VALTIOVARAINMINISTERIÖ

Selvitys digitaalisen turvallisuuden arvioinnin kehitystarpeista

LUONNOS
18.2.2021

Sisällys

TIIVISTELMÄ

Tässä raportissa kuvataan julkisen hallinnon digitaalisen turvallisuuden arvioinnin tunnistettuja haasteita ja esitetään näitä korjaavia kehitystoimenpiteitä. 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 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 hyväksymisen sijaan digitaalisen turvallisuuden lähtökohtana tulisi olla 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 arviointitoimintaa koskeva lainsäädäntö rajoittuu arviointilain osalta tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuteen, jonka painopiste on teknisen tietoturvallisuuden arvioinnissa. Kaikille digitaalisen turvallisuuden osa-alueille ei ole säännöksissä asetettuja arviointiperusteita, kuten vähimmäisvaatimuksia ja arviointikriteeristöjä. Turvallisuuden riittävän tason määrittely kuitenkin edellyttää, että kaikille digitaalisen turvallisuuden osa-alueille määritellään arviointiperusteet, joiden avulla vähimmäisvaatimusten toteutuminen tai muu vaatimustenmukaisuus voidaan todeta luotettavasti.

Selvitystä varten haastateltiin 23 eri organisaation asiantuntijaa. Selvityksessä kuvattu nykytila perustuu näistä haastatteluista saatuihin näkemyksiin. Hyväksytyn arviointilaitoksen aseman saavuttamiseksi yhteisön täytyy tällä hetkellä hakea ensin kansallisen akkreditointiyksikön (FINAS) akkreditointi, minkä jälkeen sen on haettava erikseen Traficomin hyväksyntä (1405/2011 5 §). Ensimmäisen osan vaatimustenmukaisuuden osoittaminen on kirjattu lakiin (920/2005) ja jälkimmäinen osa on säädetty arviointilaitoslakiin (1405/2011 5.3 §). Haastatteluissa todettiin, että hakuprosessin pitkä kesto ja pätevyyden arvioinnissa käytettyjen kriteerien tulkinnanvaraisuudet ovat merkittäviä markkinoille pääsyn hidasteita. Haastatteluissa todettiin, että henkilöiden vaihtuvuuden takia prosessien ja kriteerien tulkinnoissa on henkilöriippuvuutta. Arviointien pätevyysalueiden vaatimusten pitäisi perustua julkisesti saatavilla oleviin määrityksiin, jotka johdetaan säädöksistä ja soveltuvin osin kansainvälistä vaatimuksista. Kaikille kaupallisille arviointeja tekeville arviointilaitoksille on asetettu samat vaatimukset seurannalle, raportoinnille ja kyseisen arviointilaitoksen pätevyysalueille.

Riippumattomia ja luotettavia tietoturvallisuuden arviointeja voivat tällä hetkellä tehdä hyväksytyt arviointilaitokset pätevyysalueidensa puitteissa sekä Liikenne- ja viestintävirasto. Kaupalliset toimijat hinnoittelevat arviointipalvelunsa markkinaehtoisesti, kun taas viraston hinnoittelun on noudatettava säänneltyjä maksuperusteita (1406/2011 12 §). Toisaalta kaupalliset arviointilaitokset voivat mukauttaa resurssejaan virastoa joustavammin, eikä viranomaisresurssien jatkuvaa lisäämistä voida pi-

tää kokonaistaloudellisuuden näkökulmasta kestävänä ratkaisuna. Digitaalisen turvallisuuden arvioinnit tulisikin yhä laajemmin toteuttaa markkinaehtoisesti toimivien hyväksyttyjen arviointilaitosten tehtävinä. Digitaalisen turvallisuuden arviointilaitosten pätevyyden arviointi (akkreditointi) voisi olla yksin kansallisen akkreditointiyksikön (vrt. 920/2005) tehtävä ja akkreditoinnin jälkeen arviointilaitos voisi toimia akkreditoituna arviointilaitoksena.

Haastatteluissa todettiin, että tietoturvallisuuden arviointiperusteissa on tulkinnanvaraisuuksia koskien vähimmäisvaatimuksia ja arviointikriteeristöjä, soveltuvia vaatimukset täyttäviä toteutuksia ja hyväksyttäviä teknisiä ratkaisuja. Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:n mukaan ”*Kyberturvallisuuskeskuksen toiminta edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden toteutumista*”. Toimintaympäristön digitalisoitumisen aiheuttaman jatkuvan muutoksen takia arviointeja tilaavat viranomaiset pyytävät Liikenne- ja viestintävirastolta (Traficom) tulkintoja ja linjauksia tietojärjestelmäturvallisuuden toteuttamisesta. Toimintaympäristön muutoksista johtuen nämä arviointiperusteiden tulkintaa tai toteutusten teknisiä yksityiskohtia koskevat linjaukset ja tulkinnat ovat vain osin vakiintuneita. Haastatteluissa todettiin, että henkilöiden vaihtuvuuden takia tulkinnoissa on myös henkilöriippuvuutta. Tulkintapyyntöjen on koettu hidastavan merkittävästi niin palvelujen tuottajien, arviointilaitosten kuin arviointeja tilaavien viranomaisten ja yhteisöjen toimintaa. Arviointilaitoksella ei ole velvollisuutta pyytää tulkintalinjauksia yksittäiseen arvioon liittyen, mutta haastatteluissa todettiin, että tulkinnan pyytäminen koetaan usein välttämättömäksi.

Haastatteluissa todettiin, että sääntely ei tällä hetkellä riittävästi velvoita vaatimustenmukaisuuden säännölliseen ja jatkuvaan varmistamiseen. Tiedonhallintalakiin (906/2019) on kuitenkin 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 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. Ehdotettiinkin, 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).

Yksi keino arvioida ja tunnistaa järjestelmään kohdistuvia turvallisuusriskejä on järjestelmän tietoturvallisuusarviointi. Arviointilain mukaista arviointia ei ole kansallisella tasolla säädetty pakolliseksi eikä viranomaisella ole velvollisuutta hankkia arviointilaissa tarkoitettua todistusta siitä, että tietojärjestelmä täyttää vaatimukset. Todistuksen saamiseen liittyvät muutosten, poikkeamien ja haavoittuvuuksien prosessi on kuvattu Traficomin ohjeessa "Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit". Haastatteluissa toivottiin tarkennuksia muu-

tosten, poikkeamien ja haavoittuvuuksien hallinnalle sekä käsittelylle, joille 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) Varmistetaan, että kansallinen akkreditointiyksikkö FINAS arvioi tietoturvallisuuden lisäksi myös varautumisen ja toiminnan jatkuvuuden arviointilaitosten pätevyyksiä määrävälein. FINAS voi käyttää muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä. Määritystyöhön näissä viranomaisissa osallistuvat virkamiehet eivät saa osallistua arviointilaitoksen toimintaan arvioijina.

2) Tiedonhallintalautakunta antaa yleiset tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vähimmäisvaatimusten arviointikriteerit ja arviointilaitoksen akkreditointiin liittyvät vaatimukset. Digi- ja väestötietovirasto tukee tiedonhallintalautakuntaa arviointikriteerityössä ja FINASia em. vaatimustenmukaisuuden arvioinnissa.

3) Traficomille säädetään tehtäviksi toimiminen tietoturvallisuuden lisäksi myös varautumisen ja toiminnan jatkuvuuden arviointilaitoksena sille säädetyillä pätevyysalueilla. FINAS arvioi myös näiden ns. viranomaisarviointilaitosten pätevyyden määrävälein. Näiden arviointilaitosten pätevyysalueita ovat tiedonhallintalain tarkoittamia turvallisuusluokkien III, II ja I tarkoittamia tietoja käsittelevät palvelut sekä niiden hallintajärjestelmät. Nämä viranomaisarviointilaitokset eivät arvioi fyysistä turvallisuutta, vaan tiedonhallintayksikön ja sen tilaaman fyysisen turvallisuuden arvioinnista säädetään kansallisellakin tasolla, esimerkiksi Suojelupoliisin tehtäväksi.

4) FINAS akkreditoi kaupallisia tietoturvallisuuden sekä lisäksi varautumisen ja toiminnan jatkuvuuden arviointilaitoksia hakijan hakemuksessa esittämille pätevyysalueille. Mahdolliset kilpailuoikeudelliset syyt erottaa kaupallisten arviointilaitosten ja viranomaisarviointilaitosten pätevyysalueet selvitetään. FINAS ylläpitää kuvausta mahdollisista pätevyysalueista. Pätevyysalueet voivat kattaa turvallisuusluokitteluasetuksen turvallisuusluokan IV ja III ja salassa pidettäviä ja julkisia tietoja käsittelevät palvelut sekä niiden hallintajärjestelmät. Arviointitoimeksiannot voivat koskea kuten nykyisinkin tiedonhallintalain tarkoittamia tiedonhallintayksiköitä sekä yksityistä sektoria. Arviointitoimeksiannot voivat sisältää myös arvioinnin kohteeseen liittyvän fyysisen turvallisuuden arvioinnin.

5) Tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden akkreditoitu arviointilaitos antaa arvioinnin tuloksiin perustuvan raportin. Jos arvioinnin kohde täyttää asetetut vaatimukset, niin arviointilaitos antaa erillisen todistuksen vaatimustenmukaisuudesta eli hyväksynnän. Kansallisella tasolla hyväksynnän voisivat siten antaa muutkin kuin viranomaisarviointilaitokset.

6) Viranomaiset ja yhteisöt voivat tilata arviointeja tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden akkreditoiduilta arviointilaitoksilta niiden pätevyysalueilta ja niiden määrittämillä kustannuksilla. Toimeksiannon yhteydessä tilaaja määrittää arvioinnin kohteen ja arviointiperustan tai arviointiperusta määräytyy säädösten perusteella. Vaatimustenmukaisuustodistus voidaan myöntää ainoastaan käytettäessä pätevyysalueen mukaista arviointiperustaa (esimerkiksi tiedonhallintalautakunnan antama kriteeristö tai Katakri).

7) Tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vaatimustenmukaisuuden arvioinnin tilaajan on osoitettava säännöllisillä seuranta-arvioinneilla palvelun turvallisuuden tason ylläpitäminen ja parantaminen. Säädetään tähän liittyvistä seuranta- ja valvontamenettelyistä.

8) Arvioidaan valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietoturvallisuutta, varautumista ja toiminnan jatkuvuutta koskevia vastuita ja velvoitteita. Lähtökohtana on, että yhteisille palveluille asetetaan palvelukohtaisesti tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vaatimukset.

9) Velvoitetaan suurimpia kuntien digitaalisten palvelujen tuottajia arvioimaan tuottamiensa palveluiden tietoturvallisuutta, varautumista sekä toiminnan jatkuvuutta säännöllisesti.

Haastatteluissa todettiin, että arviointiperusteiden tulee perustua normiohjaukseen ja kansainvälisesti käytössä oleviin vaatimusmäärittelyihin, joita voidaan täydentää kansallisilla vaatimuksilla, jos se on välttämätöntä. EU:n ja muiden kansainvälisten organisaatioiden sekä kahdenvälisten sopimusten tiedolle asettamat turvallisuusvaatimukset on usein otettava huomioon myös kansallisissa järjestelmissä. Vaatimusten tulee kattaa niin varautuminen ja toiminnan jatkuvuuden varmistaminen, tekninen ja hallinnollinen tietoturva, riskienhallinnan menettelyt kuin myös tietosuojavaatimukset. Digitaalisen turvallisuuden kehittämiseksi vaatimukset tulisi antaa laissa ja asetuksissa annettuja vaatimuksia tarkentavina velvoittavina määräyksinä suositusten tai ohjeiden sijaan huomioiden PL 80.2 §:stä johtuvat rajoitteet sekä sääntelykohteet. Vaatimusten asettamisessa on huomioitava digitaalisen toimintaympäristön nopea kehittyminen siten, että vaatimuksia voidaan tarvittaessa joustavasti muokata ja täydentää ylemmän tason sääntelyn pysyessä pitempään muuttumattomina.

Ehdotettujen digitaalisen turvallisuuden arviointia koskevien kehittämistoimenpiteiden suunnittelun ja toteuttamisen arvioidaan vaativan asiantuntijatyötä arviolta noin 10 htv eli 900 000 euroa. Julkisessa hallinnossa jo työskentelevät virkamiehet voivat ainakin osittain toteuttaa nämä valmistelu- ja toimeenpanotehtävät, joten kustannus ei ole kokonaisuutena uutta kustannusta. FINASin roolin vahvistaminen tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden arviointilaitosten akkreditoijana voi edellyttää lisäresursseja, jos hakemusten määrä pätevyyden arvioimiseksi merkittävästi kasvaa. FINASin akkreditointiprosessissa käyttämien toimialakohtaisten vaatimusten määrityksessä sekä arviointilaitoksiksi hakevien pätevyyksien arvioinnissa tarvitaan muiden viranomaisten tukea, mikä kasvattaa resurssitarvetta näissä viranomaisissa. Kehittämistoimenpiteiden toteuttaminen ei edellytä merkittäviä lisäyksiä arviointitoiminnan resursointiin ja siten jatkuviin kustannuksiin. Tämän taloudellisen tarkastelun ulkopuolelle on rajattu viranomaisia velvoittavien arviointien ja säännöllisten seuranta-arviointien mahdolliset kustannusvaikutukset. Kehittämistoimenpiteiden toteuttamisen arvioidaan mahdollistavan arviointitoiminnan laajentumisen ja syvenemisen, minkä avulla julkisen

hallinnon sekä koko yhteiskunnan digitaalisen turvallisuuden tilan voidaan olettaa parantuvan. Tämän ennakoidaan vähentävän väistämättä tietoturvallisuuden häiriötilanteista aiheutuvia kustannuksia.

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.

Tehtävän toteuttaa valtiovarainministeriön Haukka-hankkeessa toimiva valmisteluryhmä. Tehtävää tukemaan valtiovarainministeriön julkisen hallinnon ICT-osasto asetti säädösvalmistelun koordinaatioryhmän kaudelle 1.9.2020 – 31.12.2021. Koordinaatioryhmän jäsenet ovat lueteltu liitteessä 2. Selvitysraporttia on käsitelty koordinaatioryhmän kokouksissa. Koordinaatioryhmä ei ole osallistunut kehittämisehdotusten valmisteluun tai ohjaukseen. Selvitysraportin tarkoituksena on tukea varsinaista digitaalisen turvallisuuden arvioinnin kehittämisen säädösvalmistelutyötä. Selvitysraportissa kuvataan julkisen hallinnon digitaalisen turvallisuuden arvioinnin tunnistettuja haasteita ja esitetään näitä korjaavia kehitystoimenpiteitä. Selvitysraportin kehittämisehdotukset perustuvat haastatteluissa kerätyn aineiston perusteella valtiovarainministeriössä muodostettuun näkemyksiin kehittämistarpeista. Tehtävään liittyviä säännöksiä ja ohjeita on lueteltu liitteessä 3.

1.2 Työn toteutus

1.2.1 Haastattelut ja työpajat

Työ toteutettiin haastattelemalla arviointeja teettäviä virastojen, Traficomin, kaupallisten arviointilaitosten, sekä arviointien kohteina olevien palveluntarjoajien edustajia. Haastattelijoina toimi valtiovarainministeriön Haukka-projektiryhmä. 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. Haukka-säädösvalmistelun koordinaatioryhmän näkemyksiä kartoitettiin 11.11.2020 järjestetyssä työpajassa sekä koordinaatioryhmän kokouksissa.

Haastattelut toteutettiin joulukuun 2020 ja tammikuun 2021 aikana ja niitä tehtiin yhteensä 23. Haastattelujen aikataulu ja haastatellut organisaatiot ovat liitteenä 4.

1.2.2 Rajaus

Digitaalinen turvallisuus määritellään tässä asiayhteydessä samoin kuin valtioneuvoston julkisen hallinnon digitaalisen turvallisuuden kehittämisen periaatepäätöksessä (VM 2020:23; ks. liite 5). Digitaaliseen turvallisuuteen kuuluvat riskienhallinta, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus, kyberturvallisuus ja tietosuoja.

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 on käsitelty yleisellä tasolla.

1.3 Määritelmistä

Tässä raportissa käytetään termiä ”akkreditoitu arviointilaitos”, jolla viitataan arviointilaitokseen, joka on onnistuneesti läpäissyt pätevyyden arvioinnin. Tavoitetilassa kansallinen akkreditointiyksikkö (FINAS) arvioi ennalta asetetun kriteeristön mukaisesti arviointilaitoksen toiminnan vaatimustenmukaisuutta (akkreditointi) sekä yleisten että toimialakohtaisten vaatimusten osalta.

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, prosessi tai järjestelmän vaatimustenmukaisuudesta (vrt. 920/2005 4.1 § 9 k).

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

2 YHTEENVETO ARVIOINTITOIMINNAN NYKYTILASTA

2.1 Arviointitoiminnan rakenteet

2.1.1 Toimivalta ja soveltamisala

Tietoturvallisuuden arviointitoiminnan toimivaltaisia viranomaisia ovat valtiovarainministeriö ja Traficom. Valtiovarainministeriö voi pyytää valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraamiseksi sekä niiden kehittämiseksi Viestintävirastoa laatimaan selvityksen valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta. Traficom hyväksyy tietoturvallisuuden arviointilaitokset (1405/2011), joita valtionhallinnon viranomaiset voivat käyttää arviointien toteuttamiseksi (1406/2011 3 §). Traficomin tehtäviin kuuluvat myös mm. viranomaisen tietojärjestelmien ja tietoliikennejärjestelyjen arviointi, hyväksymistodistuksen antaminen sekä yleistä tietoturvallisuuden tasoa koskevien selvitysten tekeminen valtionhallinnon viranomaisen tietojärjestelmistä tai tietoliikennejärjestelyistä (1406/2011 4 §).

Kansainvälisten tietoturvavelvoitteiden vastuista on säädetty kansainvälisistä tietoturvavelvoitteista annetussa laissa (588/2004). Ulkoministeriö toimii kansainvälisten tietoturvavelvoitteiden toteuttamisessa kansallisena turvallisuusviranomaisena ja *Viestintävirasto* tietojärjestelmien ja tietoliikennejärjestelyjen 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 §).

