

SEÐLABANKI ÍSLANDS

Sitthvað um DORA

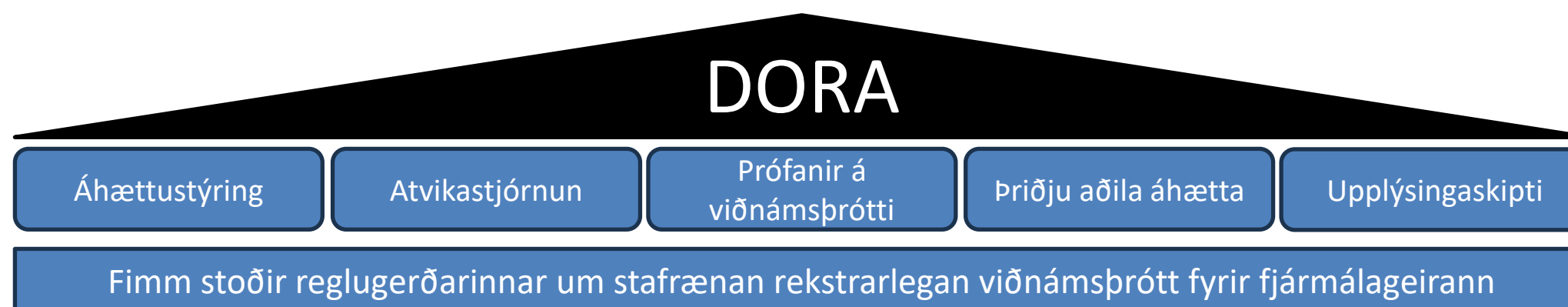


12.02.2026

TN-FMP

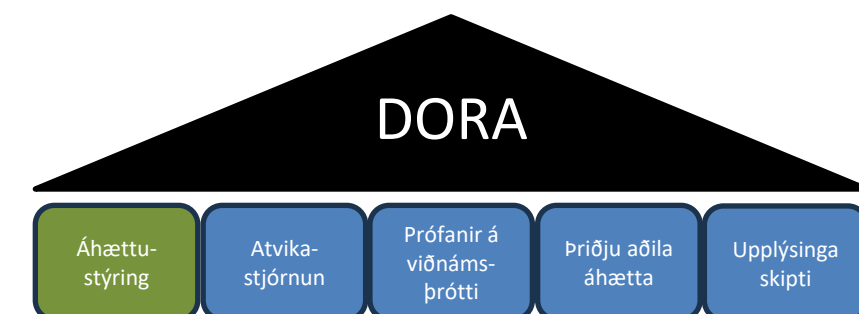
DORA – Digital Operational Resilience Act

- Reglugerð (ESB) 2022/2554 um stafrænan viðnámsþrótt fjármálamarkaðar
- DORA kom til framkvæmda innan ESB í 17. janúar 2025
- Samþykkt á Alþingi 12. nóvember 2025 og kom til framkvæmdar 1. janúar 2026
- Markmið DORA er að styrkja viðnámsþrótt aðila á fjármálamarkaði gagnvart meiri háttar rekstraratvikum
- DORA nær þvert til aðila á fjármálamarkaði, t.d. banka, sparisjóða, verðbréfafyrirtækja, og tryggingafélaga
- DORA nær til lífeyrissjóða með breytingum á lögum um lífeyrissjóði
- DORA er útfærð þannig að hún taki tillit til stærð aðila til viðbótar við hlutfallsreglu (4. gr.)



Stoð 1 - Áhættustýring

- Áhættustýring undir DORA mætti greina niður í fimm þætti
 - Að hafa öflugt stjórnskipulag og góða stjórnarhætti
 - Að vita hvað það er sem þarf að vernda
 - Að geta greint þegar atvik eru að raungerast
 - Að geta brugðist rétt við atvikum
 - Að læra, þroskast og upplýsa



Stoð 1 - Áhættustýring

Öflugt stjórnskipulag og góðir stjórnarhættir

5. grein

Stjórnunarhættir og skipulag

Áhersla á ábyrgð stjórnar við umsjón og framkvæmd ráðstafana sem tengjast áhættustýringarramma

