VALTIONEUVOSTO
STATSRÅDET

Tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnin nykytila-arvio ja kehittämisehdotukset

12.12.2024

VALTIONEUVOSTO
STATSRÅDET

Sisällysluettelo

VALTIONEUVOSTO
STATSRÅDET

VALTIONEUVOSTO
STATSRÅDET

Tiivistelmä

Toimintaympäristön muutokset ovat kasvattaneet tarvetta nostaa julkisten palveluiden ja tietojärjestelmien turvallisuuden tasoa. Kansallisen ja kansainvälisen toimintaympäristön muutoksia ovat teknologioiden ja tiedonhallinnan keskeinen rooli geopoliittisessa kilpailussa, yhä kehittyneemmät uhkat, verkottuneemmat järjestelmät, monimutkaisemmat logistiset toimitusketjut sekä kasvavien EU-tiedon käsittelytarpeiden ja Nato-jäsenyyden myötä lisääntyneet kansainväliset tietoturvallisuusvelvoitteet. Uhkilta suojautuminen on myös kehittynyt ja tiedon salaamisen merkitys osana tiedon elinkaarta ja käsittelyä on kasvanut.

Digitalisoitumisen edistyminen ja kehittyvät teknologiat kuten globaalit pilvipalvelut, tekoäly ja kvanttilaskenta ovat vaikuttamassa sekä toimintatapoihin ja mahdollisuuksiin että menettelyihin toteuttaa julkisen hallinnon tietojärjestelmiä ja palveluita. Yhteiskunnan digitalisoituessa haasteena on tietojärjestelmien kustannustason nousu suhteessa muuhun kulurakenteeseen. Nämä muutokset ovat kasvattaneet tietojärjestelmien tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arviointipalvelujen kysyntää. Turvallisuuden varmistamista kokonaisuutena ja vaatimustenmukaisuuden arviointia yhtenä varmistamisen menettelynä on siten perusteltua arvioida.

Tiedon ja datan hallintaa koskeva EU-sääntely sekä kansainvälisesti turvallisuusluokiteltujen tietojen käsittely on viime vuosina kasvanut. EU:n sisämarkkinoilla tarjottavia tuotteita ja palveluita koskevan sertifiointisääntelyn toimeenpano on vielä monelta osin valmisteluvaiheessa. Keskeinen kansallinen tietoturvallisuuden arviointia koskeva sääntely on valmisteltu yli 13 vuotta sitten. Arviointeihin liittyvää kansallista sääntelyä on valmistunut arviointisääntelyn jälkeen. Arviointisääntelyn lähtökohdat ovat edelleen tarkoituksenmukaiset, mutta niiden soveltamisen aikana on tunnistettu kehitystarpeita.

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointia toteutetaan Suomessa lakisääteisesti EU-sääntelyn, turvallisuusverkon palveluita koskevan sääntelyn sekä kansainvälisesti turvallisuusluokiteltujen tietojen ja sosiaali- ja terveystietojen käsittelyä koskevan sääntelyn perusteella. Lakisääteisen tietoturvallisuuden arvioinnin rinnalla tietoliikennejärjestelyjen, tietojärjestelmien ja palveluiden tietoturvallisuuden arviointia toteutetaan viranomaiskohtaisesti.

Säädettyjä tietoturvallisuuden vaatimustenmukaisuuden arvioijia ovat Liikenne- ja viestintävirasto sekä sen hyväksymät arviointilaitokset. Akkreditoituja arviointilaitoksia on tällä hetkellä neljä, joista kahdella on pätevyysalueena kansallisesti turvallisuusluokiteltujen tietojen käsittelyn tietoturvallisuuden arviointi ja sitä myöten myös sosiaali- ja terveystietojen käsittelyn tietoturvallisuuden arviointi.

Nato-jäsenyyden myötä kansainvälisen tietoaineistojen käsittelyyn käytettävien tietojärjestelmien lukumäärä Puolustusvoimissa ja niiden käyttö kansainvälisissä harjoituksissa on kasvanut nopeasti ja merkittävästi. Lisääntynyt arviointitarve on aiheuttanut ruuhkautumista Liikenne- ja viestintäviraston ja Puolustusvoimien arviointitoiminnassa.

VALTIONEUVOSTO
STATSRÅDET

Valtion yhteisiä tieto- ja viestintäteknisiä palveluja tuottavat valtion tieto- ja viestintätekniikkakeskus Valtori ja turvallisuusverkon palveluja Valtori ja Suomen Erillisverkot Oy. Näillä palveluntuottajilla on jatkuvasti kasvava vuosittainen uusien palvelujen ja palvelujen elinkaaren aikana tehtävien muutosten arviointitarve.

Sosiaali- ja terveydenhuollon julkisten ja yksityisten organisaatioiden hyväksytyiltä arviointilaitoksilta hankkimien lakisääteisten tietoturvallisuuden arviointien määrä on ollut lievässä kasvussa vuodesta 2021 lähtien. Kasvu johtuu arviointivelvoitteen piiriin kuuluvien tietojärjestelmien määrän kasvusta. Tällä hetkellä näitä Valviran rekisteriin merkittyjä tietojärjestelmiä ja käyttöympäristöjä on 99. Vuonna 2023 Valviran rekisteriin merkittiin 27 todistusta tietoturvallisuuden arvioinneista.