Tietosuojan arviointielinten akkreditointi on säädetty tietosuojavaltuutetun tehtäväksi (1050/2018 14.4 §) EU:n yleisen tietosuoja-asetuksen perusteella. Tietosuoja-asetuksen perusteella annettavia vaatimusmäärittelyjä valmistellaan, mutta työ on vielä kesken, eikä tietosuojan vaatimusmäärittelyn toteutumista tekeviä arviointilaitoksia näin ollen 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 ISO27001-standardin laajennus henkilötietojen käsittelyn suojaamiseksi. Organisaatiot voivat sertifioida hallintajärjestelmänsä standardin mukaisesti, mutta sertifiointi ei riitä osoittamaan yleisen tietosuoja-asetuksen vaatimusten täyttymistä.

Arviointilain (1406/2011) soveltamisala on rajattu viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointiin. Arviointilaitoslain (1405/2011) soveltamisalana on ”*elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason (tietoturvallisuuden arviointilaitos) ja jotka haluavat toiminnalleen Viestintäviraston hyväksynnän*” sekä lain soveltaminen arviointilaitosten hyväksymismenettelyyn (1405/2011 2 §). Tietoturvallisuudella tarkoitetaan luottamuksellisuuden, saatavuuden ja eheyden varmistamista (ks. liite 5). Tietoturvallisuuden katsotaan tässä yhteydessä olevan yksi digitaalisen

turvallisuuden osa, joten arviointilain näkökulma on varsin kapea. Lisäksi arviointilain mukainen arviointitoiminta kohdistuu vain tietojärjestelmiin ja tietoliikennejärjestelyihin digitaalisten palvelujen kokonaisvaltaisen turvallisuuden sijaan. Lisäksi haastatteluissa todettiin, että viranomaisen fyysisen turvallisuuden arviointitehtävää ei ole säädetty yhdellekään viranomaiselle.

2.1.2 Arviointilaitoksen akkreditointi ja seuranta

Arviointilaitoslain (1405/2011) 5 §:n mukaisesti tietoturvallisuuden arviointilaitoksen hyväksymiseksi tarvitaan sekä FINASin akkreditointi (5.1 § 1-3 k) että Traficomin hyväksyntä (5.1 § 4-5 k) omana, erillisenä arviointinaan. Traficom toimii FINAS:in asiantuntijana FINAS-prosessissa (kohdat 1-3) ja auttaa mm. näyttöauditointien kanssa. Kohtien 4 ja 5 tarkoituksena on varmistaa, että arviointilaitoksen oma tietoturvallisuus on riittävällä tasolla, jotta arviointilaitosten asiakkaiden turvallisuusluokitellut tiedot eivät vaarantuisi. Arviointilaitoksen hyväksyntäprosessin tarkkaa nykytilakuvausta ei ole saatavilla.

Traficom voi myöntää organisaatiolle hyväksytyn arviointilaitoksen aseman. FINASin suorittama tietoturvallisuuden arviointilaitosten akkreditointi perustuu yleisesti saatavilla oleviin, kansainvälisesti vahvistettuihin standardeihin.[1] Huomioitavaa kuitenkin on, että nämä kansainväliset standardit eivät ota kantaa viranomaisten turvallisuusluokitellun tiedon arvioinnin erityispiirteisiin, vaan painottuvat tietoturvallisuuden hallintajärjestelmän näkökulmaan. Kansainväliset standardit eivät huomioi myöskään kansallisen lainsäädäntömme erityispiirteitä. Näin ollen pelkkä nojautuminen kansainvälisiin standardeihin on riittämätöntä arviointilaitosten akkreditoinnissa. Traficomin suorittaman arvioinnin vaatimukset vastuuhenkilöiden luotettavuudesta, hakijan menettelytavoista ja ohjeista sekä pätevyysalueista ja niille asetetuista vaatimuksista perustuvat arviointilaitoslakiin ja lakiin vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta. Traficomin ohjeessa on täsmennetty ohjeistuksia arviointilaitokseksi hakeutumisesta.

Arviointilakien muotoilut Viestintäviraston ja hyväksyttyjen arviointilaitosten vastuista ja velvollisuuksista koetaan haastattelujen perusteella tulkinnanvaraisiksi. Ajan myötä tilanne on osittain vakiintunut ja toimivaltasuhteet koetaan nykytilanteessa melko selkeiksi. Traficomin ohjeessa 210/2016 O on kuvattu, miten hyväksyntäprosessi etenee. Jaettu vastuu, 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.

[1] Päätös P1/2018 11.6.2018 (FINAS)

2.1.3 Arviointilaitosten pätevyysalueet ja niiden arviointi

Traficom pitää yllä listaa hyväksymistään arviointilaitoksista. Akkreditoitu arviointilaitos voi tehdä tietoturvallisuuden arviointeja Traficomin myöntämän pätevyysalueensa puitteissa. Tietoturvallisuuden arviointilaitoksille hyväksytyt pätevyysalueet ovat tällä hetkellä VAHTI, Katakri TL IV, Katakri TL III sekä ISO27001. Arviointilaitoksella on oltava ISO27001 yhtenä pätevyysalueenaan. Jos arviointilaitoksella on pätevyysalueenaan VAHTI tai Katakri, se saa automaattisesti oikeuden suorittaa 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 terveydenhuollon asiakastietojen sähköisestä käsittelystä annetussa laissa (159/2007, *asiakastietolaki*) kuvatuille A-luokan järjestelmille[2] sekä sosiaali- ja terveystietojen toissijaisesta käytöstä annetussa laissa (552/2009, *toisiolaki*) kuvatuille käyttöympäristöille[3].

Pätevyysalueen hyväksyntä perustuu arviointilaitoslakiin ja lakiin vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta. Traficomin ohjeessa on täsmennetty ohjeistuksia arviointilaitokseksi hakeutumisesta. Traficomin ohjeessa (210/2016 O V8.2) arviointilaitoksen edellytetään toteuttavan Katakrin vaatimukset yhtä tasoa ylempää kuin mille se hakee hyväksyntää. Tämä johtuu siitä, että arviointilaitoksella tulee olla kyky käsitellä loppuasiakkaansa luokittelemaa tietoa sille asetettujen suojausvaatimusten mukaisesti. Arviointilaitoksen arvioidessa esimerkiksi loppuasiakkaansa TL IV-tason järjestelmää, tulee arviointilaitos saamaan 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 mikä on korkein järjestelmässä käsiteltävä tieto. Myös eri loppuasiakkaiden tiedoista koostuvan tietovarannon turvallisuusluokka on usein tulkittavissa kasautumisvaikutuksesta johtuen yksittäisten tietojen turvallisuusluokkaa korkeammaksi.

Arviointilaitoksilla on mahdollisuus sisällyttää tietojenkäsittely-ympäristökseen eri luokille soveltuvia ympäristöjä, esim. TL IV, TL III tai/ja TL II, ja toteuttaa tietojenkäsittely luokittain ko. ympäristöissä. Edellä kuvatusta johtuen arviointilaitoksen on toteutettava Katakrin TL IV -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). Auditointityökalua sovelletaan myös arviointilain mukaiseen tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden arviointiin (Katakri 2020, s. 109). Katakria käytetäänkin arviointilaitosten hyväksyntäprosessissa sen käyttötarkoituksen mukaisesti arviointilaitoksen tiedonsuojaamiskyvykkyyden arviointiin.

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

2.1.4 Arviointitoiminta

Traficomin tekemästä hyväksynnästä käytetään Traficomin arviointilaitosohjeessa (210/2016 O)[4] nimeä "viranomaishyväksyntä" erotuksena kaupallisen arviointilaitoksen myöntämästä todistuksesta (vrt. 1045/2011 9.3 §). 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. Haastattelujen 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.

Ainoastaan Traficom voi arviointilaitosten nykyisistä pätevyysalueista johtuen tehdä korkeimpien turvaluokkien järjestelmien (TL II ja TL I) arviointeja. Se voi kuitenkin tehdä arviointeja myös alempien turvaluokkien (TL IV ja TL III) tietojärjestelmistä tai tietoliikenneratkaisuista. Jälkimmäisessä tapauksessa Traficom kilpailee 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.

Tyypillisesti kansallisten tietojärjestelmien ja tietoliikennejärjestelyjen arviointeja teetetään akkreditoiduilla arviointilaitoksilla siten että arviointilaitos antaa arvioinnin tilaajalle arviointiraportin. Kansallisille arvioinneille on vain harvoin haettu todistusta. Haastattelujen perusteella todistusta ei haeta, koska sen saamiseen arvioidaan kuluvan liian kauan aikaa. Erityisesti yhteisten tieto- ja viestintäteknisten palvelujen osalta todistuksia palvelun tietoturvallisuuden tilasta olisi mahdollista laajemminkin hyödyntää siihen, että palvelujen tiedonhallintayksiköt voisivat helpommin arvioida tietoturvallisuuden tasoa. Haastatteluissa esitettiin näkemys, että koska hyväksyntää ja siihen liittyvää todistusta tietoturvallisuuden tilasta ei ole saatavilla, niin palvelun jokaisen tiedonhallintayksikön on itse tehtävä päätös palvelun käyttämiseen liittyvistä tietoturvallisuuden rajauksista usein vajavaisin tiedoin tai puutteellisella osaamisella. Lisäksi on huomioitava, että yhteisten palvelujen tuottajien tilaamat arviointiraportit ovat käytännössä aina salassa pidettäviä ulkopuolisille, eikä tiedonhallintayksiköillä 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.

