FIN-FSA
FINANSSIVALVONTA

DORA-kyselytilaisuus 6.9.2024

Euroopan parlamentin ja neuvoston asetus digitaalisesta häiriönsietokyvystä (Digital Operational Resilience Act - DORA)

Yleistä

- Olemme saaneet DORA:an liittyen kysymyksiä, joihin olemme vastanneet kysyjille suoraan. Kysymyksiä, usein samojakin, on tullut siinä määrin, että järjestimme tämän tilaisuuden, johon pyysimme etukäteen kysymyksiä. Aiemmin saamamme, tässä tilaisuudessa esitetyt ja jatkossa saamamme kysymykset vastauksineen tullaan julkaisemaan Finanssivalvonnan verkkosivuilla.
- Osa kysymyksistä on sellaisia, että vastaus on DORA-lakitekstissä tai RTS/ITS-dokumenteissa. Näihin pyydämme katsomaan vastauksen sieltä.
- On mahdollista, että Finanssivalvonnan tulkinta joihinkin kysymyksiin liittyen on väärä
  - Jos tällaisia ilmenee, niin korjaamme vastauksen verkkosivuille
- Kysymyksien perusteella ei ole laadittu esitystä, joka vastaisi kaikkiin kysymyksiin, vaan kaikki kysymykset käydään läpi aihealueittain
  - Joitakin aihealueita taustoitetaan lyhyesti
- Tilaisuuden aikana jatkokysymyksille ja uusille kysymyksille on käytössä Teams-chat
  - Jos emme ehdi tai osaa vastata näihin kysymyksiin tilaisuuden aikana, niin vastaukset julkaistaan Finanssivalvonnan verkkosivulla

Euroopan parlamentin ja neuvoston asetus digitaalisesta häiriönsietokyvystä (Digital Operational Resilience Act - DORA)

- Kyberhyökkäysten uhan lisääntyessä jatkuvasti EU haluaa vahvistaa rahoitusalan toimijoiden tietojärjestelmien turvallisuutta
- DORA kattaa lähes kaikki finanssialan toimijat, joita Finanssivalvonta jo nyt pääsääntöisesti valvoo
  - Soveltamisalasta puuttuvat työeläkeyhtiöt ja joitakin erikseen määriteltyjä pieniä toimijoita
- DORA asettaa finanssialan toimijoille laajan joukon vaatimuksia, joilla pyritään parantamaan rahoitusalan kykyä sietää vikoja ja häiriöitä
  - Tieto- ja viestintätekniikan (TVT) riskienhallinta
  - Riskienhallinta TVT-palvelujen hankinnassa
  - TVT-häiriöraportointi
  - Tiedon jakaminen kyberuhkista
  - Digitaalisen häiriönsietokyvyn testaus
  - Kriittisten TVT-palveluntarjoajien valvonta
    - Kriittisiksi katsottavat kolmannet osapuolet, jotka tarjoavat TVT-palveluita rahoitusalan toimijoille, tulevat suoraan eurooppalaisten valvontaviranomaisten valvontaan siltä osin, kun ne tarjoavat palvelujaan rahoitusalan toimijoille
- DORA astui voimaan 17.1.2023 ja sitä sovelletaan 17.1.2025 alkaen

Valvonta

- ICT- ja tietoturvariskien hallinnan valvonta
  - Toimiluvat ja rekisteröinnit
  - Jatkuva valvonta
    - Raportointi
    - Valvojan arvio
  - Tarkastukset
  - Teema-arviot