Arviointeja pyytävät toimijat ovat todenneet, että arviointien teettäminen on sekä hidasta että kallista ja arviointilaitosten vajaiden resurssien takia myös osin epävarmaa. Arviointien tekijöiden näkökulmasta arviointeja haastavat arvioitavien kohteiden keskeneräisyys ja arvioinnin pyytäjien henkilöstön käytettävyys arviointien toteuttamiseksi. Arvioinneissa aiheuttavat haasteita arviointiperusteiden vanheneminen ja tulkintaongelmat. Arviointikriteeristöille asetetuista vaatimuksista ja niiden ylläpidosta ei ole säädetty. Toimintaympäristön muuttuessa kriteeristöjä ja standardeja on tarve ylläpitää jatkuvasti.

Tässä raportissa ehdotetaan, että arviointien saatavuutta ja viranomaisyhteistyötä parannetaan viranomaisten tehtäviä tarkistamalla. Salaustuotteiden valmistajien, TEMPEST-tuotteiden valmistajien ja arviointilaitosten elinkeinotoiminnan edellytyksiä parannetaan toimintaympäristön vakautta kasvattavalla sääntelyllä. Arviointimenettelyjä sujuvoitetaan riskiperusteisesti ja arviointiperusteita selkeytetään ja täydennetään.

Tietojärjestelmien, palveluiden ja tuotteiden turvallisuuden suunnittelun ja arvioinnin on jatkossa perustuttava yhä vahvemmin riskienhallintaa. Tämä on välttämätöntä arviointien tehokkaaksi ja taloudelliseksi toteuttamiseksi. Riskejä ei voida täysin poistaa, mutta niiden vaikutuksia on riskienhallinnalla mahdollista pienentää. Arviointimenettelyiksi tulee jatkossa tunnistaa viranomaisen toteuttama arviointi, hyväksytyn arviointilaitoksen toteuttama arviointi ja itsearviointi. Tietojärjestelmien ja palvelujen vaatimustenmukaisuus tulee arvioida säädettyjen vaatimusten ja niitä tarkentavista arviointikriteeristöistä tai standardeista riskiperusteisesti valittujen kriteerien avulla.

Suomen kyberturvallisuusstrategian 2024–2035 yhtenä kehittämisehdotuksen on ”Kehitetään organisaatioiden toimintaan sekä tietojärjestelmiin liittyviä arviointi- ja hyväksymismenetelmiä sekä niihin liittyviä vaatimuksia.” Strategian toimeenpanosuunnitelmassa kehittämisehdotus on tarkennettu toimenpiteeksi: ”Ajantasaistetaan tietojärjestelmien, palveluiden ja turvallisuuskriittisten tuotteiden vaatimustenmukaisuuden arviointia koskeva lainsäädäntö sekä kehitetään organisaatioiden toimintaan ja tietojärjestelmiin liittyvää arviointitoimintaa.” Tämä raportti tukee ja mahdollistaa strategian kehittämisehdotuksen ja sitä tarkentavan toimenpiteen ja sen tavoitteiden saavuttamista.

VALTIONEUVOSTO
STATSRÅDET

1. Tietojärjestelmien vaatimustenmukaisuuden arviointitoiminta

Johdanto

Valtiovarainministeriö asetti 22.2.2024 tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän toimikaudeksi 1.3.2024–31.12.2025 (VN/36127/2023). Työryhmän ja sihteeristön jäsenet ovat liitteenä 1. Ryhmän ensimmäisenä tehtävänä oli vuoden 2024 aikana tunnistaa säädösvalmistelun kohteet ja arvioida, tarkentaa ja priorisoida niihin liittyvät säädösmuutostarpeet. Työssä tuli ottaa huomioon itsearviointien hyödyntämisen tarjoamat mahdollisuudet, kustannustehokkuus ja toimintaympäristön muutokset. Tämä nykytila-arvio ja kehittämisehdotukset -raportti on ryhmän ensimmäisen vaiheen työn lopputulos. Raportin on toimittanut työryhmän puheenjohtaja, tietohallintoneuvos Tuija Kuusisto yhdessä sihteeristön jäsenten kanssa. Raportin valmisteluun on osallistunut työryhmän ja sihteeristön lisäksi julkisen hallinnon asiantuntijoita. Raportin valmistelussa on huomioitu sidosryhmätilaisuudessa 21.11.2024 ja sähköpostitse sidosryhmätilaisuuden jälkeen annettu palaute. Sidosryhmätilaisuuteen ilmoittautui 281 henkilöä ja siihen osallistui noin 230 henkilöä julkisesta hallinnosta, elinkeinoelämästä ja yhteisöistä. Sähköpostitse jälkikäteen saatiin palautetta 11 yhteisöltä tai henkilöltä.

