VALTIOVARAINMINISTERIÖ

Selvitys digitaalisen turvallisuuden arvioinnin kehitystarpeista

10.5.2021

Sisällys

TIIVISTELMÄ

Tässä raportissa kuvataan julkisen hallinnon digitaalisen turvallisuuden arvioinnin tunnistettuja haasteita ja esitetään näitä korjaavia kehitystoimenpiteitä. NLF-asetuksessa (765/2008)[1] vahvistetaan vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevat säännöt sekä akkreditointielimiä koskevat vaatimukset. FINAS on NLF-asetuksessa tarkoitettu Suomen ainoa kansallinen akkreditointielin. Vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annettua lakia (920/2005) eli akkreditointilakia sovelletaan vaatimustenmukaisuuden arviointipalvelujen akkreditointiin ja siihen rinnastettavaan pätevyyden arviointiin. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetussa laissa (1046/2011, *arviointilaki*) säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista. Valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain mainitussa laissa tarkoitettua menettelyä taikka sellaista arviointilaitosta, joka on saanut Viestintäviraston (nykyisin Liikenne- ja viestintävirasto Traficom) hyväksynnän tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, *arviointilaitoslaki*) mukaan. Arviointiperusteina voidaan käyttää mm. lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita.

Julkisen hallinnon digitaalisten palvelujen turvallisuus edellyttää nykyistä kattavampaa turvallisuusajattelua. Tietoteknisten järjestelmien tiedon luottamuksellisuuteen ja eheyteen liittyvien suojausten hyväksymisen lisäksi digitaalisen turvallisuuden tavoitteena tulisi olla myös palvelujen toiminnan jatkuvuuden varmistaminen, jonka avulla voidaan vastata kattavammin kysymykseen siitä, milloin jokin palvelu on toteutettu niin, että se on riittävän turvallinen käyttötarkoitukseensa nähden. Nykyinen arviointilaki rajoittuu tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuteen, ja painopisteenä on teknisen tietoturvallisuuden arviointi. Kaikille digitaalisen turvallisuuden osa-alueille ei ole säännöksissä asetettuja arviointiperusteita. Turvallisuuden riittävän tason määrittely kuitenkin edellyttää, että kaikille digitaalisen turvallisuuden osa-alueille säädetään vähimmäisvaatimukset ja niiden perusteella määritetään kriteeristö, jonka avulla vähimmäisvaatimusten toteutuminen tai muu vaatimustenmukaisuus voidaan todeta luotettavasti.

Tätä selvitystä varten haastateltiin 23 eri organisaation asiantuntijaa. Selvityksessä kuvattu nykytila perustuu näistä haastatteluista saatuihin näkemyksiin sekä tarkentaviin keskusteluihin ja kirjalliseen materiaaliin, jota on saatu erityisesti FINASilta ja Traficomilta. Hyväksytyn arviointilaitoksen aseman saavuttamiseksi yhteisön täytyy tällä hetkellä hakea ensin kansallisen akkreditointiyksikön (FINAS) akkreditointi (920/2005), minkä jälkeen sen on haettava Traficomin hyväksyntä (1405/2011). Digitaalisen turvallisuuden arviointien kysynnän ennakoidaan kasvavan, joten markkinaehtoisesti toimivia hyväksyttyjä arviointilaitoksia tarvitaan jatkossa enenevässä määrin. Hakuprosessin pitkä kesto ja pätevyyden arvioinnissa käytettyjen kriteerien tulkinnanvaraisuudet nähtiin haastatteluissa merkittävinä markkinoille pääsyn hidasteina.

[1] Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (ns. NLF-asetus)

Tietojärjestelmän tietoturvallisuusarviointi on yksi keino arvioida ja tunnistaa järjestelmään kohdistuvia turvallisuusriskejä. Arviointilain mukaista arviointia ei ole kansallisella tasolla säädetty pakolliseksi, eikä viranomaisella ole velvollisuutta hankkia arviointilaissa tarkoitettua todistusta siitä, että tietojärjestelmä täyttää vaatimukset. Tiedonhallintalakiin (906/2019) on kirjattu, että elinkaarimallin mukaisesti viranomaisen on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Olennaiset tietojenkäsittelyyn kohdistuvat riskit on selvitettävä, ja tietoturvallisuustoimenpiteet on mitoitettava riskiarvioinnin mukaisesti. Kokonaisuuteen kuuluu riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen (ks. HE 284/2018 vp, 13 §:n yksityiskohtaiset perustelut). Tiedonhallintalain 13 § 5 momentissa on informatiivinen viittaus arviointilakiin. Tämän mukaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

Nykyinen sääntely ei haastateltujen henkilöiden mukaan tällä hetkellä riittävästi velvoita vaatimustenmukaisuuden säännölliseen ja jatkuvaan varmistamiseen. Ehdotettiinkin, että sääntelyssä vahvennettaisiin tiedonhallintalailla tiedonhallintayksiköille asetettuja vaatimuksia ja asetettaisiin selkeä vaatimus sekä tiedonhallintayksikön toteuttamille itsearvioinneille että ulkopuolisille arvioinneille, vertaa tietoturvallisuuden hallintajärjestelmän standardin ISO 27001:2017 vaatimukset 9.2 ja A.18.2. Traficomin tarjoamat tietojärjestelmien arviointi- ja hyväksyntäpalvelut on kuvattu Traficomin ohjeessa "Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit". Haastatteluissa toivottiin tarkennuksia muutosten, poikkeamien ja haavoittuvuuksien hallinnalle ja käsittelylle. Niille tulisi määritellä mekanismi, joka kuvaa, miten ja missä ajassa poikkeamat on korjattava, miten tehdyt korjaukset todennetaan ja miten eritasoiset poikkeamat vaikuttavat vaatimustenmukaisuuden toteutumiseen.

Digitaalisen turvallisuuden arviointia olisi mahdollista kehittää edelleen arviointitoimintaa ja toimijoiden kokonaisuutta selkeyttämällä. Kehitysehdotukset ovat seuraavat:

1) Digitaalisen turvallisuuden näkökulmasta tärkeimmät toiminnan jatkuvuuden ja varautumisen vaatimukset sisällytettäisiin tiedonhallintaa koskeviin säädöksiin.

2) Arviointeja laajennettaisiin tietoturvallisuuden arvioinnista myös toiminnan jatkuvuuden ja varautumisen arvioitiin. Arviointien nopeuttamiseksi ja resurssien käytön tehostamiseksi julkista tai luokittelematonta sekä salassa pidettävää tietoa käsittelevien palvelujen arviointien tulisi olla pääasiallisesti akkreditoitujen kaupallisten arviointilaitosten tehtävänä. Tämän vuoksi on tarpeen varmistaa, että kansallisen akkreditointiyksikkö FINAS arvioi tietoturvallisuuden lisäksi myös toiminnan jatkuvuuden ja varautumisen arviointilaitosten pätevyyksiä määrävälein. FINAS voisi kuten nykyisinkin käyttää muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä ja pätevyyden arvioinnissa.

3) FINAS päättäessään akkreditoitavien arviointilaitosten toimialakohtaisista arviointiperusteista kuulisi tiedonhallintalautakuntaa yleisten tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen vähimmäisvaatimuksista.

4) FINAS akkreditoisi kaupallisia tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitoksia hakijan hakemuksessa esittämille pätevyysalueille. Mahdolliset kilpailuoikeudelliset syyt erottaa kaupallisten arviointilaitosten ja viranomaisten arviointitehtävien pätevyysalueet selvitettäisiin.

5) FINAS ylläpitäisi kuvausta mahdollisista arviointilaitosten pätevyysalueista. Pätevyysalueet voivat kattaa turvallisuusluokitteluasetuksen turvallisuusluokan IV ja III sekä salassa pidettäviä ja julkisia tietoja käsittelevien järjestelmien tietoteknisen turvallisuuden arvioinnin, arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen ja henkilöstöturvallisuus) arvioinnin sekä korkeintaan turvallisuusluokan TL III toiminnan jatkuvuuden ja varautumisen järjestelyjen arvioinnin.

6) Säädettäisiin, että arviointilaitoksen akkreditointi- ja hyväksyntäprosessin osana arviointilaitoksesta toteutettaisiin turvallisuusselvityslain (726/2014) mukainen yritysturvallisuusselvitys, jolla mm. varmistettaisiin arviointilaitoksen kyvykkyys asiakkaiden tietojen käsittelyssä kuten salassa pidettävien tietojen suojaamisessa. Yritysturvallisuusselvitys korvaisi nykyisen Traficomin suorittaman arviointilaitoksen tietojenkäsittelyn turvallisuuden arvioinnin. Turvallisuusselvityslain mukaisesti jatkossakin henkilöturvallisuusselvityksen ja yritysturvallisuusselvityksen tekemisestä päättää suojelupoliisi, jollei turvallisuusselvityksen laatimisesta päätä pääesikunta. Liikenne- ja viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.

7) Julkisia tai salassa pidettäviä tietoja käsittelevien palvelujen arviointilaitosten hyväksyntäprosessia yksinkertaistettaisiin ja nopeutettaisiin keventämällä tilaturvallisuusvaatimuksia ja tiedon suojaamiskyvyn vaatimuksia. Selvitettäisiin, että voitaisiinko erityisesti julkisia tai salassa pidettäviä tietoja käsittelevien palvelujen arviointilaitoksiksi hakevien osalta poistaa arviointilaitoslain (1405/2011) 5§:n 1 mom. 5 kohdan vaatimus vaarantamatta arviointitoiminnan laadukkuutta.

8) Traficomille säädettäisiin tehtäviksi tietoturvallisuuden lisäksi myös toiminnan jatkuvuuden ja varautumisen arviointi. Traficom on ehdottanut, että Traficomin arvioinnit sisältäisivät arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen ja henkilöstöturvallisuus) ja tietoteknisen turvallisuuden arvioinnin: salaustuotteet (CAA), tietojärjestelmät sekä tietoliikennejärjestelyt (SAA).

9) Säädettäisiin valtiovarainministeriön ja liikenne- ja viestintäministeriön tiiviinä yhteistyönä toteuttamasta Traficomin arviointilaitosten akkreditointiin ja hyväksyntään sekä arviointitoimintaan liittyvästä ohjausmallista.

10) Tiedonhallintayksikön ja sen itselleen tilaaman fyysisen turvallisuuden arvioinnista liittyen tietoturvallisuuden tai toiminnan jatkuvuuden tai varautumisen arviointiin säädettäisiin kansallisella tasolla, esimerkiksi Suojelupoliisin tehtäväksi.

11) Puolustusvoimat on ehdottanut, että lakiin 1406/2011 säädettäisiin myös puolustusvoimat toimivaltaiseksi viranomaiseksi viranomaisarviointiin vastuualueenaan maanpuolustukseen liittyvä TL IV – TL I turvallisuusluokan tietotekninen arviointi: salaustuotteet (CAA), tietojärjestelmät sekä tietoliikennejärjestelyt (SAA). Toimivalta kattaisi edellä mainittujen kokonaisuuksien auditoinnin (arvioinnin) ja hyväksynnän. Tämä edellyttäisi muutoksia myös turvallisuusselvityslakiin.

12) Puolustusvoimat on ehdottanut, että puolustusvoimille säädettäisiin tehtäviksi tietoturvallisuuden lisäksi myös maanpuolustukseen liittyvien TL IV – TL I turvallisuusluokan salaustuotteiden, tietojärjestelmien sekä tietoliikennejärjestelyiden toiminnan jatkuvuuden ja varautumisen arviointi.

13) Sääntelyssä vahvennettaisiin tiedonhallintalailla tiedonhallintayksiköille asetettuja vaatimuksia ja asetettaisiin selkeä vaatimus sekä tiedonhallintayksikön toteuttamille itsearvioinneille että ulkopuolisille arvioinneille. Vaatimus ulkopuolisen arvioinnin tai todistuksen hankkimisesta säädettäisiin velvoittavaksi riskiarvioinnin perusteella niin, että se koskisi kriittisimpiä järjestelmiä ja toimintoja sekä korkeimpien turvallisuusluokkien järjestelmiä. Tässä yhteydessä arvioitaisiin vahvennetun sääntelyn kustannusvaikutuksia, joita on kuvattu myös tässä asiakirjassa. Säännöksissä ja ohjeistuksessa tulisi huomioida myös itsearviointi sekä kevyempi, konsultoiva tietojärjestelmien tarkastus, jonka voisi suorittaa muukin kuin akkreditoitu arviointilaitos.

14) Säädettäisiin selkeämmin arviointien tilaamisesta, mm. yhteishankintayksiköiden ja yhteisten palvelujen osalta. Viranomaiset ja yhteisöt voisivat tilata arviointeja tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen akkreditoiduilta arviointilaitoksilta niiden pätevyysalueilta ja niiden määrittämillä kustannuksilla. Toimeksiannon yhteydessä tilaaja määrittäisi arvioinnin kohteen ja arviointiperustan tai arviointiperusta määräytyy säädösten perusteella. Vaatimustenmukaisuustodistus kuitenkin myönnettäisiin kuten nykyisinkin ainoastaan käytettäessä pätevyysalueen mukaista arviointiperustaa (esimerkiksi tiedonhallintalautakunnan antama kriteeristö tai Katakri).

15) Säädettäisiin, että arviointitehtävää hoitavan viranomaisen ja arviointilaitoksen tulisi ilmoittaa tilaajalle arvio tai tarjous arvioinnin kestosta ja kustannuksista kuukauden kuluessa arvioinnin tai arviointitarjouksen pyytämisestä siinä määritettyä arvioinnin kohdetta vastaavasti.

16) Tiedonhallintalautakunta valmistelisi julkisen hallinnon tietoturvallisuuden arviointikriteeristön ottaen huomioon myös toiminnan varautumisen ja jatkuvuudenhallinnan asettamat vaatimukset.

17) Tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen vaatimustenmukaisuuden arvioinnin tilaajan olisi osoitettava säännöllisillä seuranta-arvioinneilla palvelun turvallisuuden tason ylläpitäminen ja parantaminen. Tähän liittyvistä seuranta- ja valvontamenettelyistä säädettäisiin ainakin tiedonhallintalain soveltamisalan osalta.

18) Säädetään, että tiedonhallintayksiköt, mahdollisesti yhteistoiminnassa, arvioisivat tieto- ja viestintäteknisten palveluita tuottavien alihankkijoidensa tietoturvaa koskevia vastuita ja velvoitteita. Lähtökohtana on, että kriittisille palveluille asetetaan palvelukohtaisesti turvallisuus- ja toimintavarmuusvaatimukset ja palvelujen vaatimuksenmukaisuus arvioidaan hyväksytyn arviointityökalun kriteerien mukaisesti arviointityökalun määräytyessä kunkin palvelun luonteen perusteella (esim. tiedonhallintalaissa (906/2019) säädetyt vaatimukset, ISO 27001, Katakri TL IV -tason vaatimukset).

19) Kaupallisten tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitosten valvonnan sääntelyä kehitettäisiin siten, että kyseisen pätevyysalueen valvontaan osallistuisivat Traficomin lisäksi myös muut pätevyysalueen vastuuviranomaiset koordinoidusti.

Ehdotettujen digitaalisen turvallisuuden arviointia koskevien kehittämistoimenpiteiden suunnittelun ja säädösvalmistelun arvioidaan vaativan asiantuntijatyötä arviolta yhteensä noin 12 htv eli 1 080 000 euroa. Kunkin suunnittelu- ja säädösvalmistelutehtävän rahoitus on varmistettava ennen sen aloittamista. Tämän lisäksi FINASin roolin vahvistaminen tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitosten akkreditoijana edellyttää lisäresursseja. FINASin akkreditointiprosessissa käyttämien toimialakohtaisten vaatimusten määrityksessä sekä arviointilaitoksiksi hakevien pätevyyksien arvioinnissa tarvitaan muiden viranomaisten tukea, mikä kasvattaa resurssitarvetta näissä viranomaisissa.

Tämän lisäksi on arvioitava digitaalisen turvallisuuden arvioinnin kustannukset, viranomaisia velvoittavien arviointien ja säännöllisten seuranta-arviointien mahdolliset kustannusvaikutukset sekä muut arviointitoiminnan mahdollisen kasvun aiheuttamat kustannukset. Arviointien ja arviointitodistusten tilaajat vastaavat arviointien kustannuksista, jotka ovat huomattavia. Vaatimustenmukaisuuden arviointiin arvioidaan tarvittavan noin 40 – 80 htp:ää asiantuntijahenkilöstön työpanosta jokaista arvioitavaa palvelua kohti. Esimerkiksi valtion yhteisiä tietoteknisiä palveluita on arvioitu olevan noin 130 kappaletta, joten niiden kaikkien arviointi kertaalleen vaatisi noin 22 – 48 henkilötyövuotta. Jos henkilötyövuoden hinta on 90 000 euroa, tämä tarkoittaisi yhteensä vähintään 2 – 4,3 miljoonaa euroa. Vaatimustenmukaisuuden arvioinnin kustannuksiin vaikuttavat arvioinnissa käytetty kriteeristö sekä maksuperustelain tai arvioinnin suorittamisen kilpailutuksen perusteella määräytyvä päivähinta. Tästä vaatimustenmukaisuuden arvioinnin kustannusarviosta puuttuvat vaatimustenmukaisuuden arvioinnin yhteydessä havaittavien puutteiden korjaamisen ja tietoturvallisuuden tason mahdollisen nostamisen aiheuttamat kustannukset viranomaisille. Nämä investoinnit ovat vähintään useita kymmeniä miljoonia euroja, ehkä jopa 50 – 100 milj. euroa. Tietoturvallisuuden tason nostamisen vaatimasta ajasta ja kustannuksista on aiempaa kokemusta julkisen hallinnon turvallisuusverkkohankkeesta. Korkean turvallisuuden ja varautumisen tehtäviin tarkoitettujen tieto- ja viestintäteknisten palvelujen toteuttamisen toteutuneet kustannukset olivat noin 200 miljoonaa euroa ja vuonna 2007 käynnistynyt toimeenpano kesti noin kymmenen vuotta.

Valtion yhteisten tietoteknisten palvelujen lisäksi julkisessa hallinnossa on useita tuhansia muita tietoteknisiä palveluita, joiden vaatimustenmukaisuutta on myös arvioitava. Valtiokonttorin 2020 julkaiseman luettelon perusteella valtion kirjanpitoyksiköksi luokiteltuja ministeriöitä, virastoja ja laitoksia on 65 kpl. Niiden tietoteknisten palvelujen määrää ei tarkasti tunneta. Valtion tietoteknisten palvelujen lisäksi liikelaitoksissa, kunnissa, kuntayhtymissä ja kuntien omistamissa yrityksissä on

myös useita tuhansia tietoteknisiä palveluja. Jos julkisen hallinnon kaikkien tietoteknisten palvelujen vaatimustenmukaisuuden arviointiin arvioidaan tarvittavan myös noin 40 – 80 htp:ää asiantuntijahenkilöstön työpanosta jokaista arvioitavaa palvelua kohti, olisivat yhteensä tarvittavan asiantuntijatyön määrä ja siitä johtuvat kustannukset huomattavia. Esimerkiksi tuhannen tietoteknisen palvelun arviointi vaatisi 40 000 htp eli 200 htv, mikä on noin 18 miljoonaa euroa.

