Vegvísir í frumskógi krefjandi regluverks

SKÝ

INNLEIÐING NIS2 OG CRA
á tímum takmarkalausrar gervigreindar

11. NÓVEMBER 2026

Frá regluvörslu til áfallaþols

Páll Ásgeir Davíðsson

www.rasadvisory.is

VALIÐ

Vegvísir: hvert stefnum við?



> *„Beri maður staf þennan á sér villist maður ekki í hríðum né vondu veðri þó ókunnugur sé.“*
>
> Huld, handrit Geirs Vigfússonar, 1860

TVÆR LEIÐIR

Regluvarsla

Fylgja reglunum

/

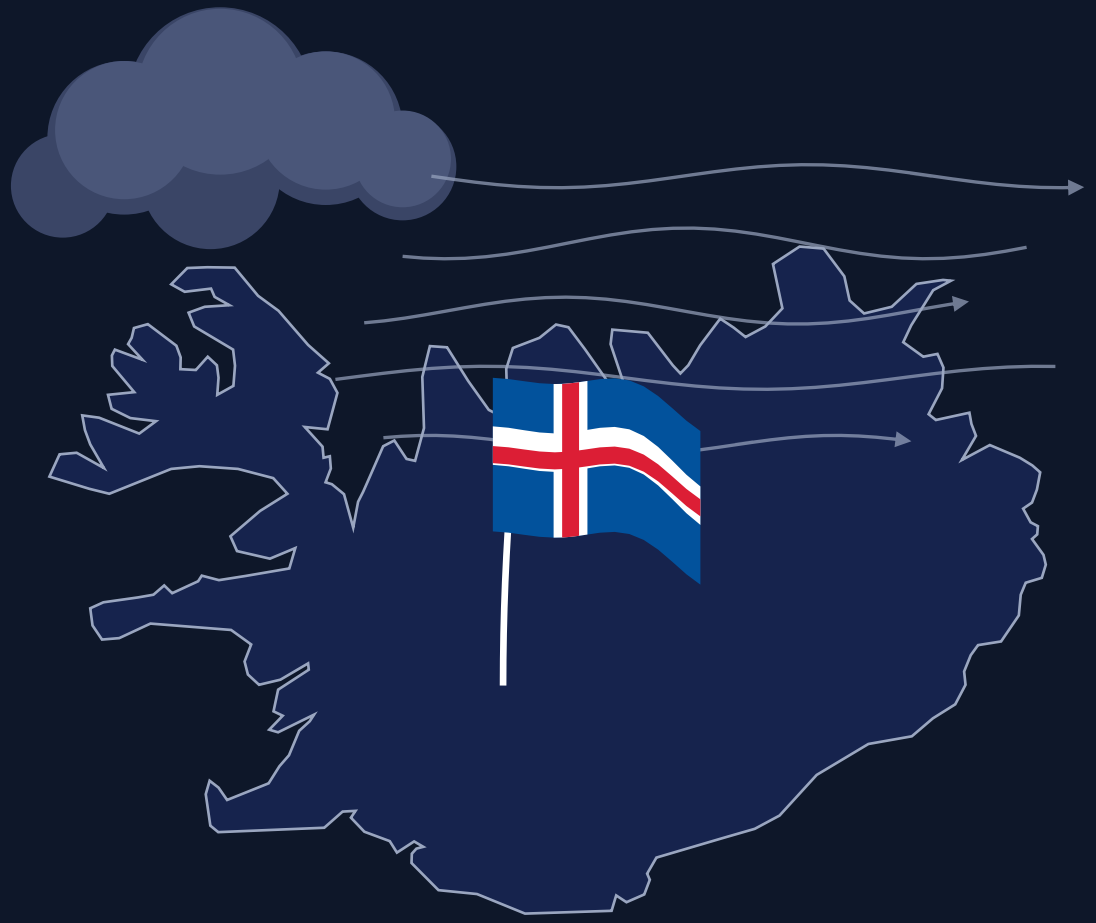
Geta

Byggja upp áfallaþol

RÁS RÁÐGJÖF

SAMHENGIÐ · 1

Óveðrið sem dynur



GERVIGREIND

„Gervigreind mun breyta bæði vörnum og árásum.“

Innviðaráðherra, 2026

BREYTT ÖRYGGISUMHVERFI

„Ytra öryggisumhverfi Íslands hefur breyst í grundvallaratriðum og til langs tíma að öllum líkindum.“

