Aukin ábyrgð stjórnenda

- nýjar kröfur NIS2

Fjarskiptastofa

Unnur Kristín Sveinbjarnard.
sviðsstjóri stafræns öryggis

EUROPEAN
COMMISSION

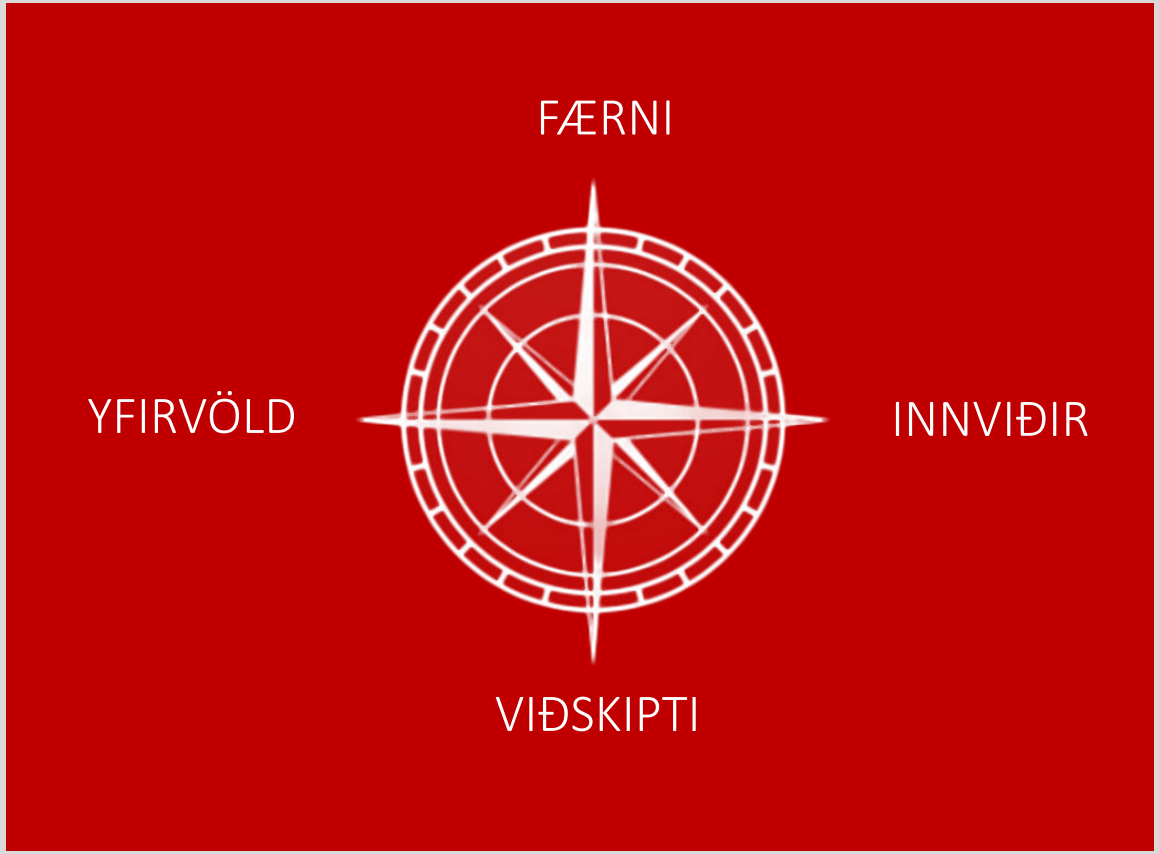
Brussels, 16.12.2020
COM(2020) 823 final

2020/0359 (COD)

Proposal for a

DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148



Stafræn þróun ESB er eitt af forgangsmálum sambandsins

Stefna um stafrænan innri markað 2015
Stefna um stafrænan áratug 2021 sem hefur það markmið að:

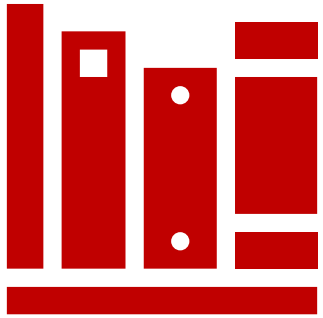
- Byggja upp stafræna getu borgara og sérfræðinga
- **Tryggja örugga stafræna innviði**
- Styðja við stafræna umbreytingu viðskipta
- Styðja við stafræna væðingu opinberrar þjónustu

Mikilvægir innviðir eru lífæð samfélagsins

Um hvað snýst NIS-2?

Fjarskiptastofa

NIS-2 tilskipun Evrópusambandsins



- Tilskipun nr. 2022/2555 um **hátt stig netöryggis** innan Evrópu
- Öll aðildarríki skulu hafa innleitt hana svo hún öðlist gildi **18. október 2024**
  - Belgía eina landið sem hefur tilkynnt framkv.stj. ESB um fulla tímanlega innleiðingu
  - Flest öll aðildarríki munu klára þetta rétt um áramót en einhver á fyrri hluta árs 2025
- EES/EFTA-ríki á annarri tímalínu:
    - Liecthtenstein hefur lagt fram frumvarp fyrir þingið – möguleg gildistaka í janúar 2025
    - Noregur vinnur að drögum til innleiðingar
    - Ísland vinnur að grunndrögum – ekki á þingmálaskrá þessa löggjafarþings