Toisaalta kehittämistoimenpiteiden toteuttamisen arvioidaan mahdollistavan arviointitoiminnan laajentumisen ja syvenemisen, minkä avulla julkisen hallinnon sekä koko yhteiskunnan digitaalisen turvallisuuden tilan voidaan olettaa parantuvan. Tämän ennakoidaan vähentävän tietoturvallisuuden häiriötilanteista ja niiden varsinaiselle toiminnalle aiheuttamista katkoksista tai jopa datan menetyksistä aiheutuvia kustannuksia. Lisäksi digitaaliselle turvallisuudelle asetettujen vaatimusten täsmentymisen ja niiden toteutumisen arvioinnin ja seuraamisen tehostumisen arvioidaan tehostavan toimintaa ennakoivasti erityisesti tietoteknisten palvelujen suunnittelu- ja toteutusvaiheissa, jolloin tietoteknisten palvelujen elinkaarien aikaiset kustannukset mukaan lukien arviointitoiminnan kustannukset ja sen johdosta tehtävien korjaustoimenpiteiden kustannukset laskisivat.

1 SELVITYKSEN TAUSTA

1.1 Selvityksen lähtökohdat

Valtioneuvosto teki 8.4.2020 periaatepäätöksen julkisen hallinnon digitaalisesta turvallisuudesta (VM 2020:33). Sen mukaisesti digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaa, toiminnan jatkuvuuden hallintaa ja varautumista sekä kyberturvallisuutta, tietoturvallisuutta ja tietosuojaa.

Valtioneuvoston periaatepäätöksen 8.4.2020 linjauksia toteuttaa Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020-2023 (Haukka) (VM 2020:33). Sen yhtenä tehtävänä on julkisen hallinnon palveluiden ja palvelutuotannon digitaalisen turvallisuuden arviointi. Tehtävään kuuluvat seuraavat osa-alueet:

1) Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista annetun lain (1046/2011) sekä tietoturvallisuuden arviointilaitoksista annetun lain (1045/2011) (jatkossa yhteisesti arviointilait) mahdolliset uudistamistarpeet selvitetään ja johtopäätösten perusteella toteutetaan mahdollinen säädösvalmistelu.

    - Valtiovarainministeriö yhdessä liikenne- ja viestintäministeriön sekä Liikenne- ja viestintäviraston (jäljempänä Traficomin) ja muiden ministeriöiden ja mahdollisesti kuntien kanssa selvittävät nykytilan ja uudistamistarpeet vuonna 2021.

    - Johtopäätösten perusteella lainvalmistelu 2021–2022. Mahdolliset uudet lakiehdotukset eduskuntaan alkusyksystä 2022.

2) Arvioidaan digitaalisten palveluiden ja infrastruktuurin varautumisen ja valmiuden vaatimuksiin ja niiden arviointimenettelyyn liittyvät sääntelytarpeet ja toteutetaan mahdollinen säädösvalmistelu.

Uudistamis- ja sääntelytarpeiden selvitystehtäviä toteuttaa valtiovarainministeriön Haukka-hankkeessa toimiva valmisteluryhmä. Tehtäviä tukemaan valtiovarainministeriön julkisen hallinnon ICT-osasto asetti säädösvalmistelun koordinaatioryhmän kaudelle 1.9.2020 – 31.12.2021. Valmisteluryhmän ja koordinaatioryhmän jäsenet on lueteltu liitteessä 1. Selvitysraporttia on käsitelty koordinaatioryhmän kokouksissa. Selvitysraportin tarkoituksena on tukea varsinaista digitaalisen turvallisuuden arvioinnin kehittämisen säädösvalmistelutyötä. Selvitysraportissa kuvataan julkisen hallinnon digitaalisen turvallisuuden arvioinnin tunnistettuja haasteita ja esitetään näitä korjaavia kehitystoimenpiteitä. Tehtävään liittyviä säännöksiä ja ohjeita on lueteltu liitteessä 2.

1.2 Työn toteutus

1.2.1 Haastattelut ja työpajat

Työ toteutettiin järjestämällä Haukka-säädösvalmistelun koordinaatioryhmän työpaja 11.11.2020 sekä haastattelemalla arviointeja teettäviä virastojen, Traficomin, kaupallisten arviointilaitosten ja arviointien kohteina olevien palveluntarjoajien edustajia. Haastattelijoina toimi valtiovarainministeriön Haukka-valmisteluryhmä. Haastatteluissa kartoitettiin digitaalisen turvallisuuden arviointiin liittyviä mahdollisia kehitystarpeita, digitaalisen turvallisuuden vaatimusten asettamista, digitaalisen infrastruktuurin arviointitoimintaa sekä älykkäiden ja oppivien järjestelmien arviointiin liittyviä näkökohtia. Lisäksi haastatteluissa koottiin näkemyksiä arviointitoiminnalla saavutettavista hyödyistä nykytilanteessa Haastattelut toteutettiin joulukuun 2020 ja tammikuun 2021 aikana ja niitä tehtiin yhteensä 23. Haastattelujen aikataulu ja haastatellut organisaatiot ovat liitteenä 3. Haastatteluissa tai työpajoissa ei käsitelty erilaisten vaatimusmäärittelyjen yksityiskohtaisia sisältöjä ts. mitä yksityiskohtaisia tai teknisiä vaatimuksia digitaalisen turvallisuuden osa-alueille tulisi asettaa, vaan vaatimuksia ja kehitystarpeita käsiteltiin yleisellä tasolla.

Haastattelujen jälkeen arviointitoiminnan nykytilan kuvauksia tarkennettiin valtiovarainministeriön, Traficomin ja FINASin välisissä keskusteluissa, joihin osallistui Traficomissa arviointitoimintaa suorittavia henkilöitä. Haukka-säädösvalmistelun koordinaatioryhmän näkemyksiä kuultiin koordinaatioryhmän kokouksissa. Koordinaatioryhmän jäsenten aloitteesta selvityksen aikana sen ulkopuolelle rajattiin kansainvälisistä tietoturvavelvoitteista annetun lain (588/2004) asiat.

1.3 Määritelmistä

Tässä raportissa käytetään termiä ”hyväksytty arviointilaitos”, kun viitataan nykyisen lainsäädännön mukaiseen toimijaan, joka on hyväksytty arviointilaitoslain (1405/2011 3-5 §§) mukaisessa menettelyssä. Termi ”akkreditoitu arviointilaitos” viittaa tässä raportissa arviointilaitokseen, joka on onnistuneesti läpäissyt pätevyyden arvioinnin tavoitetilassa ehdotetun uuden mallin mukaisesti. Tavoitetilassa kansallinen akkreditointiyksikkö (FINAS) vastaa ennalta asetetun kriteeristön mukaisesti tapahtuvasta arviointilaitoksen toiminnan vaatimustenmukaisuuden arvioinnista sekä yleisten että toimialakohtaisten vaatimusten osalta. FINAS voi käyttää tukena muita viranomaisia.

Akkreditointi tarkoittaa tässä raportissa arviointilaitoksen pätevyyden toteamista yhdenmukaisten kansainvälisten tai eurooppalaisten arviointiperusteiden mukaisesti (vrt. 920/2005 4.1 § 4 k).

Arviointi tarkoittaa tässä raportissa riippumattoman osapuolen vahvistusta palvelun, tuotteen, prosessin tai järjestelmän vaatimustenmukaisuudesta (vrt. 920/2005 4.1 § 9 k).

Akkreditoidun arviointilaitoksen suorittamaa vaatimustenmukaisuuden arviointia voi seurata vaatimustenmukaisuustodistuksen antaminen, jos arviointilaitoksen näkemys on se, että asetetut vaatimukset täyttyvät.

Termillä ”vaatimus” on tässä raportissa kaksi merkitystä. Sillä voidaan tarkoittaa lainsäädännön asettamia vaatimuksia tai määräyksissä, ohjeissa tai standardeissa esitettyjä vaatimuksia. Asiayhteydestä

tulisi ilmetä kummasta on kyse, mutta tarvittaessa on käytetty tarkennuksia, kuten ”tiedonhallinta la in vaatimus” tai ”standardin vaatimus”.

2 YHTEENVETO ARVIOINTITOIMINNAN NYKYTILASTA

2.1 Arviointitoiminnan toimivalta

NLF-asetuksessa (765/2008)2 vahvistetaan vaatimustenmukaisuuden arviointilaitosten akkreditointia koskevat säännöt sekä akkreditointielimiä koskevat vaatimukset. FINAS on NLF-asetuksessa tarkoitettu Suomen ainoa kansallinen akkreditointielin. NLF-pakettiin liittyvä sääntely (NLF-asetus ja -päätös sekä pakettiin kuuluvat tuotedirektiivisäännökset) lähtee yksiselitteisesti siitä, etteivät kansalliset akkreditointielimet tai ilmoittamisesta vastaavat toimivaltaiset viranomaiset (jollainen myös Traficom on esim. radiolaitteiden ja ilmailulaitteiden osalta) saa olla mukana arviointilaitostoiminnassa. Kansalliset akkreditointielimet eivät saa kilpailla vaatimustenmukaisuuden arviointilaitosten kanssa eikä ilmoittamisesta vastaava toimivaltainen viranomainen saa tarjota tai suorittaa mitään toimintoja, joita vaatimustenmukaisuuden arviointilaitokset tekevät. Kansallisen turvallisuuden piiriin kuuluvat asiat eivät ole NLF-asetuksen piirissä, joten se ei koske kansallisen turvallisuuden piiriin liittyvää arviointitoimintaa eli turvallisuusluokiteltua tietoa käsittelevien kohteiden arviointia.

Vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annettua lakia (920/2005) eli akkreditointilakia sovelletaan vaatimustenmukaisuuden arviointipalvelujen akkreditointiin ja siihen rinnastettavaan pätevyyden arviointiin. Lain mukaan akkreditoinnilla tarkoitetaan ”*pätevyyden toteamista yhdenmukaisten kansainvälisten tai eurooppalaisten arviointiperusteiden mukaisesti;”*. Lain 6 §:n mukaan ”*akkreditointiin sovelletaan yhdenmukaisia kansainvälisiä ja eurooppalaisia arviointiperusteita*”.

Tietoturvallisuuden arviointitoiminnan toimivaltaisia viranomaisia ovat valtiovarainministeriö ja Traficom. Valtiovarainministeriö voi pyytää Traficomia laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi sekä niiden kehittämiseksi. Traficomin tehtäviin kuuluvat mm. viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen arviointi, hyväksymistodistuksen antaminen sekä yleistä tietoturvallisuuden tasoa koskevien selvitysten tekeminen valtionhallinnon viranomaisen tietojärjestelmistä tai tietoliikennejärjestelyistä (1406/2011 4 §). Traficom hyväksyy tietoturvallisuuden arviointilaitokset (1405/2011), joita valtionhallinnon viranomaiset voivat käyttää arviointien toteuttamiseksi (1406/2011 3 §). Traficomin tehtäviä ovat myös kansainvälisiä turvallisuusluokiteltuja tietoja käsittelevien tietojärjestelmien arvioinnit ja hyväksynnät, yritysturvallisuusselvityksiin liittyvät kansalliset ja kansainväliset tietojärjestelmäarvioinnit sekä turvallisuusluokitellun tiedon suojaamiseen käytettävien tuotteiden tuoteturvallisuuden arvioinnit ja hyväksynnät.

Kansainvälisten tietoturvavelvoitteiden vastuista on säädetty kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004). Ulkoministeriö toimii kansainvälisten tietoturvavelvoitteiden toteuttamisessa kansallisena turvallisuusviranomaisena ja Traficom tietojärjestelmien ja tietoliikennejärjes-

[2] Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (ns. NLF-asetus)

telyjen tietoturvallisuutta koskevissa asioissa lain tarkoittamana määrättynä turvallisuusviranomaisena. Muita määrättyjä turvallisuusviranomaisia ovat puolustusministeriö, pääesikunta ja suojelupoliisi, jotka ”*toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa*” (588/2004 4 §).

Tietojärjestelmien tietoturvallisuuden arviointi yritysturvallisuusselvityksissä perustuu turvallisuusselvityslakiin (726/2014). Sen mukaisesti Traficom laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen (726/2014, 9 §).

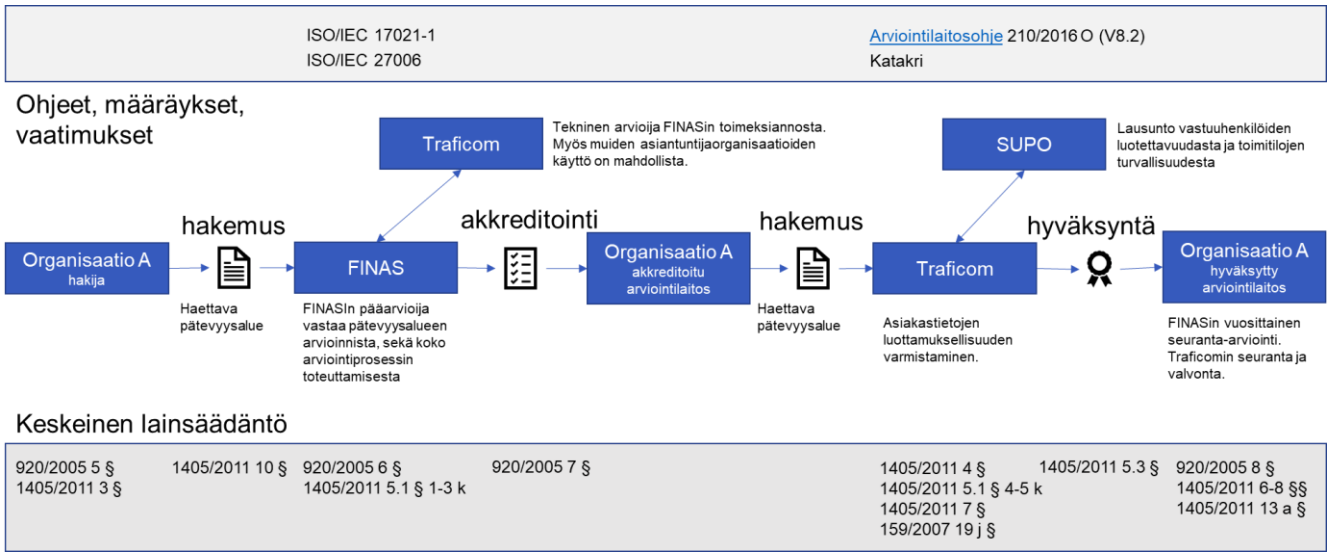
EU:n yleisessä tietosuoja-asetuksessa (EU 2016/679) säädetään sertifiointielimistä. Tietosuojalaissa (1050/2018 14.4 §) on kansalliselle tietosuojavaltuutetulle annettu tehtäväksi tietosuojan arviointitoimijoiden akkreditointi. EU:n tietosuoja-asetuksessa on myös vaihtoehtoisia menettelyjä. Tietosuojavaltuutetun tekemä akkreditointi ei ole rinnastettavissa NLF-asetuksessa (765/2008) mainittuun kansallisen akkreditointielimen akkreditointiin. NLF-asetuksessa mainitaan, että jokaisessa EU:n jäsenvaltiossa voi olla ainoastaan yksi kansallinen akkreditointielin. FINASin näkemyksen mukaan tietosuojan arviointitoimijoiden akkreditoinnissa tulisi Suomessa edetä akkreditointilain (920/2005) määrittelemällä tavalla. Tähän liittyen Traficom on tähdentänyt, että NLF-asetus ei koske kansallisen turvallisuuden piiriin liittyvää arviointitoimintaa, ja siten yllä olevat havainnot eivät päde tällaiseen arviointitoimintaan. Toisaalta on syytä kuitenkin huomata, että kansallisen turvallisuuden ylläpitämisen yhteydessä tapahtuva henkilötietojen käsittely kuuluu rikosasioiden tietosuojalain (1054/2018) piiriin eikä tietosuoja-asetusta siten sovelleta tähän.

Tietosuojan vaatimusmäärittelyn toteutumista tekeviä arviointilaitoksia ei ole vielä hyväksytty. Tietosuojan arviointi- ja hyväksymismenettelyissä ei ole EU-tason sääntelyn takia merkittävästi kansallista liikkumavaraa. Tehtyjen haastattelujen perusteella EU:n yleisen tietosuoja-asetuksen aiheuttaman kehitysryöpyn jälkeen tietosuojan parantaminen erityisesti yksityisellä sektorilla on osittain hiipunut, koska vaatimusmäärittelyjä ei ole. ISO 27701 on ISO 27001 -standardin laajennus henkilötietojen käsittelyn suojaamiseksi. Organisaatiot voivat sertifioida tietoturvallisuuden hallintajärjestelmänsä ko. standardin mukaisesti, mutta sertifiointi ei riitä osoittamaan yleisen tietosuoja-asetuksen vaatimusten täyttymistä palveluissa eikä pelkästään sen perusteella saada varmuutta palveluiden tietosuojan riittävyydestä tai teknisen toteutuksen tasosta.

Arviointilain (1406/2011) soveltamisala on rajattu viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiin. Arviointilaitoslakia (1405/2011) sovelletaan ”*elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason (tietoturvallisuuden arviointilaitos) ja jotka haluavat toiminnalleen Viestintäviraston* [nyk. Traficom] *hyväksynnän*” sekä arviointilaitosten hyväksymismenettelyyn (1405/2011 2 §). Tietoturvallisuudella tarkoitetaan luottamuksellisuuden, saatavuuden ja eheyden varmistamista (ks. liite 4). Tietoturvallisuuden katsotaan tässä yhteydessä olevan yksi digitaalisen turvallisuuden osa, joten arviointilain näkökulmaa voisi laajentaa. Lisäksi arviointilain mukainen arviointitoiminta kohdistuu vain tietojärjestelmiin ja tietoliikennejärjestelyihin digitaalisten palvelujen kokonaisvaltaisen turvallisuuden sijaan. Haastatteluissa myös todettiin, että viranomaisen fyysisen turvallisuuden arviointitehtävää ei ole säädetty yhdellekään viranomaiselle.

2.2 Arviointilaitoksen akkreditointi, hyväksyntä ja seuranta

Arviointilaitoslain (1405/2011) 5 §:n mukaisesti tietoturvallisuuden arviointilaitoksen hyväksyntäprosessi on kaksivaiheinen ja se on esitetty kuvassa 1. Ensimmäisessä vaiheessa FINAS arvioi hakijan kyvyn toimia tietoturvallisuuden arviointilaitoksena (5.1 § 1-3 k) ja akkreditoi vaatimukset täyttävän hakijan. Osana akkreditointia on hakijan teknisen toiminnan pätevyyden arviointi, jossa FINAS voi käyttää toimeksiannon perusteella ulkopuolista toimijaa. Käytännössä teknisen toiminnan arvioinnissa ja näyttöauditointien tukena toimii Traficom, mutta myös muita toimijoita voisi käyttää, kunhan niillä on riittävä osaaminen. FINASin pääarvioija kuitenkin vastaa koko arviointiprosessin toteuttamisesta tukeutuen teknisen arvioijan tekemään arviointiin.