Tämä raportti on pohjana työryhmän työn toisessa vaiheessa toteutettavalle tarkemmalle säädösvalmistelulle. Toisessa vaiheessa tavoitteena on vuoden 2025 loppuun mennessä valmistella hallituksen esityksen muotoon ehdotukset tietojärjestelmien ja yhteisten palvelujen vaatimustenmukaisuuden arviointia koskevan lainsäädännön ajantasaistamiseksi.

Tietojärjestelmien, palveluiden ja tuotteiden vaatimustenmukaisuuden arviointi on keskeinen menettely edistää ja yhtenäistää kyber- ja tietoturvallisuutta, tietosuojaa, varautumista sekä jatkuvuudenhallintaa digitalisoituvassa yhteiskunnassa. Arviointi tuottaa tietoa organisaatioiden kyberturvallisuusuhkien ja digiriskien hallinnalle sekä mahdollistaa toiminnan ja tietojen käytön ja jakamisen turvaamista. Tässä selvityksessä ei käsitellä tietosuojan vaatimustenmukaisuuden arvioinnin nykytilaa tai kehittämisehdotuksia. Tietosuojavaatimukset on kuitenkin huomioitava tietojärjestelmien ja palveluiden henkilötietojen käsittelyn vaatimustenmukaisuuden arvioinnissa.

Tiedon ja datan hallinta koskeva EU-sääntely sekä kansainvälisesti turvallisuusluokiteltujen tietojen käsittely on viime vuosina kasvanut. EU:n sisämarkkinoilla tarjottavia tuotteita ja palveluita koskevan sertifiointisääntelyn toimeenpano on vielä monelta osin valmisteluvaiheessa. Viittaukset Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881, jäljempänä *kyberturvallisuusasetus CSA,* mukaiseen sertifiointiin ovat lisääntymässä. Sertifiointeihin liittyvien vaatimustenmukaisuuden arviointipalvelutarpeiden odotetaan kasvavan uusien säädösten myötä.

Julkisen hallinnon tietojärjestelmien ja yhteisten palvelujen vaatimustenmukaisuuden arvioinnin keskeinen kansallinen sääntely, eli laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), jäljempänä *arviointilaki*, sekä laki tietoturvallisuuden arviointilaitoksista (1405/2011), jäljempänä *arviointilaitoslaki* (jäljempänä yhdessä *arviointilait*) on valmisteltu yli 13 vuotta sitten. Keskeistä arviointeihin liittyvää kansallista sääntelyä kuten laki julkisen hallinnon tiedonhallinnasta (906/2019), jäljempänä *tiedonhallintalaki*, valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019), jäljempänä *turvallisuusluokitteluasetus* sekä turvallisuusselvityslaki (726/2014) on valmistunut arviointilakien jälkeen. Arviointilakien lähtökohdat ovat edelleen tarkoituksenmukaiset, mutta niiden soveltamisen aikana on tunnistettu kehitystarpeita.

EU:n ja Naton turvallisuusluokitellun tiedon suojaamista koskevat laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), laki Tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä (907/2023) ja laki Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välillä tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta (224/2012).

Tietojärjestelmien ja tietoliikennejärjestelyjen vaatimustenmukaisuuden arviointia toteutetaan Suomessa lakisääteisesti EU:n sääntelyn perusteella sekä kansainvälisesti turvallisuusluokiteltujen tietojen ja sosiaali- ja terveystietojen käsittelyyn liittyen. Lisäksi valtioneuvoston asetuksen julkisen hallinnon turvallisuusverkkotoiminnasta (1109/2015), jatkossa *turvallisuusverkkoasetus,* 10§:n mukaan *Turvallisuusverkon palvelujen tietoturvallisuus- ja varautumisvaatimusten täyttyminen on arvioitava ja todettava noudattaen* arviointilakia ja kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia. Valtiovarainministeriö on antanut julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015), jäljempänä *turvallisuusverkkolaki*, 14.4 §:n mukaisella toimivallalla määräyksen koskien turvallisuusverkkolain mukaisten palvelujen ja niihin liitettävien viranomaisten tietojärjestelmien arviointia. Lakisääteisen tietoturvallisuuden arvioinnin rinnalla valtionhallinnon viranomaisilla on eriäviä käytäntöjä pyytää tietoliikennejärjestelyjen, tietojärjestelmien ja palveluiden tietoturvallisuuden vaatimustenmukaisuuden arviointia tai hyväksyntää.

Vaatimustenmukaisuuden arviointia haastavat kansallisten ja kansainvälisten tietoturvavelvoitteiden yhteensovittaminen, kehittyvät teknologiat kuten monikansalliset pilvipalvelut sekä EU- ja NATO-turvallisuusluokiteltavia tietoja ja tietojärjestelmiä koskevat vaatimukset ja vaatimustenmukaisuuden osoittamis- ja arviointikriteeristökäytännöt. Arviointilakeja on muutettu vain kertaalleen hallituksen esityksellä HE 57/2013 vp uuden turvallisuusselvityslain säätämisen yhteydessä välttämättömien muutosten tekemiseksi. Varsinaista arviointitoimintaa tai arviointilaitosten hyväksymistä tai valvontaa koskevaan kansalliseen sääntelyyn ei ole tehty lainkaan muutoksia arviointilakien voimaantulon vuoden 2012 jälkeen.