Nykytilanteessa tietoturvallisuuden vaatimukset koetaan tulkinnanvaraisiksi. Sekä arviointilaitokset että palveluntuottajat ovat pyytäneet Traficomilta tulkintoja Katakri-kriteeristön osalta. Tulkinnat tehdään virkavastuulla ja ne ovat luonteeltaan yleisiä. Arviointilaitoksella tulee olla pätevyysalueensa mukainen osaaminen yksittäisissä arvioinneissa nousevien tulkintakysymysten ratkaisemiseksi.

[4] 210/2016 O V8.2 kappale 3.5

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*”[5]. Lautakunnan mahdollinen rooli arviointiperusteiden tulkintojen tai niihin liittyvien linjausten antajana ei käy ilmi Traficomin ohjeissa.

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, joten arviointia joudutaan tekemään ainakin osittain uudestaan arvioinnin kestäessä. Tämän johdosta arviointeja tilaavat viranomaiset ja arviointilaitokset usein pyytävät Liikenne- ja viestintävirastolta (Traficom) tulkintoja ja linjauksia tietojärjestelmäturvallisuuden toteuttamisesta. Toimintaympäristön muutoksista johtuen nämä arviointiperusteiden tulkintaa tai toteutusten teknisiä yksityiskohtia koskevat linjaukset ja tulkinnat ovat 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. Muuttuvien tulkintojen takia palveluntuottajat voivat joutua tekemään järjestelmiin merkittäviä teknisiä ja toiminnallisia muutoksia ja muutosten takia aiemmin tehdyt arvioinnin osat saatetaan joutua uusimaan.

Traficomin tulkintasuosituksilla ei kuitenkaan ole tarkoitus puuttua yksittäisen arvioinnin lopputulokseen, vaan arviointilaitokset tekevät työtään itsenäisesti pätevyysalueen mukaisesti. Arviointilaitoksella ei olekaan velvollisuutta pyytää tulkintalinjauksia yksittäiseen arvioon liittyen, mutta haastatteluissa todettiin, että tulkinnan pyytäminen koetaan usein välttämättömäksi. Salaustuotteiden hyväksyntä voidaan arviointiprosessin yhteydessä tehdä ns. Crypto Approval Authority (CAA) -pikaprosessina.

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 seurantaarviointeja ei ole määritelty velvoittaviksi, vaan arvioinnin kohteen on itse ilmoitettava arvioijalle, jos järjestelmään on tehty merkittäviä muutoksia, mikäli 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).

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

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

perusteella vaatimustenmukaisuus voitaisiin todeta. Haastatteluissa todettiin, 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.

2.1.5 Resurssit

Traficomille lainsäädännön kautta määrättyjä tehtäviä ovat mm. arviointilaitosten hyväksyminen, tietoturvallisuuden arviointi ja tuotehyväksynnät. Traficomille osoitettujen toimeksiantojen kesto on pitkä – useista kuukausista vuoteen, mistä koituu ylimääräisiä kustannuksia arvioinnin kohteelle, sekä käyttäjäorganisaatiolle. Arviointitoimintaan liittyvät tehtävät ja niiden resursointi eivät vaikuta olevan tasapainossa arviointien viiveiden perusteella. Lisäksi haastatteluissa todettiin, että Traficomin rooli arviointien tekijänä ja arviointilaitosten pätevyyden arvioijana ei ole hyvän hallintotavan mukaista.

Traficomin vuoden 2019 tilinpäätöksen mukaan viraston henkilötyövuosien kokonaistoteuma vuonna 2019 oli 919 henkilötyövuotta, josta vuoden 2019 aikana uusia palkattuja työntekijäitä oli 64 henkilöä. Arviointitoimintaan käytettyjen resurssien kokonaismäärää 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. Myöskään kaupallisten arviointilaitosten arviointitoiminnan resursseista ei ole tarkkaa tietoa, mutta kokonaisuudessaan Kiwa Inspecta Suomi työllistää yli 600 henkilöä[6], Nixu yli 400 henkilöä[7] ja KPMG yli 1400 henkilöä[8] Suomessa. Akkreditoitujen arviointilaitosten arviointien tekemiseen osallistuu arvion perusteella yhteensä muutamia kymmeniä henkilöitä. Akkreditoidun 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.

Tilanteeseen, jossa arviointilaitoksena toimiva yritys kohtaa muutoksia omassa toiminnassaan, esimerkiksi yritysoston tai toiminnan lakkaamisen kautta, ja joka tilanne voi johtaa arviointitoiminnassa kertyneiden tietojen päätymiseen ennalta suunnittelemattomille tahoille, ei ole varauduttu nykyisissä säädöksissä.

2.2 Digitaalisen turvallisuuden vaatimukset ja kriteeristöt

Tietoturvallisuuden vaatimuksia on kirjattu tiedonhallintalain lisäksi sektorikohtaiseen sääntelyyn. Arviointilaki painottuu järjestelmien tekniseen arviointiin. Varautumiselle ja toiminnan jatkuvuudelle ei ole arviointia koskevaa sääntelyä, vaikka toiminnan jatkuvuuden varmistaminen tunnistetaan vallitsevana kehityssuuntana, joka on keskeinen osa digitaalisen turvallisuuden kokonaisuutta ja tukee

[6] https://image.slidesharecdn.com/jyrkilahnalahtikiwainspecta14-190215141649/95/jyrki-lahnalahti-kiwa-inspecta-1422019-3-638.jpg?cb=1550240301

[7] https://www.nixu.com/sites/default/files/NIXU_Vuosikatsaus_2019.pdf

[8] https://assets.kpmg/content/dam/kpmg/fi/pdf/2020/01/KPMG_vuosikertomus_2019_2.pdf

osaltaan tietoturvallisuuden toteutumista. Tietoturvallisuuden arviointiperusteina voidaan käyttää mm. kansallisia tai kansainvälisiä säännöksiä ja ohjeita tai vahvistettuja standardeja (1405/2011 10 §, 1406/2011 7 §).

Katakri on kansainvälisistä tietoturvavelvoitteista annettua lakia (588/2004) täsmentävä. Sitä käytetään myös turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen arvioinneissa. Sen käytölle kansallisissa arvioinneissa ei kuitenkaan ole riittävää säädöspohjaa. VAHTI-ohjeet ovat pääosin valtionhallinnon käyttöön tarkoitettuja (mm. vanhentunut VAHTI 2/2010). Vanhentuneita VAHTI-ohjeita ja aiempia Katakri-versioita käytetään edelleen. Edellä mainittujen arviointiperusteiden soveltuvuus koko julkisen hallinnon käyttöön on rajallinen, koska kuntasektorilla turvallisuusluokittelua ei käytetä (1109/2019). Digitaalisen turvallisuuden osa-alueiden vaatimusmäärittelyt eivät laajasti perustu kansainvälisiin standardeihin (mm. ISO27001 - Tietoturvallisuuden hallinta, ISO22301 - Jatkuvuuden hallinta, ISO31000 - Riskienhallinta), joita olisi tarvittaessa täydennetty kansallisilla erityisvaatimuksilla.

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 kuitenkin 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 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.

2.3 Digitaalisen infrastruktuurin arviointitoiminta

Digitaalista infrastruktuuria ei ole yksikäsitteisesti määritelty eikä ole yhteistä käsitystä siitä, mitä kokonaisuuksia digitaaliseen infrastruktuuriin sisältyy. On kyseenalaista, onko digitaalisen infrastruktuurin käsitteelle käyttöä arviointitoiminnan yhteydessä. Esimerkiksi liikenteen ohjausjärjestelmien käsittely varsinaisesta väyläinfrastruktuurista irrallaan ei ole välttämättä mielekästä.

Toiminnan jatkuvuudelle ja varautumiselle ei ole vaatimusmäärittelyä. Tästä syystä on teetetty tietoturvallisuuden arviointeja aiemman tietoturvallisuusasetuksen (681/2010) perusteella 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, mutta siinä käsiteltävät tiedot voivat olla julkisia (esim. VNK:n hätätiedotusjärjestelmä ja viranomaisten voimassa oleviin koronarajoituksiin ja –ohjeistuksiin liittyvät sivustot).

2.4 Oppivien ja älykkäiden järjestelmien arviointi

Tekoäly- ja koneoppimisratkaisuissa laskentatehon tuottavat suuret, kansainväliset toimittajat, joilla ei välttämättä ole intressiä toteuttaa kansallisia viranomaisvaatimuksia. Traficom pitää yllä mm. luetteloa hyväksytyistä salausratkaisuista. Tällaisten ratkaisujen integrointi pilvipalvelutoimittajan ympäristöön voi olla vaikeaa.