Kuva 1. Arviointilaitoksen akkreditointi- ja hyväksyntäprosessi.

Toisessa vaiheessa akkreditoitu arviointilaitos hakee Traficomilta hyväksynnän (5.1 § 4-5 k) valitsemilleen pätevyysalueille. Traficomin suorittaman arvioinnin vaatimukset vastuuhenkilöiden luotettavuudesta, hakijan menettelytavoista ja ohjeista sekä pätevyysalueista ja niille asetetuista vaatimuksista perustuvat arviointilaitoslakeihin. Nykytilassa arviointilaitoslain nojalla suojelupoliisille varataan tilaisuus lausua arviointilaitoksen vastuuhenkilöiden luotettavuudesta ja sen toimitilojen turvallisuudesta. Toisen vaiheen keskeisenä tavoitteena on varmistaa, että arviointilaitoksen oma tietoturvallisuus on riittävällä tasolla, jotta arviointilaitosten asiakkaiden turvallisuusluokitellut tiedot eivät vaarantuisi. Arviointilaitosten oman tietojenkäsittelyn turvallisuutta arvioidaan suhteessa turvallisuusluokitellun tiedon suojaamiselle asetettuihin lakisääteisiin velvoitteisiin (2020 alusta lukien tiedonhallintalaki, 906/2019 sekä turvallisuusluokitteluasetus, 1101/2019). Lakisääteisten velvoitteiden täyttymisen arvioinnissa hyödynnetään työkaluna Katakria, johon on koottu keskeiset kansallisen turvallisuusluokitellun tiedon suojaamiseen kohdistuvat vaatimukset. Traficom myöntää organisaatiolle hyväksytyn arviointilaitoksen aseman, kun hakija täyttää arvioinnin vaatimukset.

NLF-asetuksen (765/2008) 4 artiklassa asetetaan kansallisia akkreditointielimiä koskevat vaatimukset, joihin muun muassa kuuluu, että akkreditointielimen velvollisuudet ja tehtävät on erotettava selkeästi muiden kansallisten viranomaisten velvollisuuksista ja tehtävistä. NLF-asetuksessa säädetään muistakin akkreditointielintä ja sen toimintaa koskevista vaatimuksista kuten siitä, että kansallisen

akkreditointielimen toiminnan on turvattava toimintansa objektiivisuus ja puolueettomuus. Traficom täsmentää, että NLF-asetusta ei sovelleta kansalliseen turvallisuuteen liittyvään arviointitoimintaan.

Akkreditointilain mukaisesti arviointiperusteiden käyttöönotosta päättää akkreditointiyksikkö kuultuaan akkreditointijärjestelmän ja vaatimustenmukaisuuden arviointipalvelujen kannalta keskeisiä tahoja. Suomen akkreditointiyksikkönä toimivan FINASin suorittama tietoturvallisuuden arviointilaitosten akkreditointi perustuu yleisesti saatavilla oleviin, kansainvälisesti vahvistettuihin standardeihin.[3] Nämä kansainväliset standardit eivät ota kantaa viranomaisten turvallisuusluokitellun tiedon arvioinnin erityispiirteisiin, vaan painottavat tietoturvallisuuden hallintajärjestelmän näkökulmaa. Tilanteissa, joissa hakija hakee FINASilta akkreditointia turvallisuusluokitellun tiedon arviointiin (ns. Katakri/VAHTI -pätevyys), FINASin hallinnoimaan prosessiin sisältyy Traficomin antamassa arviointilaitosohjeessa (Ohje tietoturvallisuuden arviointilaitoksille, 210/2016 O, päivitetty 18.12.2020) määritellyn turvallisuusluokitellun tiedon arvioinnin pätevyyden arviointi. Kansainvälisissä standardeissa ei huomioida myöskään kansallisen lainsäädännön erityispiirteitä, esimerkiksi turvallisuusluokitellun tiedon suojaamiseen kohdistuvia vaatimuksia, jotka huomioidaan Traficomin suorittamassa arviointilaitosten hyväksyntäprosessin toisessa vaiheessa.

Nykytilanteen eräänä haasteena on, että nykyisten arviointilaitosten osaamisalueet eivät täysin vastaa viranomaisarvioinnilta eli viranomaisen/Traficomin tekemältä arvioinnilta vaadittavaa sisältöä, ja arviointilaitosten pätevyysalueita on jouduttu hyväksymään osittaisina. Arviointilaitosten pätevyysalueet eivät kata esimerkiksi salausratkaisujen, yhdyskäytäväratkaisujen tai hajasäteilysuojausten riittävyyden arviointia kuin osittaisina ja rajauksin.

Arviointilain ja arviointilaitoslain muotoilut Traficomin ja hyväksyttyjen arviointilaitosten vastuista ja velvollisuuksista koetaan haastattelujen perusteella tulkinnanvaraisiksi. Ajan myötä tilanne on osittain vakiintunut ja toimivaltasuhteet koetaan nykytilanteessa melko selkeiksi. Hyväksyntäprosessin eteneminen on kuvattu Traficomin ohjeessa 210/2016 O. Prosessin monivaiheisuus ja haastatteluissa esiin nostettu vaatimusten tulkinnanvaraisuus ovat johtaneet siihen, että hakuprosessi kestää kauan; vastausten saaminen sähköpostilla esitettyihin kysymyksiin voi kestää useita kuukausia. Haastatteluissa todettiin, että prosessin monimutkaisuuden ja pitkän keston takia markkinoille ei ole tullut uusia arviointilaitoksia. Arviointilaitosten akkreditointiprosessissa on havaittu, että keskeisin este arviointilaitosten akkreditoinnille turvallisuusluokitellun tiedon arviointiin on ollut se, että hakijalla ei ole prosessin alkuvaiheessa ollut riittävää ymmärrystä edellytettävästä osaamisesta ja tällaisen osaamisen hankkiminen (henkilöstö, laitteistot, ohjelmistot) on osoittautunut kaupallisilla toimijoilla aikaa vieväksi.

Traficomin kansainvälistä tietojärjestelmien arviointi- ja hyväksyntätoimintaa valvoo nykytilassa säännöllisesti kaksi kansainvälistä viranomaisyhteisöä. Esimerkiksi EU:n säännöllisesti toteuttamilla tarkastuskäynneillä arvioidaan sekä EU:n turvallisuusluokitellun tiedon käsittelyyn hyväksyttyjen tietojärjestelmien suojauksia suhteessa EU:n turvallisuussääntöön myös Suomessa että Traficomin Kyberturvallisuuskeskuksessa arviointiin käytettäviä menettelyjä. Traficom osallistuu säännöllisesti eri maiden hyväksyntäviranomaisista (SAA, Security Accreditation Authority, Suomessa Traficomin

[3] Päätös P1/2018 11.6.2018 (FINAS)

NCSA-toiminto) koostuviin yhteistyöelimiin, joissa eri maiden toimintaa peilataan ja parhaita käytäntöjä jaetaan viranomaistoimijoiden kesken vapaamuotoisemmin. Traficom ei näe perustelluksi lisätä kansalliseen valtionhallintoon enää päällekkäistä arviointitoiminnan valvontaa.

Kaupallisten arviointilaitosten hyväksyntämenettelyn yhtenä alkuperäisenä tavoitteena oli tarjota yrityksille mahdollisuus saada luotettava arvio omien toimiensa tietoturvallisuuden tasosta ja näin hyväksyttyjen arviointilaitosten yritysasiakkaiden on ollut mahdollista johdonmukaisesti varautua sellaisia tilanteita varten, joissa niiden tietoturvallisuuden taso on hankintakilpailussa menestymisen ehdoton edellytys, kuten puolustus- ja turvallisuusalan kansainvälisissä ja kansallisissa hankinnoissa tai yhteistyöhankkeissa (ks. HE 45/2011 vp, 1 §:n yksityiskohtaiset perustelut). Toisaalta nykyään asiakastietolaissa (159/2007) ja toisiolaissa (552/2019) on säädetty hyväksytyille tietoturvallisuuden arviointilaitoksille arviointitehtäviä, joita vain ne voivat tehdä.

Nykyisissä säädöksissä ei ole varauduttu tilanteeseen, jossa arviointilaitoksena toimivan yrityksen toiminta muuttuu esimerkiksi yritysoston tai toiminnan lakkaamisen kautta, jolloin arviointitoiminnassa kertyneet tiedot saattavat päätyä ennalta suunnittelemattomille tahoille. Vertailun vuoksi todettakoon, että eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista annetussa laissa (278/2016) vastaavaan asiaan on varauduttu lain 6 §:n 4 momentin säännöksellä. Sen mukaan: ”*Jos ilmoitettu laitos on lopettanut toimintansa tai sen hyväksyminen on peruutettu, on toimivaltaisen viranomaisen ryhdyttävä asianmukaisiin toimenpiteisiin sen varmistamiseksi, että laitoksen asiakirjat käsittelee toinen ilmoitettu laitos tai ne pidetään ilmoittamisesta ja markkinavalvonnasta vastaavien viranomaisten pyynnöstä näiden nähtävillä.*”

2.3 Arviointilaitosten pätevyysalueet ja niiden arviointi

Traficom pitää yllä listaa hyväksymistään arviointilaitoksista. Hyväksytty arviointilaitos voi tehdä tietoturvallisuuden arviointeja Traficomin myöntämän pätevyysalueen puitteissa. Tietoturvallisuuden arviointilaitoksille hyväksytyt pätevyysalueet ovat tällä hetkellä VAHTI, Katakri TL IV, Katakri TL III sekä ISO27001. VAHTI-pätevyys perustuu kumottuun tietoturvallisuusasetukseen (681/2010) ja sen sisältämien tietoturvatasojen yksityiskohtaiset kuvaukset sisältämään VAHTI-ohjeeseen 2/2010. VAHTI-arviointi ”*kattaa VAHTI-ohjeissa 2/2010, 3/2010, 3/2012, 1/2013, 2/2013 ja 5/2013 kuvatut vaatimukset soveltuvin osin*.”[4] FINASin akkreditointi edellyttää, että arviointilaitoksella on oltava ISO27001 yhtenä pätevyysalueenaan, vaikka arviointilaitoksella olisi tarve vain Katakri-/VAHTI-pätevyydelle. Jos arviointilaitoksella on pätevyysalueenaan VAHTI tai Katakri, se saa automaattisesti oikeuden tehdä asiakastietolain (159/2007 19 k §) mukaisia A-luokan tietojärjestelmien tietoturvallisuuden arviointeja.

Arviointilaitoksille ei ole myönnetty korkeimpien tietoturvallisuusluokkien pätevyysalueita. Tällä hetkellä hyväksyttyjä arviointilaitoksia on kolme, joista kahdella on pätevyysalueena turvallisuusluokan IV ja III tietoja käsittelevien järjestelmien arviointi (ns. Katakri-pätevyys). Arviointilaitos voi VAHTI- tai Katakri-pätevyyden saatuaan tehdä tietoturvallisuuden arviointeja sosiaali- ja terveyden-

4 Traficom Arviointilaitosohje 210/2016 O (V8.2) kappale 3.2.1

huollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007, *asiakastietolaki*) kuvatuille A-luokan järjestelmille[5] sekä sosiaali- ja terveystietojen toissijaisesta käytöstä annetussa laissa (552/2009, *toisiolaki*) kuvatuille käyttöympäristöille[6].

Pätevyysalueen hyväksyntä perustuu arviointilaitoslakiin ja lakiin vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta. Traficomin ohjeessa on täsmennetty arviointilaitokseksi hakeutumisen menettelyä. Traficomin ohjeessa (210/2016 O V8.2) arviointilaitoksen edellytetään täyttävän lakisääteiset turvallisuusluokiteltuun tietoon kohdistuvat suojausvaatimukset, joiden täyttymisen arviointiin hyödynnetään työkaluna Katakria yhtä tasoa ylempää kuin mille hakija hakee hyväksyntää. Tämä johtuu siitä, että arviointilaitoksen tulee kyetä käsittelemään loppuasiakkaansa luokittelemaa tietoa sille asetettujen suojausvaatimusten mukaisesti. Arviointilaitoksen arvioidessa esimerkiksi loppuasiakkaansa TL IV-tason järjestelmää, saa arviointilaitos arviointiprosessin aikana asiakkaansa luokittelemaa ko. järjestelmää koskevaa tietoa (esimerkiksi verkkokuvat ja tiedot kytkennöistä muihin järjestelmiin). Järjestelmien turvallisuustoteutuksiin liittyvät tiedot luokitellaan eräissä tapauksissa luokkaa korkeammalle kuin korkein järjestelmässä käsiteltävä tieto. Myös eri loppuasiakkaiden tiedoista koostuvan tietovarannon turvallisuusluokka on kasautumisvaikutusten takia usein tulkittavissa yksittäisten tietojen turvallisuusluokkaa korkeammaksi.

Arviointilaitoksilla on mahdollisuus sisällyttää tietojenkäsittely-ympäristökseen eri luokille soveltuvia ympäristöjä, esim. TL IV, TL III tai TL II, ja toteuttaa tietojenkäsittely luokittain ko. ympäristöissä. Loppuasiakkaan luokiteltujen tietojen suojaamisen takia arviointilaitoksen on toteutettava Katakrin TL III -tason vaatimukset, jos haettavana pätevyysalueena on ainoastaan ISO27001. On kuitenkin huomattava, ettei Katakri ole vaatimusluettelo, vaan ”*tietoturvallisuuden auditointityökalu, jota voidaan käyttää arvioitaessa kohdeorganisaation kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa*.” (Katakri 2020 s. 5). Katakria käytetäänkin arviointilaitosten hyväksyntäprosessissa käyttötarkoituksensa mukaisesti arviointilaitoksen tiedonsuojaamiskyvykkyyden arviointiin.

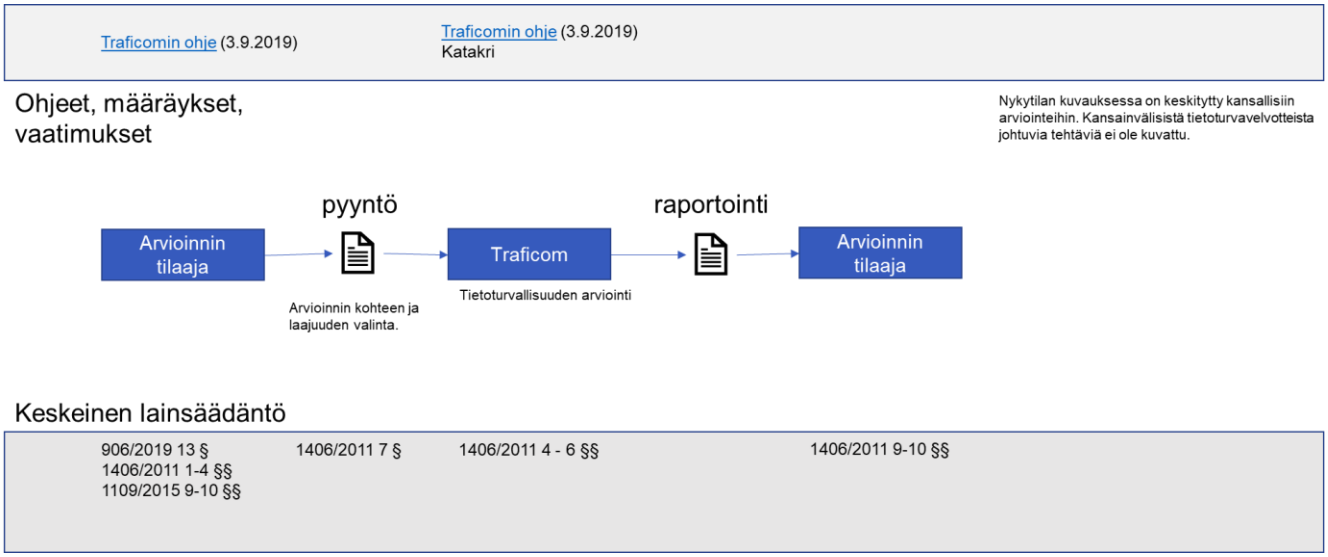
2.4 Arviointitoiminta

Viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn vaatimustenmukaisuuden arviointi tehdään toimeksiannosta, jonka voi tehdä viranomaisen lisäksi se, joka tekee hankintoja viranomaisen lukuun, tuottaa viranomaiselle tietojenkäsittely- tai tietoliikennepalveluja tai hoitaa em. palvelujen järjestämiseen liittyviä palvelutehtäviä (1406/2011 4 §). Arvioinnin voi tehdä arviointilain mukaan Traficom tai hyväksytty arviointilaitos sille hyväksytyn pätevyysalueen mukaisesti. Traficomin suorittama tietoturvallisuuden arviointiprosessi on esitetty kuvassa 2 ja arviointilaitoksen prosessi on kuvassa 3.

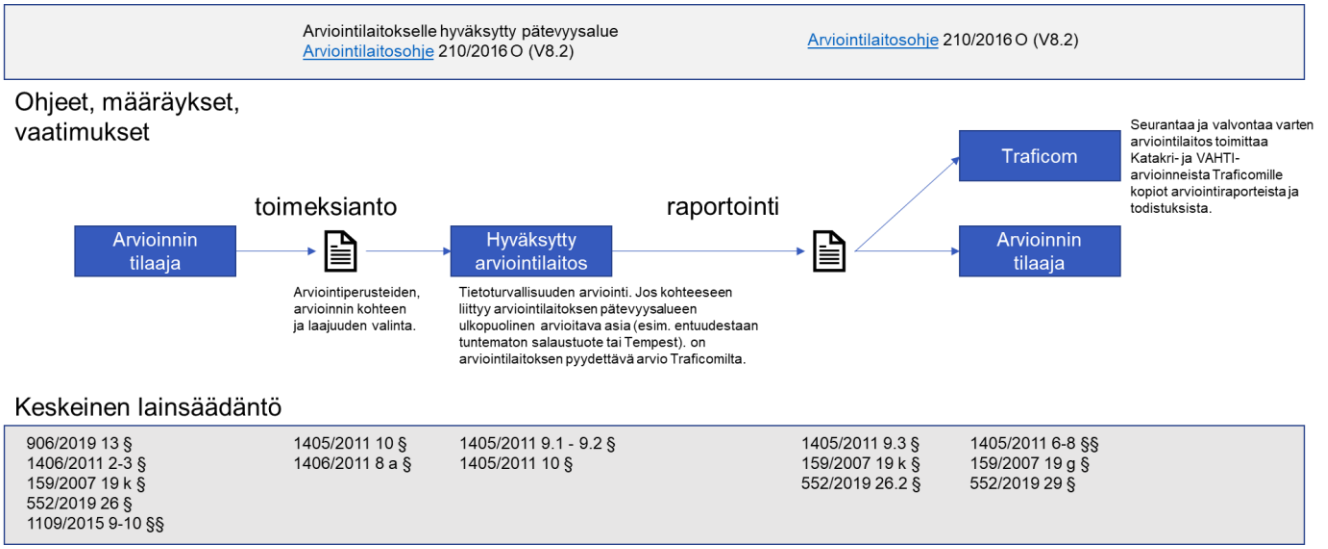
Ainoastaan Traficom voi arviointilaitosten nykyisten pätevyysalueiden takia tehdä korkeimpien turvaluokkien järjestelmien (TL II ja TL I) arviointeja. Se voi kuitenkin tehdä arviointeja myös turvaluokkien TL IV ja TL III tietojärjestelmistä tai tietoliikennejärjestelyistä. Arviointilaitoslain valmis-

[5] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007 19k
[6] Laki sosiaali- ja terveystietojen toissijaisesta käytöstä 552/2019 26 §

telun yhteydessä todettiin, että valtiovarainministeriön ja liikenne- ja viestintäministeriön tulisi yhdessä ohjata Traficomin arviointitoimintaa. Arviointilain perusteluissa todetaan mm., että Traficomin ”*tulosohjausta lakiehdotuksen mukaisissa uusissa tehtävissä on tarkoitus toteuttaa valtiovarainministeriön ja liikenne- ja viestintäministeriön tiiviinä yhteistyönä*”[7].