Valvonta

- Onko teillä suunnitelmissa auditoida DORAa?
  - Tulemme valvomaan DORA:n vaatimusten noudattamista.
- Mikä mielestänne erityisesti muuttuu Doran myötä aiempiin vaatimuksiin verrattuna? Erityisesti, mikä mielestänne muuttuu sisäisen tarkastuksen velvoitteiden osalta? Jos nämä aiheet riskienhallintajärjestelmä, toiminnan organisointi, poikkeamien hallinta ja raportointi, häiriönsietokyky ja ulkoistukset ovat olleet sisäisen tarkastuksen riskiperusteisen tarkastamisen kohteena jo aiemmin, niin onko tarvetta tehdä tarkastusohjelmaan muutoksia?
  - Muutokset ovat sellaisia, että tarkastusohjelma todennäköisesti voi säilyä ennallaan.
- Onko valvottavan vastuulla perustella dokumentaatiossa, miten ja miksi DORA-asetuksen vaatimat asiat on täytetty, vai riittääkö toteutettujen asioiden dokumentointi ja FIVA arvioi riittävyyden suhteessa valvottavan toimintaan? Esimerkiksi tarvitseeko pienimuotoista toimintaa harjoittavan valvottavan ottaa dokumentaatiossa kantaa siihen, miksi kaikkia DORA:n vaatimuksia ei ole toteutettu?
  - Valvottavien ohjeista ja prosessikuvauksista käy pitkälti ilmi noudatetaanko vaatimuksia. Erillistä dokumentaatiota tai selvitystä DORA:n noudattamisesta emme odota, vaikka käytännössä sellainen valvottavilla muodostuukin DORA:n implementoinnin yhteydessä.
- Kuinka usein sisäisen tarkastuksen tulisi tarkastaa osa-aluetta?
  - Tämä perustuu valvottavan omaan harkintaan.

Soveltamisala

- Pysyykö valvottavien toimijoiden kategorisointi ennallaan vai jakaako Fiva jollakin perusteella valvottavia DORA-perusteisesti uudelleen? (Jotta pystytään arvioimaan, mitä velvoitteita kuhunkin toimijaan määräysten perusteella kohdistuu.)
  - Ei muutoksia
- Minkälaisia helpotuksia on pienemmille toimijoille, ja onko tällaisen pienemmän toimijan kriteerit määritelty?
  - Ks. DORA
- Millaisia heijastusvaikutuksia Doralla on työeläkevakuutusyhtiöihin eli tuleeko sovellettavaksi jossain tilanteessa, jos kyllä, missä?
  - Ei suoraan heijastusvaikutuksia, mutta toki on mahdollista, että tarvetta vastaaville vaatimuksille työeläkevakuutusyhtiöille tarkastellaan tulevaisuudessa
- Vaikuttaako DORA-velvoitteisiin (lain silmissä tai käytännössä) jos palveluntarjoaja on myös DORA:ssa tarkoitettu finanssiyhteisö?
  - Ei

Soveltamisala

- Tuleeko ns. Brexit-luvan saaneen sijoituspalveluyhtiön (SiPaL 5:7.2) soveltaa DORAa toiminnassaan, jos yhtiön ainoa toimipaikka sijaitsee Englannissa?
  - DORA ei sinänsä suoraan sovellu kolmannen maan yrityksiin. Luonnoksessa hallituksen esitykseksi kuitenkin esitetään, että sijoituspalvelulain 7 luvun 2 §:ään lisätään viittaus DORAan. Sijoituspalvelulain 1 luvun 7 §:n mukaan kolmannen maan yrityksiin soveltuu mm. sijoituspalvelulain 7 luvun 2 §. DORAn säännöksiä tulisi tämän sijoituspalvelulakiin ehdotetun viittauksen kautta sovellettavaksi myös kolmannen maan yrityksiin, joilla on toimilupa tarjota sijoituspalveluja Suomessa.
- Voisitteko vahvistaa, että DORA-asetusta ei sovelleta rekisteröitymisvelvollisiin vaihtoehtorahastojen hoitajiin.
  - DORA:a ei sovelleta direktiivin 2011/61/EU 3 artiklan 2 kohdassa tarkoitettuihin vaihtoehtoisten sijoitusrahastojen hoitajiin
- Miltä osin käytännössä yksinkertaistettu TVT-riskinhallintajärjestelmä (art. 16 velvoitteet) eroaa mikroyritystä koskevista velvoitteista? Ovatko nämä toisensa poissulkevat vai toisiaan täydentäviä?
  - Jos mikroyritys kuuluu 16 artiklan piiriin, niin 5-15 artiklaa ei sovelleta.