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.

Oppivat ja älykkäät järjestelmät eivät muuta keskeisiä arviointitehtäviä tai arviointitehtävien organisoimista. Näiden järjestelmien digitaalisen turvallisuuden arviointi poikkeaa kuitenkin muista digitaalisista palveluista ja tietojärjestelmistä siten, että mm. järjestelmien algoritmien arviointi edellyttää syvällistä erikoisosaamista. Algoritmit kuten yleensäkin ohjelmistot voivat lisäksi olla yritysten liikesalaisuuksia, jolloin niiden arviointi on vaikeaa tai jopa mahdotonta. Toiminnallisuuksien arviointi on mahdollista, mutta järjestelmien muutokset oppimisen myötä voivat muuttaa toiminnallisuuttakin hyvin nopeasti. Esimerkiksi hallintaviitekehyksen AI in control[9] 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 järjestelmän opettavan tiedon eettisyys ja luotettavuus ovat arvioinnin kannalta oleellisia seikkoja.[10] Keskeisiä kysymyksiä ovat myös kertyvän tiedon hallintaoikeus ja saatavuus sekä tiedon uudelleen käytettävyys ja sijainti globaaleissa tietoverkoissa ja näiden hallintaan liittyvät kysymykset.

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

3 ARVIOINTITOIMINNAN HYÖDYT HAASTATTELUJEN PERUSTEELLA

Nykytilanteessa arviointitoiminnan hyötyinä nähtiin ennen kaikkea julkisen ja yksityisten toimijoiden yhteistyö sekä tietoturvallisuuden osa-alueita vahvistavat velvoittavat arviointikriteerit. 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 ja yksityisten toimijoiden yhteistyön malli on tietoturvallisuuden arvioinnin näkökulmasta melko hyvä. Kriteeristöjen mukaisia arviointeja ovat voineet tehdä Traficomin lisäksi myös akkreditoidut 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.

Arviointilakeja pidettiin hyödyllisenä, sillä se vahvistaa organisaatioiden tietoturvallisuuden ja tietoliikennejärjestelyjen asian- ja vaatimustenmukaisuutta. Lainsäädännöstä saatavia rajauksia ja viittauksia digitaalisen turvallisuuden kehittämiseen 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

Arviointitoiminta on merkittävä tekijä turvallisten palvelujen tuottamisessa ja tarjoamisessa. Arviointitoiminnan kehittämisehdotukset perustuvat haastatteluissa kerätyn aineiston perusteella valtiovarainministeriössä muodostettuun näkemyksiin kehittämistarpeista. Arviointitoimintaa on painottunut valtiotoimijoihin. Kuntien laajasti käytettyjen digitaalisten palvelujen säännöllistä arviointia tulisi tehostaa. Arviointitoiminnassa tulisi huomioida digitaalisen turvallisuuden eri osa-alueet nykyistä paremmin, sekä vähentää arviointiperusteisiin liittyvää tulkinnanvaraisuutta, ja selventää eri toimijoiden rooleja sekä varmistaa arviointien laatu ja yhteismitallisuus. Tietosuojan vaatimukset perustuvat EU:n yleiseen tietosuoja-asetukseen, joten kansallista liikkumavaraa on vain hyvin vähän, eikä tässä raportissa ole kuvattu tietosuojan arviointitoiminnan kehitysehdotuksia. Arviointitoimintaan liittyviä kehitysehdotuksia on käsitelty myös liikenne- ja viestintäministeriön raportissa[11].

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 tietojen käsittely-ympäristö.

Digitalisoituneen yhteiskunnan toimintaympäristö sisältää lukuisia verkostoja, jossa toimijoiden välillä vallitsee erilaisia ja muuttuvia keskinäisriippuvuuksia. 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. Digitaalisten palvelujen turvallisuudesta tulisi varmistua koko palveluverkoston laajuisesti. Arviointitoiminnalla saadaan ajan hetkeen sidottu kuva digitaalisen turvallisuuden vaatimusten toteutumisesta, joten arviointeja pitäisi toteuttaa kaikissa palvelun elinkaaren vaiheissa säännöllisesti. Kuitenkin vasta arvioinnissa tunnistettujen poikkeamien korjaaminen ja kehityskohteiden parantaminen johtaa digitaalisen turvallisuuden kehittymiseen jatkuvan parantamisen mallin mukaisesti.

4.1 Arviointitoiminnan keskeiset tehtävät

Arviointitoimintaan liittyvät keskeiset tehtävät ovat arviointilaitoksen pätevyyden arviointi määrävälein, arviointiperusteiden määritys, vähimmäisvaatimusten ja arviointikriteeristöjen asettaminen ja näiden ylläpito sekä arviointilaitoksille että niiden tekemille arvioinneille, arviointitoimeksiantojen tekeminen sisältäen arviointikohteen ja arvioinnin laajuuden osoittamisen, arviointilaitoksen suorittama arviointi/auditointi ja hyväksynnän myöntäminen (vaatimustenmukaisuuden toteutumisen hyväksyntä), sekä arvioinnin tulosten perusteella tehtävien muutosten hallinta. Arviointitoimintaa koskevia säännöksiä tulisi muuttaa siten, että julkisen hallinnon digitaalisen turvallisuuden arvioinnista säädettäisiin nykyistä selkeämmin. Arviointilaitosten pätevyyden arvioinnin säännöksiä tulisi soveltaa sekä arvioijina toimiviin viranomaisiin että kaupallisiin arviointilaitoksiin.

[11] Liikenne- ja viestintäministeriön julkaisuja 2021:1

4.1.1 Arviointilaitoksen akkreditointi ja seuranta

Arviointilaitoksen hyväksyntäprosessia pitäisi yksinkertaistaa prosessin nopeuttamiseksi ja toiminnan tehostamiseksi siten, että käsittelyn kesto on paremmin ennustettavissa ja kaikki akkreditoinnissa käytettävät vaatimukset ja arviointilaitoksen tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden pätevyyden arviointikriteeristöt on kuvattu selkeästi yhtenä kokonaisuutena. Tämä tarkoittaa, että kansallinen akkreditointiyksikkö FINAS arvioisi tietoturvallisuuden lisäksi varautumisen ja toiminnan jatkuvuuden arviointilaitosten pätevyyksiä määrävälein. FINAS voisi käyttää muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä. Määritystyöhön näissä viranomaisissa osallistuvat virkamiehet eivät saisi osallistua arviointilaitoksen toimintaan arvioijina. Siten on perusteltua erottaa pätevyyden arvioinnissa FINASia tukevat tiedonhallintayksiköt niistä, jotka toimivat arviointilaitoksina. Tämän ei arvioida aiheuttavan muutoksia henkilömääriin Traficomissa, koska arviointitoiminta on yhteiskunnan digitalisoitumisen lisääntymisen myötä jatkuvasti kasvava alue.

Tiedonhallintalautakunta voisi antaa yleiset tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vähimmäisvaatimusten arviointikriteerit ja arviointilaitoksen akkreditointiin liittyvät vaatimukset. Digi- ja väestötietovirasto voisi tukea tiedonhallintalautakuntaa arviointikriteerityössä ja FINASia em. vaatimustenmukaisuuden arvioinnissa.

Arviointilaitosten pätevyysarvioinnin vaatimusten tulisi olla samat kaikille arviointilaitoksille riippumatta siitä, onko kyseessä kaupallinen yritys vai viranomainen, jolle arviointitoiminta on määrätty lakisääteisenä tehtävänä. Vaatimusten asettamisessa tulee kiinnittää huomiota siihen, että ne ovat realistisia ja mahdollisimman yksiselitteisiä. Tulkinnanvaraiset tai epäselvät vaatimukset hankaloittavat prosessin sujuvaa etenemistä. Akkreditointia hakevalle toimijalle pitää kuitenkin asettaa vaatimukset, joilla varmistetaan arviointilaitoksen toiminnan laatu, turvallisuus ja riippumattomuus sekä laitoksen suorittamien arviointien laatu ja yhteismitallisuus. On huomattava, että akkreditointi ei ole hyväksyntäprosessi.

Kansallista luottamuksellista tietoa (TL III) käsittelevien palveluiden ja järjestelmien arviointia voisivat tehdä tilaajan valinnan perusteella viranomainen, joka toimii FINASin tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden arviointilaitoksia koskevien vaatimusten mukaisesti - tai markkinaehtoinen, akkreditoitu arviointilaitos. Arviointien nopeuttamiseksi ja resurssien käytön tehostamiseksi pitäisi TL IV -luokiteltua, salassa pidettävää, julkista tai luokittelematonta tietoa käsittelevien palvelujen tai järjestelmien arviointien olla pääasiallisesti akkreditoitujen kaupallisten arviointilaitosten tehtävä, koska tällaisia palveluja ja järjestelmiä on lukumääräisesti eniten.