Kuva 2. Traficomin suorittaman tietoturvallisuuden arvioinnin prosessi.



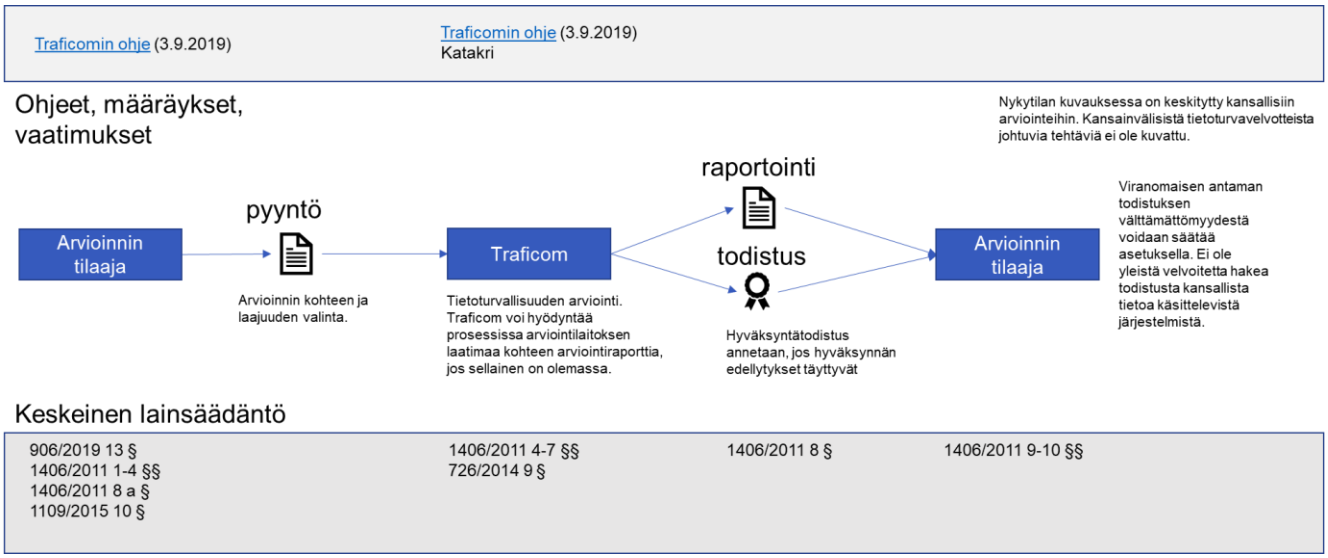
Kuva 3. Arviointilaitoksen suorittaman tietoturvallisuuden arvioinnin prosessi.

Turvaluokkien TL IV ja TL III tietojärjestelmien ja tietoliikennejärjestelyjen arviointien alueella Traficom toimii samoilla markkinoilla kaupallisten toimijoiden kanssa, mutta hinnoittelee palvelunsa maksuperustelain mukaisesti (1406/2011 12 §). Toisaalta kaupallisilla toimijoilla on käytössään enemmän resursseja arviointien tekemiseksi ja niiden on viranomaista helpompi mukauttaa arviointihenkilöstönsä määrää tarvittaessa. Traficom on vuoden 2019 jälkeen tehnyt vain yksittäisiä arvioin-

[7] HE 45/2011

tilakiin perustuvia TL IV tason arviointeja ja on keskittynyt korkeampien turvallisuusluokkien käsittely-ympäristöjen arviointeihin. Arviointilaitokset tekevät vuosittain useita kymmeniä TL IV tai TL III tason arviointeja.

Arviointilaitoksen on annettava tekemästään arvioinnista todistus, jos kaikki vaaditut arviointiperusteena käytetyt vaatimukset täyttyvät (1405/2011 9.3 §). Traficom voi pyynnöstä myöntää todistuksen/viranomaishyväksynnän tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden vaatimustenmukaisuudesta (1406/2011 8 §). Traficomin tekemästä hyväksynnästä käytetään Traficomin arviointilaitosohjeessa (210/2016 O V8.2) nimeä "viranomaishyväksyntä" erotuksena kaupallisen arviointilaitoksen myöntämästä todistuksesta (vrt. 1045/2011 9.3 §). Traficomin suorittaman viranomaishyväksynnän prosessi on esitetty kuvassa 4.



Kuva 4. Traficomin suorittaman viranomaishyväksynnän prosessi.

Tyypillisesti kansallisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja teetetään hyväksytyillä arviointilaitoksilla siten, että arviointilaitos antaa arvioinnin tilaajalle arviointiraportin, ja tiedon omistava viranomainen arvioi jäännösriskit ja tekee omistamiaan tietoja koskevan erillishyväksynnän riskienhallintakäytäntöjensä sekä tiedonhallintalain 13 § mukaisesti. Kansallisille arvioinneille on vain harvoin haettu lisäksi arviointilaitoksen todistusta tai Traficomin todistusta/yleishyväksyntää/viranomaishyväksyntää. Asetuksella voidaan säätää, että valtionhallinnon viranomaisten on hankittava todistus tietojärjestelmistä tai tietoliikennejärjestelyistä, joissa käsitellään tietoja, joiden turvaluokka on TL I tai TL II (1406/2011 8 a). Tällaista asetusta ei ole annettu. Haastatteluissa todettiin, että on epäselvää, missä tilanteissa kansallisten tietojärjestelmien tai tietoliikennejärjestelyjen arviointien ja todistuksen hankkiminen on välttämätöntä. Arvioinnin ja hyväksynnän termit olivat haastatteluissa esitettyjen näkemysten perusteella epäselviä.

Haastattelujen perusteella todistusta suoritetusta arvioinnista ei haeta, koska sen saamiseen arvioidaan kuluvan liian kauan aikaa. Todistuksen hakemiselle ei toisaalta ehkä nähdä olevan tarvetta, sillä tiedonhallintalaki mahdollistaa viranomaisille tietoturvallisuustoimenpiteiden mitoittamisen kyseisen

[8] 210/2016 O V8.2 kappale 3.5

viranomaisen riskiarvioinnin mukaisesti (13 §). Kuitenkin erityisesti yhteisiä tieto- ja viestintäteknisten palveluja koskevia todistuksia palvelun tietoturvallisuuden tilasta olisi mahdollista laajemminkin hyödyntää siihen, että palveluja käyttävät tiedonhallintayksiköt voisivat helpommin arvioida palvelujen tietoturvallisuuden tasoa. Haastatteluissa esitettiin näkemys, että koska hyväksyntää ja siihen liittyvää todistusta tietoturvallisuuden tilasta ei ole saatavilla, on jokaisen tiedonhallintayksikön itse tehtävä päätös yhteisen palvelun käyttämiseen liittyvistä tietoturvallisuuden rajauksista. Tämä päätös joudutaan usein tekemään vajavaisin tiedoin tai puutteellisella osaamisella. Lisäksi on huomioitava, että yhteisten palvelujen tuottajien tilaamat arviointiraportit ovat käytännössä aina salassa pidettäviä ulkopuolisille, eikä tiedonhallintayksiköillä siten ole välttämättä tiedonsaantimahdollisuutta raportteihin.

Organisaatiot voivat toteuttaa itsearviointeja valitsemiensa arviointiperusteiden mukaisesti. Itsearvioinnin tuloksia voidaan käyttää digitaalisen turvallisuuden puutteiden ja kehityskohteiden tunnistamiseen, oman toiminnan kehittämiseen ja ulkopuolisen tekemään arviointiin valmistautumiseen. Itsearvioinnit kuuluvat esimerkiksi osaksi ISO27001-standardin vaatimuksia ja organisaatio voi käyttää itsearvioinnissa ulkopuolista apua.

Nykytilassa arviointilaitoksen suorittamissa Katakri-/VAHTI-arvioinneissa vaatimustenmukaisuuden todentamisessa edellytetään käytettävän useampaa lähdettä luotettavan tuloksen varmistamiseksi. Esimerkiksi päivityskäytäntöjen toteutus tulee todentaa vähintään henkilöstöä haastattelemalla, prosessikuvauksiin tai vastaaviin tutustumalla, päivitystason tutkinnalla järjestelmän "sisältä päin" eli esimerkiksi tarkastamalla turvapäivitysten asennusaikaleimat itse järjestelmästä sekä tekemällä kohteeseen ulkoa päin haavoittuvuusskannaus. Nykytilanteessa tietoturvallisuuden vaatimukset koetaan kuitenkin tulkinnanvaraisiksi. Sekä arviointilaitokset että palveluntuottajat ovat pyytäneet Traficomilta Katakri-kriteeristön tulkintoja. Traficomille ei kuitenkaan varsinaisesti ole säädetty ohjaus- tai kansallisten tietoturvallisuusvaatimusten valvontatoimivaltaa. Tulkinnat tehdään virkavastuulla ja ne ovat luonteeltaan yleisiä. Tulkintojen tekeminen voi edellyttää syvällistä tutkimustyötä esimerkiksi vasta markkinoille tulleen salaustuotteen lähdekoodiin, mikä voi joskus pidentää luotettavan linjauksen laadintaan tarvittavaa aikaa. Tulkinnat pyritään laatimaan myös hyvin aikaa kestäviksi, jotta ne eivät vanhentuisi esimerkiksi yksittäisen ohjelmistokirjaston päivittymisen myötä. Arviointilaitoksella tulee olla pätevyysalueensa mukainen osaaminen yksittäisissä arvioinneissa nousevien tulkintakysymysten ratkaisemiseksi. Haastatteluissa esitettiin, että keskeisenä haasteena taustalla on myös yksityiskohtaisempien ns. virallisten vaatimusmäärittelyjen puuttuminen. Tiedonhallintalautakunnan tehtävänä on ”*edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista*”[9]. Lautakunnan mahdollinen rooli arviointiperusteiden tulkintojen tai niihin liittyvien linjausten antajana ei käy haastattelujen perusteella ilmi Traficomin ohjeissa riittävän selkeästi.

Tietoturvallisuuden arviointi kohdistuu tällä hetkellä tietotekniseen järjestelmään, joka sisältää erilaisia teknisiä ratkaisuja. Digitaalisen toimintaympäristön ja teknologian nopean kehittymisen takia tehdyt ratkaisut (esimerkiksi salaustuotteiden uudet ratkaisut, käyttöjärjestelmien ja varusohjelmistojen uudet versiot) voivat muuttua arvioinnin aikana. Haastatellut henkilöt kertoivatkin, että arviointia saatetaan joutua tekemään osittain uudestaan, jos arviointi kestää pitkään. Tämän takia arviointeja

[9] https://vm.fi/tiedonhallintalautakunnan-tehtavat

tilaavat viranomaiset ja arviointilaitokset usein pyytävät Traficomilta tulkintoja ja linjauksia tietojärjestelmäturvallisuuden toteuttamisesta. Toimintaympäristön muutosten takia nämä arviointiperusteiden tulkintaa tai toteutusten teknisiä yksityiskohtia koskevat linjaukset ja tulkinnat ovat haastateltavien kertoman mukaan vain osin vakiintuneita. Haastatteluissa todettiin, että henkilöiden vaihtuvuuden takia tulkinnoissa on myös henkilöriippuvuutta ja että yksittäiset arvioinnit hidastuvat, kun Traficom ei anna tulkintasuosituksia riittävän nopeasti. Tulkintapyyntöjen on koettu hidastavan merkittävästi niin palvelujen tuottajien, arviointilaitosten kuin arviointeja tilaavien viranomaisten ja yhteisöjen toimintaa. Palvelujen tuottajille ja käyttäjille arviointien venyminen jopa vuoden mittaiseksi voi aiheuttaa kohtuuttomia haittoja. Haastattelussa esitettiin myös näkemys, jonka mukaan muuttuvien tulkintojen takia palveluntuottajat voivat joutua tekemään järjestelmiin merkittäviä teknisiä ja toiminnallisia muutoksia ja muutosten takia aiemmin tehdyt arvioinnin osat saatetaan joutua uusimaan.

Haastatteluissa kuullut näkemykset vaikuttavat pohjautuvan monin paikoin virheelliseen tietoon Traficomin ja arviointilaitosten rooleista. Traficomin tulkintasuosituksilla ei ole tarkoitus puuttua yksittäisen arvioinnin lopputulokseen, vaan arviointilaitokset tekevät työtään itsenäisesti pätevyysalueen mukaisesti. Arviointilaitoksella ei ole velvollisuutta pyytää tulkintalinjauksia yksittäiseen arvioon liittyen, pois lukien tilanteet, joissa arviointilaitoksen pätevyysalueet eivät kata kyseistä arvioinnin osa-aluetta. Tällainen tilanne voi tulla vastaan esimerkiksi silloin, kun kohteessa on käytössä turvallisuuskriittisessä roolissa sellainen salausratkaisu, jonka luotettavuuteen ei ole kohdistettu entuudestaan syvällistä arviointia. Salaustuotteiden hyväksyntä voidaan arviointiprosessin yhteydessä tehdä ns. Crypto Approval Authority (CAA) -pikaprosessina. Haastatteluissa todettiin, että tulkinnan pyytäminen koetaan usein välttämättömäksi, mutta ei ole selvitetty tarkemmin, mihin tällainen kokemus perustuu.

Traficomin Kyberturvallisuuskeskuksen ylläpitämä ajantasainen tilannekuva pohjautuu sekä kansallisiin että kansainvälisiin tietolähteisiin. Traficomin Kyberturvallisuuskeskuksen tunnustettuna vahvuutena on ollut julkisissa viestintäpalveluissa havaittujen ilmiöiden ja muun muassa yleisten hyökkäysten vaikuttavuuden arviointi ja suhteutus arvioitaviin järjestelmiin. Erityisesti turvallisuusluokiteltua tietoa käsitteleviin järjestelmiin kohdistuvien riskien arviointi pohjautuu Traficomissa sekä kansallisilta että kansainvälisiltä yhteistyökumppaneilta saatavaan uhkatietoon nykypäivän hyökkäyksistä ja niiden torjunnassa tehokkaiksi osoittautuneista menetelmistä. Osa erityisesti kansainvälisiltä viranomaisyhteistyökumppaneilta saatavasta tiedosta on luovutettu ja käytettävissä vain Kyberturvallisuuskeskukselle tiedon omistavan viranomaisen vaatimuksesta. Traficom on pystynyt jakamaan tätä tilannekuvatietoa arviointilaitoksille osittaisena, tyypillisesti yleisten vaatimustulkintojen kautta.

Tiedonhallintalaki (906/2019 13 §) edellyttää tiedonhallintayksiköiltä riskien arviointia ja tietoturvallisuustoimenpiteiden mitoittamista riskiarvioinnin mukaisesti. Koska arviointilait on annettu jo useita vuosia aikaisemmin, ei riskiperusteisuutta ole välttämättä aina huomioitu riittävästi tietoturvallisuuden suunnittelussa, toteutuksessa ja arvioinneissa, mikä kävi ilmi haastatteluissa. Puutteellinen tilannekuva ja riskiperusteisuuden jättäminen huomiotta saattaa ohjata viranomaiset kohdentamaan resurssinsa epäoleellisten riskien torjuntaan ja jättämään merkittävät nykypäivän riskit huomioimatta.

Asiakasorganisaatiot näkevät tietoturvallisuuden arvioinnit usein kertasuoritteena, koska velvoitetta säännöllisiin arviointeihin ei ole. Arvioinnista saatu todistus on sosiaali- ja terveydenhuollon järjestelmille voimassa enintään viisi vuotta ja muille järjestelmille enintään kolme. Säännöllisiä seuranta-arviointeja ei ole määritelty velvoittaviksi, vaan arvioinnin kohteen on itse ilmoitettava arvioijalle, jos järjestelmään on tehty merkittäviä muutoksia ja arvioinnista on myönnetty todistus. Merkittäviä muutoksia ei määritellä tarkemmin, mutta eri viranomaisille on annettu mahdollisuus antaa tällaisia määrityksiä (ks. esim. 159/2007 19 g § 4. momentti). Tietoturvallisuuden arviointeja ohjaavassa lainsäädännössä on eroavaisuuksia esimerkiksi myönnettävien todistusten voimassaoloajoissa sekä toimitilaturvallisuuden arviointia koskevissa tehtävissä.

Arvioinneissa löydetään tyypillisesti toteutuksia, jotka eivät ole täysin vaatimusten mukaisia. Tällaiset poikkeamat voivat olla vakavuudeltaan erilaisia ja ne yleensä kuvataan arviointiraportissa. Arviointilakien mukaan arvioinnista annetaan (1045/2011 9 §) tai voidaan antaa (1046/2011 8 §) todistus vaatimustenmukaisuudesta, mutta poikkeamien laadulle tai määrälle ei ole selkeitä kriteereitä, joiden perusteella vaatimustenmukaisuus voitaisiin todeta. Vaatimustenmukaisuus voidaan kuitenkin jo nykytilassa todeta tilanteessa, jossa vaatimuksen henki täyttyy vastaavan tason korvaavilla suojauksilla toteutettuna. Menettely on käytössä sekä Traficomin että sen hyväksymien tietoturvallisuuden arviointilaitosten arvioinneissa. Turvallisuusluokitellun tiedon suojausten arviointeihin (1406/2011) on määritetty poikkeamien kolmiportainen luokittelutapa. Se on yhtenevä arviointilaitosten, Traficomin sekä myös usean kansainvälisen toimijan käyttämän luokittelumäärittelyn kanssa. Haastatteluissa esitettiin näkemys, että Traficomin "viranomaishyväksynnän" luonne on enemmän tarkastus, joissa todetaan, että vaatimus joko täyttyy tai ei täyty, eikä arviointiin liity mahdollisuutta hyväksyntään riskiarvioinnin ja jäännösriskikäsittelyn kautta. Haastatteluissa esitetty näkemys vaikuttaa pohjautuvan virheelliseen tietoon, sillä Traficomin "viranomaishyväksyntäprosessissa" nimenomaan verrataan kohteen toteutusta aina siihen arvioituihin yleisiin riskeihin peilattuna. Haastattelujen perusteella vaikuttaisikin siltä, että Traficomin myöntämän ns. yleishyväksynnän ja esimerkiksi kunkin viranomaisen vastuulle kuuluvan erillishyväksynnän eroavaisuuksissa on epäselvyyksiä.