Skipa þarf tiltekið hlutverk sem fylgist með **útvistun til þjónustuaðila UFT**

Stjórn skal **viðhalda þekkingu og færni** til að skilja og meta UFT áhættu og áhrif hennar á starfseminni

6. grein

Áhættustýringarrammi í UFT

Hafa traustan, yfirgripsmikinn og vel skjalfestan **áhættustýringarramma** fyrir UFT sem a.m.k. nær yfir stefnuáætlanir, stefnur, verklagsreglur, o.fl. sem þarf til að vernda UFT eignir

Regluleg endurskoðun á áhættustýringarrammanum skal framkvæmd af endurskoðanda og skal endurskoðandinn búa yfir **nægilegri þekkingu, hæfni og sérþekkingu** varðandi UFT áhættu

Ramminn skal innihalda **stefnuáætlun um stafrænan rekstrarlegan viðnámsþrótt** þar sem fram kemur hvernig hann skal innleiddur

7. grein

UFT kerfi, samskiptareglur og búnaður

Aðilar skulu nota og halda **uppfærðum UFT kerfum** sem eru viðeigandi, áreiðanleg, með nægilegra getu til að vinna rétt út gögnum og **geta ráðið við umfram álagi**

DORA

Áhættu-
stýring

Atvika-
stjórnun

Prófanir á
viðnáms-
þrótti

Þriðju aðila
áhætta

Upplýsinga
skipti

Stoð 1 - Áhættustýring

Vita hvað það er sem þarf að vernda

8. grein Auðkenning

Greina, flokka og skjalfesta

- alla starfspætti, hlutverk og ábyrgðarsvið sem UFT styður við
- upplýsingaeignir og UFT eignir sem styðja við þessa starfspætti og hlutverk
- hæði í tengslum við UFT áhættu

Endurskoða eftir þörfum og a.m.k. árlega hvort **flokkunin** og hvers kyns viðeigandi gögn séu fullnægjandi

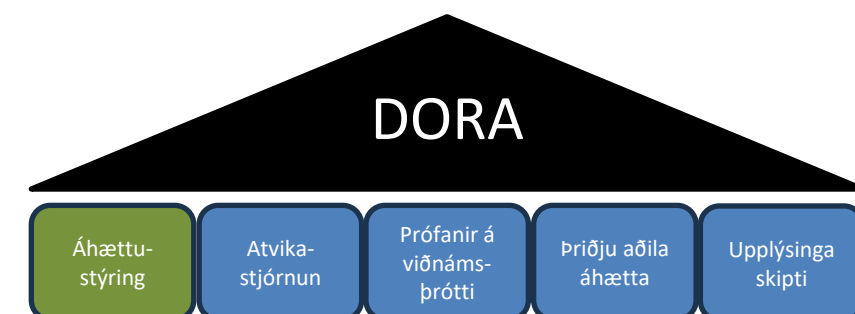
Bera skal kennsl á **uppsprettur UFT áhættu**, meta netógnir og veikleikar og endurmeta árlega áhættusviðsmyndir sem hafa áhrif á félagið

Gera skal **áhættumöt** á öllum stórfelldum breytingum á innviðum net- og upplýsingakerfa, í ferlum eða verklagsreglum

Tilgreina allar upplýsingaeignir og UFT eignir, netbúnað og vélbúnað og **kortleggja þau sem teljast mikilvæg**

Kortleggja samskipan upplýsingaeignanna og UFT eignanna, og tengsl og innbyrðis hæði milli mismunandi upplýsingaeigna og UFT eigna

Greina og skjalfesta öll ferli sem eru **háð þriðju aðilum** sem veita UFT þjónustu og **greina samtengingar við þriðju aðila** sem veita UFT þjónustu sem styður nauðsynlega eða mikilvæga starfsemi



Stoð 1 - Áhættustýring

Greina þegar atvik eru að raungerast

9. grein Verndun og forvarnir

Stöðugt vakta og hafa eftirlit með öryggi og virkni UFT kerfa og -búnaðar og lágmarka áhrif UFT áhættu