FINAS toteuttaa arviointilaitosten seurantaa vuosittaisilla seuranta-arvioinneilla. Edelleen voisi selvittää mahdollisuuksia tiivistää liikenne- ja viestintäministeriön ja valtiovarainministeriön yhteistä Traficom arviointitoiminnan ohjausta. Jos arviointilaitos ei täytä akkreditoinnille asetettuja vaatimuksia, sen akkreditointi voidaan perua. Erilliselle valvontamenettelylle ei välttämättä ole tarvetta ja valvontatoiminnon perustaminen johtaa helposti uuden pullonkaulan syntymiseen. Arviointilaitosten lukumäärän kasvu voi kuitenkin edellyttää lisää resursseja niin akkreditointiprosessiin kuin seuranta-arviointeihinkin. Lisäksi tulisi säädöksin varautua tilanteeseen, jossa arviointilaitoksen hallussa ole-

vat arviointitiedot ovat yrityksen toiminnan muutosten johdosta joutumassa ennalta suunnittelemattoman tahon haltuun. Viranomaisen arviointitoimintaa arvioitaisiin määrävälein samalla tavalla kuin muiden arviointilaitosten toimintaa.

Arviointilait ottavat tällä hetkellä kantaa ainoastaan tietoturvallisuuteen ja siinäkin painotus on turvaluokitellun tiedon teknisessä suojaamisessa. Digitaalisen turvallisuuden kehittäminen julkisessa hallinnossa edellyttää, että sen kaikille osa-alueille (tietoturva, riskienhallinta, kyberturvallisuus, varautuminen ja toiminnan jatkuvuus sekä tietosuoja) asetetaan vaatimukset (ks. kappale 4.1.3) ja arviointilaitosten pätevyydet asetetaan näiden vaatimusten mukaisesti. Akkreditoidun arviointilaitoksen pätevyysalueita määrittävät arviointikriteeristöt, joiden arviointiin laitoksella on akkreditointiyksikön tekemän arvioinnin perusteella riittävät edellytykset. Pätevyyden arviointiin ja osoittamiseen käytettävien vaatimusten ja niiden arviointiperusteiden tulee pohjautua säännöksiin ja vaatimusmäärittelyjen perustua saatavilla oleviin, vahvistettuihin kansainvälisiin standardeihin. Tiedonhallintalautakunnan tulisi antaa digitaalisen turvallisuuden vähimmäisvaatimusten arviointiin käytettävät arviointikriteerit sekä pätevyysarvioinnissa käytettävät yleiset tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden arviointilaitosten vaatimukset.

4.1.2 Arviointien arviointiperustan määrittäminen

Arviointilait sallivat erityyppisten vaatimusmäärittelyjen käytön tietoturvallisuuden arviointiperusteina (1405/2011 10 §, 1406/2011 7 §). Riskien arviointi toteutuksen perusteena on sekä tiedonhallintalain (906/2019) 13 §:n että käytännössä kaikkien kansainvälisten hallintaviitekehysten edellyttämä menettely. Arviointiperustaa tulisi kehittää edelleen siten, että arvioinneissa ja hyväksymisissä entistä paremmin huomioidaan 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 niin viranomaisissa kuin arviointilaitoksissa ja palvelun tuottajissa.

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.

Julkisen hallinnon digitaalisten palvelujen turvallisuuden arviointiperusteiden tulee perustua säännöksiin. Vaatimusmääritykset tulisi antaa velvoittavina siten muotoiltuina, että niitä voidaan jousta-

vasti muokata digitaalisen toimintaympäristön nopean kehittymisen myötä. Vaatimusmääritysten tulisi pohjautua kansainvälisiin standardeihin ja muihin yleisesti käytettyihin vaatimusluetteloihin[12]. Digitaaliselle turvallisuudelle asetettavat vaatimukset ja arviointikriteerit tulisi määritellä niin, että niiden velvoittavuudesta ei synny olemassa olevan tilanteen kaltaista tulkinnanvaraisuutta. Vaatimusten toteutumista arvioitaessa on huomioitava palvelun käyttötarkoitus, palvelun käytön riskit, palvelussa käsiteltävien tietojen suojaaminen ja palvelun saatavuustarpeet. Hallintakeinojen toteutuksessa käytettyjen ratkaisujen tulee perustua tiedonhallintayksikön (vast.) ajantasaiseen riskiarvioon, jonka tiedonhallintayksikkö on hyväksynyt.

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, sekä kuvata, mitä nämä tilanteet, riskit, perusteet ja kriteerit ovat. Arviointikriteeristön tulee soveltua mm. palvelujen kehittämisen aikana tehtäviin arviointeihin, hankintavaiheessa palvelulle asetettujen vaatimusten todentamiseen sekä käytön aikaisiin arviointeihin.

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 niiden palvelujen arviointikriteerien kanssa.

4.1.3 Arviointitoimeksiannon laatiminen

Akkreditoitu arviointilaitos suorittaa arvioinnin tilaajan toimeksiannosta. Arviointitoimeksiannossa asetetaan arvioinnin kohde, kerrotaan arvioinnissa käytettävät arviointiperusteet ja asetetaan arvioinnille aikataulu. Arvioinnin tilaajan kannalta on erityisen tärkeää, että arvioinnin toteutus aikataulueen 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.

Arviointitoimeksiannossa kuvataan arviointilaitokselle annettava tehtävä, jonka lopputuloksena syntyy raportti arviointiperusteena käytettävien vaatimusten toteutumisesta. Kun toimeksianto suoritetaan digitaalisen palvelun turvallisuuden todentamiseksi joidenkin viranomaista velvoittavien säännösten perusteella, niin arvioinnissa on käytettävä velvoittavaa säädäntöä (esimerkiksi tiedonhallintalaki). 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.

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

Arviointeja käytetään digitaalisten palvelujen elinkaaren eri vaiheissa vaatimustenmukaisuuden todentamiseen. 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, varautumisen ja toiminnan jatkuvuuden akkreditoiduilta arviointilaitoksilta niiden pätevyysalueilta ja niiden määrittämillä kustannuksilla. Toimeksiannon yhteydessä tilaaja määrittäisi arvioinnin kohteen ja arviointiperustan tai arviointiperusta määräytyisi säädösten perusteella. Tämä tarkoittaa, että esimerkiksi yritykset voisivat tilata Katakri-kriteeristön perusteella tehtävän arvioinnin ilman, että kehitettävällä järjestelmällä tai palvelulla on vielä viranomaisasiakasta. Vaatimustenmukaisuustodistus voitaisiin myöntää ainoastaan käytettäessä pätevyysalueen mukaista arviointiperustaa (esimerkiksi tiedonhallintalautakunnan antama kriteeristö tai Katakri).

4.1.4 Arvioinnin toteutus

Kansallisen digitaalisen turvallisuuden velvoittavasta arvioinnista ei ole riittävästi sääntelyä. Ehdotetaan, että 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).

Arviointilaitoksen suorittamassa arvioinnissa vaatimustenmukaisuuden osoittamiseksi käytetään tyypillisesti vähintään kahta lähdettä (esim. haastattelut ja asiakirjojen katselmointi) luotettavan tuloksen varmistamiseksi. Arviointikriteeristössä voitaisiin tarvittaessa velvoittaa käyttämään lisäksi muita arviointimenetelmiä, joita voisivat olla esimerkiksi lähdekoodin katselmukset, haavoittuvuustestaukset ja tunkeutumisyritykset (ns. penetraatiotestaus).

4.1.5 Vaatimustenmukaisuuden osoittaminen

Arvioinnin tulosten raportointi ja vaatimustenmukaisuuden osoittaminen eli hyväksyntä ovat erillisiä käsitteitä. Valtiovarainministeriön tulisi arvioida valtion yhteisten tieto- ja viestintäteknisten palveluiden tuottajien tietoturvallisuutta, varautumista ja toiminnan jatkuvuutta koskevia vastuita ja velvoitteita. Lähtökohtana tulisi olla, että yhteisille palveluille asetetaan palvelukohtaisesti tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vaatimukset. Akkreditoitujen arviointilaitosten tulisi tehdä arviointeja asetettujen vaatimusten täyttymisestä, ja niiden täyttyessä antaa tätä koskeva todistus vaatimuksenmukaisuudesta, samalla tavalla kuin kansainvälisten ISO-standardien sertifiointimenettely on toteutettu. Todistus vaatimuksenmukaisuudesta olisi voimassa esimerkiksi kolme 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/sallittu. Arvioinnin kohteena olevan organisaation mahdollisuuksia hyväksyä digitaalisen turvallisuuden ratkaisut riskien arvioinnin, riskienhallintatoimenpiteiden toteuttamisen ja jäännösriskien hyväksymisen perusteella tulisi edistää. Arvioinnissa havaitut poikkeamat edellyttävät korjaamista ennen vaatimustenmukaisuuden todistuksen saamista. Riskienhallintatoimenpiteiden toteuttamisen ja jäännösriskien hyväksyntämenettelyn kautta palvelun väliaikainen tai määräaikainen käyttöönotto voisi olla sallittua, jos tämä palvelun vaatimuksia koskevassa säädännössä on todettu/sallittu.

Palveluntuottajat ja palvelujen kehittäjät voisivat käyttää vaatimustenmukaisuudesta annettavaa todistusta esimerkiksi osoittamaan palvelua hankkivalle viranomaiselle, että palvelu täyttää viranomaisen digitaaliselle palvelulle asetettavat 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.