Meira en kröfur á mikilvæga innviði

1 GETA AÐILADARRÍKJA

Eftirlitsstjórnvöld

CSIRTs

Netöryggisstefnur

Upplýsingagjöf um veikleika

Rammi um hættustjórnun

2 SKYLDUR Á AÐILA

Stjórnkerfi net- og upplýsingaöryggis

Tilkynningarskylda

Ábyrgð æðstu stjórnenda

3 SAMSTARF RÍKJA

NIS samstarfshópur

CSIRTs samstarf

CyCLONe

Gagnagrunnur um veikleika

Gagnagrunnur um stafræn grunnvirki

Umfang NIS-2

1 NAUÐSYNLEGIR AÐILAR

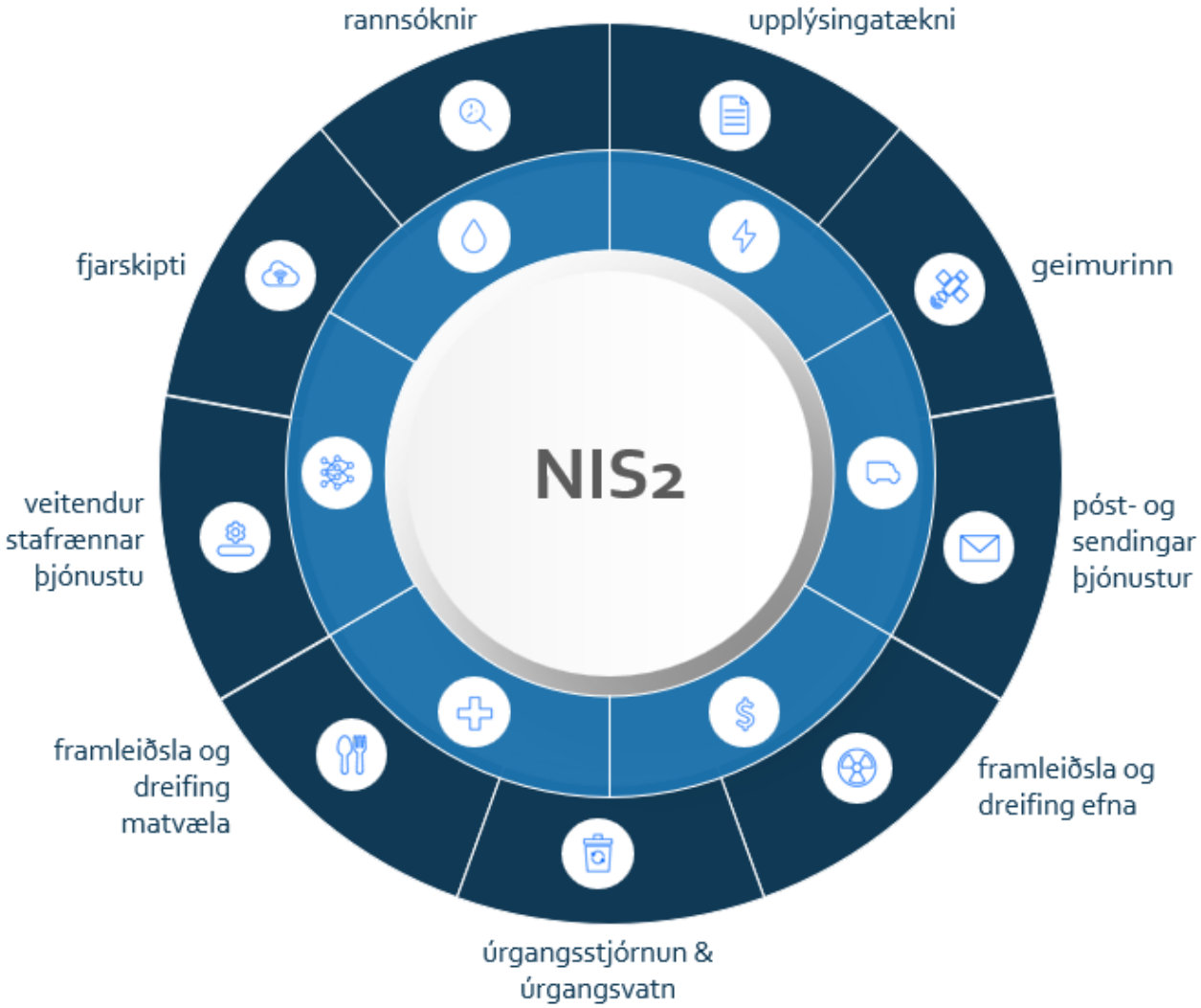
- Orka (rafmagn, olía, gas, svæðisbundin hitun og vetni)
- Samgöngur (loft, vatn, vegir og lestir)
- Bankastarfsemi (DORA)
- Innviðir fjármálamarkaða (DORA)
- Heilbrigði (heilbrigðisþjónusta, rannsóknir og framleiðsla lyfja og lækningalyf)
- Drykkjarvatn
- Úrgangsvatn
- Stafræn grunnvirki (IXP, DNS TDL, skýjaþjónustur, gagnaver, dreifinet efnis, fjarskipti, traustþjónustur)
- Geimstarfsemi
- Upplýsingatækni B2B (MSP&MSSP)
- Opinberir aðilar (lands- og sveitarstjórnarstig)

(nýtt í NIS-2)