Kansalliset arvioinnit nähdään perustelluksi pitää mahdollisimman yhtenevinä kansainvälisiin arviointeihin nähden. Mikäli kansallisten arviointien käytännöt eriytyisivät kansainvälisten arviointien käytännöistä, niin kansallisten arviointien hyödyntämis- ja hyväksilukemismahdollisuudet suoritettaessa kansainvälisiä arviointeja hankaloituisivat. Tämä johtaisi samojen tietojärjestelmäympäristöjen arviointitarpeeseen aina uudelleen jokaisen kansainvälisen tarpeen näkökulmasta. Tämä hidastaisi kansainvälisen tietoaineiston sähköisen käsittelyn aloittamista sekä aiheuttaisi myös lisäkustannuksia osin päällekkäisistä arvioinneista. Ulkoministeriö näkee, että pyrkimys esimerkiksi enemmän riskipohjaiseen, joustavampaan arviointiin on yhtenäistettäessä hankalampaa.

2.5 Resurssit

Traficomille osoitettujen toimeksiantojen kesto on pitkä, useista kuukausista vuoteen, mistä koituu ylimääräisiä kustannuksia arvioinnin tilaajalle sekä arvioitavan palvelun tuleville käyttäjille. Vastaavasti kuten myös tietoturvallisuuden kaupallisilla arviointilaitoksilla, arvioinnin kesto ei sellaisenaan kuitenkaan kerro resurssien riittävyydestä, koska kestoon vaikuttavat ulkoiset tekijät, kuten arviointitoimeksiannon laajuus, tilaajan resurssitilanne sekä kohteen lähtötaso suhteessa mahdollisesti tavoiteltavaan yleishyväksyntään. Arviointitoimintaan liittyvät tehtävät ja niiden resursointi eivät vaikuta

haastattelujen perusteella olevan tasapainossa arviointien viiveiden perusteella. Haastatteluissa todettiin, että Traficomin rooli arviointien tekijänä ja arviointilaitosten pätevyyden arvioijana ei ole hyvän hallintotavan mukaista. Tämä ei vastaa Traficomin käsitystä asiasta. Traficom on tunnustettu, osaava ja arvostettu toimija tietoturvallisuuden arvioinnin alueella[10] ja se on järjestänyt sisäisesti arviointeihin liittyvän toimintansa niin, että arviointilaitostoiminta ja arviointitoiminta on henkilö- ja yksikkötasolla eriytetty. Lisäksi tietojärjestelmäturvallisuuteen liittyvää neuvontaa eivät anna samat henkilöt, jotka osallistuvat edellä mainittuun arviointitoimintaan. Hyvän hallinnon ja tarkastustoiminnan periaatteet ohjaavat Traficomin toimintaa.

Arviointitoimintaan liittyvän kyvykkyyden rakentamisessa ja ylläpidossa merkittävässä asemassa on menetelmien yhteensopivuus ja vastaavuus kansainvälisten organisaatioiden ja niiden jäsenmaiden käyttämien menetelmien kanssa. Traficomin Kyberturvallisuuskeskuksen kyvykkyyden rakentamisessa ja ylläpidossa merkittävässä asemassa on Kyberturvallisuuskeskuksen kansainvälisiltä viranomaisyhteistyökumppaneilta saadut hyvät käytännöt ja osin myös yhteinen kehitystyö. Tämä on tehnyt mahdolliseksi edistyksellisen, myös kansainvälistä vertailua kestävän kyvykkyyden ylläpitämisen Suomen rajallisilla resursseilla. Vaativiin tietojärjestelmätarkastuksiin ja arviointilaitosten hyväksymisprosessiin liittyvää asiantuntijuutta on saatavilla rajallisesti ja Traficomilla on kestänyt vuosikymmen rakentaa kyvykkyytensä nykyiseen, kansainvälistä vertailua kestävään tasoon. Rajalliset henkilöstöresurssit on saatu tehokkaasti hyödynnettyä panostamalla erityisesti pitkäjänteiseen osaamisen ja toiminnan kehittämiseen ja muun muassa suunnitelmalliseen perehdyttämiseen.

Traficomin vuoden 2019 tilinpäätöksen mukaan viraston henkilötyövuosien kokonaistoteuma vuonna 2019 oli 919 henkilötyövuotta, josta vuoden 2019 aikana uusia palkattuja työntekijöitä oli 64 henkilöä. Arviointitoimintaan käytettyjen resurssien kokonaismäärä ei ole tiedossa. Traficom on järjestänyt arviointilaitosten valvontaa sekä korkeimpien turvallisuusluokkien tietojärjestelmien ja tietoliikennejärjestelyjen arviointia varten turvaluokitusta vastaavat tilat ja suojatut järjestelmät, joiden kustannukset ovat olleet huomattavat. Traficomin arviointitoiminnalle kustannuksia aiheuttavat esimerkiksi salaus- ja yhdyskäytävätuotteiden arviointiin välttämättömät laboratoriot. Laboratoriot edellyttävät erityislaitteistoa ja -ohjelmistoja sekä testausmenetelmien ja osaamisen pitkäjänteistä kehitystyötä. Kyseisten testausmenetelmien kehitys ja laadunhallinta toteutuvat nykyisellään yhteistyössä Kyberturvallisuuskeskuksen kansainvälisen yhteistyöverkoston kanssa, mikä nähdäänkin välttämättömänä edellytyksenä arvioiden luotettavuudelle myös kansallisiin tarpeisiin. Esimerkiksi kansallista turvallisuusluokiteltua tietoa suojaavien salaus- ja yhdyskäytäväratkaisutuotteiden tulisi kestää myös sellaisia hyökkäysmenetelmiä, joista Suomi ei ilman kansainvälistä yhteistyötä saisi tietoa. Toisaalta ei ole realistista olettaa, että Suomen rajallisilla resursseilla olisi edes mahdollista kehittää ja ylläpitää kattavaa uhkatietoa edistyneimmistä hyökkäysmenetelmistä ja niiden torjunnassa tehokkaiksi todetuista suojausmenetelmistä ilman läheistä kansainvälistä yhteistyötä. Tämä pätee suoraan myös muuhun tietojärjestelmien arviointitoimintaan. Traficomilla on tarvittavat laboratoriot, osaaminen sekä kansainväliset yhteistyöverkostot käytettävissään.

[10] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla: Työryhmän loppuraportti [linkki, 2.2.2021], Liikenne- ja viestintäministeriön julkaisuja 2021:1

Hyväksyttyjen arviointilaitosten arviointitoiminnan resursseista ei ole tarkkaa tietoa, mutta kokonaisuudessaan Kiwa Inspecta Suomi työllistää yli 600 henkilöä[11], Nixu yli 400 henkilöä[12] ja KPMG yli 1400 henkilöä[13] Suomessa. Hyväksyttyjen arviointilaitosten arviointien tekemiseen osallistuu arvion perusteella yhteensä muutamia kymmeniä henkilöitä. Hyväksytyn arviointilaitoksen tekemän arvioinnin kesto ei sellaisenaan kerro resurssien riittävyydestä, koska kestoon vaikuttavat ulkoiset tekijät, kuten arviointitoimeksiannon laajuus, tilaajan resurssitilanne sekä mahdollisiin tulkintoihin ja tuotehyväksyntöihin kuluva aika. Vuosittain tehtävien tietoturvallisuuden arviointitoimeksiantojen lukumäärät eivät ole tiedossa.

2.6 Digitaalisen turvallisuuden vaatimukset ja kriteeristöt

Arviointilakien mukaan tietoturvallisuuden arviointiperusteina voidaan käyttää mm. kansallisia tai kansainvälisiä säännöksiä ja ohjeita tai vahvistettuja standardeja (1405/2011 10 §, 1406/2011 7 §). Tietoturvallisuuden vaatimuksia on kirjattu tiedonhallintalain lisäksi sektorikohtaiseen sääntelyyn. Arviointilaki painottuu järjestelmien tekniseen arviointiin. Toiminnan jatkuvuudelle ja varautumiselle ei ole arviointia koskevaa sääntelyä. Tiedonhallintalaista näitä olisi tosin johdettavissa. Toiminnan jatkuvuuden varmistaminen tunnistetaan vallitsevana kehityssuuntana. Se on keskeinen osa digitaalisen turvallisuuden kokonaisuutta ja tukee osaltaan tietoturvallisuuden toteutumista. Tietoturvallisuuden arviointeja on teetetty lakanneen tietoturvallisuusasetuksen (681/2010) perusteella tietoturvallisuuden korotetulle tai korkealle tasolle, jotta jatkuvuuden varmistamiseen liittyviä kontrolleja saataisiin mukaan arviointiin. On kuitenkin huomattava, etteivät turvallisuusluokitus ja toiminnan jatkuvuuden varmistamisen vaatimukset riipu välttämättä toisistaan. Tietojärjestelmän eheys- tai käytettävyysvaatimukset voivat olla erittäin korkeita, vaikka siinä käsiteltävät tiedot olisivat julkisia, esimerkiksi VNK:n hätätiedotusjärjestelmä ja viranomaisten voimassa oleviin koronarajoituksiin ja -ohjeistuksiin liittyvät sivustot.

Katakri-kriteeristö on viranomaisten ja elinkeinoelämän yhteistyössä laatima työkalu, johon on koottu keskeiset kansallisen ja kansainvälisen turvallisuusluokitellun tiedon suojaamiseen kohdistuvat turvallisuusluokkien IV, III ja II vaatimukset. Katakri on kansainvälisistä tietoturvavelvoitteista annettua lakia (588/2004) täsmentävä. Sitä käytetään myös turvallisuusselvityslain (726/2014) mukaisissa kansallisissa ja kansainvälisissä arvioinneissa sekä turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arvioinneissa (1406/2011). Katakrin käytölle kansallisissa arvioinneissa ei kuitenkaan ole riittävää säädöspohjaa. Se ei sisällä salassa pidettävien tietojen eikä toiminnan jatkuvuuden hallinnan ja varautumisen arviointikriteerejä. VAHTI-ohjeet ovat pääosin valtionhallinnon käyttöön tarkoitettuja (mm. vanhentunut VAHTI 2/2010). Vanhentuneita VAHTI-ohjeita ja aiempia Katakri-versioita käytetään kuitenkin edelleen. Katakri-kriteeristön ja Vahti-ohjeiden soveltuvuus koko julkisen hallinnon käyttöön on rajallinen, koska kuntasektorilla turvallisuusluokittelua ei käytetä (1109/2019). Digitaalisen turvallisuuden vaatimusmäärittelyjen tulisi perustua kansainvälisiin standardeihin (mm. ISO27001 – Tietoturvallisuuden hallinta,

[11] https://image.slidesharecdn.com/jyrkilahnalahtikiwainspecta14-190215141649/95/jyrki-lahnalahti-kiwa-inspecta-1422019-3-638.jpg?cb=1550240301
[12] https://www.nixu.com/sites/default/files/NIXU_Vuosikatsaus_2019.pdf
[13] https://assets.kpmg/content/dam/kpmg/fi/pdf/2020/01/KPMG_vuosikertomus_2019_2.pdf

ISO22301 – Jatkuvuuden hallinta, ISO31000 – Riskienhallinta), joita on täydennetty kansallisilla erityisvaatimuksilla. Tämä on myös osin puutteellista nykyisissä vaatimusmäärittelyissä.

Digitaalisen turvallisuuden arviointiperusteina käytettävien arviointikriteeristöjen ja vaatimusmäärittelyjen velvoittavuus ja säädösperuste ovat haastattelujen perusteella epäselviä. Ohjeisiin tai suosituksiin perustuvat toteutukset voivat johtaa puutteellisiin digitaalisen turvallisuuden kontrollien toteutuksiin, jos toteutukset eivät perustu realistisiin uhka- ja riskiarvioihin. Riskienhallinta on useimpien vaatimusmäärittelyjen keskeinen osa, mutta riskien arviointi, riskien hallintakeinoista päättäminen ja mahdollisten jäännösriskien hyväksyntä on tehtävä realistisesti ja ammattitaitoisesti. Riskien vaikutusten aliarviointia ei tulisi käyttää perustelemaan hallintakeinojen puutteellisia toteutuksia.

Haastatteluissa todettiin, että sääntely ei tällä hetkellä riittävästi velvoita vaatimustenmukaisuuden säännölliseen ja jatkuvaan varmistamiseen. Tiedonhallintalakiin (906/2019) on kirjattu, että elinkaarimallin mukaisesti tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Olennaiset tietojenkäsittelyyn kohdistuvat riskit on selvitettävä ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Kokonaisuuteen kuuluu riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella sekä tietoturvallisuustoimenpiteiden toteuttaminen (ks. HE 284/2018 vp, 13 §:n yksityiskohtaiset perustelut). Tiedonhallintalain 13 § 5 momentissa on informatiivinen viittaus arviointilakiin. Tämän mukaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

2.7 Oppivien ja älykkäiden järjestelmien arviointi

Tekoäly- ja koneoppimisratkaisuissa tarvittavan laskentatehon tuottavat suuret, kansainväliset toimittajat, joilla ei välttämättä ole intressiä toteuttaa kansallisia viranomaisvaatimuksia. Traficom pitää yllä mm. luetteloa turvallisuusluokitellun tiedon suojaamiseen hyväksytyistä salausratkaisuista. Tällaisten ratkaisujen integrointi monikansallisten pilvipalvelutoimittajan ympäristöön voi olla vaikeaa. Toisaalta integroinnille ei yleensä ole tarvettakaan, sillä turvallisuusluokitellun tiedon käsittelyä ei yleisesti tulisi toteuttaa ympäristöissä, joihin arvioidaan kohdistuvan lainsäädäntöjohdannaisia riskejä. Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa pilvipalveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa ja tarjoamaan esimerkiksi suora tai epäsuora pääsy pilvipalvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Pääsääntöisesti lainsäädännöllä on velvoitettu palveluntarjoaja luovuttamaan tietoja poliisille tai tiedusteluviranomaisille tutkittavaksi.[14]

Terveydenhuollon järjestelmien arviointi perustuu valmistajan määrittelyyn käyttötarkoituksesta ja tähän määrittelyyn liittyviin vaatimuksiin. Oppivan järjestelmän toiminnan arviointia tulisi tehdä vaiheittain järjestelmän kehittyessä, mitä pidetään epärealistisena lähestymistapana. Myöskään algoritmien arviointia ei pidetä mahdollisena.

[14] Tiedonhallintalautakunta, Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (VM 2021:5)

Oppivat ja älykkäät järjestelmät eivät muuta keskeisiä arviointitehtäviä tai arviointitehtävien organisoimista. Näiden järjestelmien digitaalisen turvallisuuden arviointi poikkeaa kuitenkin muista digitaalisista palveluista ja tietojärjestelmistä, koska arvioinnissa tulee mm. varmistaa, että järjestelmän algoritmit suorittavat älykkäät tehtävänsä siten kuin esimerkiksi automaattisesta päätöksenteosta on säädetty. Tämä järjestelmien käyttämien algoritmien arviointi edellyttää syvällistä erikoisosaamista. Algoritmit, kuten yleensäkin ohjelmistot, voivat lisäksi olla yritysten liikesalaisuuksia, jolloin niiden arviointi on vaikeaa tai jopa mahdotonta. Toiminnallisuuden arviointi on mahdollista, mutta oppimisen myötä tapahtuvat järjestelmien muutokset voivat muuttaa toiminnallisuutta hyvin nopeasti. Esimerkiksi hallintaviitekehyksen AI in control[15] avulla on mahdollista arvioida järjestelmän johdonmukaisuutta (integrity), reiluutta (fairness), selitettävyyttä (explainability) ja kestokykyä (resilience) sen elinkaaren aikana. Nykyiset vaatimusmäärittelyt eivät sellaisenaan sovellu myöskään oppimisessa käytettävän tiedon turvallisuuden arviointiin, koska järjestelmää opettavan tiedon eettisyys ja luotettavuus ovat arvioinnin kannalta oleellisia seikkoja.[16] Keskeisiä kysymyksiä ovat lisäksi kertyvän tiedon hallintaoikeus ja saatavuus sekä tiedon uudelleen käytettävyys ja sijainti globaaleissa tietoverkoissa ja näiden hallintaan liittyvät kysymykset.

[15] https://advisory.kpmg.us/articles/2019/kpmg-artificial-intelligence-in-control.html [26.1.2021]
[16] ks. esim. Achieving Trustworthy AI - A Model for Trustworthy Artificial Intelligence

3 ARVIOINTITOIMINNAN HYÖDYT HAASTATTELUJEN PERUSTEELLA

Nykytilanteessa arviointitoiminnan hyötyinä nähtiin ennen kaikkea julkisen sektorin ja yksityisten toimijoiden yhteistyö sekä tietoturvallisuuden osa-alueita vahvistavat velvoittavat arviointikriteerit sikäli kuin niitä on asetettu. Tarkasteltaessa lainsäädäntöä ajallisesti nähtiin, että arviointilaki ja arviointilaitoslaki tulivat hyvin senhetkiseen tarpeeseen kymmenen vuotta sitten lainsäädännön valmistuessa. Omalta osaltaan edellä mainitut lait ovat lisänneet ja vahvistaneet valtionhallinnossa organisaatioiden rakenteita esimerkiksi asiakastietojen suojaamisessa. Arviointilain velvoittava linjaus arviointilaitosten käyttämisestä on yhtenäistänyt arviointitoimintaa. Myös kansainvälisten vaatimusten yhdistyminen tietoturvallisuuden kansallisiin arviointeihin nähtiin positiivisena.

Haastattelujen perusteella julkisen sektorin ja yksityisten toimijoiden yhteistyön malli on tietoturvallisuuden arvioinnin näkökulmasta melko hyvä. Kriteeristöjen mukaisia arviointeja ovat voineet tehdä Traficomin lisäksi myös hyväksytyt arviointilaitokset. Kaupallisten toimijoiden käyttämistä arvioinneissa pidettiin yleisesti hyvänä, sillä se osittain helpottaa resurssipuutteiden paikkaamista, nopeuttaa arviointeja ja jakaa tietoa osapuolten välillä arviointeihin liittyvistä toiveista. Vaikka haastatteluissa nähtiin tarvetta hyväksyttyjen arviointilaitosten määrän lisäämiselle, toimii arviointilaitosten rajattu määrä ja vaativa pätevyyden arviointiprosessi joidenkin näkemysten mukaan laadun takeena.

Arviointilakia ja arviointilaitoslakia pidettiin hyödyllisinä, sillä ne vahvistavat organisaatioiden tietoturvallisuuden ja tietoliikennejärjestelyjen asian- ja vaatimustenmukaisuutta. Lainsäädännöstä saatavia digitaalisen turvallisuuden kehittämisen rajauksia ja viittauksia voidaan käyttää esimerkiksi neuvotteluissa ja myynnissä tarjousten tarkoituksenmukaiseen rajaukseen. Arviointitoiminnan velvoittava lainsäädäntö lisää arviointitoiminnan läpinäkyvyyttä, koska tällöin osapuolet tietävät paremmin vaatimukset etukäteen.