Säädettyjä tietoturvallisuuden vaatimustenmukaisuuden arvioijia ovat Liikenne- ja viestintävirasto sekä sen hyväksymät arviointilaitokset. Akkreditoituja arviointilaitoksia on tällä hetkellä neljä, joista kahdella on pätevyysalueena kansallisesti turvallisuusluokiteltavia tietoja käsittelevien tietojärjestelmien tietoturvallisuuden vaatimustenmukaisuuden arviointi ja sitä myöten myös sosiaali- ja terveystietojen käsittelyn tietoturvallisuuden arviointi.

Nato-jäsenyyden myötä kansainvälisen tietoaineistojen käsittelyyn käytettävien tietojärjestelmien lukumäärä Puolustusvoimissa ja niiden käyttö kansainvälisissä harjoituksissa on kasvanut nopeasti ja merkittävästi. Naton turvallisuusluokitellun tiedon käsittelyyn tarkoitettujen viranomaisten tarkastettavien ja akkreditoitavien tietojärjestelmien lukumäärä on lähes kymmenkertaistunut huhtikuun 2022 ja huhtikuun 2024 välillä. Lisääntynyt arviointitarve on aiheuttanut ruuhkautumista Liikenne- ja viestintäviraston ja Puolustusvoimien arviointitoiminnassa.

Valtion yhteisiä tieto- ja viestintäteknisiä palveluja tuottaa valtion tieto- ja viestintätekniikkakeskus Valtori ja turvallisuusverkon palveluja Valtori ja Suomen Erillisverkot Oy. Näillä palveluntuottajilla on jatkuvasti kasvava vuosittainen uusien palvelujen ja palvelujen elinkaaren aikana tehtävien muutosten arviointitarve.

Keskeisiä kansallisia arviointikriteeristöjä ovat ISO/IEC 27001 -standardi, kansallisen turvallisuusviranomaisen (NSA) julkaisema kansallinen turvallisuusauditointikriteeristö Katakri, Liikenne- ja viestintäviraston julkaisema pilvipalveluiden turvallisuuden arviointikriteeristö Pitukri sekä Tiedonhallintalautakunnan suositus Julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri): Suositus ja kriteeristö (VM 2022:43 ja päivitys VM 2023:46) sekä Julkriin perustuva suositus tietoturvallisuudesta hankinnoissa (VM 2023:57). Tietoturvallisuuden arviointilaitosten akkreditoinnissa FINASin soveltamat standardit ovat ISO/IEC 17021 ja ISO/IEC 27006, jotka liittyvät yleisesti johtamisjärjestelmiä ja erityisesti tietoturvallisuuden johtamisjärjestelmiä auditoiviin ja sertifioiviin arviointielimiin.

Jatkossa kansainvälisten standardien ja kriteerien hyödyntäminen vaatimustenmukaisuuden arvioinneissa on yhä tärkeämpää. EU:ssa markkinoille tarjottavien tuotteiden ja palveluiden arvioinneissa käytetyt arviointiperusteet ovat usein jäsenmaita velvoittavia kansainvälisiä standardeja tai skeemoja. Julkinen hallinto voi hyödyntää niiden mukaisesti arvioituja tietojärjestelmiin sisällytettyjä elementtejä.

Arviointilakien mahdollisia uudistamistarpeita on aikaisemmin arvioitu useammassa eri yhteydessä: valtiovarainministeriön kolme selvitystä vuodelta 2021, Liikenne- ja viestintäviraston muistio arviointilaitoslain kehitystarpeista vuodelta 2022 ja puolustushallinnon selvitys vuodelta 2024. Orpon hallituksen hallitusohjelmakirjauksen mukaan *salaustuotteiden hyväksyntäprosessia nopeutetaan, jotta kotimainen kyberteknologia saadaan nopeammin markkinoille. Suomi hankkii itselleen kansainvälisiä tietoturvahyväksyntöjä myöntävän maan aseman EU:ssa.* Toimintaympäristön muutosten, teknologioiden kehittymisen, EU-sääntelyn laajentumisen, kansallisen sääntelyn vanhentuneisuuden ja tehtyjen selvitysten perusteella julkisen hallinnon tietojärjestelmien ja yhteisten palvelujen sekä niiden hyödyntämisen tietoturvallisuuden sekä toiminnan jatkuvuuden ja varautumisen vaatimustenmukaisuuden arvioinnin sääntelyn ajantasaistaminen ja tehostaminen on välttämätöntä tässä asiakirjassa esitettyjen ehdotusten perusteella.

Suomen kyberturvallisuusstrategian 2024–2035 yhtenä kehittämisehdotuksen on ”Kehitetään organisaatioiden toimintaan sekä tietojärjestelmiin liittyviä arviointi- ja hyväksymismenetelmiä sekä niihin liittyviä vaatimuksia.” Strategian toimeenpanosuunnitelmassa kehittämisehdotus on tarkennettu toimenpiteeksi ”Ajantasaistetaan tietojärjestelmien, palveluiden ja turvallisuuskriittisten tuotteiden vaatimustenmukaisuuden arviointia koskeva lainsäädäntö sekä kehitetään organisaatioiden toimintaan ja tietojärjestelmiin liittyvää arviointitoimintaa.” Tämä raportti tukee ja mahdollistaa strategian kehittämisehdotuksen ja sitä tarkentavan toimenpiteen ja sen tavoitteiden saavuttamista.