Ríkislögreglustjóri, 2026

NETÁRÁSIR

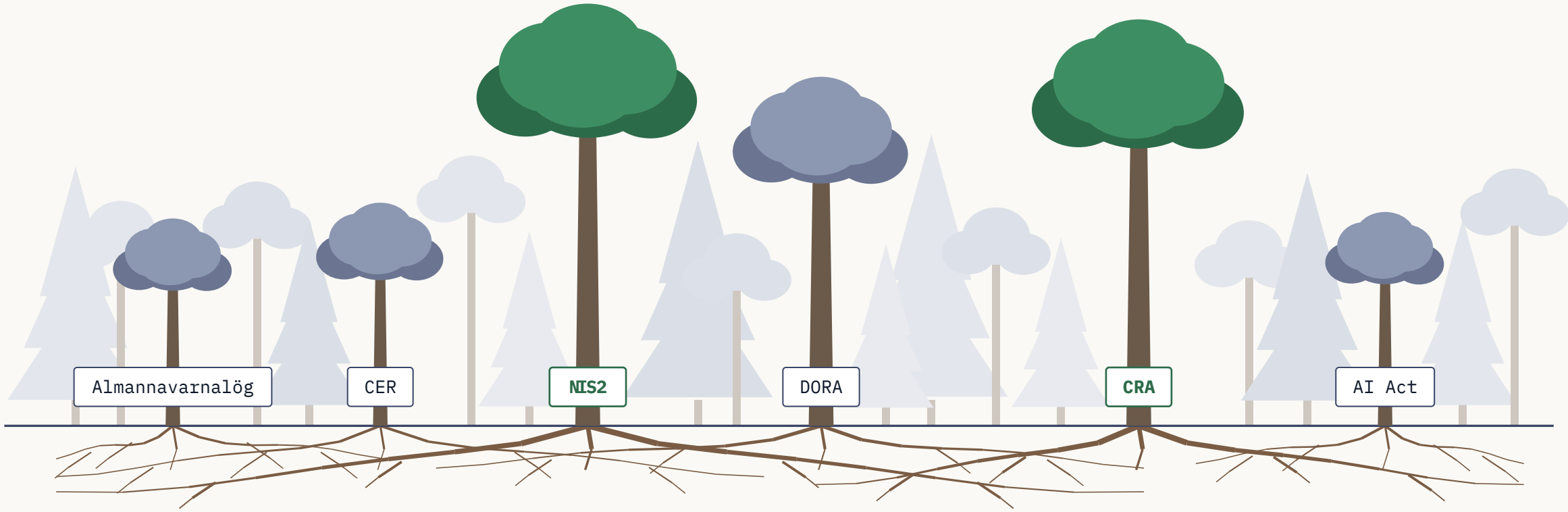
700 → 2.312

netöryggisatvik sem CERT-IS skráði, 2022 → 2025

CERT-IS, ársyfirlit 2023–2025