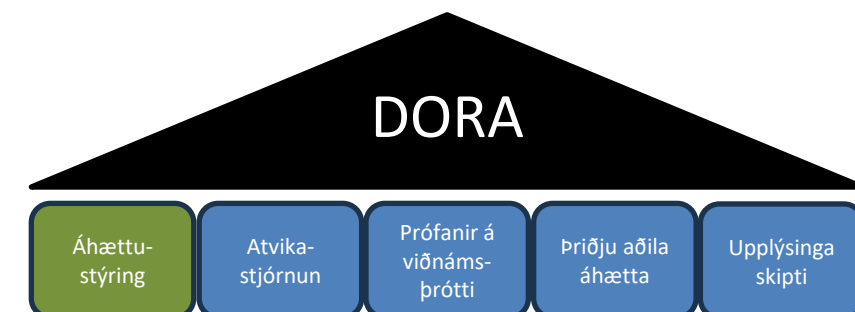
Tryggja viðnámsprótt, samfellu og aðgengileika UFT kerfa, einkum þeirra sem styðja við nauðsynlega eða mikilvæga starfsemi

- Öryggi gagnaflutningsleiða
- Lágmarka hættu á spillingu eða tapi á gögnum, óheimilum aðgangi og tæknilegum annmörkum sem geta hindrað starfsemi
- Koma í veg fyrir skerðingu á tiltækileika, áreiðanleika, ósvikni og réttleika, brot á leynd og tap á gögnum
- Tryggja að gögn séu varin fyrir áhættu sem stafar af gagnastjórnun, þ.m.t. ófullnægjandi stjórnsýslu, áhættu í tengslum við vinnslu og mannlegum mistökum

10. grein Greining

Hafa kerfi til að greina atvik án tafar, þ.m.t. vandamál sem varða afköst tölvuneta og atvik sem tengjast UFT

Kerfið skal leyfa marglaga stýringar, skilgreina viðvörunarmörk og viðmiðanir til að virkja og hefja viðbragðsferli við atvikum sem tengjast UFT, þ.m.t. **sjálfvirk viðvörunarkerfi** fyrir viðeigandi starfsfólk sem ber ábyrgð á viðbrögðum við atvikum sem tengjast UFT



Stoð 1 - Áhættustýring

Bregðist rétt við atvikum



11. grein

Viðbrögð og endurreisn

Setja fram **heildstæða stefnu um rekstrarsamfellu** í UFT sem sértæka stefnu sem myndar órjúfanlegan þátt og er óaðskiljanlegur hluti af heildarstefnu um rekstrarsamfellu

Innleiða viðeigandi **viðbragðs- og endurreisnaráætlanir í UFT** sem lúta **úttektum**

Prófa reglulega áætlanir um rekstrarsamfellu

Gera rekstraráhrifagreiningu m.t.t. útsetningar gagnvart meiriháttar rekstrarröskunum

Hafa krísustjórnunarteymi sem, ef áætlanir eru virkjaðar, skal m.a. setja fram skýrar verklagsreglur til að stjórna krísusamskiptum innan og utan fyrirtækis

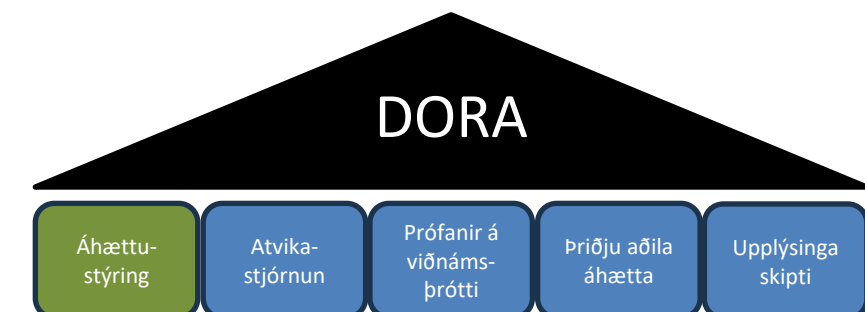
12. grein

Stefnur og verklag við öryggisafritun, verklag og aðferðir við endurheimt og endurreisn

Útfæra og skjalfesta:

- **stefnur og verklag um öryggisafritun** sem tilgreina umfang gagnanna sem falla undir öryggisafritun og lágmarkstíðni öryggisafritunar sem byggist á mikilvægi upplýsinga eða trúnaðarstigi gagna
- verklag og aðferðir við **endurheimt og endurreisn**

Við endurreisn skal **framkvæma nauðsynlegar athuganir** til að tryggja áfram hæsta stig heilleika gagna



Stoð 1 - Áhættustýring

Læra, þroskast og upplýsa



13. grein Lærdómur og þróun

Hafa yfir að ráða **getu og starfsfólki** til að **safna upplýsingum** um **veikleika og netógnir**, atvik sem tengjast UFT, einkum netárásir, og greina líkleg áhrif þeirra á stafrænan rekstrarlegan viðnámsprótt

Koma á **greiningarferli** fyrir atvik í kjölfar þess að alvarlegt atvik raskar kjarnastarfsemi þeirra, **greina orsakir raskana** og bera kennsl á nauðsynlegar úrbætur

Lærdómur sem dreginn er af prófunum og raunverulegum atvikum **skal nýttur og stjórn upplýst**

Kortleggja þróun UFT áhættu til lengri tíma, greina tíðni, tegundir, umfang og þróun atvika, einkum netárásir og mynstur þeirra

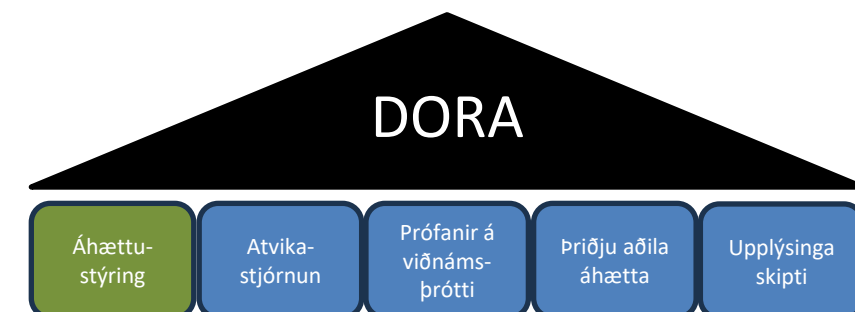
Þróa áætlanir um öryggisvitund í UFT og þjálfun í stafrænum rekstrarlegum viðnámsprótti sem **skyldubundinn** hluta af þjálfunaráætlunum sínum fyrir starfsfólk

Vakta viðeigandi tæknilega framþróun með viðvarandi hætti, einnig með það í huga að skilja hugsanleg áhrif af nýtingu slíkrar nýrrar tækni á öryggiskröfur

14. grein Samskipti

Hafa **krísusamskiptaáætlanir** sem gera kleift að **upplýsa** viðskiptavini og mótaðila, sem og almenning, á ábyrgan hátt um a.m.k. alvarleg atvik eða veikleika

Að minnsta kosti einum einstaklingi skal falið að **innleiða samskiptaáætlun** vegna atvika sem tengjast UFT og sinna því hlutverki að **upplýsa almenning og fjölmiðla** í þeim tilgangi



Stoð 1 - Áhættustýring

Einfaldaður áhættustýringarrammi



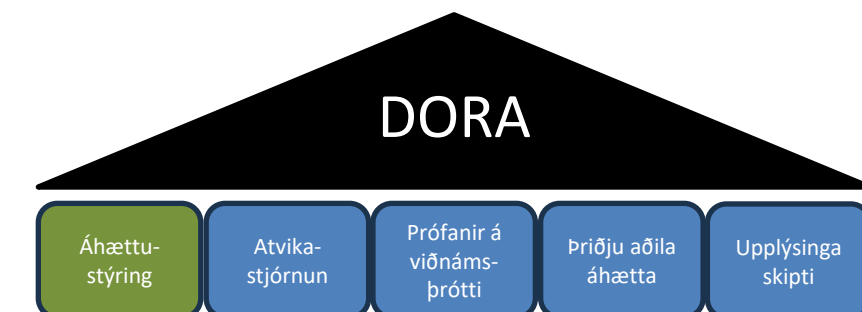
16. grein

Einfaldaður áhættustýringarrammi fyrir upplýsinga- og fjarskiptatækni

Tilteknir smærri aðilar á fjármálamarkaði eru undanskildir ákvæðum 5.-15. gr. DORA en í staðinn þurfa þeir að uppfylla kröfur um einfaldaðan áhættustýringarramma skv. 16. gr.

