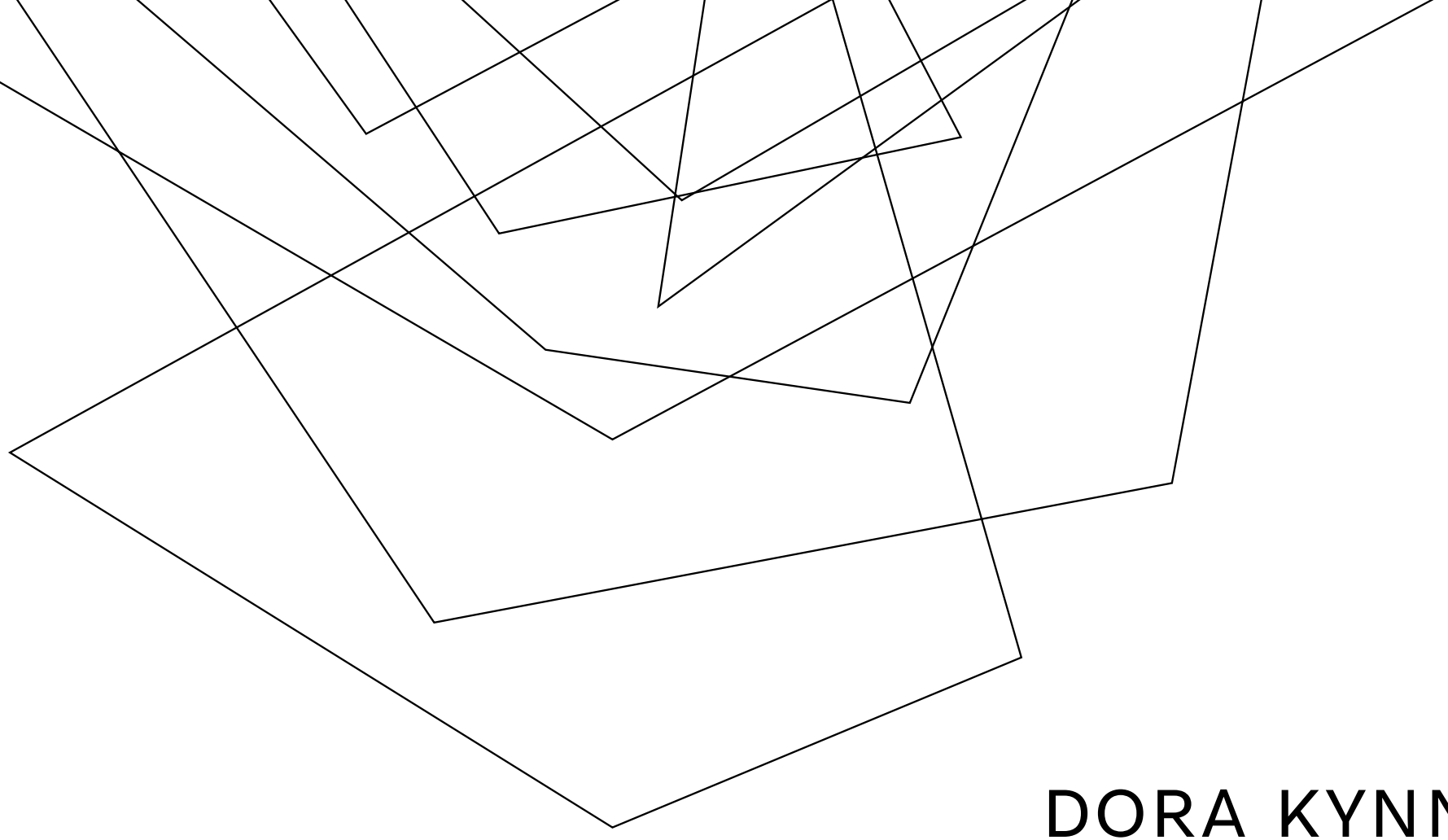


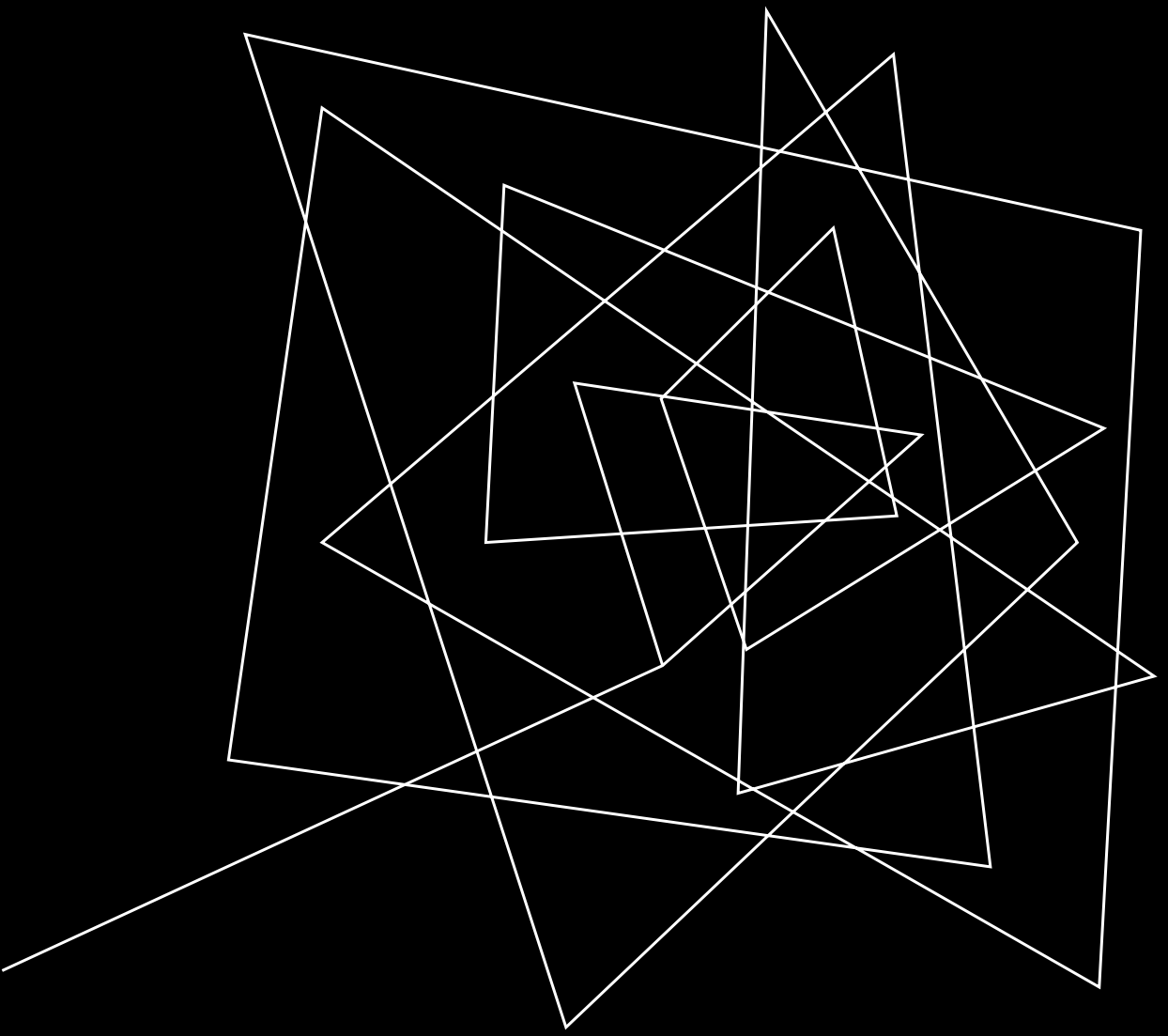
DORA KYNNING

Marinó G. Njálsson, Harpan ehf.
oryggi@internet.is

UM DORA

Setur fram heildstæðar kröfur um **stafrænan rekstrarlegan viðnámsþrótt** fyrir fjármálageirann með áherslu á áhættustjórnun, atvikastjórnun, prófanir, birgjakeðjuna og upplýsingagjöf til eftirlitsaðila

Innleiðing á reglugerð (EU) 2022/2554 og tilskipun (EU) 2022/2556 sem tóku gildi innan ESB 17. janúar 2025.



ÁSKORANIR

ÁSKORANIR SKIPULAGSHEILDA

Kröfur koma úr ólíkum áttum og hafa mismunandi vægi

Hvaðan koma kröfur:

- Öryggisstefna (og aðrar stefnur).
- Áhættumat.
- Lög, reglugerðir, stjórnvaldsfyrirmæli.
- Staðlar og öryggisfyrirmæli.

NÝLEG STARFSAUGLÝSING FRÁ FJÁRMÁLAFYRIRTÆKI

Menntunar- og hæfniskröfur

- Háskólapróf sem nýtist í starfi, t.d. á sviði upplýsingatækni, tölvunarfræði, hugbúnaðar-verkfræði, viðskiptafræði eða tengdra greina.
- Að lágmarki 5 ára reynsla af störfum á sviði upplýsingaöryggis.
- Reynsla af upplýsingaöryggisstjórnkerfum og/eða öðrum stjórnkerfum (t.d. ISO 27001).