Implementointi

- Alan sääntely esim. riskienhallintajärjestelmän osalta on jo aiemmin ollut kattavaa - mikä nyt muuttuu ja miten se vaikuttaa yhtiöihin tosiasiallisesti?
  - Suurin osa DORA:n vaatimuksista on ollut jo Finanssivalvonnan määräys- ja ohjekokoelmassa, Euroopan valvontaviranomaisten ohjeissa ja lainsäädännössä. Nyt vaatimuksia on yhtenäistetty, osin tarkennettu ja joitakin vaatimuksia lisätty. Yhtiöiden tulee käydä läpi DORA:n vaatimukset ja tehdä tarvittavat muutokset toimintatapoihin ja ohjeistuksiin.
- Miten ja millä aikataululla Dora implementoidaan MOK 8/2014?
  - MOK 8/2014 ja muut MOK:it päivitetään siten, että päällekkäisyydet DORA:n kanssa poistetaan. Päivitys tehdään syksyllä 2024 ja muutokset tulevat voimaan 17.1.2025.
- Kertoisitteko vielä odotettavissa olevien RTS:ien ja ITS:ien hyväksyntäaikataulusta ja prosessista?
  - RTS/ITS –luonnokset on toimitettu komission hyväksyttäväksi kahdessa erässä (1/2024 ja 7/2024). Hyväksynnälle ei ole aikataulua, mutta varmaankin syksyn aikana. TVT-sopimusrekisterin sisällön määrittelevä ITS palautui kesällä valmisteltavaksi (LEI:tä ei voi käyttää).

Implementointi

- Is the FIN-FSA, due to the DORA requirements on ICT-Incident Classification and Notification of Major ICT-related incidents, considering updates of FIVA 8/01.00/2014 chapter 9.1 "Reporting of disruptions and faults in operations”?
  - Kyllä
- Has the FIN-FSA considered replacing the requirements related to significant/key processes in FIVA 8/2014 with the DORA requirements related to Critical and Important Functions?
  - Ei

Implementointi

- Olen ymmärtänyt että DORA kumoaa PSD2 häiriöraportoinnin sääntelyn ja jatkossa esim. maksupalveluiden häiriöraportoinnin sääntely perustuu suoraan asetukseen (DORA). Fivalla on voimassa useampia MOKeja, joissa vedotaan PSD2 sääntelyn vaatimuksiin häiriöraportoinnin osalta, milloin Fiva päivittää kyseiset MOKit ja ohjeistaa maksupalveluiden uudet, DORAn mukaiset raportointivelvoitteet. Maksupalveluiden osalta DORA ymmärtäkseni sisältää myös sääntelyn operatiivisten häiriöiden, ei siis pelkästään teknisten häiriöiden, raportoinnin osalta. DORA 23 artikla ja DORA 3 artiklan 9 kohta. Päivittyykö tältä osin myös Fivan ohjeistus operatiivisten riskien ja häiriöiden osalta?
  - Kyllä, tähän ja muuhun raportointiin liittyvät MOK-ohjeet ja käytännön ohjeet Finanssivalvonnan verkkosivuilla päivitetään
- Tuleeko Doran myötä päivityksiä ja millä aikataululla EBA:n ohjeistukseen Euroopan pankkiviranomaisen ohjeet ”Tieto- ja viestintätekniikka- (ICT) sekä turvallisuusriskien hallinnasta” tai Finanssivalvonnan määräyksiä ja ohjeita 8/2014 "Operatiivisen riskin hallinta rahoitussektorin valvottavissa” ja Finanssivalvonnan määräyksiä ja ohjeita 1/2012 ”Ulkoistaminen rahoitussektoriin kuuluvissa valvottavissa”.
  - MOK 8/2014 ja muut MOK:it päivitetään siten, että päällekkäisyydet DORA:n kanssa poistetaan. Päivitys tehdään syksyllä 2024 ja muutokset tulevat voimaan 17.1.2025.
  - Euroopan valvontaviranomaiset päivittävät DORA:aan liittyvät ohjeet ennen 17.1.2025