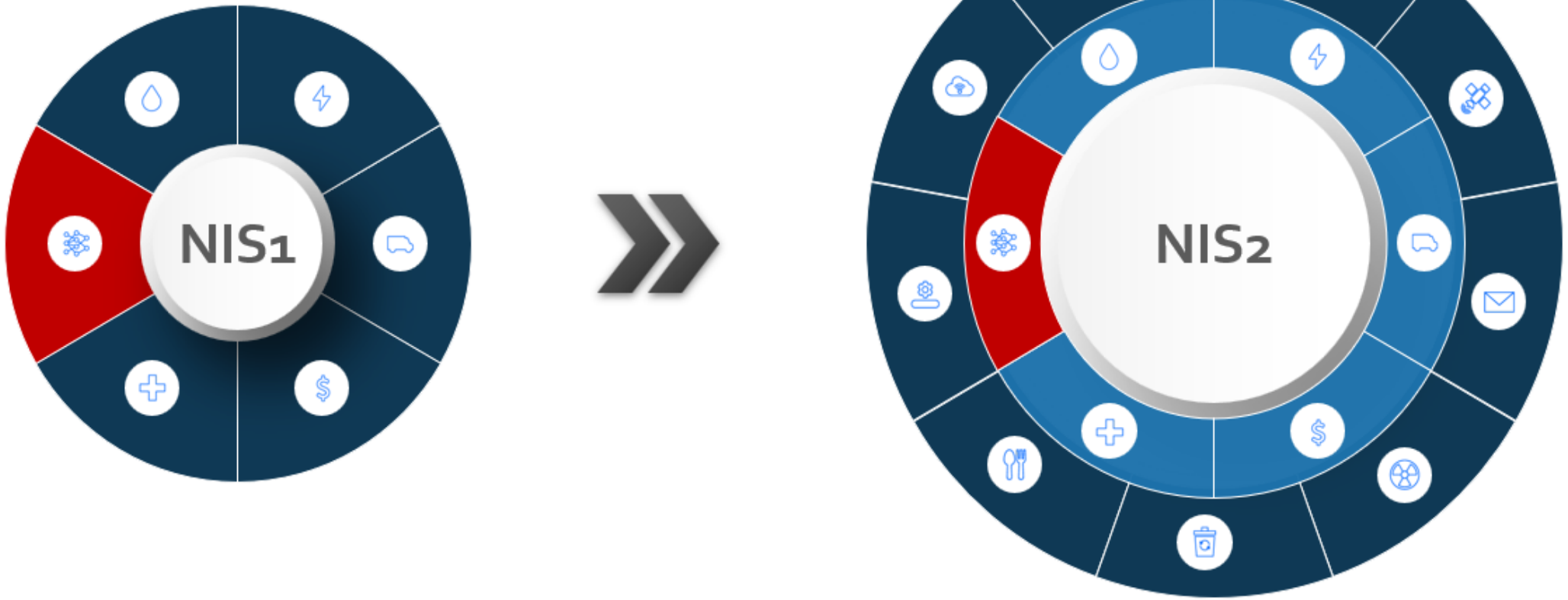
2 MIKILVÆGIR AÐILAR

- Póst og sendingarþjónusta
- Úrgangsstjórnun
- Efni / Lyf (framleiðsla og dreifing efna)
- Matvæli (framleiðsla, vinnsla og dreifing)
- Leitarvélar á netinu
- Netmarkaðir
- Dreifiveitur efnis
- Rannsóknastarfsemi

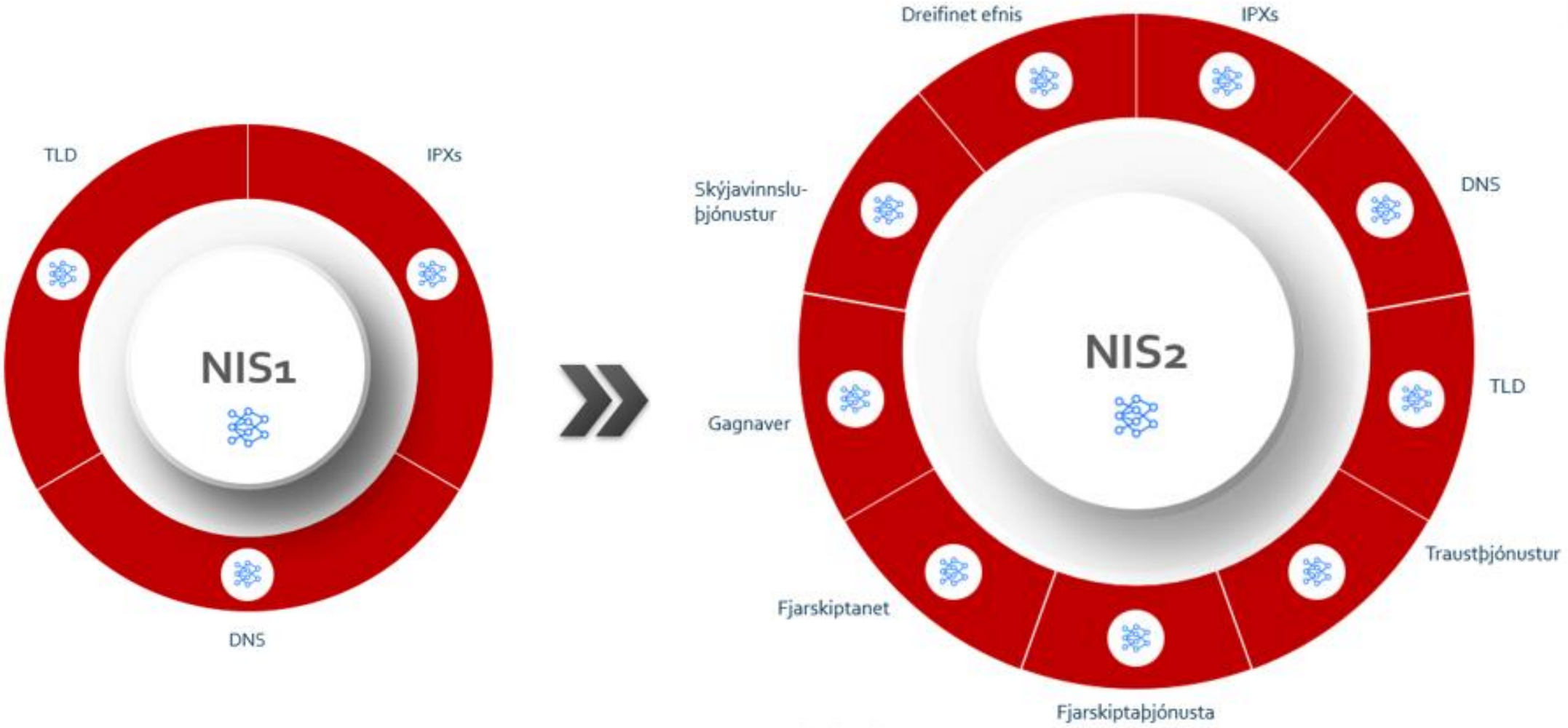
(nýtt í NIS-2)