- Þekking á lögum og regluverki á sviði net- og upplýsingaöryggis (t.d. DORA) er kostur.
- Drifkraftur, skipulagshæfni, sjálfstæð vinnubrögð og frumkvæði.
- Góð samskiptafærni og reynsla af teymisvinnu.
- Gott vald á íslensku og ensku, bæði í ræðu og riti.
- Þekking á lífeyris- eða fjármálamarkaði er kostur.

Helstu verkefni og ábyrgð

- Gegnir stöðu öryggisstjóra XXX.
- Hefur umsjón með stjórnkerfi upplýsingaöryggis og þróun þess.
- Leiðir viðnáms- og öryggisprófanir og samræmingar-verkefni.
- Sér um viðhald og eftirfylgni endurreisnar-, neyðar- og viðbragðsáætlana.
- Hefur umsjón með úttektaráætlunum og stýrir vinnu við úrlausn öryggisatvika.
- Sér um samskipti við Fjármálaeftirlit vegna upplýsingaöryggismála.
- Hefur umsjón með innri og ytri úttektum tengdum upplýsingaöryggi.
- Fylgist með ytra regluverki upplýsingaöryggis og stuðlar að því að sjóðurinn starfi í samræmi við það.
- Sinnir öðrum verkefnum innan áhættustýringar sem tengjast upplýsingatækni, s.s. greiningu og áhættumati.