Arviointilain mukaisen tietoturvallisuuden arvioinnin nähtiin toimivan hyvänä kertaluonteisena ensiarviointina tietojärjestelmän ja tietoliikennejärjestelyjen vaatimustenmukaisuudesta. Arvioinnilla turvallisuustarpeet saadaan parhaassa tapauksessa täytettyä ennen käyttöönottoa ja osoitettua järjestelmän vaatimustenmukaisuus. Arviointilaitoksen tekemän arvioinnin hyötynä nähtiin olevan ulkopuolisen ja riippumattoman kolmannen osapuolen näkemys arvioinnin kohteena olevan organisaation kehityskohteista. Arvioinnin ulkoishyötynä arvioija toimii arvioinnin ohella tietoturvallisuuden ja digitaalisen turvallisuuden lähettiläänä kouluttaessaan ja konsultoidessaan yleistasolla arvioinnin kohteena olevaa organisaatiota. Tapauksissa, joissa arviointeja on toteutettu useammin kuin vain kertaluonteisesti, ne ovat auttaneet ylläpitämään tietoturvallisuuden tasoa.

4 ARVIOINTITOIMINNAN KEHITTÄMINEN

4.1 Arviointitoiminnan kehittämisestä

Arviointitoiminta on merkittävä tekijä turvallisten palvelujen tuottamisessa ja tarjoamisessa. Arviointitoiminnan kehittämisehdotukset perustuvat haastatteluissa kerätyn aineiston perusteella valtiovarainministeriössä muodostettuihin ja Haukka-säädösvalmistelun koordinaatioryhmässä keskusteltuihin näkemyksiin kehittämistarpeista.

Arviointitoimintaan liittyvät keskeiset tehtävät ovat arviointilaitoksen arviointiperusteiden määritys ja pätevyyden arviointi määrävälein, arviointikriteeristöjen asettaminen ja näiden ylläpito, arviointitoimeksiantojen tekeminen sisältäen arviointikohteen ja arvioinnin laajuuden osoittamisen, arviointilaitoksen suorittama arviointi tai auditointi ja vaatimustenmukaisuustodistuksen myöntäminen sekä arvioinnin tulosten perusteella tehtävien muutosten hallinta. Arviointitoimintaa koskevia säännöksiä tulisi muuttaa siten, että julkisen hallinnon digitaalisen turvallisuuden arvioinnista säädettäisiin nykyistä selkeämmin.

Viranomaisten suorittamat arviointitehtävät tulisi entistä enemmän kohdentaa kansallisen turvallisuuden näkökulmasta kriittisiin kohteisiin ja kasvattaa kaupallisten arviointilaitosten toimintaa muilla alueilla. Valtiovarainministeriön ja liikenne- ja viestintäministeriön yhteistyönä toteuttamasta Traficomin arviointilaitosten akkreditointiin ja hyväksyntään sekä arviointitoimintaan liittyvästä ohjausmallista ei ole sääntelyä. Tästä ohjausmallista tulisi säätää. Traficom ei näe perustelluksi lisätä kansalliseen valtionhallintoon enää kansainvälisten toimijoiden jo suorittaman valvonnan kanssa päällekkäistä arviointitoiminnan valvontaa.

Nykyisin arviointitoiminta on painottunut valtiotoimijoihin sekä salassa pidettäviin ja turvallisuusluokiteltuihin tietoihin. Tämä rajaus ei ole enää perusteltavissa eikä se kata yhteiskunnan laajempaa tarvetta huolehtia digitaalisesta turvallisuudesta. Siten julkisia ja salassa pidettäviä tietoja käsittelevien palvelujen sekä kuntien ja kuntayhtymien digitaalisten palvelujen säännöllistä arviointia tulisi tehostaa. Arviointitoiminnassa tulisi huomioida digitaalisen turvallisuuden eri osa-alueet nykyistä paremmin, vähentää arviointiperusteisiin liittyvää tulkinnanvaraisuutta, selventää eri toimijoiden rooleja sekä varmistaa arviointien laatu ja yhteismitallisuus.

Digitalisoituneen yhteiskunnan toimintaympäristö sisältää lukuisia verkostoja, joissa vallitsee erilaisia ja muuttuvia keskinäisriippuvuuksia toimijoiden välillä. Tästä syystä yksittäisenkään palvelun digitaalinen turvallisuus ei toteudu vain palvelun käyttäjäorganisaation, tuottajan tai kehittäjän toteuttamilla hallintakeinoilla. Palvelun kehittäjällä voi olla erityisosaamista edellyttäviä alihankkijoita. Digitaalisiin palveluihin liittyy poikkeuksetta tietoliikenneyhteyksiä, joiden runkoyhteyksiä tarjoavat tietoliikenneoperaattorit. Tämän vuoksi digitaalisten palvelujen turvallisuudesta tulisi varmistua koko palveluverkoston laajuisesti. Arviointitoiminnalla saadaan vain yhteen ajanhetkeen sidottu kuva digitaalisen turvallisuuden vaatimusten toteutumisesta, joten arviointeja pitäisi toteuttaa kaikissa palvelun elinkaaren vaiheissa säännöllisesti. Arvioinnissa tunnistettujen poikkeamien korjaaminen ja kehityskohteiden parantaminen johtaa digitaalisen turvallisuuden kehittymiseen jatkuvan parantamisen mallin mukaisesti.

Teknologisten ja toiminnallisten muutosten takia myös vähimmäisvaatimuksia sekä niistä johdettuja arviointikriteereitä ja vaatimusmäärittelyjä tulee muokata nykyiseen ja tulevaan toimintaympäristöön paremmin soveltuviksi. Vaatimuksiin kohdistuvia muutoksia ja päivityksiä tulisi voida tehdä mahdollisimman joustavasti. Arviointien tavoitteena ei saa olla ainoastaan suositusten ja vaatimusten täyttäminen vaan turvallinen tietojenkäsittely-ympäristö.

Tiedonhallintalaissa säädetyt, tietoturvallisuustoimenpiteisiin kohdistuvat vaatimukset tarkoittavat tietosuojalainsäädännössä tarkoitettuja teknisiä ja organisatorisia toimia henkilötietojen suojaamiseksi. Tässä raportissa ei ole kuvattu tietosuojan arviointitoiminnan kehitysehdotuksia. Arviointitoimintaan liittyviä kehitysehdotuksia on käsitelty myös liikenne- ja viestintäministeriön Titukri-raportissa[17], josta on rajattu ulkopuolelle kansallisen turvallisuuden piiriin kuuluvat asiat. Kansallisen turvallisuuden ylläpitämisen yhteydessä tapahtuva henkilötietojen käsittely kuuluu rikosasioiden tietosuojalain (1054/2018) piiriin eikä siihen siis sovelleta tietosuoja-asetusta.

4.2 Arviointilaitoksen akkreditointi ja seuranta

Arviointilaitoksen hyväksyntäprosessia pitäisi yksinkertaistaa prosessin nopeuttamiseksi ja toiminnan tehostamiseksi siten, että käsittelyn kesto on paremmin ennustettavissa ja prosessissa käytettävät vaatimukset ja arviointilaitoksen tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen pätevyyden arviointiperusta on kuvattu selkeästi yhtenä kokonaisuutena. Kansallinen akkreditointiyksikkö FINAS arvioisi tietoturvallisuuden lisäksi toiminnan jatkuvuuden ja varautumisen arviointilaitosten pätevyyksiä määrävälein. FINAS vastaisi näiden arviointilaitosten toiminnan vaatimustenmukaisuuden arvioinnista ennalta asetetun kriteeristön mukaisesti sekä yleisten että toimialakohtaisten vaatimusten osalta. FINAS voisi käyttää Traficomia ja tarvittaessa myös muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä kuten nykyisinkin. Määritystyöhön näissä viranomaisissa osallistuvat virkamiehet eivät saisi osallistua arviointilaitoksen toimintaan arvioijina myöskään kansallisen turvallisuuden piiriin kuuluvan arviointitoiminnan osalta.

FINAS ylläpitäisi kuvausta mahdollisista arviointilaitosten pätevyysalueista. Pätevyysalueet voivat kattaa turvallisuusluokitteluasetuksen turvallisuusluokan IV ja III, sekä salassa pidettäviä ja julkisia tietoja käsittelevien järjestelmien tietoteknisen turvallisuuden arvioinnin sekä arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen ja henkilöstöturvallisuus) arvioinnin, sekä korkeintaan turvallisuusluokan TL III toiminnan jatkuvuuden ja varautumisen järjestelyjen arvioinnin.

Arviointilaitosten hyväksyntäprosessia yksinkertaistettaisiin ja nopeutettaisiin keventämällä tilaturvallisuusvaatimuksia ja tiedon suojaamiskyvyn vaatimuksia silloin, kun arviointilaitos ei hae pätevyyttä turvallisuusluokiteltua tietoa käsittelevien järjestelmien arviointiin. Tällöin arviointilaitoksen pätevyysalueina voisivat olla esimerkiksi toiminnan jatkuvuus tai varautuminen tai julkisia tai salassa pidettäviä tietoja käsittelevät tietojärjestelmät. Tällöin on huomioitava, että arvioitavat toiminnan jatkuvuuden ja varautumisen järjestelyjä koskevat tiedot eivät myöskään saisi olla turvallisuusluokiteltuja, mikä rajaa arviointitoimeksiantoja. Arviointilaitosten pätevyysarvioinnin vaatimusten tulee kuitenkin olla pätevyysalueittain yhtäläiset kaikille arviointilaitoksille.

[17] Liikenne- ja viestintäministeriön julkaisuja 2021:1

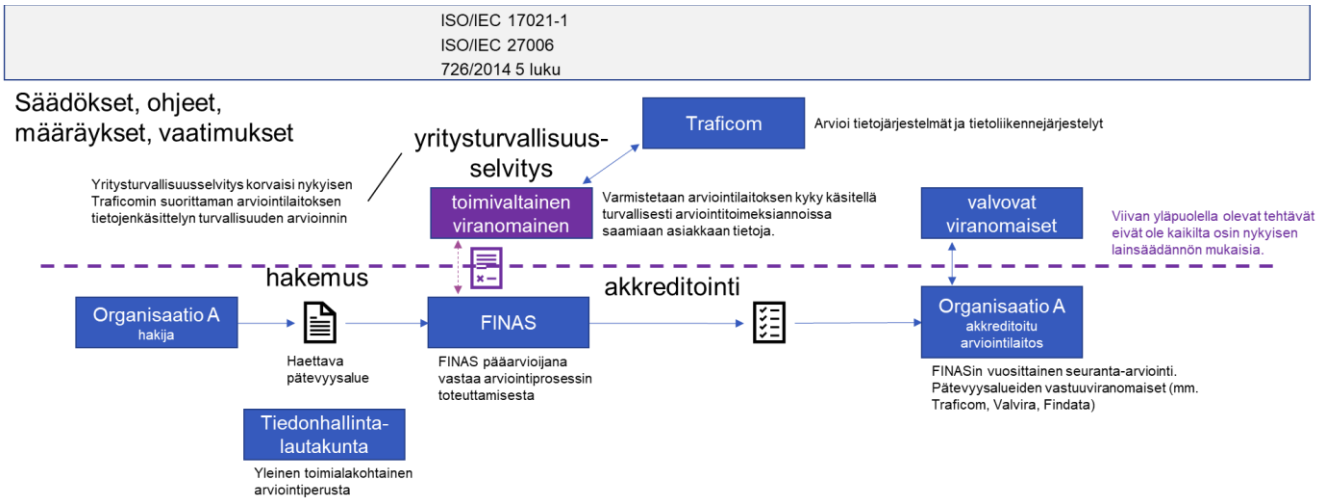
Traficom keskittyisi jatkossakin tiedonhallintalain tarkoittamien turvallisuusluokkien TL III, TL II ja TL I tietoja käsittelevien tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiin, johon kuuluvat hallinnolliset, toiminnalliset ja tekniset tietoturvavaatimukset ja -toimenpiteet. Tämä sisältää tietoteknisen turvallisuuden sekä viranomaisten osalta myös arvioitavaan tietojärjestelmään liittyvään turvallisuusjohtamisen (hallinnollinen ja henkilöstöturvallisuus) arvioinnin. Arvioinnit koskevat sähköisessä muodossa olevan tiedon suojaamisen arviointia, joten turvallisuusjohtamisen arviointi on perusteltua liittää johonkin tietojärjestelmään tai tietojenkäsittely-ympäristöön. Tämä tukee myös sitä, että turvallisuusjohtamisen arviointia voidaan peilata konkreettista tietojärjestelmää tai tietojenkäsittely-ympäristöä vasten, mikä antaa turvallisuusjohtamisen käytännön tason jalkautumisesta luotettavamman kuvan. Tietojärjestelmään liittyvästä fyysisen turvallisuuden arvioinnista säädettäisiin erikseen. Kansallista turvallisuusluokan TL III tietoa käsittelevien palveluiden ja järjestelmien arviointia voisivat tehdä tilaajan valinnan perusteella viranomainen tai markkinaehtoinen, akkreditoitu arviointilaitos.

Turvallisuusselvityslakia (726/2014) ei ollut säädetty arviointilakeja säädettäessä. Turvallisuusselvityslain mukaisesti Traficom laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen (726/2014, 9 §). Tulisikin selvittää, voitaisiinko arviointilaitoksen hyväksymisen arviointilaitoslain mukaiset kohdat 4 ja 5 eli se, että ”*laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan; ja laitoksella on asianmukaiset ohjeet toimintaansa ja sen seurantaa varten.*” yhdenmukaistaa turvallisuusselvityslain kanssa esimerkiksi siten, että arviointilaitokselta edellytettäisiin yritysturvallisuusselvitystä. Yritysturvallisuusselvitys korvaisi arviointilaitoksen tietojenkäsittelyn turvallisuuden arvioinnin, ts. L 1405/2011:n 5 §:n 1 mom. 4 kohdan. Yritysturvallisuusselvitys ei kuitenkaan kattaisi 5 kohtaa eikä Traficomin myöntämään hyväksyntään liittyvää rajoituksia mm. pätevyysalueesta (ks. 5 §:n 4 mom: "*Hyväksymistä koskevaan päätökseen voidaan sisällyttää arviointilaitoksen pätevyysaluetta, valvontaa sekä sellaisia toimintaa koskevia rajoituksia ja ehtoja, jotka ovat tarpeen arviointilaitoksen tehtävien asianmukaisen hoidon varmistamiseksi.*"). Nämä liittyvät kiinteästi arviointilaitosten valvontaan. Toisaalta akkreditointilain 7 §:ssä todetaan: "*Akkreditointipäätöksessä määritellään arviointielimen akkreditoitu pätevyysalue ja vahvistetaan menettelytavat, joilla pätevyyttä pidetään yllä ja seurataan.*" Tulisikin harkita, voitaisiinko erityisesti julkisia tai salassa pidettäviä tietoja käsittelevien palvelujen arviointilaitoksiksi hakevien osalta poistaa L 1405/2011 5 §:n 1 momentin 5 kohdan vaatimus vaarantamatta arviointitoiminnan laadukkuutta.

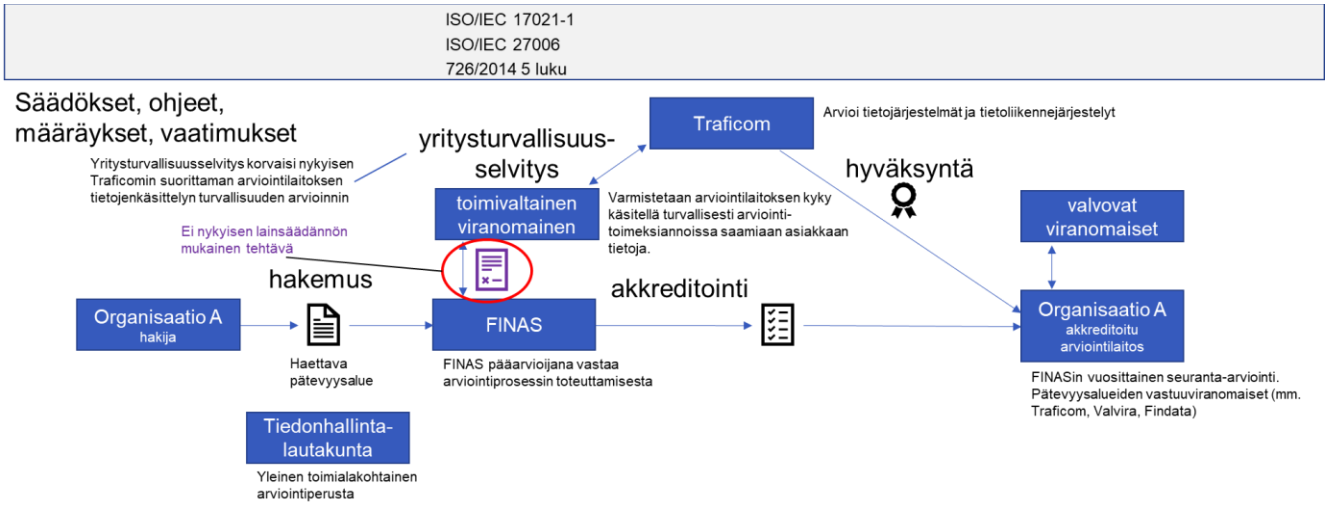
Yritysturvallisuusselvityksen sisältö määräytyisi haettavan pätevyysalueen perusteella siten, että esimerkiksi turvallisuusluokka TL IV pätevyysalueeksi hakevalle asetettaisiin tiukemmat tietojärjestelmien ja tietoliikennejärjestelyjen vaatimukset kuin julkisen tiedon arvioinnin pätevyysaluetta hakevalle. Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyiden turvallisuusjärjestelyjen oikeudeton paljastuminen kolmannelle osapuolelle voi vaarantaa viranomaisen toiminnan. Siten markkinaehtoisilta arviointilaitoksilta tulisi edellyttää yritysturvallisuusselvitystä, jotta niille voitaisiin myöntää pätevyysalueeksi Katakri TL III.

NLF-sääntelyä ei sovelleta kansallisen turvallisuuden piiriin kuuluvaan arviointitoimintaan. Traficomin rooli viranomaisena, jota FINAS kuulee arviointiperustasta päättäessään, olisi arvioitava NLF-

paketin valossa siltä osin kuin kuuleminen ei liity kansallisen turvallisuuden piiriin kuuluvaan arviointitoimintaan. FINAS voisi jatkossa kuulla myös muita viranomaisia kuten tiedonhallintalautakuntaa tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitosten toimialakohtaisesta arviointiperustasta päättäessään. Arviointilaitoksen akkreditoinnin tavoitetilan prosessit on esitetty kuvissa 5 ja 6. Kuvassa 5 on kuvattu luonnosprosessi tilanteesta, jossa arviointilaitokseksi haetaan julkisen tai salassa pidettävän tiedon pätevyysalueille. Myös julkisen tai salassa pidettävän tiedon pätevyysaluetta hakevista yrityksestä tehtäisiin yritysturvallisuusselvitys. Esimerkiksi julkista tai henkilötietoa käsittelevän järjestelmän turvallisuustiedot voivat olla turvallisuusluokiteltavia, jos järjestelmän tietojen laiton hankinta voi johtaa varautumisen tai Suomen turvallisuuden vaarantumiseen. Kuvassa 6 on vastaava luonnosprosessi turvallisuusluokitellun tiedon/kansallisen turvallisuuden pätevyysalueille.