TVT-riskienhallinta

- Mitkä ovat DORAn vähimmäisvaatimukset IT-riskien hallinnalle?
  - Ks. DORA
- Article 5.2 (g) – what types of costs should be included in the DORA budget other than costs related to resilience training?
  - Kaikki kustannukset, jotka DORA:n mukainen ICT- ja tietoturvariskien hallinta vaatii
- Kuinka yksityiskohtainen riskienhallinnan viitekehyksen on oltava, so. riittääkö että riskit kohdistetaan tiettyyn omaisuusluokkaan vai vaaditaanko tarkempaa määrittelyä?
  - Ks. DORA
- Kuinka pienen ja lähes yksinomaan ulkoistettuja palveluita käyttävän toimijan tulisi suhtautua riskienhallintamallin yksityiskohtaisiin teknisluonteisiin dokumentaatiovaatimuksiin?
  - DORA-vaatimuksia tulee noudattaa
- Voiko insidentti kohdassa käyttää riskiperusteista harkintaa?
  - Ei, DORA-vaatimuksia ja määritelmiä tulee noudattaa
- Mitä organisatorisia tahoja ja rooleja teistä tarkoittaa 13 artiklan 6 kohdan ylin johto kun puhutaan erilaisista finanssialan toimijoista, heidän hallinto- ja johtorakenteista?
  - ”ylempi johto” tarkoittaa tässä toimivan johdon lisäksi myös ”ylimmän hallintoelimen” jäseniä
- Level2 Artikla 27, kohdat 1 ja 2: onko fivalla suosituksia/toimintamalleja miten mainittuja tietoja tullaan toimittamaan viranomaisille?
  - TVT-riskinhallintajärjestelmän uudelleentarkastelusta laadittava raportti toimitetaan Finanssivalvonnan ohjeiden mukaisesti pyydettäessä

Riskienhallinta TVT-palvelujen hankinnassa

- TVT-palvelu
  - TVT-järjestelmien kautta yhdelle tai useammalle sisäiselle tai ulkopuoliselle käyttäjälle jatkuvasti tarjottavia digitaalisia ja datapalveluja, mukaan lukien laitteistot palveluna ja laitteistopalvelut, joihin sisältyy teknisen tuen tarjoaminen laitteiston tarjoajan ohjelmisto- tai laiteohjelmistopäivitysten kautta, lukuun ottamatta perinteisiä analogisia puhelinpalveluja
- ”TVT-ulkoistus” = ”finanssiyhteisön sopimusjärjestely TVT-palvelujen käytöstä liiketoimintojensa hoitamista varten”
- Millainen dokumentaatio on "riittävä" valvottavan kannalta palveluntarjoajilta?
  - Ks. DORA
- Miten valvottavan pitää huomioida DORA olemassa olevissa sopimuksissa palveluntarjoajien suuntaan?
  - DORA:a tulee noudattaa 17.1.2025 alkaen
- Vaikuttaako DORA-velvoitteisiin (lain silmissä tai käytännössä) jos palveluntarjoaja on myös DORA:ssa tarkoitettu finanssiyhteisö?
  - Ei