Arviointilaitosten toimintaa valvovan viranomaisen havaitsema, virheellisillä tai puutteellisilla perusteilla annettu todistus voi johtaa siihen, että arviointilaitos menettää pätevyysalueensa tai asemansa hyväksyttynä arviointilaitoksena. Arviointilaitokselle voidaan asettaa myös muita sanktioita (esim. taloudelliset seuraamukset), mikäli se ei täytä arviointilaitokselle asetettuja velvoitteitaan. Jos esimerkiksi Digi- ja väestötietovirasto tukee FINASia arviointilaitoksen akkreditointiin liittyvän toimialakohtaisen vaatimustenmukaisuuden arvioinnissa, niin Digi- ja väestötietovirasto voisi toimia myös kyseisten arviointilaitosten valvovana viranomaisena.

4.2 Arviointitoiminnan tehtävien vaihtoehtovertailu

Tässä kappaleessa kuvataan yksinkertaistettuna nykyinen arviointitoiminnan malli, vaihtoehtoinen toteutusmalli sekä rooleja, joita arviointitoiminnassa tarvitaan.

4.2.1 Arviointitoiminnan nykymalli

Tietoturvallisuuden arviointitoimintaan kuuluu kolme kokonaisuutta: 1) arviointilaitosten vaatimustenmukaisuuden arviointi, 2) arviointien tekeminen ja 3) hyväksymistodistuksen antaminen. Arviointitoiminnan yksityiskohtaista nykytilan kuvausta ei ole saatavilla.

Viranomaisen tietojärjestelmän tai tietoliikennejärjestelyn vaatimustenmukaisuuden arviointi tehdään toimeksiannosta, jonka voi tehdä viranomainen lisäksi se, joka tekee hankintoja viranomaisen lukuun, tuottaa viranomaiselle tietojenkäsittely- tai tietoliikennepalveluja tai hoitaa em. palvelujen järjestämiseen liittyviä palvelutehtäviä (1406/2011 4 §). Arvioinnin voi suorittaa arviointilain mukaan Traficom tai akkreditoitu arviointilaitos sille hyväksytyn pätevyysalueen mukaisesti. Traficom toimii myös itse arviointilaitoksena, eikä viraston pätevyyttä ole riippumattomasti arvioitu tai valvottu. Arviointilaitoslain valmistelun yhteydessä todettiin, että valtiovarainministeriön ja liikenne- ja viestintäministeriön tulisi yhdessä ohjata Traficomin toimintaa.

Arviointilaitoksen on annettava tekemästään arvioinnista todistus, jos kaikki vaaditut arviointiperusteena käytetyt vaatimukset täyttyvät (1405/2011 9.3 §). Traficom voi pyynnöstä myöntää viranomaishyväksynnän tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden vaatimustenmukaisuudesta. (1406/2011 8 §).

Traficom on laajasti tunnustettu erittäin osaava ja arvostettu toimija tietoturvallisuuden arvioinnin alueella[13]. Haastattelujen perusteella todettiin, että Traficomin rooli arviointien tekijänä ja arviointilaitosten pätevyyden arvioijana ei ole hyvän hallintotavan mukaista. Tämä ei vastaa Traficomin käsitystä asiasta.

4.2.2 Arviointitoiminnan vaihtoehtoinen toteutusmalli

Arviointilaitoksen hyväksyntäprosessia yksinkertaistettaisiin prosessin nopeuttamiseksi ja toiminnan tehostamiseksi siten, että käsittelyn kesto on paremmin ennustettavissa ja kaikki akkreditoinnissa käytettävät vaatimukset ja arviointilaitoksen tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden pätevyyden arviointikriteeristöt on kuvattu selkeästi yhtenä kokonaisuutena. FINAS on akkreditointien vaatimusten vahvistamisesta annetussa NLF-asetuksessa (765/2008) tarkoitettu Suomen ainoa kansallinen akkreditointielin, joten sillä voidaan perustellusti katsoa olevan riittävä osaaminen arviointilaitosten vaatimustenmukaisuuden toteamiseen. FINAS arvioisi tietoturvallisuuden lisäksi myös varautumisen ja toiminnan jatkuvuuden arviointilaitosten pätevyyksiä määrävälein. FINAS voisi edelleen käyttää muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä. Määritystyöhön näissä viranomaisissa osallistuvat virkamiehet eivät saisi osallistua arviointilaitoksen toimintaan arvioijina.

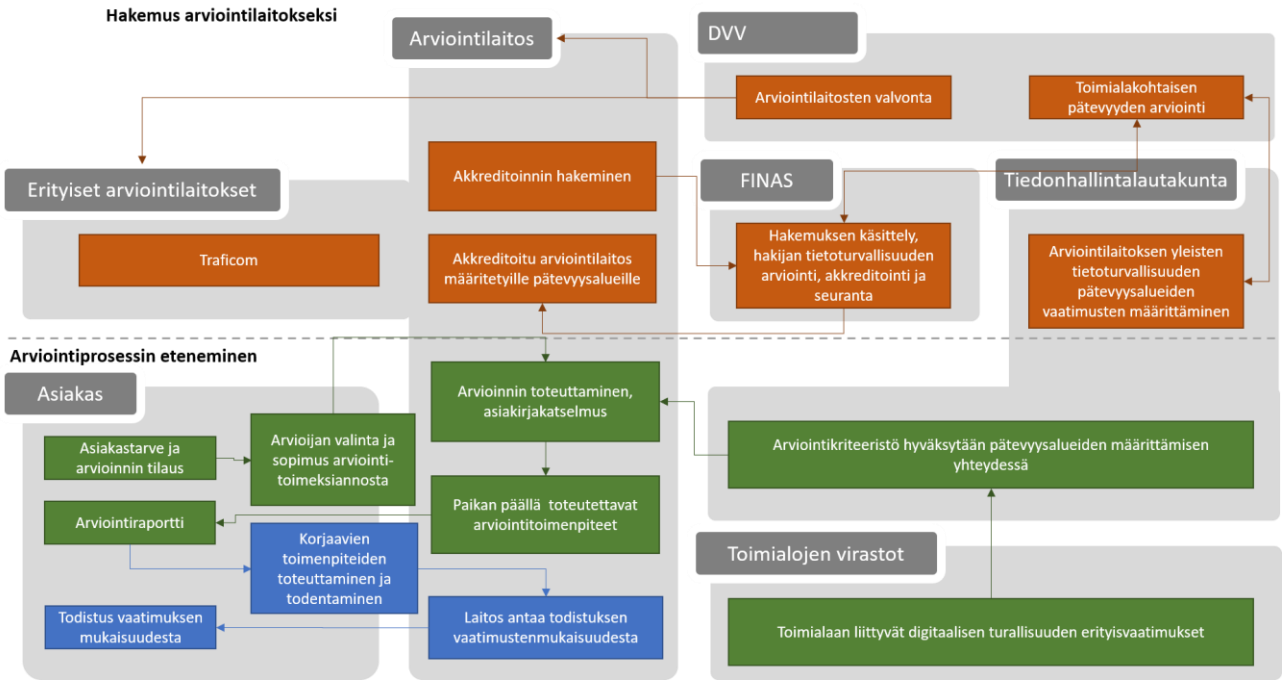
Siten on perusteltua erottaa pätevyyden arvioinnissa FINASia tukevat tiedonhallintayksiköt niistä, jotka toimivat arviointilaitoksina. Tämän ei arvioida aiheuttavan muutoksia henkilömääriin Traficomissa, koska arviointitoiminta on yhteiskunnan digitalisoitumisen lisääntymisen myötä jatkuvasti kasvava alue.

Tiedonhallintalautakunta voisi antaa yleiset tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden vähimmäisvaatimusten arviointikriteerit ja arviointilaitoksen akkreditointiin liittyvät vaatimukset. Digi- ja väestötietovirasto voisi tukea tiedonhallintalautakuntaa arviointikriteerityössä ja FINASia em. vaatimustenmukaisuuden arvioinnissa.

Arviointiprosessin keston lyhentäminen edellyttää henkilöresurssien lisäämistä arviointien tekemiseen ja arviointiperusteiden tulkinnanvaraisuuden vähentämistä. Viranomaisresurssien jatkuvaa lisäämistä ei voida pitää kestävänä ratkaisuna, vaan arviointien tekemisessä tulisi hyödyntää kaupallisia arviointilaitoksia. 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 lisää kilpailua ja varmistaa siten arvioinneille oikean kustannustason.

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

Tässä mallissa arviointeja voivat tilata kaikki viranomaiset ml. yhteishankintayksiköt sekä yhteisöt kuten palveluiden kehittäjät ja palveluntarjoajat. Arvioinnit perustuvat tässä mallissa vaatimusmäärityksiin, jotka kattavat tietoturvallisuuden lisäksi varautumisen sekä toiminnan jatkuvuuden hallinnan alueet. Koska arviointiperusteet perustuvat säännöksiin, ja arviointilaitoksen pätevyyden arvioi viranomainen ja arviointien vaatimusmääritykset ovat viranomaisen antamia, on perusteltua, että todistuksen vaatimustenmukaisuudesta voi antaa akkreditoitu arviointilaitos, eikä muita erillisiä todistuksia tarvita, ellei viranomaisen tai muun tahon hyväksyntää erityisestä syystä katsota välttämättömäksi.