ÞRÍSKIPTING FERLISINS

STJÓRNUN (E. GOVERNANCE)

Laga þarf innleiðingu að markmiðum skipulagsheildarinnar

ÖRYGGIS- OG ÁHÆTTUSTJÓRNUN

Bera kennsl á, meta og meðhöndla áhættu – Viðfangsefnið hér.

HLÍTING (E. COMPLIANCE)

Greina, innleiða og tryggja hlítingu við kröfur laga, reglugerða og samninga

ALMENNT VERKLAG

Forvinna

Tryggja að kröfur séu tilgreindar.

Bera kennsl á ógnir og veilur

Ákvarða stigmögnun út frá áhættu.

Tengja við þekktar leiðbeiningar.

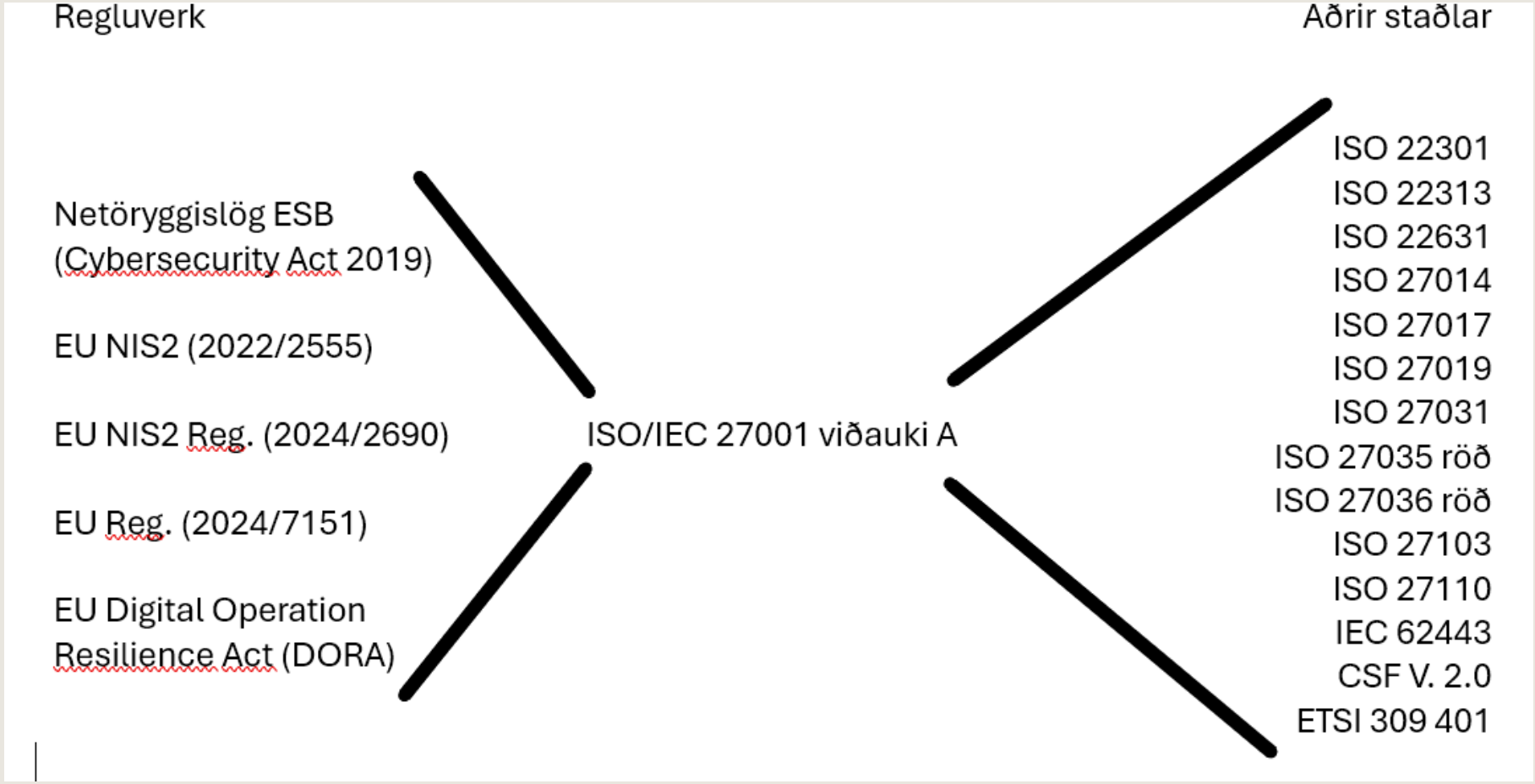
Innleiðing

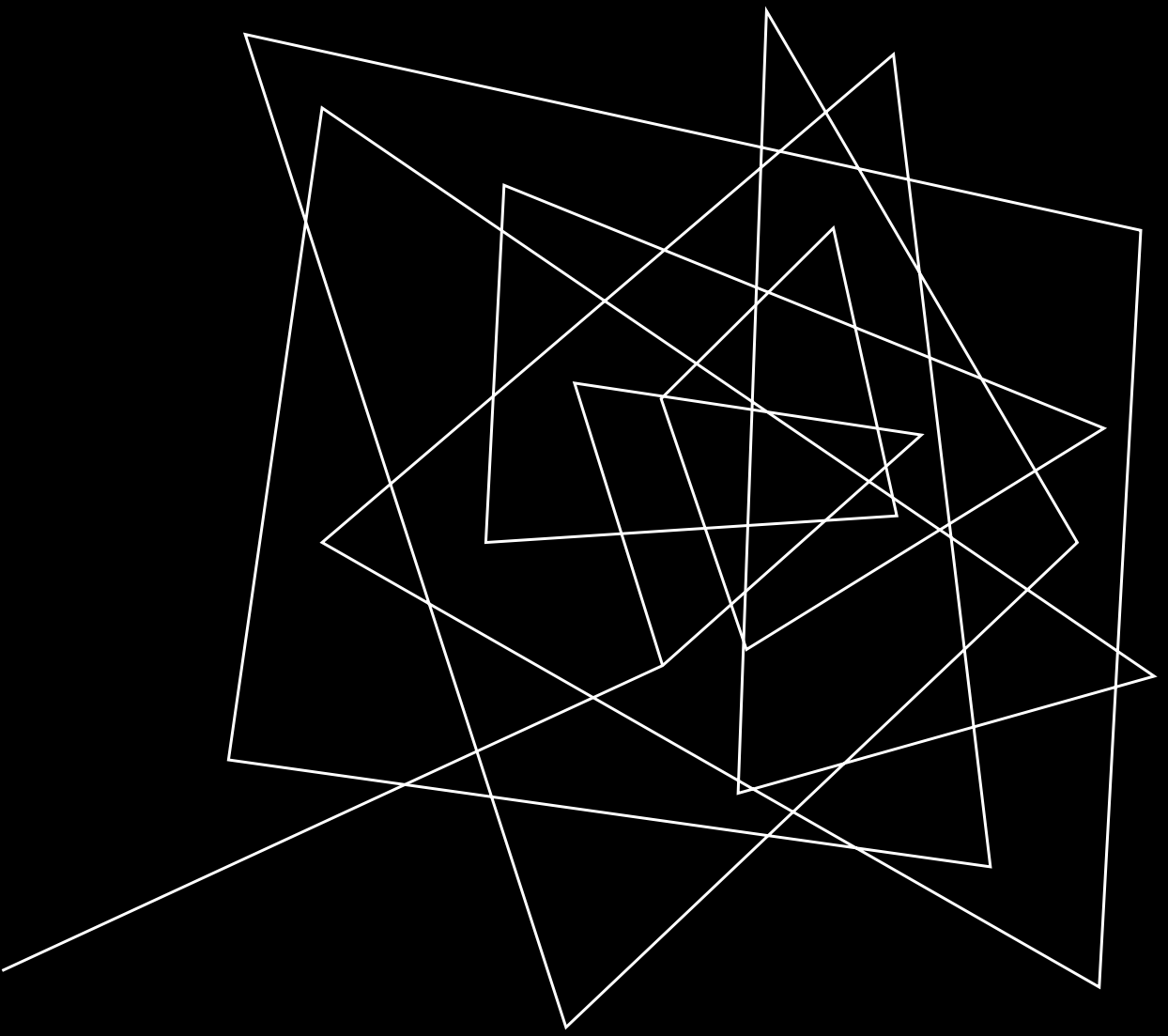
- Velja úrræði.
- Draga úr áhættu.
- Uppfylla kröfur sem best er hægt.
- Skjalfesta niðurstöður.
- Hrinda í framkvæmd.
- Skjalfesta yfirlýsingu um nothæfi.

Úttektir

- Skoða varpanir milli krafna og niðurstaðna.
- Staðfesta virkni úrræða.
- Kanna stöðu yfirlýsingar um nothæfi.
- Bera kennsl á göt.

FLÆKJAN


Regluverk
Netöryggislög ESB (Cybersecurity Act 2019)
EU NIS2 (2022/2555)
EU NIS2 Reg. (2024/2690)
EU Reg. (2024/7151)
EU Digital Operation Resilience Act (DORA)
ISO/IEC 27001 viðauki A
Aðrir staðlar
ISO 22301
ISO 22313
ISO 22631
ISO 27014
ISO 27017
ISO 27019
ISO 27031
ISO 27035 röð
ISO 27036 röð
ISO 27103
ISO 27110
IEC 62443
CSF V. 2.0
ETSI 309 401



BREYTINGAR Á REGLUM

FYRRI RÉTTARFARSREGLUR

NIS 1

Fyrri netöryggislöggjöf ESB sem fjármálafyrirtæki féllu undir, en ekki tryggingafélög.