Hverjir falla undir NIS-2? Mun fleiri svið atvinnulífsins falla nú undir… *(ekki tæmandi listi)



Tökum sem dæmi stafræn grunnvirki



Stafræn grunnvirki fara út þremur tegundum þjónustu í níu tegundir

Telur þú þig falla þarna undir?

NIS-2 próf væntanlegt!

- ✓ Fellur sú þjónusta sem þú veitir undir skilgreiningu á flokkum og undirflokkum?
- ✓ Ef svo er, þarf í öðru lagi að athuga stærðarviðmiðin:
  - ✓ 50 starfsmenn eða fleiri
  - ✓ Yfir 10 m.kr. í ársveltu/efnahag
- ✓ Ef þau eru ekki uppfyllt þarf í þriðja lagi að athuga hvort að þjónustan falli undir önnur skilyrði óháð stærðarmörkum.
  - Samþjónustuveitendur lénsheitakerfa (DNS).
  - Opinberar stofnanir

- Aðilinn er eini veitandi þjónustunnar í aðildarríki þar sem þjónustan er nauðsynleg fyrir viðhald annarrar krítískrar þjónustu.
- Rof á þeirri þjónustu sem að aðili veitir gæti haft umtalsverð áhrif á almannaöryggi, almannavernd og almannaheilsu (public health).
- Rof á þeirri þjónustu sem að aðilinn veitir gæti ytt undir (induce) umtalsverða kerfislæga áhættu, sér í lagi í sektorum þar sem slík truflun (ETD) haft áhrif yfir landamæri.
- Aðilinn er kritískur vegna sérstaks mikilvægis, á landsvísu eða tilteknu landsvæði, fyrir tiltekinn sector eða þjónustutegund, eða fyrir aðra sérstaka sektora í aðildarríki.