Kuva 5. Menettely, kun haettava pätevyysalue kattaa julkisia tai salassa pidettäviä, luokittelemattomia tietojen käsittelevät tietojärjestelmät ja tietoliikennejärjestelyt.



Kuva 6. Menettely, kun haettava pätevyysalue kattaa turvaluokiteltujen tai kansalliseen turvallisuuteen liittyviä tietoja käsittelevät tietojärjestelmät ja tietoliikennejärjestelyt.

Arviointiperustan asettamisessa tulee kiinnittää huomiota siihen, että se on mahdollisimman yksikäsitteinen. Tulkinnanvarainen tai epäselvä arviointiperusta hankaloittaa prosessin sujuvaa etenemistä. Akkreditointia hakevalle toimijalle pitää kuitenkin asettaa arviointiperusta, jolla varmistetaan arviointilaitoksen toiminnan laatu, turvallisuus ja riippumattomuus sekä laitoksen suorittamien arviointien laatu ja yhteismitallisuus. Titukri-raportissa[18] kuvatusti toimialakohtaista tietoturvallisuuden arviointia ja tietoturvallisuuden arviointilaitosten määrää on tarpeen lisätä. Samalla on varmistettava, että arviointitoiminnan korkea laatu ja ammattitaito säilyvät.

Arviointien nopeuttamiseksi ja resurssien käytön tehostamiseksi pitäisi turvallisuusluokittelematonta salassa pidettävää ja julkista tai luokittelematonta tietoa käsittelevien palvelujen tai järjestelmien arviointien olla pääasiallisesti akkreditoitujen kaupallisten arviointilaitosten tehtävä, koska tällaisia palveluja ja järjestelmiä on lukumääräisesti eniten. Markkinaehtoisten toimijoiden on viranomaista helpompaa mukauttaa arviointitoiminnassa mukana olevan henkilöstön määrä arviointien kysynnän perusteella. Tehokas ja ennustettava arviointilaitosten pätevyyden arviointiprosessi helpottaa uusien arviointilaitosten pääsyä markkinoille, mikä lisäisi kilpailua ja varmistaisi siten arvioinneille oikean kustannustason.

Kaupalliset arviointilaitokset voisivat myös arvioida TL IV -luokiteltua tietoa käsitteleviä palveluja. TL-luokitellun tiedon osalta on kuitenkin huomioitava, että turvallisuusluokan IV tiedon suojausten viranomaisarviointien olisi hyvä olla mahdollisimman yhtenevä kansainvälisen RESTRICTED-luokan tietojen arviointien kanssa, sillä suurin kv-aineiston käsittelytarve kohdistuu nimenomaan RESTRICTED-luokan tietoihin. Mikäli esimerkiksi arviointilaitosten tekemät kansalliset TL IV -kohteiden arvioinnit eriytyisivät Traficomin tekemistä RESTRICTED-kohteiden arvioinneissa käytetyistä menettelyistä ja tulkintakäytännöistä, ei arviointilaitosten tekemiä arviointeja voisi hyödyntää tilanteissa, joissa arviointilaitoksen arvioimaa kohdetta haluttaisiin myöhemmin käyttää myös esim. EU RESTRICTED -tietojen käsittelyyn. Pahimmillaan tilanne voisi johtaa siihen, että ensin arviointilaitos arvioisi jonkin laajan valtionhallinnon moniviranomaisympäristön, mikä tuottaisi merkittävät kustannukset ympäristön laajuuden takia. Tämän jälkeen ympäristöön tehtäisiin mahdollisesti merkittäviä kustannuksia aiheuttavia muutoksia, joilla tavoiteltaisiin TL IV -vaatimustenmukaisuuden saavuttamista kansallisesti eriytyneiden tulkintojen mukaisesti. Tämän jälkeen Traficomin tulisi arvioida (L 588/2004) ko. laaja moniviranomaisympäristö kokonaisuudessaan vielä uudestaan, koska arviointilaitoksen arviointia ei voitaisi eriytyneiden menettelyjen ja tulkintojen myötä enää käytännössä hyödyntää. Eriytyneiden menettelyjen ja tulkintojen takia Traficomin arviointi paljastaisi laajasta ympäristöstä todennäköisesti aikaisemmin havaitsemattomia puutteita, minkä korjaaminen voisi aiheuttaa taas merkittäviä kustannuksia arvioinnin kohteelle. Kokonaisuutena tällaisen eriytyneen arviointiskenaarion kustannukset olisivat erittäin merkittäviä, viiveistä puhumattakaan.

Erityisesti, jos velvoittavuutta arviointeihin ja vaatimustenmukaisuustodistusten hankkimiseen laajennetaan, tulisi Puolustusvoimille säätää toimivalta arvioida kansallisia tietoaineistoja käsitteleviä tietojärjestelmiä. Puolustusvoimat on ehdottanut, että lakiin 1406/2011 säädettäisiin myös Puolustusvoimat toimivaltaiseksi viranomaiseksi viranomaisarviointiin vastuualueenaan maanpuolustukseen liittyvät TL IV – TL I turvallisuusluokan salaustuotteet (CAA), tietojärjestelmät sekä tietoliikennejärjestelyt (SAA). Toimivalta kattaisi edellä listattujen kokonaisuuksien auditoinnin (arvioinnin) ja

[18] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla, LVM 2021:1

hyväksynnän. Tämä edellyttäisi muutoksia myös turvallisuusselvityslakiin. Puolustusvoimien ehdotuksesta puolustusvoimille säädettäisiin tehtäviksi tietoturvallisuuden lisäksi myös maanpuolustukseen liittyvien TL IV – TL I turvallisuusluokan salaustuotteiden, tietojärjestelmien sekä tietoliikennejärjestelyiden toiminnan jatkuvuuden ja varautumisen arviointi.

Arviointitehtävän säätämisessä Puolustusvoimille tulee samalla varmistaa, että arviointitoiminta organisoidaan Puolustusvoimien sisällä itsenäiseksi ja riippumattomaksi toiminnoksi. Arviointitehtävä edellyttäisi myös resurssitarkastelua, joka tulee huomioida mahdollisessa arviointilain päivittämistyön seurannaisvaikutuksissa. Kyvykkyys arviointitehtävän hoitamiseen edellyttää osaamisen kehittämistä ja aikaa. Muutoksille tarvitaan riittävät siirtymäajat, jotta nykyistä toimintatapaa ei vaaranneta ennen valmiutta uuteen toimintatapaan.

FINAS toteuttaa arviointilaitosten seurantaa vuosittaisilla seuranta-arvioinneilla. Jos arviointilaitos ei täytä akkreditoinnille asetettuja vaatimuksia, sen akkreditointi voidaan perua. Arviointilaitosten lukumäärän kasvu voi kuitenkin edellyttää lisää resursseja niin akkreditointiprosessiin kuin seuranta-arviointeihinkin. Lisäksi tulisi säädöksin varautua tilanteeseen, jossa arviointilaitoksen hallussa olevat arviointitiedot ovat yrityksen toiminnan muutosten takia joutumassa ennalta suunnittelemattoman tahon haltuun.

Kaupallisten tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitosten valvontaa tulisi kehittää siten, että kunkin pätevyysalueen valvontaan osallistuisivat Traficomin lisäksi myös muut pätevyysalueen vastuuviranomaiset koordinoidusti. Arviointilaitostehtävien valvontaan osallistuisivat siten myös ne viranomaiset, joiden tehtäviin arvioitavan palvelun vaatimustenmukaisuuden varmistaminen tai ohjaaminen kuuluu. Traficomin lisäksi valvontaviranomaisina toimisivat siten esimerkiksi tietosuojavaltuutetun toimisto sekä Terveyden ja hyvinvoinnin laitos. Valvontavastuiden jakaantumisesta eri viranomaisten kesken tulisi säätää esimerkiksi verkko- ja tietosuojadirektiivissä (NIS) kuvatulla tavalla. Arviointilaitosten toimintaa valvovan viranomaisen havaitsema, virheellisillä tai puutteellisilla perusteilla annettu todistus voi johtaa siihen, että arviointilaitos menettää pätevyysalueensa tai asemansa akkreditoituna arviointilaitoksena. Arviointilaitokselle voidaan asettaa myös muita sanktioita (esim. taloudelliset seuraamukset), mikäli se ei täytä arviointilaitokselle asetettuja velvoitteitaan. Viranomaisen arviointitoimintaa voitaisiin jatkossa harkita myös arvioitavan määrävälein.

4.3 Arviointien arviointiperustan määrittäminen

Julkisen hallinnon digitaalisten tietojärjestelmien turvallisuuden arviointiperusteiden tulee perustua säännöksiin. Digitaalisen turvallisuuden kehittäminen julkisessa hallinnossa edellyttää, että sen kaikille osa-alueille eli tietoturvalle, riskienhallinnalle, kyberturvallisuudelle, toiminnan jatkuvuudelle ja varautumiselle sekä tietosuojalle asetetaan vaatimukset. Arviointilait ottavat tällä hetkellä kantaa ainoastaan tietoturvallisuuteen ja painotus on turvallisuusluokitellun tiedon teknisessä suojaamisessa. Tärkeimmät tietojärjestelmiin liittyvät toiminnan jatkuvuuden ja varautumisen vaatimukset tulisi sisällyttää tiedonhallintalakiin.

Riskien arviointi toteutuksen perusteena on sekä tiedonhallintalain 13 §:n että käytännössä kaikkien kansainvälisten hallintaviitekehysten edellyttämä menettely. Arviointiperustaa tulisi kehittää edelleen siten, että arvioinneissa ja hyväksymisissä huomioidaan entistä paremmin riskien arviointiin perustuva toiminta. Tämä koskee myös hankintoja. Digitaalisten palvelujen suunnittelua, hankintoja ja tuottamista varten kukin viranomainen tarkentaa digitaaliselle turvallisuudelle asetettuja vähimmäisvaatimuksia. Tämä johtaa usein päällekkäiseen työhön viranomaisissa, arviointilaitoksissa ja palvelun tuottajissa. Tarvitaan siten julkisen hallinnon yhtenäisiä vähimmäisvaatimuksia.

Arviointiperusteiden määrittämisen ja vaatimusmäärittelyjen valintaa tulisi ohjata digitaalisten palvelujen riittävä turvallisuus palvelun koko elinkaaren aikana. Riittävyyden tasoa määritettäessä tulisi huomioida palvelussa käsiteltävien tietojen lisäksi myös palvelulle asetetut saatavuus- ja eheysvaatimukset. Jos palvelussa esimerkiksi käsitellään henkilötietoja, kohdistuu henkilötietojen käsittelyyn tietosuoja- ja tietoturvavaatimuksia turvaluokasta (tai sen puuttumisesta) riippumatta. Toisena esimerkkinä voivat olla turvallisuusviranomaisen julkiset verkkosivut, jotka pahantahtoinen hyökkääjä kaappaa. Tällöin sivuston kautta voidaan levittää virheellistä tietoa viranomaisen nimissä, mikä voi olla osa laajempaa hybridivaikuttamisoperaatiota. Tällaisen uhkan torjuminen edellyttää tietoturvan, toiminnan jatkuvuuden ja varautumisen riittävän vahvaa toteutusta. Vastuuta digitaalisen palvelun turvallisuudesta ja riskien ottamisesta ei voi ulkoistaa esimerkiksi sillä perusteella, ettei hallintakeinoa ole toteutettu, koska se ei ole sisältynyt palvelun vaatimusmäärittelyyn.

Arviointikriteeristöt tulisi muotoilla siten, että ne mukautuvat joustavasti digitaalisen toimintaympäristön nopean kehittymisen myötä. Niiden tulisi pohjautua kansainvälisiin standardeihin ja muihin yleisesti käytettyihin vaatimusluetteloihin[19] niiltä osin kuin kyse ei ole kansallisen lainsäädännön, kansallisen turvallisuuden, varautumisen tai muiden kansallisten erityispiirteiden arvioinneista, joita kansainväliset standardit eivät kata. Niiden toteutumista arvioitaessa on huomioitava palvelun käyttötarkoitus, palvelun käytön riskit, palvelussa käsiteltävien tietojen suojaaminen ja palvelun saatavuustarpeet. Hallintakeinojen toteutuksessa käytettyjen ratkaisujen tulee perustua tiedonhallintayksikön (tai vastaavan) ajantasaiseen riskiarvioon, jonka tiedonhallintayksikkö on hyväksynyt. Toisaalta palvelun arvioinnissa tulee huomioida myös tiedonhallintayksikön ja ulkopuolisen riippumattoman arvioinnin riskienarvioinnin eroavat roolit ja perusteet. Tiedonhallintayksikön riskienarvioinnissa korostuu viranomaisen toiminnan erityispiirteiden huomiointi. Ulkopuolisen riippumattoman arvioinnin roolina on puolestaan arvioida suojauksia tiedonkäsittelyyn kohdistuvia yleisiä riskejä vasten. Siten ulkopuolisessa arvioinnissa tulisi nousta esille esimerkiksi tilanteet, joissa tiedonhallintayksikön riskienarviointi on ollut puutteellinen eivätkä toteutetut suojaukset ole riittävän tehokkaita nykypäivän riskejä vastaan. Kuten nykytilassakin, ulkopuolisen arvioijan näkemys riskeistä tulisi pohjautua ajantasaiseen tilannekuvaan.

Julkisen hallinnon digitaalisten palvelujen turvallisuuden arvioinnissa käytettävässä arviointikriteeristössä tulee määritellä eri digitaalisen turvallisuuden osa-alueiden vähimmäiskriteerit, joiden avulla kaikkia palveluja arvioidaan. Sen lisäksi arviointikriteeristössä pitäisi osoittaa, missä tilanteissa, mihin riskeihin vastaten, millä perusteilla ja millä digitaalisen turvallisuuden osa-alueella tarvitaan vähimmäistason ylittäviä kriteerejä. Lisäksi tulisi kuvata, mitä nämä tilanteet, riskit, perusteet ja kriteerit ovat. Arviointikriteeristön tulee soveltua mm. palvelujen kehittämisen aikana tehtäviin arviointeihin,

[19] Esimerkiksi ISO-standardit, ISF, COBIT, PCI DSS, jne.

hankintavaiheessa palvelulle asetettujen vaatimusten todentamiseen sekä käytön aikaisiin arviointeihin. Oppivien ja itsenäisesti kehittyvien järjestelmien laajenevan käytön myötä tarvitaan myös näitä järjestelmiä koskevia arviointikriteerejä. Lisäksi huomiota tulisi kiinnittää eri toimialojen, kuten sosiaali- ja terveysalan tietoturvallisuuden arvioinneissa käytettyyn arviointiperustaan. Tiedonhallintalaissa olevat vähimmäisvaatimukset pitäisi tarkemmin yhteensovittaa myös näiden toimialakohtaisten vähimmäisvaatimusten ja arviointikriteerien kanssa.

Julkisen hallinnon digitaalisen turvallisuuden arviointikriteeristön laadinnassa voitaisiin hyödyntää kansallista riskiarviota, joka linjaa mihin tietoturvallisuusriskeihin valtionhallinnon toimijoiden on pystyttävä vastaamaan. Tässä yhteydessä voitaisiin huomioida kansallisten toimijoiden toisistaan poikkeavat uhkaprofiilit. Riskiarvion pohjalta voitaisiin johtaa vaatimukset, jotka liittyvät tunnistettuihin riskeihin. Kriteerit valitaan siten, että vaatimusten toteutumista voidaan arvioida. Tarvitaan myös vaatimuksiin pohjautuvat järjestelmä- ja palveluhankintojen hankintavaatimukset, joiden jatkuvasta kehittämisestä ja ylläpidosta on huolehdittava.

Titukri-raportissa[20] esitetään velvoitetta toimialakohtaisten vaatimusmäärittelyjen tekemiselle ja velvoitusta pyytää vaatimusmäärittelyistä lausunto Traficomin Kyberturvallisuuskeskukselta. Jos palvelua joudutaan arvioimaan usealla eri kriteeristöllä, arviointikustannukset kasvavat. Tiedonhallintalautakunnan tehtäviin kuuluu julkisen hallinnon tietoturvallisuuden arviointikriteeristön valmistelu. Tähän liittyen on valmisteltava myös toiminnan jatkuvuuden ja varautumisen arviointikriteeristö, jolla arvioitaisiin esimerkiksi sitä, mihin toimintoihin digitaalisen turvallisuuden vaarantuminen vaikuttaa tai mitkä palvelut voivat keskeytyä digitaalisen turvallisuuden vaarantumisen takia.

Toimialakohtaisten vaatimusten tai kriteerien ja niistä poikkeamisten tulisi perustua julkisesti saatavilla olevaan tietoon, määritelmiin ja Traficomin Kyberturvallisuuskeskuksen asiantuntijoiden kanssa yhteistyössä toteutettuihin vaatimuksiin sekä ohjeisiin. Toimialakohtaisten vaatimusten ajantasaisuutta ja päivitystarpeita tulisi seurata ja vaatimuksia tulisi tarvittaessa tarkentaa vuosittain esimerkiksi Kyberturvallisuuskeskuksen organisoimassa tarkastelufoorumissa, jonka näkemyksiä kuultaisiin Kyberturvallisuuskeskuksen ohjeita valmisteltaessa. Tällaisella menettelytavalla voitaisiin ennakoida ja puuttua vaatimusten sisältöön tarvittaessa sekä varmistaa, ettei vaatimusten hallintaan liity henkilöitymistä.

4.4 Arviointitoimeksiannon laatiminen

Akkreditoitu arviointilaitos suorittaa arvioinnin tilaajan toimeksiannosta. Arviointitoimeksiannossa asetetaan arvioinnin kohde, kerrotaan arvioinnissa käytettävät arviointiperusteet ja asetetaan arvioinnille aikataulu. Arvioinnin lopputuloksena syntyy raportti sen tuloksista sekä tilaajan niin pyytäessä myös todistus arviointiperusteena käytettävien vaatimusten toteutumisesta. Arvioinnin tilaajan kannalta on erityisen tärkeää, että arvioinnin toteutus aikatauluineen noudattaa toimeksiannossa tehtyä suunnitelmaa, jotta tilaajan työmäärä ja kustannukset voidaan ennakoida luotettavasti. Arviointitoimeksiannon kohdetta ja laajuutta asetettaessa tulisi huomioida tuotettava palvelu pelkän tietojärjestelmän tai tietoliikennejärjestelyn sijasta. Tulisi säätää, että arviointitehtävää hoitavan viranomaisen ja arviointilaitoksen on ilmoitettava tilaajalle arvio tai tarjous arvioinnin kestosta ja kustannuksista

[20] Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla, LVM 2021:1

kuukauden kuluessa arvioinnin tai arviointitarjouksen pyytämisestä siinä määritettyä arvioinnin kohdetta vastaavasti. Jos arvioinnin kohde tai laajuus muuttuu alustavasti määritellystä, voi arviointilaitos päivittää tarjousta vastaamaan tarkennettua kohdetta ja laajuutta. Jos tilaaja päättää arvioinnin kohteen tai laajuuden muutoksesta arviointiprosessin aikana, on arviointilaitoksella oikeus antaa muutoksista johtuvista töistä erillinen lisätyötarjous.

