Netöryggistilskipun ESB

Unnur Kristín Sveinbjarnardóttir
sviðsstjóri stafræns öryggis
unnur@fjarskiptastofa.is

Fjarskiptastofa

Örstutt um mig…

Í grunninn lögfræðingur með LLM gráðu í Evrópurétti frá Edinborgarháskóla,
fjarskipta- og fjölmiðlarétt frá Florence School of Regulation,
PLC gráðu í opinberri stefnumótun og leiðtogahæfni frá Harvard háskóla

Starfað hjá Fjarskiptastofu nú í yfir áratug á sviði netöryggis og tæknimála.
Leitt starf við gerð laga á sviði netöryggis, framkvæmd áhættumata
á fjarskiptainnviðum og sértækum ógnum

Starfar í dag sem sviðsstjóri stafræns öryggis þar sem teymið leiðir uppbyggingu á eftirliti með netöryggi mikilvægra innviða hér á landi

NIS-2
á 25 mínútum

Samhengi hlutanna

Netöryggistilskipun

- Hvað felst í NIS-2?
- Hvaða aðilar falla undir NIS-2?
- Hvað þurfa þeir að gera?
- Hvað ef ekkert er gert?

Innleiðing á Íslandi

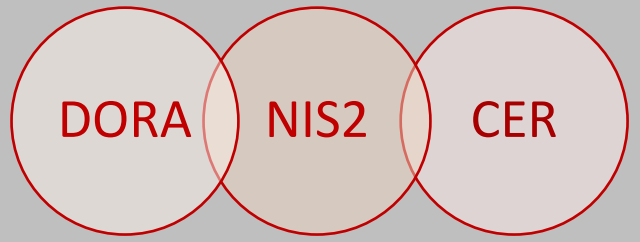
Vegverð innan Evrópu

<u>Stafræn þróun ESB er eitt af forgangsmálum sambandsins</u>

ESB gaf út netöryggisstefnu sambandsins í desember 2020

Markmið er m.a. að:

- auka styrk sambandsins og aðildarríkja til að tryggja stafrænt sjálfstæði álfunnar (e. digital sovereignty)
- efla áfallaþol (resilience) Evrópu gegn netógnum og tryggja að allir borgarar og fyrirtæki geti notið góðs af traustri og áreiðanlegri stafrænni þjónustu



NIS-2 tilskipun Evrópusambandsins

- Tilskipun nr. 2022/2555. Í desember 2022 samþykkti ESB nýja netöryggistilskipun, NIS-2 - tekur gildi 18. október 2024

- Fellir úr gildi fyrri tilskipun, NIS-1 frá 2016 sem var efnislega innleidd á Íslandi 2020

- Þessar breytingar hafa áhrif á alla þá sem starfa við upplýsingatækni með einum eða öðrum hætti

Hvað felst í NIS-2?

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, vegis 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, fjarkipti, traustþjónustur)
- Geimstarfsemi
- Upplýsinga- og fjarskiptatækni
- Opinberar stofnanir

(nýtt í NIS-2)

2 MIKILVÆGIR AÐILAR

- Póst og sendingarþjónusta
- Úrgangsstjórnun
- Efni / Lyf (framleiðsla og dreifing efna)
- Matvæli (framleiðsla, vinnsla og dreifing)
- Veitendur stafrænnar þjónustu (leitarvélar, netmarkaðir, miðlar)
- Rannsóknastarfsemi

(nýtt í NIS-2)