Aukin ábyrgð æðstu stjórnenda

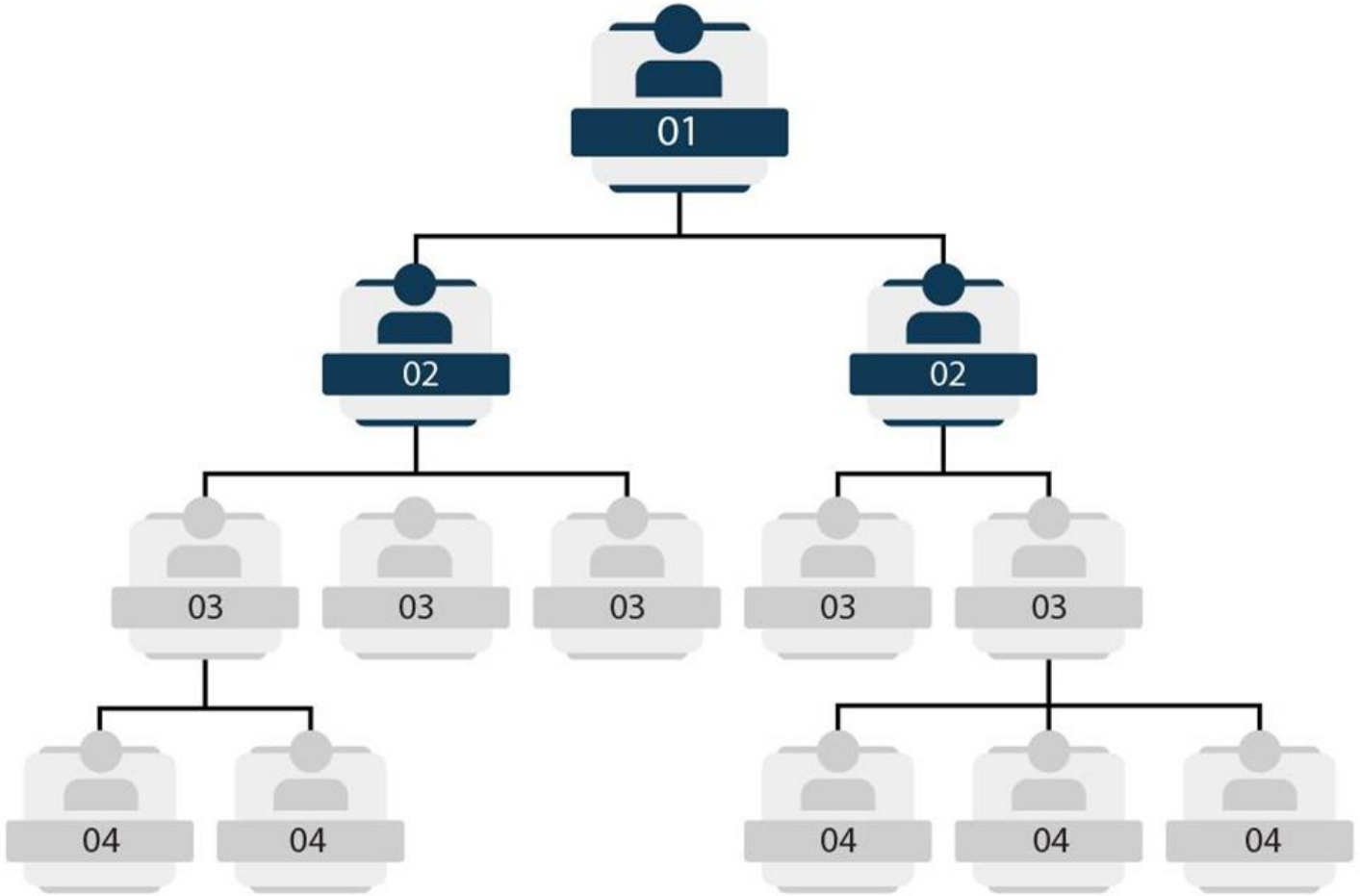
Fjarskiptastofa

Skýlaus krafa um ábyrgð æðstu stjórenda

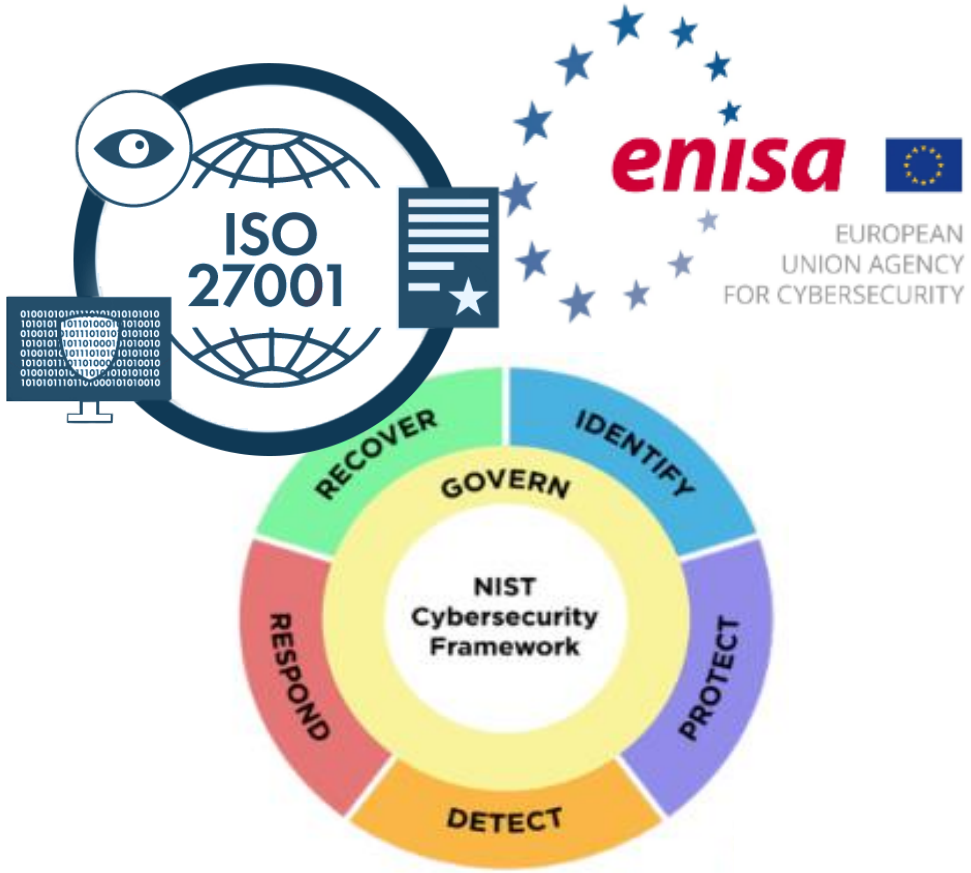
Á hverju bera æðstu stjórnendur ábyrgð?