Tieto- ja viestintäteknisten palvelujen eli tietojärjestelmien ja tietoliikennejärjestelyjen elinkaaren eri vaiheissa vaatimustenmukaisuuden todentaminen tulee tarvittaessa toistaa seuranta-arvioineilla esimerkiksi toimintaympäristön muuttumisen takia. Vaatimusmäärittelyjen laatimisen helpottamiseksi ja arviointien tehostamiseksi julkishallinnon tarjoamia ja sen käyttämiä palveluja kehitettäessä sekä niitä hankittaessa tulee voida viitata samoihin vaatimuksiin, joita käytetään myöhemmin arvioitaessa palvelua sen käytön aikana.

Sekä viranomaisten että yhteisöjen tulisi voida tilata arviointeja tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen akkreditoiduilta arviointilaitoksilta niiden pätevyysalueilta ja niiden määrittämillä kustannuksilla. Toimeksiannon yhteydessä tilaaja määrittäisi arvioinnin kohteen ja arviointiperustan tai arviointiperusta määräytyisi säädösten perusteella (esimerkiksi tiedonhallintalaki). Tämä tarkoittaa, että esimerkiksi yhteishankintayksikkö voisi yrityksen tai viranomaisen puolesta tilata Katakri-kriteeristön perusteella tehtävän arvioinnin esimerkiksi yrityksen kilpailutuksessa tarjoamalle palvelulle. Vaatimustenmukaisuustodistus voitaisiin myöntää ainoastaan käytettäessä pätevyysalueen mukaista arviointiperustaa (esimerkiksi tiedonhallintalautakunnan antama kriteeristö tai Katakri). Tilaaja voi myös valita käytettäväksi velvoittavia säännöksiä tarkentavia tai laajentavia arviointikriteeristöjä, joiden mukaiselle arvioinnille arviointilaitoksella on pätevyys. Tilaaja voi käyttää tällaisen arvioinnin tuloksia esimerkiksi digitaalisen turvallisuutensa parantamiseksi, toimintansa kehittämiseksi tai vaatimustenmukaisuuden puutteidensa tunnistamiseksi.

4.5 Arvioinnin toteutus

Kansallisen digitaalisen turvallisuuden velvoittavasta arvioinnista ei ole riittävästi sääntelyä. Ehdotetaan, että sääntelyssä vahvennettaisiin tiedonhallintalailla tiedonhallintayksiköille asetettuja vaatimuksia ja asetettaisiin selkeä vaatimus sekä tiedonhallintayksikön toteuttamille itsearvioinneille että ulkopuolisille arvioinneille (vrt. tietoturvallisuuden hallintajärjestelmän standardin ISO 27001:2017 vaatimukset 9.2 ja A.18.2). Vaatimus ulkopuolisen arvioinnin tai todistuksen hankkimisesta säädettäisiin velvoittavaksi riskiarvioinnin perusteella niin, että se koskisi kriittisimpiä järjestelmiä ja toimintoja sekä korkeimpien turvallisuusluokkien järjestelmiä. Tulisi arvioida, riittäisikö itsearviointi joissain tapauksissa riittävän turvallisuuden varmistamiseksi, jos esim. arviointilaitos tarkastaisi itsearvioinnin. Lainsäädännössä tulisi tunnistaa ja ohjeistuksessa tulisi huomioida myös kevyempi, konsultoiva tietojärjestelmien tarkastus, jonka voisi suorittaa muukin kuin akkreditoitu arviointilaitos.

Valtiovarainministeriö arvioi valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietoturvaa koskevia vastuita ja velvoitteita. Säädettäisiin, että tiedonhallintayksiköt, mahdollisesti yhteistoiminnassa, arvioivat alihankkijoidensa tällaisia velvoitteita. Kriittisille palveluille tulee asettaa palvelukohtaisesti turvallisuus- ja toimintavarmuusvaatimukset. Palvelujen vaatimuksenmukaisuus arvioidaan hyväksytyn arviointityökalun kriteerien mukaisesti arviointityökalun määräytyessä kunkin

palvelun luonteen perusteella (esim. tiedonhallintalaissa (906/2019) säädetyt vaatimukset, ISO 27001, Katakri TL IV –tason vaatimukset). Arviointien velvoittavuudelle tulee säätää toimeenpanon vaatima siirtymäaika.

Nykytilassa Katakri- ja VAHTI-kriteeristöjen vaatimuskohtaiset todennusmenetelmät arvioidaan ja hyväksytään osana arviointilaitoksen akkreditointi- ja hyväksyntäprosessia, ja arviointilaitokset ovat jo nykytilassa velvoitettuja toimimaan hyväksytettyjen todennuskuvausten mukaisesti. Vastaava luotettavan todentamisen menettely tulisi laajentaa myös muiden pätevyysalueiden arviointeihin, jotta arviointilaitoksen arvioinnin tulokset eivät pohjautuisi esimerkiksi vain dokumentaation katselmointiin ja haastatteluihin. Tulee välttää tilannetta, jossa kriteeristö määrittelee hyväksyttävän toteutustavan. Kuten jo nykytilassa Katakri-kriteeristön arvioinneissa, arvioijalle tulee jatkossakin antaa mahdollisuus käyttää harkintaa ja hyväksyä myös vaihtoehtoisia toteutustapoja edellyttäen, että toteutustavat antavat vähintään samantasoisen suojan. Tarvittaisiin myös lisää selkeitä toteutusesimerkkejä, jotka kuvaisivat toteutusvaihtoehtoja erilaisiin tuotantoympäristöihin.

4.6 Vaatimustenmukaisuuden osoittaminen

Arvioinnin tulosten raportointi ja vaatimustenmukaisuuden osoittaminen ovat erillisiä käsitteitä. Akkreditoitujen arviointilaitosten tulisi tehdä arviointeja asetettujen vaatimusten täyttymisestä ja niiden täyttyessä antaa tätä koskeva todistus vaatimuksenmukaisuudesta kuten nykyisinkin ja samalla tavalla kuin kansainvälisten ISO-standardien sertifiointimenettely on toteutettu. Todistus vaatimuksenmukaisuudesta olisi voimassa esimerkiksi viisi vuotta, mutta todistuksen voimassaolo edellyttäisi säännöllisesti tehtäviä seuranta-arviointeja. Seuranta-arvioinnit voisivat olla varsinaista arviointia suppeampia ja ne voisivat kohdistua tarkennettuna johonkin erikseen sovittavaan palvelun tai vaatimusmäärittelyn osaan.

Jos arvioinnissa on todettu poikkeamia, niiden korjaamiseksi tulee laatia aikataulutettu suunnitelma ja arviointilaitoksen tulee arvioida tehdyt korjaukset ennen todistuksen myöntämistä. Poikkeamien määrästä ja laadusta riippuen palvelu voidaan ottaa käyttöön tai sen käyttöä voidaan jatkaa ehdollisesti, jos näin on palvelun vaatimuksia koskevassa säädännössä todettu ja sallittu. Arvioinnin kohteena olevan organisaation mahdollisuuksia hyväksyä digitaalisen turvallisuuden ratkaisut riskienhallinnan keinoin tulisi edistää. Riskienhallintatoimenpiteiden toteuttamisen ja jäännösriskien hyväksyntämenettelyn kautta palvelun käyttöönotto voisi olla sallittua, jos tämä palvelun vaatimuksia koskevassa säädännössä on todettu ja sallittu. Riskienhallinnasta ei kuitenkaan saa muodostua menettelyä, jolla digitalisen turvallisuuden vaatimukset ohitetaan.

Palveluntuottajat ja palvelujen kehittäjät voisivat käyttää vaatimustenmukaisuudesta annettavaa todistusta esimerkiksi osoittamaan palvelua hankkivalle viranomaiselle, että palvelu täyttää viranomaisen tietojärjestelmälle ja tietoliikennejärjestelylle asettamat vaatimukset, kun tällaiset vaatimukset on etukäteen asetettu. Viranomaisen tekemien palvelujen ja tuotteiden hankinta yksinkertaistuu ja palveluiden turvallisuustaso paranee, kun vaatimuksiin sisällytetään säännöllisesti toistuvat seuranta-arvioinnit. Seuranta-arviointeja on toistettava säännöllisesti. Seuranta-arviointien laajuuteen vaikuttavat tietojärjestelmään tai tietoliikennejärjestelyyn tehtyjen muutosten laajuus sekä toimintaympäristön muutokset kuten tunnistetuissa ulkoisissa uhkatekijöissä tapahtuvat muutokset.

LIITE 1: SELVITYKSEN VALMISTELURYHMÄT

Haukka-hankkeessa toimivaan tämän selvityksen valmisteluryhmään ovat kuuluneet Haukka-hankepäällikkö, tietohallintoneuvos Tuija Kuusisto, erityisasiantuntija Niko Mäkilä, lainsäädäntöneuvos Eeva Lantto, erityisasiantuntija Tomi Voutilainen sekä KPMG:n konsultteja.

Selvitystyötä on tukenut julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020-2023 (Haukka) mukainen säädösvalmistelun koordinointiryhmä, johon ovat kuuluneet:

- Aku Hilve, valtiovarainministeriö, puheenjohtaja (31.12.2020 asti)
- erityisasiantuntija Niko Mäkilä, valtiovarainministeriö, puheenjohtaja (1.1.2021 alkaen)
- tietohallintoneuvos, Haukka-hankepäällikkö Tuija Kuusisto, valtiovarainministeriö
- lainsäädäntöneuvos Eeva Lantto, valtiovarainministeriö
- erityisasiantuntija Mika Tuikkanen, valtiovarainministeriö
- tietohallintojohtaja Ari Uusikartano, ulkoministeriö
- lainsäädäntöneuvos Taina Riihinen, oikeusministeriö
- johtava asiantuntija Kimmo Janhunen, oikeusministeriö
- turvallisuuspäällikkö Kari Santalahti, sisäministeriö
- tietoturvapäällikkö Harri Mäntylä, puolustusministeriö
- hallitusneuvos Sami Aalto, opetus- ja kulttuuriministeriö, varajäsen erityisasiantuntija Laura Niemi, opetus- ja kulttuuriministeriö
- johtava tietohallintoasiantuntija Jaana Merta, maa- ja metsätalousministeriö
- ylitarkastaja Erica Karppinen, liikenne- ja viestintäministeriö, varajäsen kyberturvallisuusjohtaja Rauli Paananen, Traficom
- erityisasiantuntija Teemupekka Virtanen, sosiaali- ja terveysministeriö
- ylitarkastaja Roni Kiviharju; erityisasiantuntija Tomi Marjamäki, ympäristöministeriö
- johtava asiantuntija Ville Autero, työ- ja elinkeinoministeriö
- erityisasiantuntija Jari Ylikoski, Kuntaliitto
- tietoturvapäällikkö Kari Nykänen, Oulun kaupunki
- tietoturvapäällikkö Seppo Ruotsalainen, Kuopion kaupunki
- yksikönpäällikkö Eija Alavesa, Traficom
- johtaja Mikko Pitkänen, Digi- ja viestintävirasto
- johtaja Risto Suominen, FINAS
- johtava asiantuntija Tomi Kelo, Traficom
- johtaja Johanna Erkkilä, Traficom
- tietoturvapäällikkö Pia Satopää, Puolustusvoimat
- Petri Hakonen, Puolustusvoimat
- tietoturva-asiantuntija Jonna Ylikauppila, Kansaneläkelaitos
- yksikönjohtaja Pertti Nieminen, Kansaneläkelaitos

LIITE 2: SELVITYKSEEN LIITTYVÄT SÄÄNNÖKSET

Tietoturvallisuuden arviointia koskevia asioita sisältyy useaan säännökseen ja ohjeeseen. Kansallisen tietoturvallisuuden arviointitoiminnan kannalta keskeisimmät säännökset ovat luettelon alussa. Myös muihin säännöksiin ja ohjeisiin viitattiin haastatteluissa ja nykytilakuvauksen tarkentamiseksi käydyissä keskusteluissa.

- Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta (ns. NLF-asetus)
- 920/2005 Laki vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta
- 1405/2011 Laki tietoturvallisuuden arviointilaitoksista
- 1406/2011 Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista
- 906/2019 Laki julkisen hallinnon tiedonhallinnasta
- 1101/2019 Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta
- 588/2004 Laki kansainvälisistä tietoturvavelvoitteista
- EU 2016/679 (artiklat 42 - 43) Yleinen tietosuoja-asetus
- 552/2019 (21 - 34 §) Laki sosiaali- ja terveystietojen toissijaisesta käytöstä
- 159/2007 (19a - 19m §, 20 - 20g §) Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (asiakastietolaki)
- 1552/2011 (124 §) Valmiuslaki
- 1050/2018 Tietosuojalaki
- VM 2020:61 Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta (tiedonhallintalautakunnan suositukset)
- 210/2016 O Ohje tietoturvallisuuden arviointilaitoksille V8.2 (18.12.2020)
- Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit – Tilaajaorganisaation näkökulma (3.9.2019)

Selvitykseen liittyvissä haastatteluissa viitattiin alla olevan listan hallintaviitekehyksiin, vaatimusmäärittelyihin ja arviointikriteeristöihin:

- ISO 27001 - tietoturvallisuus
- ISO 22301 - toiminnan jatkuvuus
- ISO 31000 - riskienhallinta
- VM 22/2017 - riskienhallinta (ISO31000)
- THL määräys 1/2015 liite 1 - A-luokan järjestelmien tietoturvavaatimukset
- Traficom M67A - Teletoiminnan tietoturva
- Katakri 2020 - kyberturvallisuus
- VAHTI 2/2010 – tietoturva (vanh.)
- VAHTI 2/2016 - toiminnan jatkuvuus
- VAHTI 2/2012 - ICT-varautuminen (vanh.)

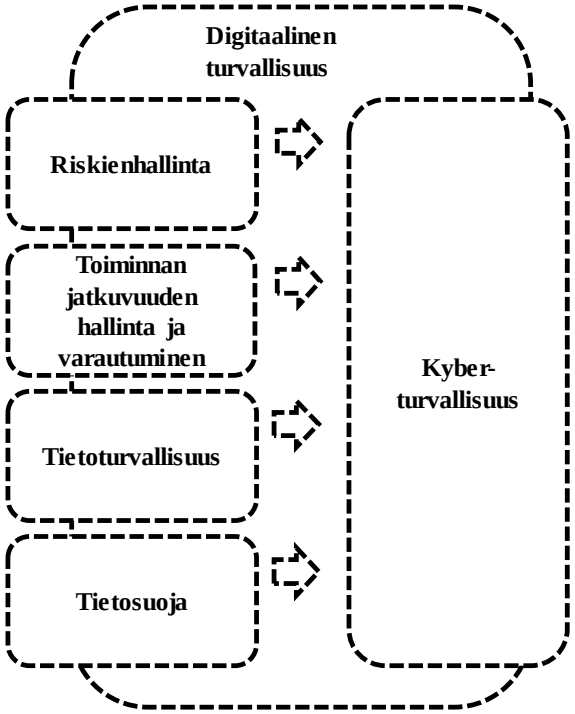
LIITE 3: HAASTATTELUT

Pvm	Haastateltu organisaatio
24.11.2020	Inspecta Sertifiointi
30.11.2020	TietoEvry
1.12.2020	Fimea
1.12.2020	Nixu Certifications Oy
1.12.2020	Huld
4.12.2020	Valtori
9.12.2020	valtioneuvoston kanslia
9.12.2020	Suomen Erillisverkot Oy
10.12.2020	Fujitsu Finland Oy
12.1.2021	tietosuojavaltuutetun toimisto
13.1.2021	Kyberturvallisuuskeskus
18.1.2021	Valvira
18.1.2021	Hansel
19.1.2021	KPMG IT Sertifiointi Oy
20.1.2021	Poliisihallitus
21.1.2021	ulkoministeriö (UM)
22.1.2021	Rajavartiolaitos
25.1.2021	suojelupoliisi
25.1.2021	Traficom
26.1.2021	Puolustusvoimat
26.1.2021	Kuntaliitto
27.1.2021	FINAS
2.2.2021	työ- ja elinkeinoministeriö (TEM)

LIITE 4: TERMIT

Digitaalinen turvallisuus

Digitaalisen turvallisuuden viitekehykseen sisältyy riskienhallintaan, toiminnan jatkuvuudenhallintaan ja varautumiseen sekä kyberturvallisuuteen, tietoturvallisuuteen ja tietosuojaan liittyviä asioita[21]. Terminä uusi ja vakiintumaton. Usein kyberturvallisuuden synonyymi. OECD:ssä on käytössä termi digital security[22].



Kyberturvallisuus

Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan[23]. Kybertoimintaympäristön synonyyminä voidaan käyttää termiä digitaalinen toimintaympäristö. Yleisesti ottaen termillä tarkoitetaan tavoitetilaa, jossa digitaalisessa ympäristössä olevat tiedot ja prosessit on suojattu erilaisilta, erityisesti ulkopuolelta tulevilta uhkilta liittyen luottamuksellisuuteen, eheyteen ja käytettävyyteen.

Tietoturvallisuus

Järjestelyt, joilla pyritään varmistamaan tiedon luottamuksellisuus, eheys ja saatavuus[24]. Tavoitetila, jossa digitaalisessa ympäristössä olevat tiedot ja prosessit on suojattu luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyviltä uhilta. Vanhempi termi, joka on

[21] Julkisen hallinnon digitaalinen turvallisuus, VM 2020:23
[22] Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document, 2015
[23] Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)
[24] Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)

	tarkoittanut samaa asiaa kuin digitaalinen turvallisuus tai kyberturvallisuus. Tässä dokumentissa tietoturvallisuudella tarkoitetaan sitä digitaalisen turvallisuuden aluetta, joka ei ole kyberturvallisuutta.
Tietosuoja	Ihmisten yksityisyyden suojeleminen ja yksilöä koskevien tietojen suojaaminen oikeudettomalta käytöltä henkilötietoja käsiteltäessä[25].
Riskienhallinta	Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet[26].
Jatkuvuudenhallinta	Organisaation prosessi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle kaikissa olosuhteissa[27].
Varautuminen	Toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa[28].

[25] Sanastokeskus TSK TEPA-termipankki, Tieteen termipankki 06.08.2019
[26] Sanastokeskus TSK TEPA-termipankki, Kokonaisturvallisuuden sanasto (TSK 50, 2017)
[27] Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)
[28] Sanastokeskus TSK TEPA-termipankki, Kokonaisturvallisuuden sanasto (TSK 50, 2017)