- Lítil og ótengd verðbréfafyrirtæki
- Greiðslustofnanir sem eru undanþegnar samkvæmt tilskipun (ESB) 2015/2366
- Stofnanir sem eru undanþegnar samkvæmt tilskipun 2013/36/ESB
- Rafeyrisfyrirtæki sem eru undanþegin samkvæmt tilskipun 2009/110/EB
- Litlar stofnanir um starfstengdan lífeyri

Ekki er búist við að mörg félög á Íslandi muni falla undir þessa grein



Stoð 2 - Atvikastjórnun

17. grein

Atvikastjórnunarferli sem tengist UFT og skipulag

Skilgreina, koma á og innleiða **atvikastjórnunarferli**

- **Snemmbæra viðvörðunarávísá**
- Verklagsreglur til að **bera kennsl á**, rekja, skrá, flokka og draga í dilka atvik og um viðbrögð við atvikum
- Tilkynningar til framkvæmdastjórnar og **stjórnar**

Skrá skal öll atvik sem tengjast upplýsinga- og fjarskiptatækni og verulegar netógnir

18. grein

Flokkun á atvikum sem tengjast UFT og netógnum

Flokka skal atvik eftir **skilgreindum viðmiðunum** sem tilgreind eru í reglugerðinni

Flokkun á netógnum m.t.t. mikilvægis þeirra þjónustna sem eru í hættu

19. grein

Tilkynningar um alvarleg atvik og valfrjálst um verulegar netógnir

Tilkynna skal um **alvarleg atvik** sem tengjast UFT til fjármálaeftirlitsins og að eigin frumkvæði tilkynna um **verulegar netógnir**

Tilkynningar um alvarleg atvik verða á svipuðu formi og tilkynningar sem aðilar senda inn vegna laga um greiðsluþjónustu eða leiðbeinandi tilmæla 1/2019

Hvað varðar aðila sem falla undir lög nr. 78/2019 (netöryggislög) þá munu tilkynningar um alvarleg atvik (frávik) með DORA aðeins tilkynnast til fjármálaeftirlitsins og ekki til CERT-IS.

Fjármálaeftirlitið sér um að áframsenda tilkynningar til CERT-IS

DORA

Áhættu-
stýring

Atvika-
stjórnun

Prófanir á
viðnáms-
þrótti

Þriðju aðila
áhætta

Upplýsinga
skipti

Stoð 3 – Prófanir á viðnámsþrótti

Almennar prófanir

24. grein

Almennar kröfur um framkvæmd prófunar á stafrænum rekstrarlegum viðnámsþrótti

Koma á, viðhalda og endurskoða trausta **og alhliða prófunaráætlun** um stafrænan rekstrarlegan viðnámsþrótt

Fylgja **áhættumiðaðri nálgun**

Tryggja að **óháðir aðilar framkvæmi prófanir**, hvort sem það eru innri eða ytri aðilar

Setja sér verklagsreglur og stefnur til að **forgangsraða, flokka og ráða bót á vandamálum** og koma á **innri staðfestingaraðferð**

25. grein

Prófun á UFT búnaði og kerfum

Prófunaráætlunin þarf að kveða á um framkvæmd viðeigandi prófana, s.s.

- mat og skönnun á veikleikum
- greiningu á opnum hugbúnaði
- mat á öryggi netkerfis
- greiningu á gloppum
- úttektir á **raunlægu öryggi**
- spurningalista og skönnunarhugbúnaðarlausnir
- **úttektir á frumkóta**, þar sem mögulegt er
- **sviðsmyndatengdar** prófanir
- Samhæfisprófanir
- prófanir á frammistöðu
- prófanir enda á milli (e. end to end)
- **innbrotsprófanir**

DORA

Áhættu-
stýring

Atvika-
stjórnun

Prófanir á
viðnáms-
þrótti

Þriðju aðila
áhætta

Upplýsinga
skipti

Stoð 3 – Prófanir á viðnámsþrótti

Auknar prófanir (TLPT)