Æðstu stjórnendur skulu:

1. samþykkja ráðstafanir til áhættustýringar netöryggis
2. hafa yfirumsjón með innleiðingu þeirra
3. hafa þekkingu og getu til að greina áhættu og meta áhættustýringu netöryggis og áhrif þeirra á þjónustu fyrirtækisins
4. bera ábyrgð á skorti á hlítingu



Hvað eru ráðstafanir til áhættustýringar netöryggis? (1)



- Í raun krafa um innleiðingu á **virku stjórnkerfi net- og upplýsingaöryggis**

- Nær til allrar starfsemi fyrirtækisins eða stofnunarinnar (operational, organizational and technical)

- Aðilar þurfa að viðhafa **fastmótað verklag** svo þeir geti
  - auðkennt/greint áhættu
  - varist áhættu
  - uppgötvað áhættu
  - brugðist við áhættu og
  - endurreist þjónustu

- Byggja þarf á alþjóðlegum viðurkenndum stöðlum um bestu framkvæmd - “state-of-art”

Ráðstafanir til áhættustýringar netöryggis (1)

Skulu byggja á „all-hazard“ aðferðafræði og innihalda að lágmarki:

- Stefnur um áhættumat og öryggi net- og upplýsingakerfa
- Atvikameðhöndlun
- Rekstrarsamfellu, endurreisnaráætlun og hættustjórn
- Öryggi net- og upplýsingakerfa m.t.t. **innleiðingu kerfa, þróun og viðhalds**, þ.m.t. veikleikagreiningu og upplýsingagjöf
- **Öryggi birgjakeðju**, þ.m.t. öryggistengda þætti sem varða tengsl við birgja og þjónustuveitendur
- Stefnur og **ferla til að meta virkni** stjórnskipulags og öryggisráðstafana
- Lágmarksaðferðir hvað varðar þjálfun
- Stefnur varðandi dulkóðun
- Öryggisráðstafanir varðandi starfsfólk, aðgangsstýringar og fleira
- Notkun fjölþátta auðkenningarleiða, örugg tal-, mynd- og textasamskipti og örugg neyðarsamskipti innan fyrirtækis
- **Tilkynningarskylda** um alvarleg atvik til stjórnvalda

Ráðstafanir til áhættustýringar netöryggis (1)

- Framkvæmdagerð ESB mælir fyrir um tæknilegar og aðferðarfræðilegar kröfur fyrir **stafræna markaðinn**
- Samráð sumarið 2024 – 154 umsagnir
- Unnið úr niðurstöðum með aðildarríkjum
- Gildistaka er 18. október nk.
- Umræða innan Evrópu um þýðingu gerðanna fyrir aðra markaði

1. POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU)
- 1.1. Policy on the security of network and information systems
- 1.2. Roles, responsibilities and authorities

2. RISK MANAGEMENT POLICY (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)
- 2.1. Risk management framework
- 2.2. Compliance monitoring
- 2.3. Independent review of information and network security

3. INCIDENT HANDLING (ARTICLE 21(2), POINT (B), OF DIRECTIVE (EU) 2022/2555)
- 3.1. Incident handling policy
- 3.2. Monitoring and logging
- 3.3. Event reporting
- 3.4. Event assessment and classification
- 3.5. Incident response
- 3.6. Post-incident reviews

4. BUSINESS CONTINUITY AND CRISIS MANAGEMENT (ARTICLE 21(2), POINT (C), OF DIRECTIVE (EU) 2022/2555)
- 4.1. Business continuity and disaster recovery plans
- 4.2. Backup management
- 4.3. Crisis management

5. SUPPLY CHAIN SECURITY (ARTICLE 21(2), POINT (D), OF DIRECTIVE (EU) 2022/2555)
- 5.1. Supply chain security policy
- 5.2. Directory of suppliers and service providers

6. SECURITY IN NETWORK AND INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE (ARTICLE
- 6.1. Security in acquisition of ICT services or ICT products
- 6.2. Secure development life cycle
- 6.3. Configuration management
- 6.4. Change management, repairs and maintenance
- 6.5. Security testing
- 6.6. Security patch management
- 6.7. Network security
- 6.8. Network segmentation
- 6.9. Protection against malicious and unauthorised software
- 6.10. Vulnerability handling and disclosure

7. POLICIES AND PROCEDURES TO ASSESS THE EFFECTIVENESS OF CYBERSECURITY RISK-MANAGEMENT MEASURES (ARTICLE

8. BASIC CYBER HYGIENE PRACTICES AND SECURITY TRAINING (ARTICLE 21(2), POINT (G), OF DIRECTIVE (EU) 2022/2555)
- 8.1. Awareness raising and basic cyber hygiene practices
- 8.2. Security training

9. CRYPTOGRAPHY (ARTICLE 21(2), POINT (H), OF DIRECTIVE (EU) 2022/2555)

10. HUMAN RESOURCES SECURITY (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)
- 10.1. Human resources security
- 10.2. Background checks
- 10.3. Termination or change of employment procedures
- 10.4. Disciplinary process

11. ACCESS CONTROL (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)
- 11.1. Access control policy
- 11.2. Management of access rights
- 11.3. Privileged accounts and system administration accounts
- 11.4. Administration systems
- 11.5. Identification
- 11.6. Authentication
- 11.7. Multi-factor authentication

12. ASSET MANAGEMENT (ARTICLE 21(2), POINT (I), OF DIRECTIVE (EU) 2022/2555)
- 12.1. Asset classification
- 12.2. Handling of information and assets
- 12.3. Removable media policy
- 12.4. Asset inventory
- 12.5. Return or deletion of assets upon termination of employment