Riskienhallinta TVT-palvelujen hankinnassa

- Mitkä järjestelyt kuuluvat DORA:n piiriin?
- Miten tulisi menetellä sopimusvaatimusten kanssa niiden toimittajien osalta, joiden kanssa finanssialan toimijalla ei ole todellisia mahdollisuuksia neuvotella sopimusehdoista?
  - DORA:n vaatimuksia tulee noudattaa
  - Teleoperaattoreiden tarjoamat tietoliikennepalvelut ovat erityisesti ongelma tässä suhteessa – emme pysty tällä hetkellä kertomaan miten tämä selviää
- Kuuluvatko luottotietopalvelut DORA:n mukaisiin ICT-palveluihin?
  - Kyllä, poislukien viranomaisen tarjoamat palvelut
- Millä tavoin finanssimarkkinatoimijan tulee suhtautua verkkopankin käyttöön DORA:n osalta? Entä varainhoitajien sijoittajaportaaleihin, jotka tulevat sijoituksen “kylkiäisenä”?
  - Ovat TVT-palveluja
- Kuinka pieniä yleisiä palveluita kuten verkkoliikenteen analysointi Matomolla tai lomakespämmin estäminen Akismet sovelluksella tulisi DORAn näkökulmasta käsitellä kun kaikkia vaadittuja ehtoja ei saa sopimuksiin, mutta kyseessä on myös palvelu, jonka poistamisella ei ole merkittävää vaikutusta palveluihin yleisesti?
  - Ovat TVT-palveluja

Riskienhallinta TVT-palvelujen hankinnassa

- Mitkä järjestelyt kuuluvat DORA:n piiriin?
  - For a Group consisting of several financial entities, will a centralized unit for submission of incident notifications and reports be considered as outsourcing to a third-party provider under Art. 19(5) of DORA?
    - Ei ole DORA:n tarkoittama sopimusjärjestely, mutta laajempi IT-tuen ulkoistus olisi

Riskienhallinta TVT-palvelujen hankinnassa

- Kriittinen tai tärkeä TVT-ulkoistus
  - tukee ” toimintoa, jonka häiriö heikentäisi olennaisesti finanssiyhteisön taloudellista tuloksellisuutta tai sen palvelujen ja toimintojen moitteettomuutta tai jatkuvuutta tai jonka keskeytyminen, vikaantuminen tai puuttuminen heikentäisi olennaisesti finanssiyhteisön kykyä noudattaa jatkuvasti toimilupansa mukaisia ehtoja ja velvoitteita tai sovellettavan finanssipalvelulainsäädännön mukaisia muita velvoitteittaan”
- DORA-asetuksessa määritellään kriittinen tai tärkeä tehtävä, mutta antaako Finanssivalvonta yksityiskohtaisia ohjeita rahoitusalan entiteettien arvioimiseksi, mitä yleensä on pidettävä kriittisinä tai merkittävinä rahoitussektorin funktioina?
  - Ei
- Milloin valvottavan alihankkija voidaan määritellä valvottavan yrityksen kannalta kriittiseksi tai tärkeäksi suhteellisuusperiaatteen mukaan? Miten valvottavan tulee seurata TVT-alihankkijaa, kun kyseessä on asiakkaan määrittelemä kriittinen 3rd party toimittaja?
  - Ks. DORA
- Voidaanko 3rd party sopimuskumppani määritellä kriittiseksi riippumatta valvottavan yhteisön koosta / kriittisyydestä?
  - Kyllä
- Lei-tunnuksen käyttö ulkoistusraporteissa: finanssimarkkinatoimija ei voi tehdä sopimusta palveluntarjoajan kanssa, jolla ei ole LEI-tunnusta?
  - Komissio palautti ao. RTS-luonnoksen valmisteluun – LEI-tunnusta ei tulla käyttämään
- Tarvitseeko TVT-ulkoistustahon suostua valvottavan tekemiin auditointeihin?
  - Kyllä
- Kuinka paljon auditoinneissa/testauksissa voi tukeutua palveluntarjoajan itsensä jo muutenkin mahdollisesti tekemiin selvityksiin?
  - Palveluntarjoajan teettämät kolmannen osapuolen arviot ovat merkittävässä roolissa, kuten nytkin