VALTIONEUVOSTO
STATSRÅDET

Arviointitoiminnan laajuus ja kustannukset Suomessa

Liikenne- ja viestintäviraston (Traficom) tehtäviin kuuluvat tietojärjestelmien turvallisuusarvioinnit ja -hyväksynnät kansainvälisistä tietoturvallisuusvelvoitteista annetun lain, turvallisuusselvityslain sekä arviointilakien mukaan. Kansainvälisen turvaluokitellun tiedon osalta Liikenne- ja viestintäviraston tehtäviin kuuluu toimia kansallisena turvallisuusjärjestelyjen hyväksyntäviranomaisena (SAA, Security Accreditation Authority), salaustuotteiden hyväksyntäviranomaisena (CAA, Crypto Approval Authority), TEMPEST-viranomaisena (NTA, National TEMPEST Authority), sekä salausteknisen materiaalin jakelusta vastaavana viranomaisena (CDA, Crypto Distribution Authority; NDA, National Distribution Authority).

Liikenne- ja viestintävirasto tarjoaa maksullista tietojärjestelmien arviointipalvelua sellaisille valtionhallinnon organisaatioiden tietojärjestelmille, joille kansainvälinen tietoturvallisuusvelvoite (esimerkiksi EU- tai Nato-tiedon käsittely) edellyttää SAA:n hyväksyntälausuntoa. Hyväksyntäpalvelua tarjotaan Suojelupoliisille tai Pääesikunnalle (turvallisuusselvityslaki 9 §) yritysturvallisuusselvitysprosessiin hakeutuneiden yritysten tietojärjestelmien tietoturvallisuuden tasosta. Arviointipalvelua tarjotaan viranomaisen määräämisvallassa oleville tai hankittavaksi suunnittelemille tietojärjestelmille, joista viranomainen on tehnyt arviointipyynnön. Valtiovarainministeriön pyynnöstä Liikenne- ja viestintävirasto tekee selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta.

Liikenne- ja viestintävirasto tekee vuosittain useita kymmeniä tietojärjestelmäarviointeja. Järjestelmien laajuus ja siten arviointien tekninen laajuus, työmäärä ja kesto vaihtelevat paljon. Osa arvioinneista on muutos- tai määräaikaisarviointeja. Arviointiprosessille on tyypillisesti varattava aikaa vähintään puolesta vuodesta vuoteen. Tarvittava aika riippuu järjestelmän arviointikypsyydestä ja esimerkiksi arvioinnin rajauksista.

Merkittävin kasvu viimeisen kahden vuoden aikana on kohdistunut kansainvälisistä tietoturvallisuusvelvoitteista johtuviin tarkastus- ja hyväksyntätehtäviin. Naton turvallisuusluokitellun tiedon käsittelyyn tarkoitettujen viranomaisten tarkastettavien ja akkreditoitavien tietojärjestelmien lukumäärä on lähes kymmenkertaistunut huhtikuun 2022 ja huhtikuun 2024 välillä. EU:n ja muun kansainvälisen turvallisuusluokitellun tiedon sähköisen käsittelyn tarkastus- ja hyväksyntätarpeissa kasvu on ollut maltillisempaa. Myös turvallisuusselvityslain nojalla tehtävissä yritysten tietojärjestelmien tietoturvallisuuden tason selvityksissä on ollut maltillista kasvua. Viranomaisten tietojärjestelmien kansallisen turvallisuusluokitellun tiedon suojaamisen arvioinneissa työmäärä on pysynyt samansuuntaisena vuodesta 2022, mikä on osin johtunut kansainvälisten tietoturvallisuusvelvoitteiden priorisoinneista. Käytännössä Liikenne- ja viestintävirasto ei ole Suomen Nato-jäsenyyden jälkeen tehnyt lainkaan TL IV ja TL III -tason kansallista turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien arviointeja. Voimavarat on käytetty Naton turvallisuusluokiteltuja tietoja käsitteleviin järjestelmiin, joihin kohdistuu akkreditointivelvoite. Kansallisten turvallisuusluokkien TL IV ja TL III arviointien osalta virasto on ohjannut hakijoita arviointilaitosten palveluiden pariin.

Liikenne- ja viestintävirasto tekee tuotearviointeja ja -hyväksyntöjä kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti. Laajan arvioinnin tekeminen uudelle tuotteelle kestää yleensä vähintään vuoden, kun

taas muutosten arviointi on nopeampaa. Liikenne- ja viestintäviraston julkisella listalla on tällä hetkellä kymmenkunta arvioitua salaustuotetta ja viitisen muuta arvioitua tuotetta. Viranomaisten pyytämiä järjestelmäkohtaisia arviointeja ei julkaista. Uusia arviointeja tai tuotepäivitysten arviointeja on yleensä samanaikaisesti käynnissä alle kymmenen.