VIÐMIÐUNARREGLUR ESB

Fjármálaeftirlitið hefur gegn um tíðina gefið út leiðbeinandi tilmæli og viðmiðunarreglur byggðar á reglugerðum ESB, m.a. leiðbeinandi tilmæli FME nr. 1/2019 vegna áhættu við rekstur upplýsingakerfa eftirlitsskyldra aðila og nr. 1/2026 um útvistun.

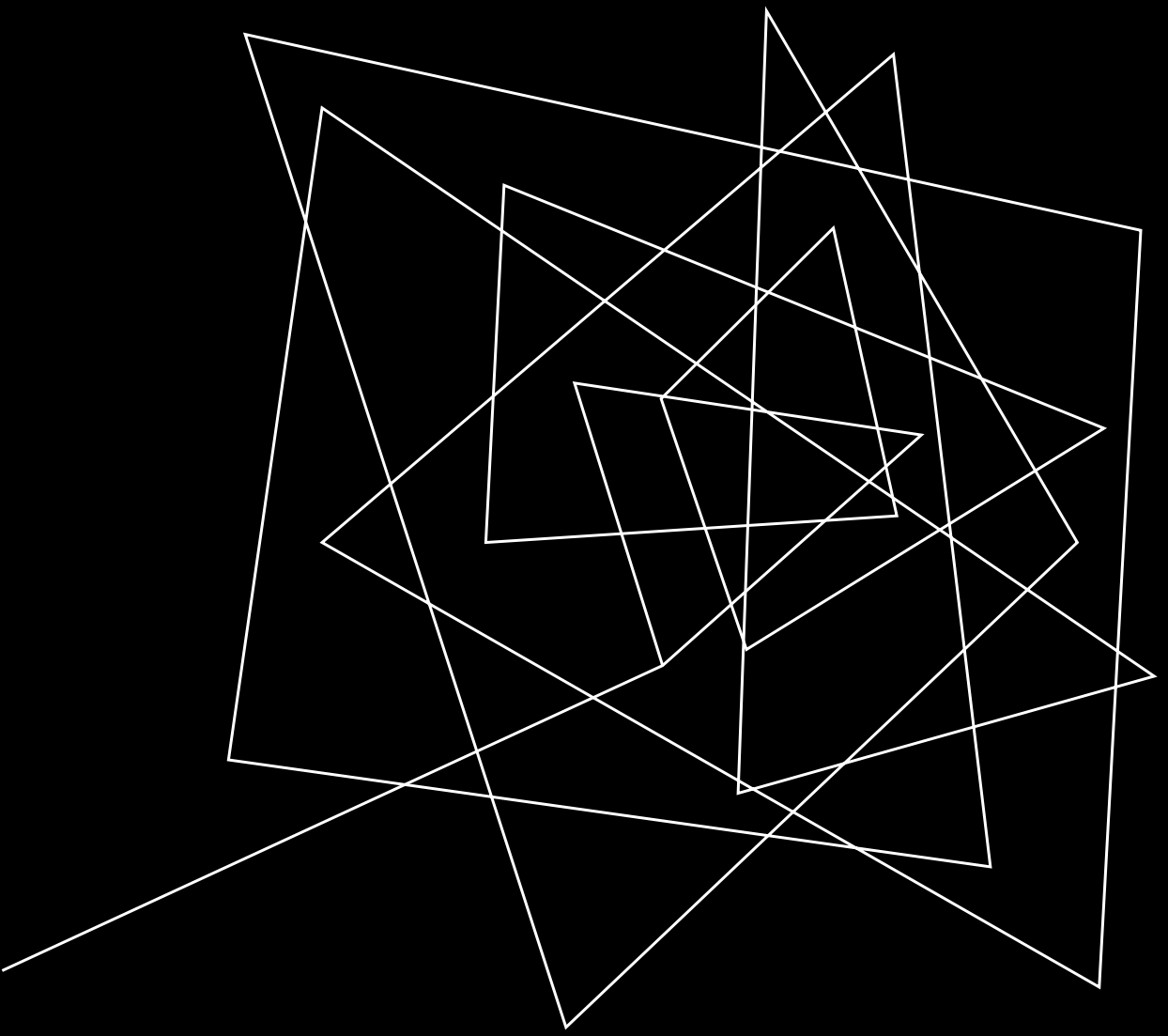
NÝJAR RÉTTARFARSREGLUR

DORA (ESB) 2022/2554 OG 2022/2556

Reglugerð og tilskipun um stafrænt viðnámsþrótt á fjármálamarkaði. Þeim fylgja sjö reglugerðir, auk þess að hafa áhrif til breytingar á mjög mörgum.