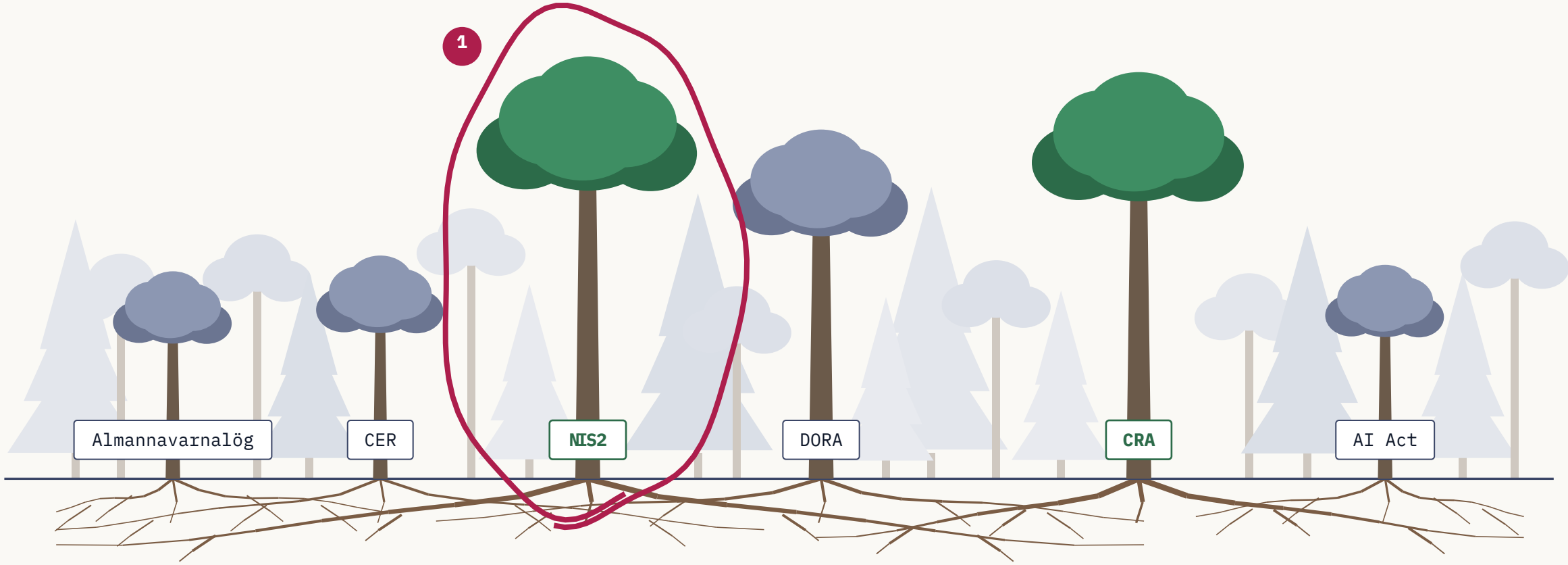
RÁS RÁÐGJÖF

Frumskógur regluverksins



RÁS RÁÐGJÖF

Frumskógur regluverksins

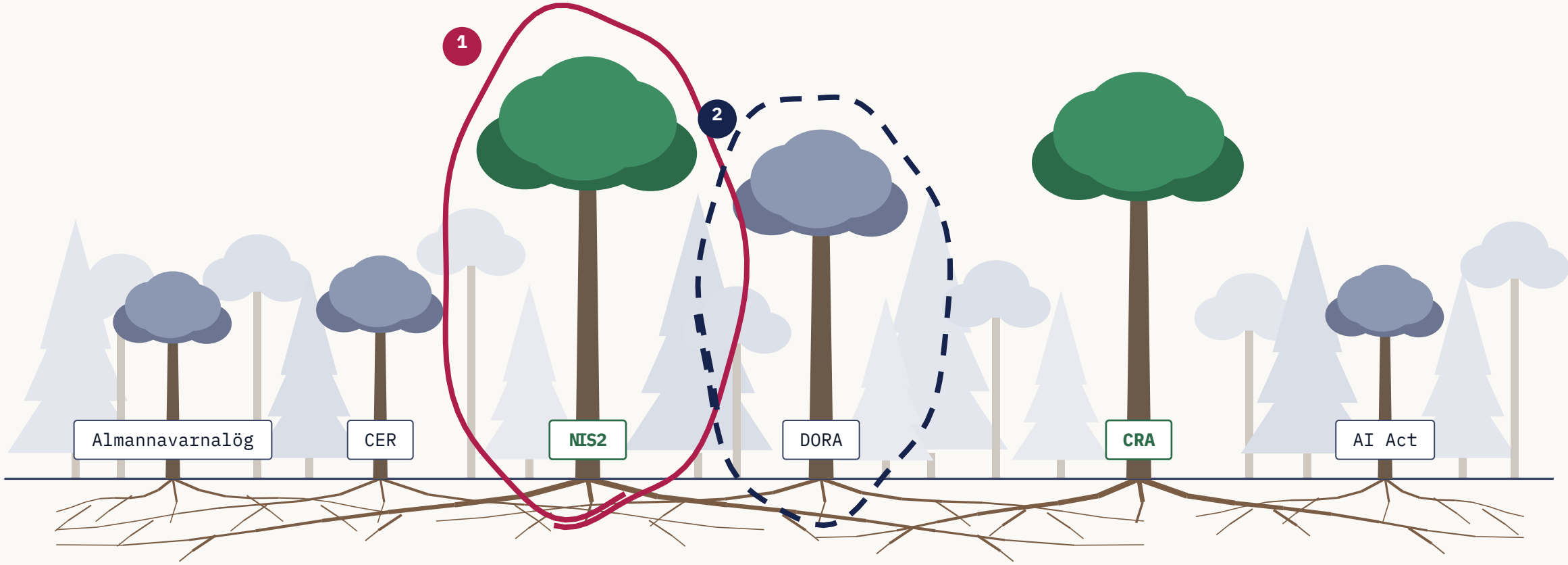