ANNEX I

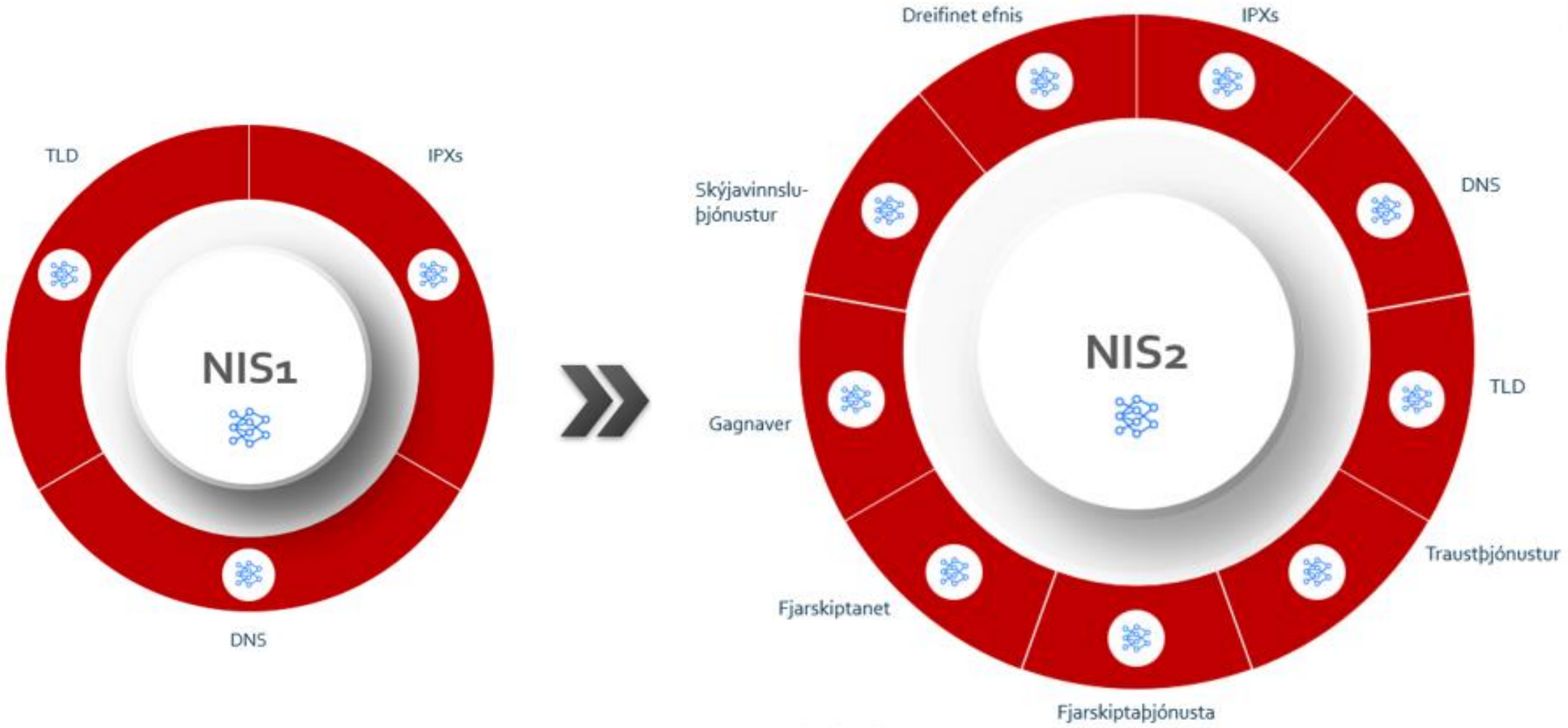
SECTORS OF HIGH CRITICALITY

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in Article 2, point (57), of Directive (EU) 2019/944 of the European Parliament and of the Council ([1]), which carry out the function of 'supply' as defined in Article 2, point (12), of that Directive
		— Distribution system operators as defined in Article 2, point (29), of Directive (EU) 2019/944
		— Transmission system operators as defined in Article 2, point (35), of Directive (EU) 2019/944
		— Producers as defined in Article 2, point (38), of Directive (EU) 2019/944
		— Nominated electricity market operators as defined in Article 2, point (8), of Regulation (EU) 2019/943 of the European Parliament and of the Council ([2]) — Market participants as defined in Article 2, point (25), of Regulation (EU) 2019/943 providing aggregation, demand response or energy storage services as defined in Article 2, points (18), (20) and (59), of Directive (EU) 2019/944 — Operators of a recharging point that are responsible for the management and operation of a recharging point, which provides a recharging service to end users, including in the name and on behalf of a mobility service provider
	(b) District heating and cooling	— Operators of district heating or district cooling as defined in Article 2, point (19), of Directive (EU) 2018/2001 of the European Parliament and of the Council ([3])
	(c) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
		— Central stockholding entities as defined in Article 2, point (f), of Council Directive 2009/119/EC ([4])

ANNEX II

OTHER CRITICAL SECTORS

Sector	Subsector	Type of entity
1. Postal and courier services		Postal service providers as defined in Article 2, point (1a), of Directive 97/67/EC, including providers of courier services
2. Waste management		Undertakings carrying out waste management as defined in Article 3, point (9), of Directive 2008/98/EC of the European Parliament and of the Council ([1]), excluding undertakings for whom waste management is not their principal economic activity



Stafræn grunnvirki fara út þremur tegundum þjónustu í níu tegundir

Telur þú þig falla þarna undir?