REGLUGERÐIR SEM BREYTAST

- (ESB) 1060/2009,
- (ESB) 648/2012,
- (ESB) 600/2014,
- (ESB) 909/2014 og
- (ESB) 2016/1011



UMFJÖLLUNAREFNI

MEGIN EFNISÞÆTTIR

ÁBYRGÐ STJÓRNAR — Stjórnir aðila fá auknar skyldur í DORA og þurfa að vera betur vakandi varðandi fjölmörg efni – gr. 5

ÁHÆTTUSTJÓRNUN — Ábyrgð á stýringu upplýsinga- og fjarskiptaáhættu aðila á fjármálamarkaði – gr. 6 - 16

ATVIKASTJÓRNUN — Koma á ferli við atvikastjórnun, flokkun atvika og tilkynningum til viðeigandi aðila, þ.m.t. stjórnar – gr. 17 - 19

VIÐNÁMSÞRÓTTUR — Skipuleggja og viðhafa reglulega ógnamiðaðar árásarprófanir á viðnámsþrótt aðila og prófanir á viðbragðsáætlunum – gr. 24 - 27

BIRGJAKEÐJA — Stjórnun á áhættu vegna þriðju aðila tengdum upplýsinga- og fjarskiptatækni, þ.m.t. val, samningar, áhættustjórnun og undirverktakar – gr. 28 - 31

ÁBYRGÐ STJÓRNAR

Áhersla er lögð á það lykilhlutverk og endanlega ábyrgð stjórnar og/eða framkvæmdastjórnar aðila á fjármálamarkaði að tryggja framfylgni við kröfur DORA

SKYLDUR STJÓRNAR (DÆMI)

Gr. 5.2 reglugerðar

Stjórn aðila á fjármálamarkaði skal skilgreina, samþykkja, hafa umsjón með og bera ábyrgð á framkvæmd allra ráðstafana sem tengjast áhættustýringarramma fyrir upplýsinga- og fjarskiptatækni sem um getur í 1. mgr. 6. gr.

ISO 27001: 5.1, A 5.4

SKYLDUR STJÓRNAR (DÆMI)

Gr. 5.2 reglugerðar

a) **bera endanlega ábyrgð á stýringu upplýsinga- og fjarskiptatækniáhættu aðila á fjármálamarkaði,**

b) **koma á stefnum**

c) **fastsetja skýr hlutverk og ábyrgðarsvið**

...

ISO 27001: 5.1, 5.2, 7.5, A 5.1, A 5.2, A 5.4

Til viðbótar úr ISO 27001 vegna gr. 5:

6.1.2, 7.1, 7.2, 7.3, 8.1, 8.2, 9.2, 9.3, A 5.19, A 5.22, A 5.23, A 5.24, A 5.29, A 5.30, A 5.35, A 5.36, A 6.3, A 8.14,

ÁHÆTTUSTJÓRNUN

Til staðar skal vera áhættustýringarrammi í upplýsinga- og fjarskiptatækni.

ÁHÆTTU-STJÓRNUN

Gr. 6 - 16 reglugerðar

..hafa **traustan, yfirgripsmikinn** og vel skjalfestan **áhættustýringarramma**...til að bregðast við upplýsinga- og fjarskiptatækniáhættu og **tryggja hátt stig stafræns rekstrarlegs viðnámsþróttar.**

Ítarlegri lýsingar eru síðan í greininni. Kröfur um ráðstafanir eru síðan í næstu 10 greinum á eftir.

ISO 27001: 5.1, 5.2, 5.3, 6.1, 7.4, 7.5, 8.1, 8.2, A 5.1, A 5.2, A 5.3, A 5.4, A 5.5, A 5.37 og fjölmargar aðrar greinar og stýringar.

ISO 27005; ISO 31000; ENISA; CIS; NIST RMF..

ÁHÆTTU-STJÓRNUN

Gr. 6 reglugerðar

Áhættustjórnun

Örfyrirtæki: Einfalt fyrirkomulag áhættustjórnunar

Litlir aðilar: Fylgja leiðbeiningum í grein 6 í ISO 27001

Millistórir aðilar: Fylgja leiðbeiningum í ISO 31000 til viðbótar við ISO 27001

Stórir aðilar: Innleiða aðferðafræði í ISO 27005, ENISA Risk management Standards, NIST Risk Management Framework

HELSTU ATRIÐI

- Vel skilgreind eignaskrá með upplýsinga- og fjarskiptatæknieignum (e. assets)
- Bera kennsl á ógnir og veilur (e. vulnerabilities) í rekstrarumhverfi og fylgjast með breytingum
- Skilgreina hvað telst ásættanleg áhætta og stigmögnun umfram það
- Skilgreina mælikvarða, t.d. fyrir líkindi, umfang, mikilvægi..
- Áhættumeðferð þarf að taka mið af stigvaxandi áhrifum af ógnum og veilum
- Áhættumeðferð getur verið að viðhalda eða draga úr áhættu, færa hana til, forðast eða samþykkja.

GR. 7 – 16 REGLUGERÐAR

Gr. 7: Upplýsinga- og fjarskiptatækni, samskiptareglur og búnaður

Gr. 8: Auðkenning

Gr. 9: Verndun og forvarnir

Gr. 10: Greining (Skynjun)

Gr. 11: Viðbrögð og endurreisn

Gr. 12: ..öryggisafritun..endurheimt..endureisn

Gr. 13: Lærdómur og þróun

Gr. 14: Samskipti

Gr. 15: á ekki við fyrirtæki

Gr. 16: Einfaldað áhættumat

ATVIKASTJÓRNUN

Til staðar skal vera ferli atvikastjórnunar í tengslum við upplýsinga- og fjarskiptatækni.