26. grein

Auknar prófanir á UFT-búnaði, -kerfum og -ferlum sem byggjast á ógnamiðaðri innbrotsprófun

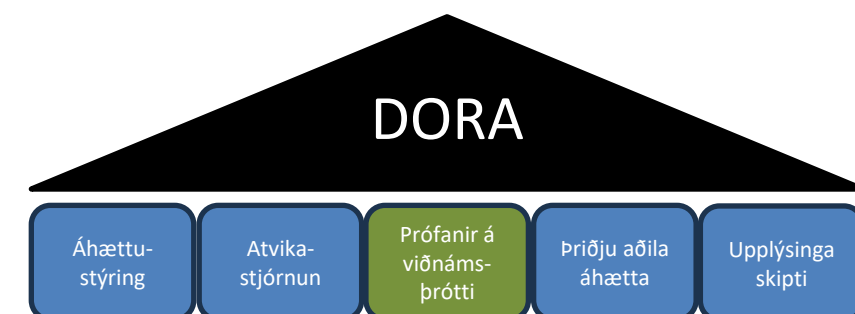
27. grein

Kröfur fyrir prófunaraðila til að framkvæma ógnamiðaða innbrotsprófun

Seðlabankinn ákveður hvaða aðilar á fjármálamarkaði, aðrir en þeir sem teljast smáir, skuli framkvæma aukna prófun. Til dæmis kerfislega mikilvægir bankir sem hafa nægilega mikinn UFT þroska.

Framkvæma aukna prófun með ógnamiðaðri innbrotsprófun á a.m.k. þriggja ára fresti

Styðst við TIBER-IS



Stoð 4 – UFT áhætta vegna 3ja aðila

28. grein Almennar meginreglur

Stýring UFT áhættu vegna þriðju aðila skal fara fram í ljósi meginreglu um meðalhóf, m.t.t.

- Eðlis, umfangs, flækjustigs og **mikilvægis hæðis** sem tengist UFT
- **Áhættu** sem leiðir af samningum um UFT þjónustu, að teknu tilliti til þess m.a. hversu **nauðsynleg eða mikilvæg** viðkomandi þjónusta er

Aðilar **bera áfram fulla ábyrgð** á því að uppfylla og standa við allar skuldbindingar og skulu hafa **útgönguáætlun**

Aðeins heimilt að gera samning við þriðju aðila sem veita UFT þjónustu sem **fylgja viðeigandi stöðlum um upplýsingaöryggi**

Árlegar skýrslur til fjármálaeftirlitsins (Registry of Information)

29. grein Bráðabirgðamat á samþjöppunar- áhættu í UFT á einingastigi

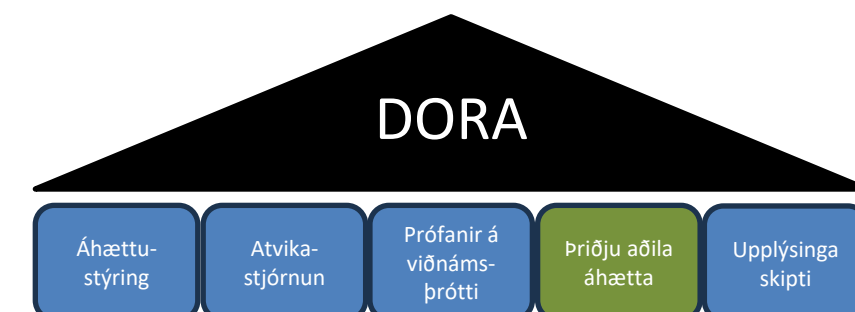
Greining og mat á áhættu skal **taka tillit til** þess hvort útvistun á UFT þjónustu sem styður við **nauðsynlega eða mikilvæga starfsemi** myndi leiða til

- samnings við þriðja aðila sem er **ekki auðvelt að skipta út**
- **verulegs fjöldi samninga hjá sama þriðja aðila**

30. grein Helstu samningsákvæði

Samningur í heild skal **fela í sér samkomulag um þjónustustig** og skjalfestur í **einu skriflegu skjali** sem skal vera aðilunum aðgengilegt á pappír eða í skjali á öðru niðurhalanlegu, **varanlegu og aðgengilegu sniði**