13. ENVIRONMENTAL AND PHYSICAL SECURITY (ARTICLE 21(2), POINTS (C), (E) AND (I) OF DIRECTIVE (EU) 2022/2555)
- 13.1. Supporting utilities
- 13.2. Protection against physical and environmental threats
- 13.3. Perimeter and physical access control

Hvað felst í yfirumsjón með innleiðingu þeirra (2)

Vera leiðtogar netöryggis í sínum rekstri

Stjórnarþátttaka í áhættustýringu

- æðstu stjórnendur þurfa að geta samþykkt niðurstöðu áhættumats með upplýstum hætti

Reglulegar úttektir á stöðu netöryggis

- æðstu stjórnendur þurfa að vita innleiðingarstöðu og þroskastig netöryggis í rekstri sínum

Beint samband við æðstu stjórnendur

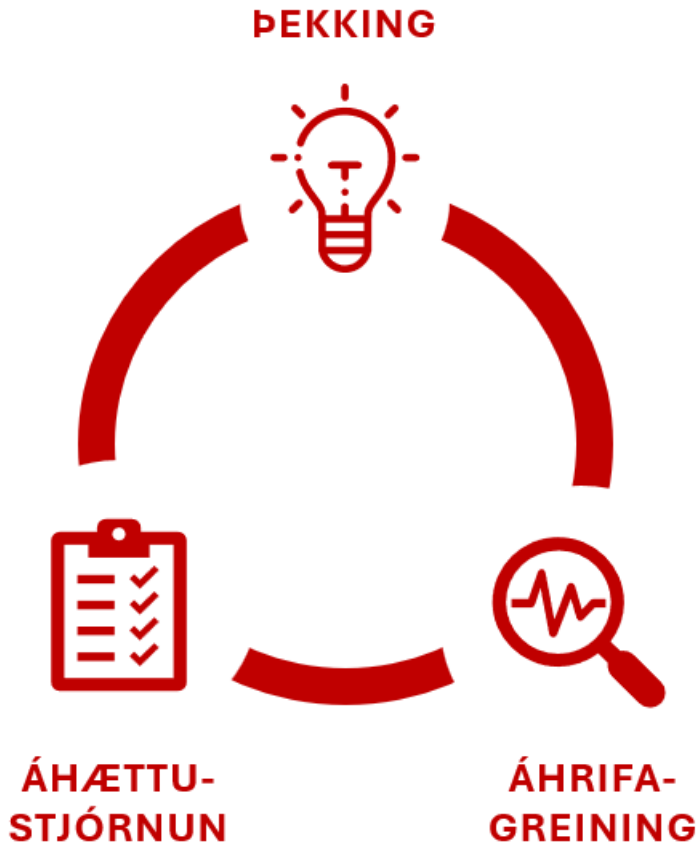
- tryggja þarf að lykistarfsmaður heyri beint undir æðsta stjórnanda og hafi beina skyldu til að tilkynna um öll málefni er varða netöryggi og áhættustýringu

Regluleg endurmat á hlutverkum og ábyrgð

- æðstu stjórnendur þurfa að tryggja viðbrögð við nýjum áskorunum á sviði netöryggis

Hvað felst í þekkingu til að greina áhættu og meta áhættustýringu og vita áhrif á þjónustu? (3)

1. Þekking á netöryggi
2. Skilningur á áhættustýringu
3. Skilningur á áhrifagreiningu



Hvað felst í þekkingu til að greina áhættu og meta áhættustýringu og vita áhrif á þjónustu? (3)

1. Þekking á netöryggi

Regluleg þjálfun í netöryggi til að átta sig á:

- Hverjar eru bestu stjórnunaraðferðir í netöryggi?
- Hvert er landslag netógnana?
- Hver eru áhrif netárása?

Skýrslugjöf um netáhættu svo sem:

- Netárásir, öryggisatvik
- Helstu hættur fyrir fyrirtækið
- Virkni öryggisráðstafana

Hvað felst í að greina áhættu og meta áhættustýringu og vita áhrif á þjónustu? (3)

2. Skilningur á áhættustýringaraðferðum

Taka þátt í áhættumati:

- Hvaða mikilvægu eignir og þjónusta eru viðkvæm?
- Hvar eru til staðar öryggisráðstafanir
- Hvernig draga þær úr ógnum?

Nota mælanlegar netöryggisvísitölur (KPI):

- Fjöldi öryggisatvika sem hafa verið greind og leyst
- Tími sem það tekur að laga veikleika
- Fjölda truflana eða lengd á rofi á þjónustu (endurreisn)

Hvað felst í að greina áhættu og meta áhættustýringu og vita áhrif á þjónustu? (3)

3. Áhrifagreining

Skilja áhrif netöryggisáhættu

- Á þjónustuframboð og rekstraröryggi
- Á getu fyrirtækisins til að ná viðskiptaáætlunum

Ákveða áhættuvilja fyrirtækisins

- Tryggja að fjárfestingar í netöryggi séu í takt við áhættustig
- Horfa þarf til taps á fjármunum, orðspors og langtíma viðskiptahagsmuna

Hvað felst í skorti á hlítingu? (4)