Riskienhallinta TVT-palvelujen hankinnassa

- Pilvipalveludataa voidaan prosessoida hyvin monessa maassa. Miten/millaisella tarkkuudella tämä fakta pitäisi huomioida sopimuksissa / riskienhallintajärjestelmässä / viranomaisraportoinnissa?
  - ICT-riskienhallinnassa tarvitaan tieto siitä missä dataa käsitellään
- Millä tarkkuustasolla keskeisten järjestelmien exit-suunnitelmien testaus pitää kuvata? Käytännössä perusjärjestelmien osalta ainoa exit on toisen korvaavan järjestelmän hankinta.
  - Ks. DORA
- Jos yhtiö hankkii kaikki ICT-palvelunsa ulkoisilta palvelutoimittajilta, niin tarvitseeko yhtiön tehdä itse säännöllisesti häiriönsietokyvyn testausta kaikille kriittisiä tai tärkeitä toimintoja tukeville ICT-järjestelmille vai riittääkö, että yhtiö vaatii kyseisten ICT-järjestelmien palvelutoimittajia tekemään häiriönsietokyvyn testauksen DORA-vaatimusten mukaisesti ja toimittamaan tiedot testausohjelmasta ja -tuloksista yhtiölle?
  - Voi nojautua toimittajan testeihin
- Milloin on ensimmäinen raportointi deadline?
  - Sopimustietojen osalta tarkoitus oli pyytää ensimmäinen raportointi 3/2025, mutta tämä tulee siirtymään
- Tuleeko koko konsernin raportoida yhteinen DORA raportti, vai tuleeko konsernissa olevan valvottavan yrityksen raportoida itsenäisesti vaikka ICT palveluntarjoajat ovat pitkälle konsernin sopimuksia?
  - TVT-sopimustiedot voi raportoida yhteisellä raportilla
- Yleisesti onko teillä jotain raportointipohjia jaettavana mitä DORAn puitteissa toivotte käytettävän?
  - Nämä määritellään RTS/ITS-dokumenteissa ja Finanssivalvonta tulee ohjeistamaan raportoinnin

Riskienhallinta TVT-palvelujen hankinnassa

- Kasvava riippuvuus kolmansien osapuolten palveluntarjoajista on kasvanut merkittävästi, erityisesti pilvipalveluiden osalta, miten rahoituslaitosten tulisi DORA mukaisesti lähestyä näiden suhteiden hallintaa ja muuttaako tämä tätä miltä osin eniten? Entä mitkä ovat odotukset kolmansien osapuolten jatkuvasta seurannasta ja vaatimustenmukaisuuden varmistamisesta koko hankintaketjun osalta vrt. aikaisempaan ohjeistukseen EBA/FSA osalta?
  - Ks. DORA
- Miten ISO 27001 sertifikaatti ja/tai NIS2 vaatimukset täyttävien organisaatioiden kuuluvat laitokset tulisi strategisesti ja taktisestii sovittaa käytäntönsä myös DORA vaatimusten täyttämiseen ilman päällekkäisyyksiä, joita varmasti kyllä syntyy väkisin? Tiivistettynä ja kärjistäen ISO27001 keskittyy tietoturvaan ja informaation hallintaan laaja-alaisesti ja NIS2 standardisoi EU tason velvoitteita kuten häiriöraportointia sekä tietoturvavelvollisuuksia. Onko olemassa yksinkertaistettua lähestymistapaa näiden hallinnointiin & dokumentointiin tai "best-practice" mallia, jotta organisaatio voisi tehokkaasti käsitellä useita sääntelyvaatimuksia? Esimerkiksi helposti havainnoida ”overlapping” alueet, joihin keskittyä, työkalujen avulla kuten self-assesmentit yhdistettynä tai muuta vastaavaa? Tärkeä asia toteuttaa kaikin puolin, mutta monelle pienemmälle valvottavalle tämä voi aiheuttaa (ei välttämättä) merkittäviä kehitystarpeita, joilla on luonnollisesti suoria- ja epäsuoria kustannuksia. Osa aihealueista on kuitenkin kunnossa ja osa taas vaatii toimenpiteitä, erityisesti jos NIS2 ja ISO27001 ovat hanskassa.
  - DORA ei käsittele näitä asioita