- ✓ 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
  - ✓ EUR 10 m í ársveltu/efnahag
- ✓ Ef þau eru ekki uppfyllt þarf í þriðja lagi að athuga hvort að þjónustan falli undir önnur skilyrði óháð stærðarmörkum.
  - Aðilinn er leiðandi í þjónustunni 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 gæti 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.

Hvaða kröfur er verið að setja?

Kröfur um áhættustýringu netöryggis

- Grunnkrafa um **virkt stjórnkerfi net- og upplýsingaöryggis**

- Nær til rekstraröryggis 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

- Þannig að **leynd, réttleiki** og **tiltækileiki** upplýsinga/kerfa sé tryggður og þar með þjónusta þeirra

- Byggja þarf á alþjóðlegum viðurkendum stöðlum um bestu framkvæmd

Hvaða lágmarkskröfur er verið að setja?

Innleiðingargerð væntanleg frá farmkvæmdastjórn ESB í október 2024

- Stefnur um áhættumat og net- og upplýsingakerfi.
- Atvikameðhöndlun.
- Rekstrarsamfellu, endurreisnaráætlun og hættustjórn.
- Öryggi net- og upplýsingakerfa m.t.t. innleiðingu kerfa, þróun og viðhalda, 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.

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

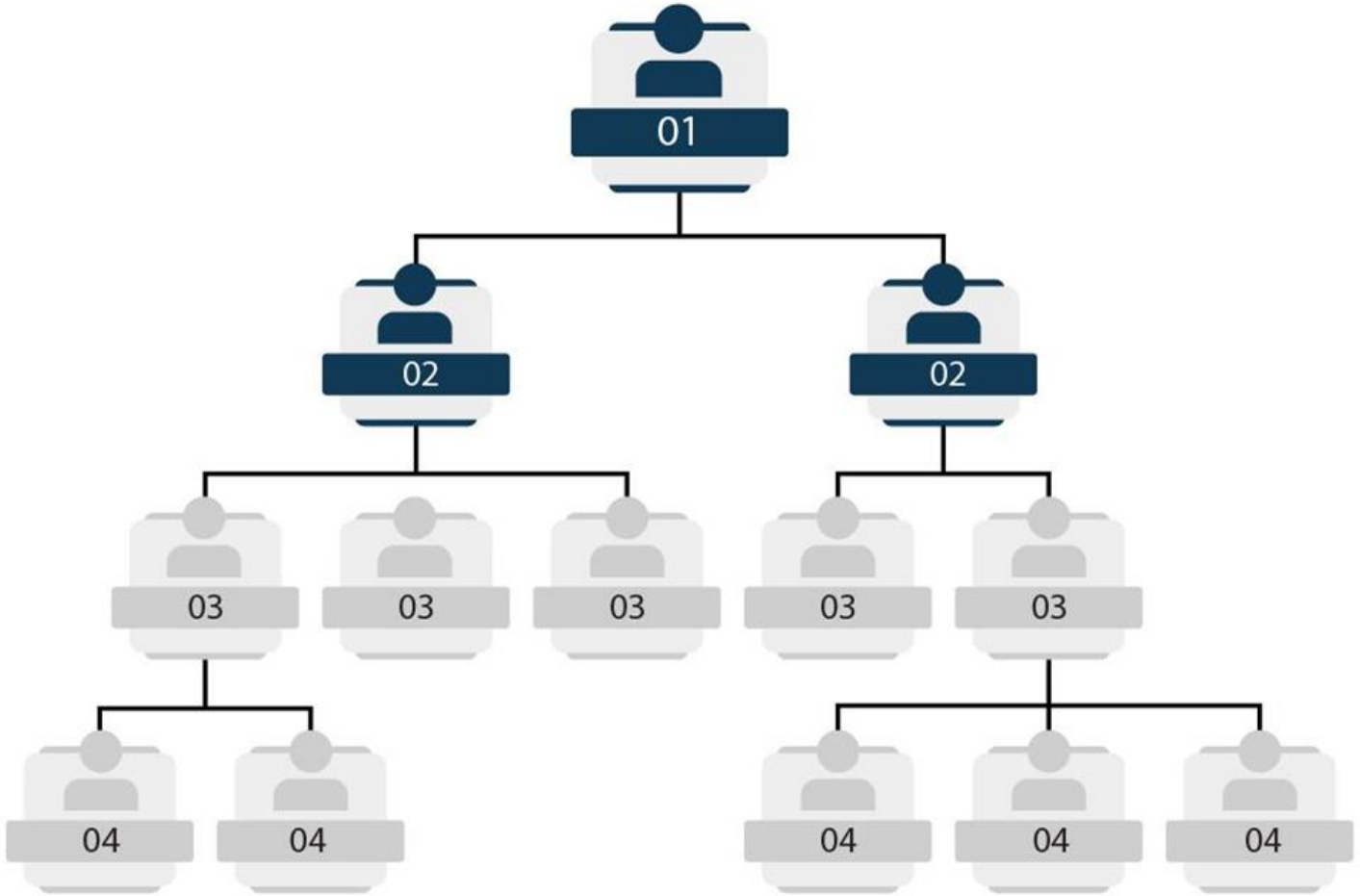
13. ENVIRONMENTAL AND PHYSICAL SECURITY (ARTICLE 21(2), POINTS (C), (E) AND (I) OF DIRECTIVE (EU) 2022/2555)
- 13.1. Supporting utilities
- 13.2. Protection against physical and environmental threats
- 13.3. Perimeter and physical access control