Liikenne- ja viestintäviraston tekemien arviointien maksuista säädetään sähköisen viestinnän maksuasetuksessa (1256/2021). Maksua peritään omakustannusarvon mukaisesti 150 euroa käytettyä työtuntia kohden.

Liikenne- ja viestintävirasto hyväksyy sekä ohjaa ja valvoo tietoturvallisuuden arviointilaitoksia. Ne tarjoavat viranomaisille ja yrityksille luotettavaa ja puolueetonta tietoturvallisuuden arviointipalvelua. Hyväksyttyjä arviointilaitoksia on nykytilanteessa neljä. Niistä kahdella on ainoastaan pätevyys tehdä tietoturvallisuuden johtamisjärjestelmän ISO/IEC 27001 -standardin mukaisia sertifiointeja. Vuoden 2023 julkisten tilinpäätöstietojen perusteella näistä toisen, vuodesta 2017 hyväksyttynä arviointilaitoksena toimineen yrityksen liikevaihto oli 18,3 miljoonaa euroa, jossa kasvua vuodesta 2021 oli 2 miljoonaa euroa. Toinen yritys on toiminut hyväksyttynä arviointilaitoksena vasta vuodesta 2023, jolloin yrityksen liikevaihto oli 217 000 euroa.

Kaksi hyväksyttyä arviointilaitosta tarjoavat tietoturvallisuuden johtamisjärjestelmän ISO/IEC 27001 -standardin mukaisten sertifiointien lisäksi tietojärjestelmien tietoturvallisuuden vaatimustenmukaisuuden arviointipalveluja. Näillä kahdella arviointilaitoksella on pätevyys arvioida kansallisesti turvallisuusluokiteltua tietoja sisältäviä tietojärjestelmiä eli niillä on Katakri-pätevyysalue. Katakri-pätevyysalueen myötä näillä arviointilaitoksilla on myös pätevyys toteuttaa sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023), jäljempänä *asiakastietolaki,* ja sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain (552/2019), jäljempänä *toisiolaki,* mukaisia arviointeja. Vuoden 2023 julkisten tilinpäätöstietojen perusteella näiden arviointitoimintaa harjoittavien yritysten liikevaihto on ollut yhteensä noin 6 miljoonaa euroa. Arviointitoiminnan liikevaihto on kasvanut merkittävästi suhteessa vuoteen 2019, jolloin liikevaihtojen summa oli noin 2,3 miljoonaa euroa. Merkittävin liikevaihdon kasvu on tapahtunut aikavälillä 2021 – 2023 (+114 %). Liikevaihdon kasvusta on pääteltävissä, että hyväksyttyjen arviointilaitosten palveluiden käyttötarve on kasvanut.

Valtori ja Suomen Erillisverkot Oy tuottavat turvallisuusverkkolain ja turvallisuusverkkoasetuksen mukaisia turvallisuusverkon palveluja. Lisäksi Valtori tuottaa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013), jäljempänä *Torilaki*, ja valtioneuvoston asetuksen valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014), jäljempänä *Toriasetus*, mukaisia palveluja. Tuotteistetut palvelut koostuvat palveluista ja niiden osista, joista jokainen todennetaan eli arvioidaan erikseen. Tämä tarkoittaa merkittävän suurta todentamistarvetta vuositasolla uusien palvelujen ja elinkaaren aikana palvelussa tehtävien muutosten kautta syntyvien todentamistarpeiden suhteen. Tämän seurauksena Valtorissa ja Suomen Erillisverkot Oy:ssä on käynnissä lukuisia tuotteistettujen palvelujen todentamisia kuukausittain mukaan lukien asiakkaiden toimialasidonnaisten tietojärjestelmien todentamiset, joihin nämä palveluntuottajat osallistuvat.

Valtorin ja Suomen Erillisverkot Oy:n hankkimien vaatimustenmukaisuuden todentamisten määrät ovat arviointilakien voimassaolon aikana lisääntyneet. Kasvu johtuu palveluiden kehittämistoimista, uusista palveluista sekä EU ja Nato -tiedon käsittelytarpeesta. Valtori on vuoden 2021 elokuun ja vuoden 2024 välisenä

aikana teettänyt yhteensä 73 todentamista, joista 40 on kohdistunut turvallisuusverkon palveluihin ja 33 Torilain mukaisiin palveluihin. Näistä kahdessa todentamisessa on ollut kyse kansainvälistä tietoa käsittelevästä järjestelmästä, jotka Liikenne- ja viestintävirasto on kansallisena turvallisuusjärjestelyjen todentajana todentanut. Suurimman osan todentamisista ovat toteuttaneet kaksi arviointilaitosta, jotka ainoina on hyväksytty turvallisuusluokkiin III ja IV kuuluvaa tietoa käsittelevien järjestelmien arviointiin. Lisäksi yhteisten valtion pilvipalveluiden tarkastuksia on toteuttanut yksi kaupallinen toimija.