Riskienhallinta TVT-palvelujen hankinnassa

- Mahdollistaako DORA:ssa mainittu suhteellisuusperiaate sen, että erilaisia kriittistä toimintoa tukevia ICT-palveluita kohdellaan DORA:n vaatimusten osalta eri tavalla riippuen siitä, miten merkittävä kyseinen ICT-palvelu on kriittisen toiminnon jatkuvuuden kannalta? Useat DORA:n velvoitteet soveltuvat kriittistä toimintoa "tukeviin" ICT-palveluihin ja -järjestelmiin, vaikka nämä ICT-palvelut ja järjestelmät eivät itsessään olisi kriittisiä. Jos DORA:n sanamuotoa tulkittaisiin tässä tiukasti, kyseiset vaatimukset koskisivat aivan kaikkia ICT-palveluita ja -järjestelmiä, kunhan ne vain tukevat kriittistä toimintoa. Suhteellisuusperiaatteen soveltaminen mahdollistaisi riskiperusteisemman lähestymistavan siinä, miten laajoja riskienhallintatoimenpiteitä vaadittaisiin kunkin kriittistä toimintoa tukevan ICT-palvelun osalta. Tällöin voitaisiin välttyä siltä, että kriittisen toiminnon jatkuvuuden kannalta merkityksettömään ICT-palveluun sovellettaisiin tiukasti DORA:n vaatimuksia esim. 30(3) artiklan sopimusehdoista, 28(8) artiklan irtautumisstrategiasta ja 24(6) artiklan vuosittaisesta testauksesta.
  - Jos ICT-palvelun häiriö voi aiheuttaa häiriön valvottavan kriittiseen tai tärkeään palveluun, niin silloin se on kriittinen

Riskienhallinta TVT-palvelujen hankinnassa

- Jos palveluntarjoajan kanssa on tehty sopimus ensisijaisesti esimerkiksi perinnän hoitamisesta ja palveluntarjoaja tarjoaa perintäpalvelun lisäksi web-portaalin, josta finanssiyhteisö voi hakea raportteja, onko tällöin kyseessä TVT-palveluntarjoaja?
  - Ei
- Article 5.3 – what does it mean to “monitor” the contracts concluded with third-party ICT service providers? Does it mean requirement setting and testing or also auditing?
  - Ks. DORA

TVT-häiriöraportointi

- Häiriöraportointi tehdään jatkossakin FISA-järjestelmän kautta. Ilmoitus muuttuu web-lomakepohjaiseksi ja häiriöilmoituslomakkeita on jatkossa vain yksi. Ohjeistus päivitetään syksyn aikana.
  - FIVA on aiemmin indikoinut julkaisevansa syksyn aikana ohjeistusta mm. häiriöraportoinnin käytänteisiin liittyen. Millä aikataululla ohjeistusta voidaan odottaa?
  - Onko FIVA:n ja/tai EBA:n PSD2 häiriöraportointipohjiin tulossa muutoksia tai ollaanko ne uusimassa kokonaan?)
  - Is the FIN-FSA considering to develop and provide a template for notification of Major ICT-related incidents? Related to the submission of notification of Major ICT-related incidents, which channel will the FIN-FSA expect financial entities to use for the notification?
  - Vastaanottaako FIVA vain DORAn mukaisia incidenttiraportteja 17.1.2025 alkaen?
  - Tarjoaako FIVA raportointia varten verkkolomakkeen tai jopa API-rajapinnan?
- Is incident reporting discussed and intended aligned with the other three Nordic FSAs?
  - Ei ole tällaista suunniteltu, mutta asia tullaan selvittämään