RÁS RÁÐGJÖF

Frumskógur regluverksins

1 Skýja- eða rekstrarþjónusta

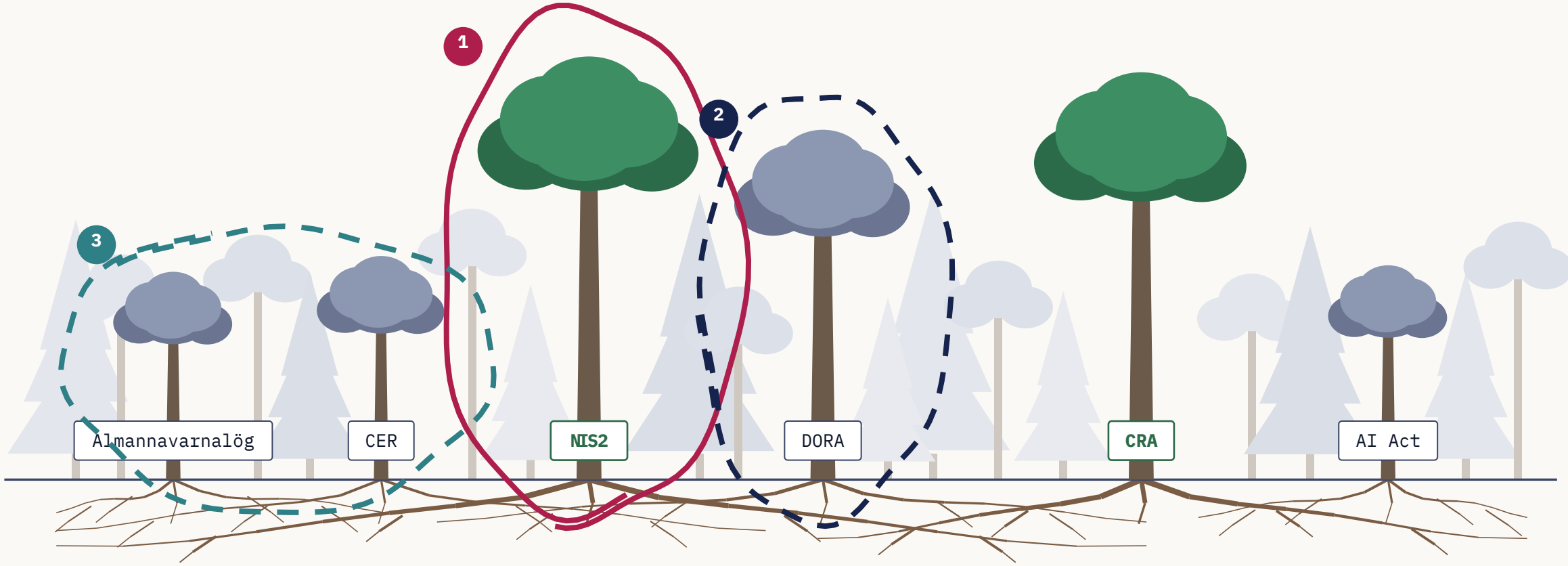
2 Birgir banka (í gegnum viðskiptavini)