Stjórnsýsluúrræði – stjórnvöld eiga að

- Gefa formlega aðvörun vegna brota
- Gefa bindandi fyrirmæli
- Fyrirskipa aðila að:
  - hætta ólögmætri hegðun
  - tryggja hlítni
  - fullnægja tilkynningarskyldu
  - fylgja tilmælum eftir öryggisúttekt
  - birta upplýsingar um brot á lögum
- Skylda aðila um að upplýsa viðskiptavini um alvarlegar netógnir og mögulegar úrbætur.
- Tilnefna tilsjónarmann til að uppfylla kröfur
- Leggja á sektir sem geta numið:
  - 1,4% af veltu eða EUR 7M fyrir mikilvæga aðila
  - 2% af veltu eða EUR 10M fyrir nauðsynlega aðila

Fellt tímabundið niður starfsleyfi, vottun eða skráningu aðila

Bannað einstaklingi tímabundið að gegna stjórnunarstöðu eða lagalegu fyrirsvari fyrir aðila

Hvað felst í skorti á hlítingu? (4)

Refsiviðurlög

- Tilskipunin kveður á um skyldu aðildarríkja um að innleiða refsingar vegna skorts á hlítingu við kröfur tilskipunarinnar
- Þær skulu vera áhrifaríkar, hafa varnaðaáhrif og byggðar á meðlhófi

Í dag er kveðið á um refsingar í netöryggislögum:

- Brot á lágmarkskröfum um áhættustýringu
- Brot á tilkynningarskyldu
- Brot á þagnarskyldu

Viðurlög geta varðað:

- allt að tveggja ára fangelsi
- fésektum á lögaðila, skv. alm. hegningarlögum
- Hlutdeild í broti er refsiverð skv. alm. hegningarlögum
- Rangar tilkynningar til CERT-IS varða alm. hegningarlög

…sem sagt

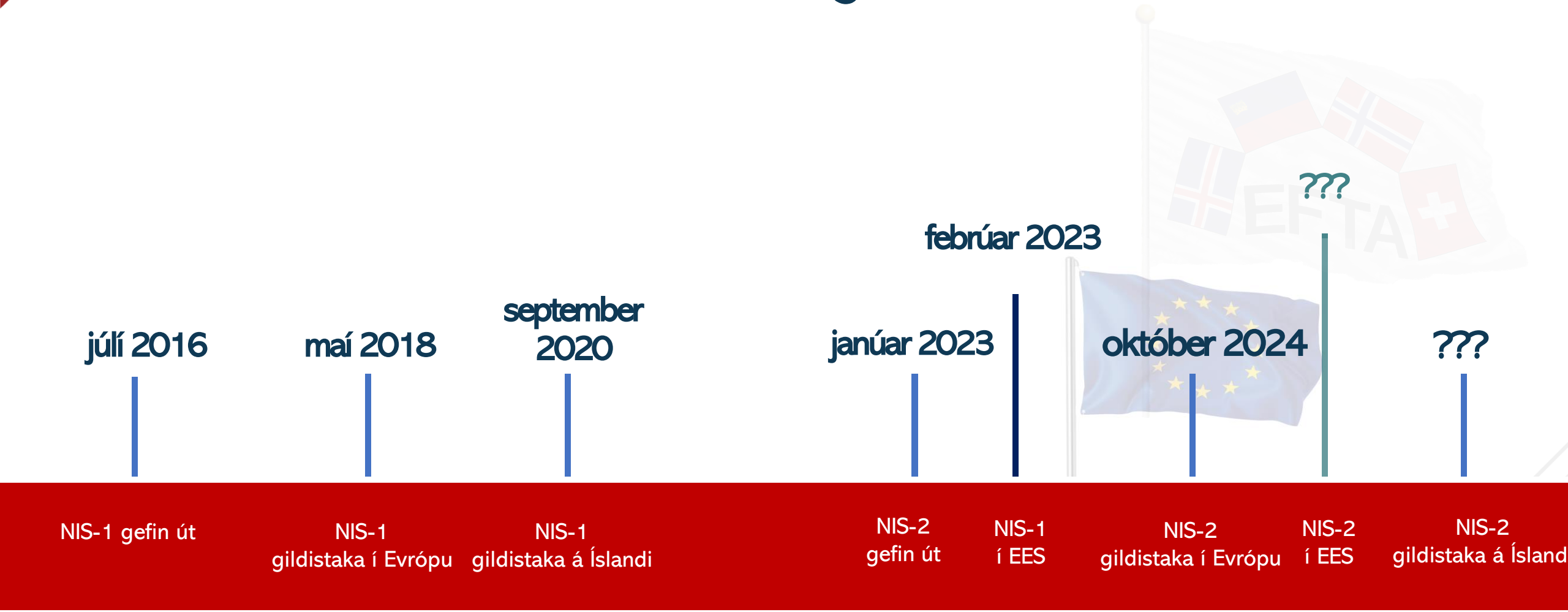
Æðstu stjórnendur skulu:

- ✓ samþykkja ráðstafanir til áhættustýringar netöryggis
- ✓ hafa yfirumsjón með innleiðingu þeirra
- ✓ hafa þekkingu og getu til að greina áhættu og meta áhættustýringu netöryggis og áhrif þeirra á þjónustu fyrirtækisins
- ✓ bera ábyrgð á skorti á hlítingu

Innleiðing NIS-2

Fjarskiptastofa

Það er kominn tími til að undirbúa sig…



Þannig hvað næst?

Setjið netöryggi í forgang í skipuriti

Við hvetjum ykkur til að hefa sem fyrst greiningu á ykkar stöðu

Hefjið innleiðingu á stjórnkerfi net- og upplýsingaöryggi

Vottanir? –Mjög góð byrjun!

Fjarskiptastofa