Suomen Erillisverkot Oy:ssä on toteutettu noin 20 itsearviointia vuodessa. Itsearvioinnit ovat vaatineet noin 300 henkilötyöpäivää ja niiden kustannukset ovat olleet noin 210 000 euroa vuodessa. Hyväksyttyjen arviointilaitosten arviointeja on toteutettu useita vuodessa. Arviointilaitosten arvioinneista johtuvat kustannukset, sekä sisäiset että ulkoiset, ovat olleet noin 57 000 euroa arviointia kohden.

Vaatimustenmukaisuuden arviointipalvelujen pyytäjien näkemyksen mukaan valtion yhteiseen tieto- ja viestintätekniseen palveluun sisältyvän osan tietoturvallisuuden vaatimustenmukaisuuden arvioinnin hinta on keskimäärin yhteensä 60 000–70 000 euroa/arviointi, josta hyväksytyn arviointilaitoksen suorittaman ulkoisen arvioinnin osuus on keskimäärin 30 000–40 000 euroa. Yksi arviointi vaatii keskimäärin sisäisenä työnä noin 35 henkilötyöpäivää (8–10 palvelun asiantuntijaa) ja ulkoinen arviointi noin 15–20 henkilötyöpäivää arviointilaitokselta. Vaatimustenmukaisuuden arvioinnin kustannuksiin vaikuttavat arvioinnissa käytetty kriteeristö sekä maksuperustelain tai arvioinnin suorittamisen kilpailutuksen perusteella määräytyvä päivähinta.

Puolustusvoimat on yli 30 hallintoyksiköstä muodostuva iso virasto, jossa tietojenkäsittely on laajaa ja monitasoista. Valtionhallinnossa merkittävä määrä tietojärjestelmien arvioinneista tehdään Puolustusvoimien tarpeisiin. Puolustusvoimien erityispiirteenä on tarve käsitellä laajasti eri turvallisuusluokkiin kuuluvaa kansallista ja kansainvälistä tietoa erilaisissa tietojenkäsittely-ympäristöissä. Puolustusvoimilla on tarve vaihtaa tietoa kansallisten viranomaisten, toisten valtioiden viranomaisten, kansainvälisten järjestöjen ja strategisten kumppanien kanssa. Sotilaallisen puolustamisen tehtävät edellyttävät Puolustusvoimilta kykyä soveltaa viranomaisia koskevaa yleistä lainsäädäntöä asiakirjojen julkisuudesta, tiedonhallinnasta, arkistoinnista ja tietoturvallisuudesta muista viranomaisista poikkeavaan toimintaympäristöön ja olosuhteisiin.

Puolustusvoimien nykyiset arviointi- ja hyväksyntäresurssit on mitoitettu kansallisten järjestelmien tietoturvallisuusvaatimusten perusteella. Puolustusvoimat arvioi itse ensisijaisesti järjestelmät, joissa käsitellään turvallisuusluokkiin I ja II luokiteltua tietoa. Alempien turvallisuusluokkien tietojärjestelmien arviointeja hankitaan tarvittaessa ostopalveluina. Salaustuotteiden arvioinnissa ei pääsääntöisesti käytetä ostopalveluita. Nato-jäsenyyden myötä kansainvälisen tietoaineistojen käsittelyyn käytettävien tietojärjestelmien lukumäärä Puolustusvoimissa ja niiden käyttö kansainvälisissä harjoituksissa kasvaa nopeasti ja merkittävästi. Lisääntynyt arviointitarve on aiheuttanut ruuhkautumista Liikenne- ja viestintäviraston ja Puolustusvoimien arviointitoiminnassa. Tämä on lisännyt Liikenne- ja viestintäviraston tarvetta sopia tietojärjestelmien arvioinnin ja hyväksynnän vastuun siirrosta Pääesikunnalle, kun se on ollut tarpeen tehtävien tarkoituksenmukaiseksi hoitamiseksi. Tehtävien siirtäminen kansainvälisiin tietoturvallisuusvelvoitteisiin perustuvissa arvioinneissa Liikenne- ja viestintävirastolta Puolustusvoimille lisää Puolustusvoimien osaamista, mutta edellyttää samalla lisäresursseja. Nämä resurssit ovat pois kansallisten järjestelmien arvioinnista ja hyväksynnästä.

Sosiaali- ja terveydenhuollon (sote) julkisten ja yksityisten organisaatioiden on tietyissä tilanteissa hankittava tietoturvallisuuden arviointia koskeva todistus asiakastietolain tai toisiolain nojalla. Sote-tietojärjestelmien vaatimustenmukaisuuden tilanne näkyy Valviran tietojärjestelmärekisteristä, joka sisältää tällä hetkellä 89 sote-asiakastietojen käsittelyyn tarkoitettua luokan A tietojärjestelmää, ja 10 toisiolain määräysten perusteella arvioitua käyttöympäristöä. Luokan A tietojärjestelmiltä edellytetään ulkoista tietoturvallisuuden arviointia eli tietoturvallisuuden arviointilaitoksen arviointia. Valviran rekisteritietojen perusteella hyväksyttyjen tietoturvallisuuden arviointilaitosten todistuksia vaatimustenmukaisuudesta on vuosittain myönnetty sote-tietojärjestelmille seuraavasti: 2021 15, 2022 21, 2023 27 ja 8/2024 15 kappaletta. Kelassa oli työn alla elokuussa 2024 11 tietoturvallisuuden arviointia. Myönnettyjen todistusten määrä näyttäisi olevan jonkin verran kasvussa, koska osa B-luokan tietojärjestelmistä on siirtynyt ja tulee vuoden 2024 aikana siirtymään A-luokkaan. Asiakastietolain ja toisiolain edellyttämien tietoturvallisuuden arviointitarpeiden määrä vaikuttaa kahden tähän arviointitehtävään hyväksytyn arviointilaitoksen palvelujen kysyntään.