RÁS RÁÐGJÖF

Frumskógur regluverksins

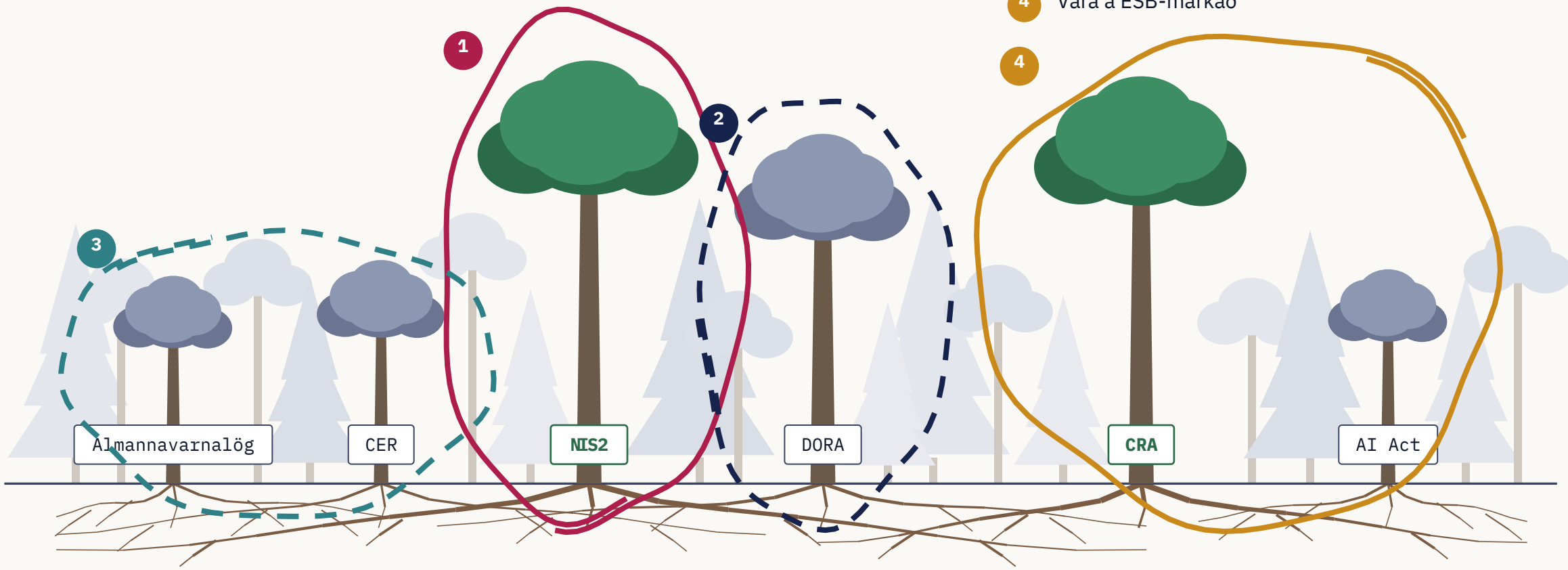
1. Skýja- eða rekstrarþjónusta
2. Birgir banka (í gegnum viðskiptavini)
3. Birgir ómissandi innviða (í gegnum viðskiptavini)



RÁS RÁÐGJÖF

Frumskógur regluverksins

1. Skýja- eða rekstrarþjónusta
2. Birgir banka (í gegnum viðskiptavini)
3. Birgir ómissandi innviða (í gegnum viðskiptavini)
4. Vara á ESB-markað