ATVIKA-STJÓRNUN

Gr. 17 - 19 reglugerðar

..koma á og innleiða atvikastjórnunarferli...til að greina, meðhöndla og tilkynna um atvik..

..samþætta vöktun, meðhöndlun og eftirfylgni..

..flokka atvik...eftir fjölda sem verða fyrir áhrifum, tímalengd, dreifingu, gagnatapi, mikilvægi kerfa..

Tilkynna um atvik

ISO 27001: 6.1.2, 7.4, A 5.2, A 5.5, A 5.7, A 5.24-5.28, A 8.8.

ISO 27035 röðin; NIST CSF, IEC 62443-2..

ATVIKA-
STJÓRNUN

Gr. 17 - 19 reglugerðar

Atvikastjórnun

Örfyrirtæki: Einfalt fyrirkomulag tilkynninga og viðbragða

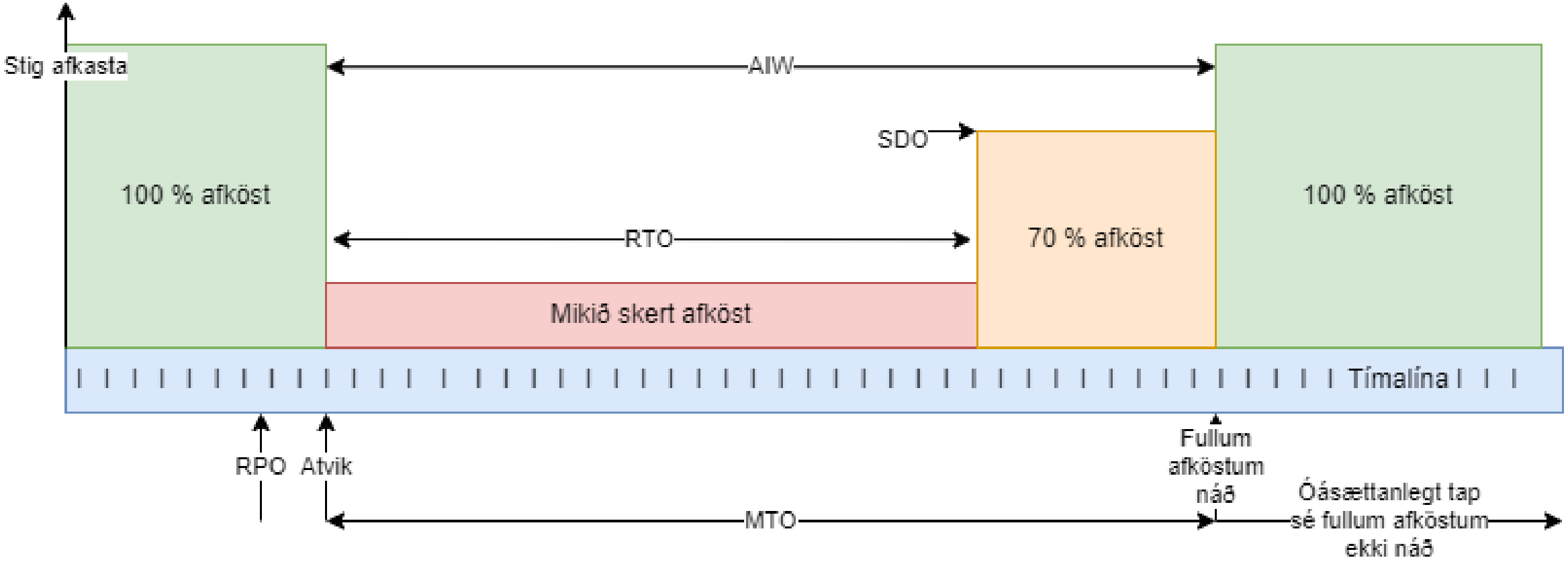
Litlir aðilar: Fylgja leiðbeiningum í stýringum 5.24 – 5.28 í ISO 27002

Millistórir aðilar: Bæta við leiðbeiningum i ISO 27035 hluta 1

Stórir aðilar: Innleiða aðferðafræði í ISO 27035 röðinni, NIST CSF 2.0 og/eða IEC 62443-2

HELSTU ATRIÐI

- Undirbúningur og skipulagning
- Hvernig staðið er að skynjun atvika eða tilkynningu þeirra
- Flokkun og ákvörðunartaka ((EU) 2024/1772)
- Viðbrögð, þ.m.t. ná stjórn, hefta útbreiðslu og stigmögnun
- Möguleg endurreisn
- Læra af atvikum
- Tilkynning til eftirlitsaðila
- Uppfærsla áhættugrunns


Stig afkasta
100 % afköst
AIW
SDO
RTO
70 % afköst
100 % afköst
Mikið skert afköst
Tímalína
RPO
Atvik
Fullum afköstum náð
MTO
Óásættanlegt tap sé fullum afköstum ekki náð

VIÐNÁMSÞRÓTTUR

Framkvæma þarf prófanir til að meta starfrænt rekstrarlegt viðnámsþrótt fyrirtækja á fjármálamarkaði.