Æðstu stjórnendur bera nú ábyrgðina!

Ábyrgð æðstu stjórnenda

Æðstu stjórnendur skulu staðfesta stjórnkerfi net- og upplýsingaöryggis, hafa yfirsýn yfir innleiðingu þess og bera ábyrgð á skorti á hlítingu

Æðstu stjórnendur skulu hljóta þjálfun og hafa þekkingu og getu til að meta áhættuþætti og stjórnkerfi net- og upplýsinga öryggis í fyrirtæki sínu



Eftirlit

“supervision and enforcement”

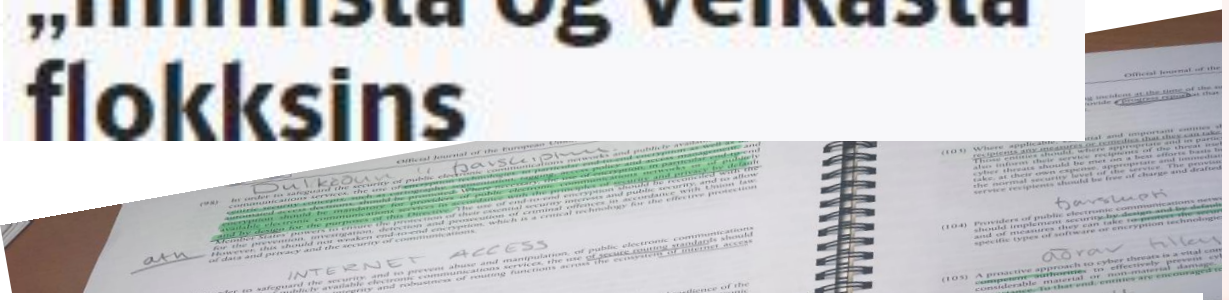
Ef ekkert er gert - hvað þá?

Ítarleg ákvæði um eftirlit

- Rík krafa um **áhættumiðað** leiðbeinandi eftirlit
  - Úttektir og öryggisprófanir
  - Tímasett fyrirmæli um úrbætur
- Viðurlög **ef fyrirmælum er ekki fylgt** eða **frávik eru alvarleg**
  - Álagning sekta
  - afturköllun starfsleyfa
  - tímabundin brottvikning æðstu stjórnanda
- Ákveðinn greinarmunur á eftirliti og viðurlögum milli nauðsynlegra aðila og mikilvægra aðila

Það er kominn tími til að undirbúa sig...

Ríkisstjórnin á valdi „minnsta og veikasta“ flokksins



Fréttir

Bjarni: „Mér fannst þetta vera mjög óskýr ályktun“

Innlent | Morgunblaðið | 9.10.2024 | 6:00

Útilokað að réttlæta samstarf

Stjórnmál

Þótt flokki „líði illa í innyflunum“ verður hann að sýna ábyrgð

Spurningar?