Tietojen jakaminen kyberuhkista

- Voiko ryhmä yrityksiä tehdä yhdessä ilmoituksen vapaaehtoisen tietojenvaihdon aloittamisesta?
  - Kyllä

Digitaalisen häiriönsietokyvyn testaus

- Mikä viranomainen tulee valvomaan ja ohjaamaan TPLT:tä (Threat-Led Penetration Testing) Suomessa? / Mikä taho Suomessa tulee olemaan TLPT Authority?
  - Suomen Pankki jatkaa TIBER-FI –kehikon hallinnointia
  - SI-pankkien osalta EKP/SSM asettaa TPLT-testausvelvoitteen ja valvoo tuloksia
  - Muiden valvottavien osalta Finanssivalvonta asettaa TPLT-testausvelvoitteen ja valvoo tuloksia
- Milloin ja missä kanavassa tiedotetaan TLPT-velvoite finanssialan toimijoille? ts ketkä toimijoista ovat velvoitettuja toteuttamaan DORAn kuvaaman TLPT-toiminnan?
  - Valvoja ilmoittaa TLPT-velvoitteesta
  - Suomen Pankki jatkaa TIBER-FI –kehikon hallinnointia
  - SI-pankkien osalta EKP/SSM asettaa TPLT-testausvelvoitteen ja valvoo tuloksia
  - Muiden valvottavien osalta Finanssivalvonta asettaa TPLT-testausvelvoitteen ja valvoo tuloksia
- Minkälaiset ICT palvelut tulevat olemaan TLPT-testien fokuksessa ja kuinka teknisiä palveluketjuja on tarkoitus testata - 1) vain alkupäästä katsoen ja raportoiden vai 2) koko toimitusketjun hierarkiasta tuottaen testiraportit joka tasolta?
  - Yritykset suunnittelevat itse testaukset sellaisiksi, että ne noudattavat DORA:n vaatimuksia
- Joko TLPT-testaajien / testausta tarjoavien tahojen akkreditointi on käynnissä ja onko lista julkinen?
  - Suomessa TIBER-FI –kehikon puitteissa tehty testaus noudattaa DORA:n vaatimuksia
  - Jos yritys haluaa järjestää kokonaan itse testauksen, niin sen on itse varmistettava, että se noudattaa DORA:n TLPT-testaamista koskevia vaatimuksia
- Milloin Fiva/toimivaltainen viranomainen ilmoittaa 26 artiklan 8 kohdan kolmannen alakohdan mukaiset finanssiyhtiöt?
  - 17.1.2025 mennessä

Kriittisten ICT-palveluntarjoajien valvonta

- Miten IT-palvelutarjoajan pitäisi varautua tilanteeseen, jossa organisaatio on sekä DORA:n (oletettavasti TVT ulkoistuksen kohteena), että NIS2:n piirissä (IT-palveluntarjoajana). Esimeriksi incidentin tapauksessa kumman säätelyn suuntaan pitäisi alkaa raportoimaan DORA-valvojalle vai NIS2-valvojalle vai molemmille?
  - Tällä hetkellä Suomessa NIS-soveltamisalaan kuuluvat finanssialan yritykset raportoivat vain Finanssivalvonnalle, emme osaa sanoa pystytäänkö kriittisten ICT-palveluntarjoajien raportointi järjestämään vain DORA-valvojalle tai NIS2-valvojalle
- Ei eksaktia kysymystä, mutta tieto esim JET ja LO järjestäytymisestä, aikataulu ja yhteistoiminta viranomaisten kanssa auttaisi syksyn suunnittelua yhdessä CTPPsien kanssa.
  - Järjestäytyminen tapahtuu 2025.
- Miten/kuka määritetään mitkä toimijat ovat ns. "critical ICT third party provider”
  - Euroopan valvontaviranomaisten ja kansallisten valvojien muodostama valvonta määrittelee valvottavat ICT-palveluntarjoajat valvottavilta kerättävän rekisteritiedon perusteella. Käytännössä tämä tapahtunee syksyllä 2025.