Miklar **kröfur til innihalds samninga**



Stoð 4 – UFT áhætta vegna 3ja aðila

Eftirlitsrammi mikilvægra þriðju aðila

31. grein

Tilnefning mikilvægra þriðju aðila sem veita UFT þjónustu

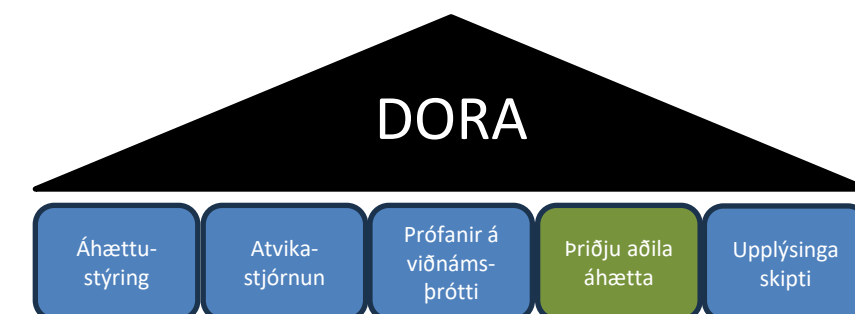
Evrópsku eftirlitsstofnanirnar (EBA, ESMA og EIOPA) útnefna mikilvæga þriðju aðila sem veita UFT þjónustu í kjölfar mats

Útnefningin byggir á viðmiðum eins og kerfislægum áhrifum á stöðugleika og kerfiseiginleikum eða mikilvægi aðila sem reiða sig á þriðja aðilann

Mikilvægir þjónustuaðilar verða undir eftirliti aðaleftirlitsaðila (e. Lead overseer)

Litlar sem engar líkur á að íslenskur aðili verði útnefndur sem mikilvægur þjónustuaðili

Þetta fyrirkomulag dregur úr þörf aðila til að hafa eftirlit með þjónustuaðilum sem eru mjög stórir og mikilvægir innan Evrópu, eins Microsoft, Amazon og Oracle.



Stoð 5 - Upplýsingaskipti

45. grein

Fyrirkomulag upplýsingaskipta vegna upplýsinga og greiningargagna um netógnir

Til að **einfalda upplýsingamiðlun** milli aðila á fjármálamarkaði

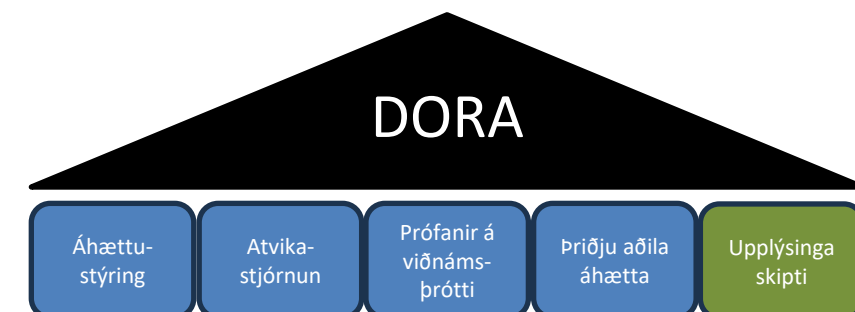
Heimilt að skiptast á upplýsingum og greiningargögnum um netógnir, úrræði, aðferðir og verklagsreglur, netöryggisviðvaranir og samskipunarúrræðitól

- miða að því að **efla stafrænan rekstrarlegan viðnámsprótt** aðila á fjármálamarkaði
- eiga sér stað á **traustum sameiginlegum vettvangi**
- er framkvæmd með **fyrirkomulagi til upplýsingaskipta** sem verndar hugsanlega viðkvæmt eðli þeirra

Í fyrirkomulagi upplýsingaskipta skal skilgreina **skilyrði fyrir þátttöku**

Aðilar sem taka þátt í slíkum vettvangi skulu tilkynna fjármálaeftirlit Seðlabanka Íslands um það

Um er að ræða valkvæð upplýsingaskipti



Takk fyrir