tlp/>
<https://www.cert.is/tlp>



TLP:RED

Mjög viðkvæmar
upplýsingar s.s.
gögn í kerfum



TLP:AMBER

Viðkvæmar upplýsingar
s.s. IP tölur og lén



Viðvörðun og upplýsingar til
dreifingar innan þröngs hóps
þeirra sem nauðsynlega
þurfa að vera upplýstir



TLP:GREEN

Gögn sem má
miðla víðar



Viðvörðun og upplýsingar til
dreifingar innan einstakra geira
þjónustuhóps



TLP:WHITE

Gögn sem má
miðla án takmarkana



Opinber viðvörðun um
áhættu og varnir

*Ábyrg en skilvirk upplýsingamiðlun og samvinna
eykur líkur á að takist að ná utan um öryggisatvik
tímanlega og lágmarka skaða.*

cert@cert.is
incidents@cert.is

PGP: BF14 84D3 1D39 9C9F 2C70 9054 3938 E161 13E9 308B

CERT.IS



510 1540

<https://oryggisatvik.island.is/>

<https://www.cert.is>