VIÐNÁMS-ÞRÓTTUR

Gr. 24 – 27 reglugerðar

..til að greina veikleika, annmarka og gloppur í starfrænum rekstrarlegum viðnámsþrótti...**skulu aðilar útbúa prófunaráætlanir og framkvæma prófanir.**

ISO 27001: 6.1.2, 7.1, 7.2, 7.4, 9.2, 10.1, 10.2, A 5.3, A 5.5, A 5.19-5.23, A 5.26, A 5.30, A 5.35, A 5.36, A 8.8, A 8.19, A 8.25, A 8.29, A 8.31, A 8.33

TIBER-EU, TIBER-IS, eba Operational Resilience

HELSTU ATRIÐI

- Setja upp prófunaráætlanir
- Skilgreina umfang og aðferðir
- Skilja hverjar ógnirnar eru
- Finna prófunaraðila sem er hæfur
- Framkvæma ógnamiðuðu árásarprófunina
- Rýna skýrslu til að meta hvort bregðast þurfi við einhverju og þá hvernig.

STJÓRNUN ÞRIÐJU AÐILA

Aðferðir skulu vera til staðar, til að stýra áhættu vegna þriðju aðila (oftast þjónustuveitenda)

STJÓRNUN ÞRIÐJU AÐILA

Gr. 28 - 31 reglugerðar

..skulu **stýra** upplýsinga- og samskiptatækniáhættu vegna **þriðju aðila**...í ljósi **meginreglu um meðalhóf**..

Skoða skal samþöppunaráhættu..vera með **samningsbundið fyrirkomulag**..

ISO 27001: 6.1, 7.4, 8.2, 8.3, A 5.1, A 5.5, A 5.9, A 5.19, A 5.20, A 5.21, A 5.22, A 5.23, A 5.31, A 5.34, A 8.32

ISO 27036 röðin; NIST CSF 2.0, ISO 27017

STJÓRNUN ÞRIÐJU AÐILA

Gr. 28 – 31 reglugerðar

Stjórnun þriðju aðila

Örfyrirtæki: Einfalt fyrirkomulag

Litlir aðilar: Fylgja leiðbeiningum í stýringum A 5.19 til A 5.23 í ISO 27002

Millistórir aðilar: Bæta við leiðbeiningum í ISO 27036 hluta 1 og 2.

Stórir aðilar: Innleiða ISO 27036 staðlaröðina og/eða fylgja NIST CSF 2.0

HELSTU ATRIÐI

- Reglur um val á þjónustuaðila
- Þarfagreining
- Öryggiskröfugreining
- Skjalfestir samningar við alla stærri aðila (erfitt að gera það við minni)
- Ekkert ætti að kaupa nema með samþykki
- Skoða þarf: gagnavernd, hvar hugbúnaður er keyrður, fylgir keðja þriðju aðila
- Vöktun, heimild til úttektar
- Krafa um árásarprófun
- Riftun samnings

TIL VIÐBÓTAR

- **Framfylgni krafna**: Verkefni sem áður voru á ábyrgð öryggisstjóra eru núna hjá bæði stjórnarmönnum og framkvæmdastjóra/forstjóra.
- **Sérstakar heimildir:** Er á ábyrgð stjórnar að veita, þegar ráðstafanir eru óvenjulegar eða mikils háttar.
- **Vitund**: Mælt er með þekkingu á grunnatriðum upplýsinga- og netöryggis til viðbótar við kröfum DORA.
- **Vöktun**: Í (EU) 2022/2554 er vísað til vöktunar vegna áhættustýringa fyrir upplýsinga- og fjarskiptatækni, vegna notkunar mikilvægra þriðju aðila og vegna eftirfylgni atvika.
- **Netöryggi**: Viðbótarkrafa sem er utan DORA. Um alla Evrópu er netöryggisvitund orðin mjög mikilvæg. Þá er verið að vísa til getu til að greina svikapóst, verjast óværum í niðurhlöðnum skjölum, notkun öruggrar (fjölþátta) auðkenningar, vernda leynilegar auðkenningarupplýsingar, o.s.frv.

TILLÖGUR UM ÞJÁLFUNAREFNI

Governance and Risk Management

1. Management responsibilities
2. Risk management framework
3. Risk assessments
4. (Internal) ICT audit

Operational Management

5. Asset management
6. Change management
7. ICT operations

Continuity Management

8. Backup management
9. Response & recovery

Incident Management

10. Incident classification
11. Incident management

Software and Systems Development

12. Acquisition, development, and maintenance
13. Project management

Third-party Risk Management

14. Third-party due diligence and selection
15. Third-party (standard) contract management
16. Third-party (critical) contract management
17. Third-party risk management
18. Subcontracting management

Resilience Testing

19. Digital operation resilience testing
20. Threat-led penetration testing

Security Management

21. Architectural and network security
22. Security monitoring & log management
23. Data and (legacy) system security
24. Encryption and cryptography
25. Identity and access management
26. Physical and environmental security
27. Security awareness
28. Vulnerability and patch management

TAKK FYRIR

Marinó G. Njálsson

Harpan ehf.

898-6019

oryggi@internet.is