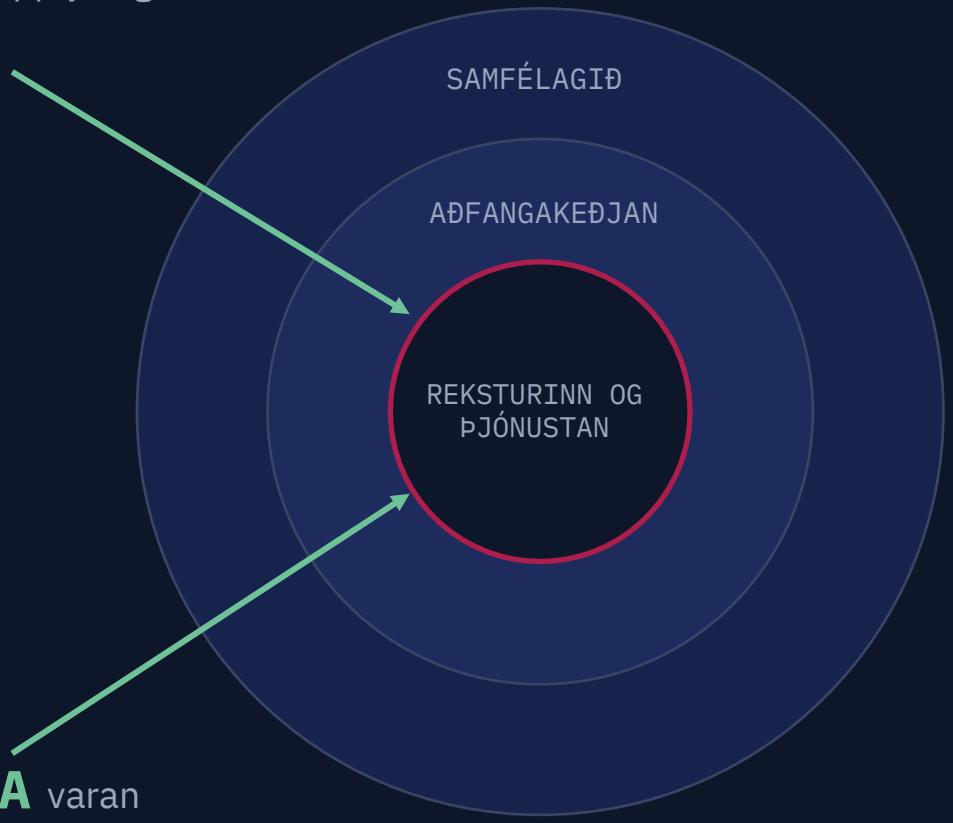


RÁS RÁÐGJÖF

SAMHENGIÐ · 3

Nægja reglurnar?

NIS2 upplýsingakerfin



CRA varan

REGLURNAR VARÐA AFMÖRKUÐ SVIÐ

NIS2 og CRA vernda kerfin og vöruna – ekki reksturinn í heild.

REGLURNAR ELTA VERULEIKANN

Gervigreindarreglugerð ESB var lögð fram 2021, áður en ChatGBT kom fram.

Kröfum til gervigreindarkerfa á sviðum þar sem hættan er mikil frestað til 2027–2028.

REGLUR OG GETA FARA EKKI ALLTAF SAMAN

Lög um öryggi net- og upplýsingakerfa mikilvægra innviða í gildi frá 2020.

„talsverður hluti rekstraraðila uppfyllir ekki viðmiði Fjarskiptastofu hvað varðar hlítni við lágmarkskröfur netöryggislaga“

Fjarskiptastofa, samhæft sjálfsmat 2025

RÁS RÁÐGJÖF

REGLUVÖRSLUGILDRAN

„Adherence to the rules, originally conceived as a means, becomes transformed into an end-in-itself.“

„Að fylgja reglunum, sem upphaflega var leið að markmiði, verður markmið í sjálfu sér.“

ROBERT K. MERTON · BUREAUCRATIC STRUCTURE AND PERSONALITY · 1940

RÁS RÁÐGJÖF

REGLUVARSLA EÐA ÁFALLAÞOL

Regluvörslugildran

REGLUVARSLA	FORSENDUR FYRIR ÁFALLAÞOLI
Ein regla í einu	→ **Heildstæð nálgun á allan reksturinn og alla áhættu**
Skjöl og gátlistar	→ **Prófuð viðbrögð**
Ábyrgð hjá regluverði	→ **Ábyrgð hjá stjórnendum**
Úttekt	→ **Raunveruleg geta þegar á reynir**

RÁS RÁÐGJÖF

LEIÐIN

Markmiðið er áfallaþol



Reglurnar eru inntak í aðferðina, ekki sjálfstætt verkefni

Aðferðin er sú sama, hver sem reglan er.

REYND AÐFERÐ

Alþjóðlegur staðall (ISO 22301) og besta framkvæmd – ekki ný uppfinning.

UNDIRSTAÐAN

Forysta, ábyrgir stjórnarhættir og stöðugar umbætur

RÁS RÁÐGJÖF

Í FRAMKVÆMD

Sama aðferð, ólík efnistök

ÁFALLAÞOL
Grunnurinn · ISO 22301

01 Greining	02 Áætlun	03 Innleiðing	04 Æfingar og umbætur
Samhengi og lagakröfur, áhættumat, áhrifagreining (BIA): mikilvæg starfsemi og þolanlegt rof ISO 22301: 4, 8.2	Leiðir til að tryggja samfellu: forgangsröðun, varaleiðir, aðföng ISO 22301: 6, 8.3	Viðbragðsskipulag, áætlanir, samskipti og krísustjórnun ISO 22301: 7, 8.4	Æfingar, mat á getu, rýni stjórnenda og umbætur ISO 22301: 8.5–8.6, 9–10

Hvað bæta reglurnar við?