Kuva 2: Arviointitoiminnan tavoiteprosessien yksinkertaistettu kuvaus

4.2.3 Arviointitoiminnassa tarvittavat tehtävät

Toteutuksesta riippumatta arviointilaitos- ja arviointitoiminnassa tarvitaan vaatimusmäärittelyjen toteuttamiseksi roolien ja vastuiden kuvaukset. Nämä on kuvattu yleisellä tasolla seuraavassa taulukossa.

Rooli	Kuvaus	Tehtävät
Arviointilaitoksen pätevyyden arviointi	Arviointilaitoksen vaatimustenmukaisuuden arvioinnissa selvitetään hakijan kyky toimia tietoturvallisuuden, varautumisen ja toiminnan jatkuvuuden hallinnan arviointilaitoksena. Arviointi perustuu ennalta vahvistettuihin vaatimusmäärittelyihin. Arviointilaitoksen akkreditoija pitää kirjaa akkreditoiduista arviointilaitoksista ja valvoo arviointi-	- arviointilaitokseksi hakevan arviointi määrävälein - pätevyysalueen hyväksyntä

Rooli	Kuvaus	Tehtävät
	laitosten toimintaa akkreditointiprosessin mukaisten seuranta-arviointien avulla.	
Arviointilaitoksen pätevyyden arviointikriteerien antaja	Arviointilaitoksen pätevyyden arviointi perustuu kansainvälisesti vahvistettuihin, arviointitoimintaa koskeviin standardeihin sekä digitaalista turvallisuutta koskeviin vaatimusmäärityksiin. Arviointilaitoksen pätevyyden arvioinnin vaatimuksia voidaan koota useista lähteistä ja vaatimusmääritysten antajana on riippumaton toimija.	- arviointilaitoksen pätevyyden arvioinnin vaatimusmääritysten kokoaminen - vaatimusmääritysten antaminen
Arviointikriteeristön antaja	Julkisen hallinnon digitaalisen turvallisuuden arviointi perustuu ennalta vahvistettuun vaatimusmääritykseen, joka perustuu säännöksiin ja yleisesti käytettyihin kansainvälisiin viitekehyksiin. Digitaalisen turvallisuuden arviointikriteeristön antaa arvioinneista riippumaton toimija.	- digitaalisen turvallisuuden osa-alueiden vaatimusmääritysten kokoaminen - vaatimusmääritysten antaminen
Arvioinnin tilaaja	Digitaalisen turvallisuuden arviointi tehdään aina toimeksiannon perusteella. Toimeksiannossa tilaaja ja arviointilaitos sopivat arvioinnin kohteesta ja laajuudesta. Julkisen hallinnon palvelujen digitaalista turvallisuutta arvioidaan tiedonhallintalautakunnan antaman vaatimusmääritysten mukaisesti. Arvioinnin tilaajana voi olla viranomainen tai yhteisö kuten palvelun kehittäjä tai palvelun tuottaja.	- arviointitoimeksianto arviointilaitokselle

Arvioinnin tekijä	Julkisen hallinnon digitaalisten palvelujen turvallisuutta arvioidaan palvelujen digitaalisen turvallisuuden kehittämiseksi. Kun arvioinnin tekee akkreditoitu tai erityinen arviointilaitos, se antaa vaatimusten toteutumisesta todistuksen. Muiden toimijoiden tekemät arviot rinnastetaan itsearviointiin ja niitä voidaan käyttää esimerkiksi kehityskohteiden tunnistamiseen.	- vaatimustenmukaisuuden arviointi
		- arviointiraportin kirjoittaminen
		  ○ poikkeamien kirjaus
		  ○ korjaussuunnitelman ja aikataulun hyväksyminen
		  ○ toteutettujen korjausten arviointi
		- vaatimustenmukaisuustodistuksen antaminen, kun kaikki vaatimukset täyttyvät

LIITE 1: KOORDINAATIORYHMÄN KOKOONPANO

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman 2020-2023 (Haukka) mukaisen säädösvalmistelun koordinointia varten asetettuun työryhmään kuuluivat:

- Aku Hilve, valtiovarainministeriö, puheenjohtaja (31.12.2020 asti)
- erityisasiantuntija Niko Mäkilä, valtiovarainministeriö, puheenjohtaja (1.1.2021 alkaen)
- 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
- Ville Autero, työ- ja elinkeinoministeriö
- erityisasiantuntija Jari Ylikoski, Kuntaliitto
- tietoturvapäällikkö Kari Nykänen, Oulun kaupunki
- Seppo Ruotsalainen, Kuopion kaupunki
- yksikönpäällikkö Eija Alavesa, Traficom
- johtaja Mikko Pitkänen, Digi- ja viestintävirasto

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

LIITE 2: SELVITYKSEEN LIITTYVÄ LAINSÄÄDÄNTÖ JA KRITEERISTÖT

Tietoturvallisuuden arviointiin liittyviä vaatimuksia on kirjattu moniin lakeihin. Arviointitoiminnan kannalta keskeisimmiksi laeiksi on arvioitu kaksi listalla ensimmäisenä olevaa lakia. Myös muihin lakeihin viitattiin haastatteluissa.

- **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
- 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
- 920/2005 Laki vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta
- 588/2004 Laki kansainvälisistä tietoturvavelvoitteista
- 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
- 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.)

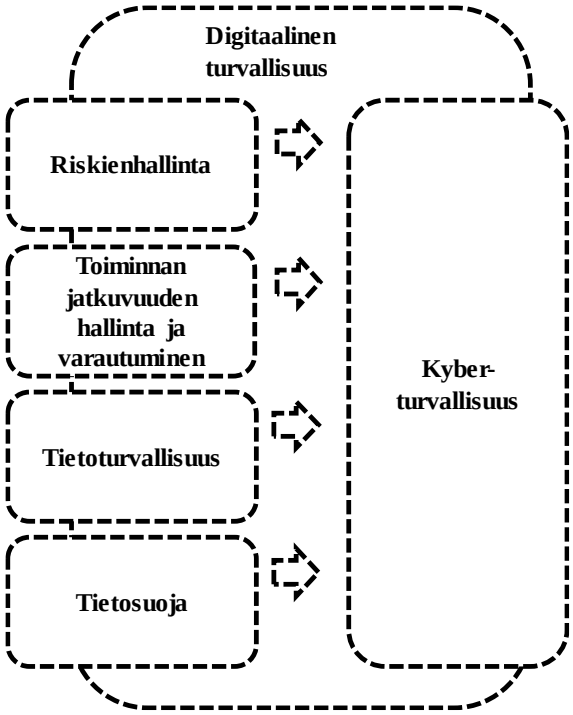
LIITE 3: HAASTATTELUT

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

Kyberturvallisuuden, tietoturvallisuuden, tietosuojan, riskienhallinnan sekä toiminnan jatkuvuudenhallinnan ja varautumisen muodostama kokonaisuus[14]. Termi on uusi ja vakiintumaton. OECD:ssä on käytössä termi digital security[15].



Kyberturvallisuus

Tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan[16.] 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[17]. Tavoitetila, jossa digitaalisessa ympäristössä olevat tiedot ja prosessit on suojattu luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyviltä uhilta. Vanhempi termi, joka on

[14] Pilkahduksia tulevaisuuteen, Tietopolitiikka, tekoäly ja robotisaatio hyvinvoinnin ja taloudellisen menestyksen mahdollistajana Suomessa, Valtiovarainministeriön julkaisuja – 2019:22
[15] Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document, 2015
[16] Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)
[17] 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[18].
Riskienhallinta	Järjestelmällinen toiminta, joka sisältää riskianalyysin sekä tarvittavien toimenpiteiden suunnittelun, toteutuksen, seurannan ja korjaavat toimenpiteet[19].
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[20].
Varautuminen	Toiminta, jolla varmistetaan tehtävien mahdollisimman häiriötön hoitaminen ja mahdollisesti tarvittavat tavanomaisesta poikkeavat toimenpiteet häiriötilanteissa ja poikkeusoloissa[21].

[18] Sanastokeskus TSK TEPA-termipankki, Tieteen termipankki 06.08.2019
[19] Sanastokeskus TSK TEPA-termipankki, Kokonaisturvallisuuden sanasto (TSK 50, 2017)
[20] Sanastokeskus TSK TEPA-termipankki, Kyberturvallisuuden sanasto (TSK 52, 2018)
[21] Sanastokeskus TSK TEPA-termipankki, Kokonaisturvallisuuden sanasto (TSK 50, 2017)

LIITE 5: KIRJALLISUUSVIITTEITÄ

Gillespie, N, Curtis, C, et. al. (2020) Achieving Trustworthy AI - A Model for Trustworthy Artificial Intelligence [linkki pdf-artikkeliin; 26.1.2021], The University of Queensland, Australia & KPMG Australia, 1.11.2020

Kyberturvallisuuskeskus (2019) Luottamuksen lähteillä, [linkki, 1.2.2021]

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