RÁS RÁÐGJÖF

Í FRAMKVÆMD

Sama aðferð, ólík efnistök

	01 Greining	02 Áætlun	03 Innleiðing	04 Æfingar og umbætur
ÁFALLAÞOL Grunnurinn · ISO 22301	Samhengi og lagakröfur, áhættumat, áhrifagreining: mikilvæg starfsemi og þolanlegt rof ISO 22301: 4, 8.2	Leiðir til að tryggja samfellu: forgangsröðun, varaleiðir, auðlindir ISO 22301: 6, 8.3	Viðbragðsskipulag, áætlanir, samskipti og krísustjórnun ISO 22301: 7, 8.4	Æfingar, mat á getu, rýni stjórnenda og umbætur ISO 22301: 8.5–8.6, 9–10
NIS2 · DORA Upplýsingakerfin	Ógnir og veikleikar í upplýsingakerfum, netöryggi birgja NIS2 21(2)(a),(d) · DORA 8, 28	Afritun, endurheimt kerfa, aðgangsstýring, dulkóðun NIS2 21(2)(c),(h)–(j) · DORA 9, 11–12	Meðhöndlun atvika, tilkynning innan 24/72 klst. NIS2 21(2)(b), 23 · DORA 17–19	Mat á virkni ráðstafana, þjálfun, prófanir NIS2 21(2)(f),(g) · DORA 24–26

RÁS RÁÐGJÖF

Í FRAMKVÆMD

Sama aðferð, ólík efnistök

	01 Greining	02 Áætlun	03 Innleiðing	04 Æfingar og umbætur
ÁFALLAÞOL Grunnurinn · ISO 22301	Samhengi og lagakröfur, áhættumat, áhrifagreining: mikilvæg starfsemi og þolanlegt rof ISO 22301: 4, 8.2	Leiðir til að tryggja samfellu: forgangsröðun, varaleiðir, auðlindir ISO 22301: 6, 8.3	Viðbragðsskipulag, áætlanir, samskipti og krísustjórnun ISO 22301: 7, 8.4	Æfingar, mat á getu, rýni stjórnenda og umbætur ISO 22301: 8.5–8.6, 9–10
NIS2 · DORA Upplýsingakerfin	Ógnir og veikleikar í upplýsingakerfum, netöryggi birgja NIS2 21(2)(a),(d) · DORA 8, 28	Afritun, endurheimt kerfa, aðgangsstýring, dulkóðun NIS2 21(2)(c),(h)–(j) · DORA 9, 11–12	Meðhöndlun atvika, tilkynning innan 24/72 klst. NIS2 21(2)(b), 23 · DORA 17–19	Mat á virkni ráðstafana, þjálfun, prófanir NIS2 21(2)(f),(g) · DORA 24–26
CRA Varan	Áhættumat vörunnar allan líftímann: árásarflötur, íhlutir CRA 13(2), 13(5)	Öryggi í hönnun, skilgreint stuðningstímabil CRA I. viðauki I · 13(8)	Meðferð veikleika, uppfærslur, tilkynning innan 24 klst. CRA I. viðauki II · 14. gr.	Reglulegar öryggisprófanir og endurskoðun CRA I. viðauki II

RÁS RÁÐGJÖF

AF HVERJU GETA?

Ávinningurinn

01

Ein vinna, margar kröfur

Eitt kerfi í stað margra regluvörsluverkefna. Minni tvíverknaður.

02

Viðbúnaður við hinu óvænta

Æfð viðbrögð duga líka þar sem reglurnar ná ekki til.

03

Traust á markaði

Sýnileg geta, t.d. með vottun, verður að samkeppnisforskoti.

04

Hluti af stjórnun

Ábyrgð færist frá regluverði til stjórnenda, þar sem það á heima.

> Áfallaþol er lífrænt ferli

RÁS RÁÐGJÖF

LOKAORÐ

Eiga takmarkalaus gervigreind og krefjandi reglugerðir samleið?



Áfallaþol rekstrarins er stefnan.

Reglurnar vísa veginn.

Getan ber okkur alla leið.

Já – ef áherslan er á getu.

RÁS RÁÐGJÖF

TAKK FYRIR

RÁS
Áfallaþol · Rekstrarsamfella

RÁS hjálpar fyrirtækjum og stofnunum að búa sig undir breytt öryggisumhverfi, áföll og nýjar öryggiskröfur.

Páll Ásgeir Davíðsson
Framkvæmdastjóri
Sími 842 0222
Netfang pall@rasadvisory.is