Työryhmässä kesällä 2024 toteutetun kartoituksen perusteella tunnistettiin seuraavia arviointikustannuksia ja -määriä ministeriöissä ja hallinnonaloilla:

- Valtioneuvoston kanslian pyytämiä arviointilakien mukaisia tietoturvallisuuden arviointeja on työn alla kaksi. Ne perustuvat kansainvälisiin tietoturvavelvoitteisiin ja arvioitsijana on Liikenne- ja viestintävirasto.

- Poliisi ja Hätäkeskuslaitos ovat käyttäneet keskimäärin noin kaksi miljoonaa euroa vuodessa toimialasidonnaisten tietojärjestelmien tietoturvallisuuden arviointeihin. Tästä osa on ollut arviointilaitoksille maksettuja kustannuksia, osa organisaation oman henkilöstön kustannuksia ja osa Valtorin kustannuksia.

- Työ- ja elinkeinoministeriön hallinnonalalla tietoturvallisuuden arviointien vuosittaiset kustannukset jakaantuvat organisaatioittain 30 000–120 000 euron välille ja arvioitujen tietojärjestelmien määrä 2–10 järjestelmän välille. Osa organisaatioista arvioi arviointien määrän pysyvän samana, osa niiden lisääntyvän jonkin verran ja osa niiden lisääntyvän merkittävästi. Arviointien määrän arvioitiin myös voivan laskevan, jos tietojärjestelmähankkeita ei pystytä edistämään resurssien puuttuessa. Arvioinneista vain osa on ollut arviointilakien mukaisia arviointeja, sillä vain osa organisaatioista on käyttänyt hyväksyttyjä arviointilaitoksia arvioinneissa. Arvioiduista tietojärjestelmistä muutamassa käsitellään kansallista turvallisuusluokiteltua tietoa ja suurimmassa osassa salassa pidettävää tietoa tai henkilötietoa.

- Liikenne- ja viestintäministeriön hallinnonalla on vuosittain arvioitu keskimäärin noin 10 tietojärjestelmän tietoturvallisuus arviointilaitosten toimesta. Hallinnonalan virastojen tietojärjestelmien tietoturvallisuuden arviointeihin käyttämää omaa työpanosta ei ole arvioitu kaikissa virastoissa. Kahden viraston osalta arviointeihin arvioitiin käytettävän vuodessa yhteensä noin 230 henkilötyöpäivää. Hyväksytyiltä arviointilaitoksilta on hankittu vuosittain noin 220–230 henkilötyöpäivää arviointilakien mukaisia arviointipalveluja. Palvelujen hankintakustannusten arvioidaan olevan vuositasolla noin 300 000 euroa. Muilta tietoturvapal-

VALTIONEUVOSTO
STATSRÅDET

veluja tarjoavilta yrityksiltä on hankittu vuosittain noin 720–750 henkilötyöpäivää arviointeihin liittyviä palveluja. Kustannusten arvioidaan olevan vuositasolla noin 650 000 euroa. Arviointilakien mukaiset arvioinnit ovat henkilötyöpäivinä siten noin 20 % ja euromääräisesti noin 30 % kaikista vaatimustenmukaisuuden arvioinneista liikenne- ja viestintäministeriön hallinnonalalla.

Digi- ja väestötietoviraston (DVV) digiturvan kokonaiskuvapalvelun vuoden 2024 tietojen perusteella kaikkien organisaatioiden vastausten keskiarvio koskien väittämää ”Tietoturvallisuuteen ja tietojärjestelmiin liittyvä auditointeja tehdään säännöllisesti” on 0,54 (N=176, asteikko 0–1, jossa 0 tarkoittaa ei ja 1 kyllä). Kuntien (N=92) vastausten keskiarvo on 0,44; kuntayhtymien (N=16) 0,59; hyvinvointialueiden (N=16) 0,47; korkeakoulujen (N=9) 0,39 ja valtionhallinnon (N=40) 0,78. Tietoturvallisuuteen ja tietojärjestelmiin liittyviä auditointeja toteutetaan siten korkeakouluissa ja kunnissa vähemmän kuin valtionhallinnossa. Toisaalta kuntien ja kuntayhtymien muita organisaatioita matalampi vastausten keskiarvo voi myös viitata siihen, että väitteen on tulkittu tarkoittavan vain arviointilain mukaisia arviointeja eikä itsearviointeja ole huomioitu. DVV:n väitettä tulisi tarkentaa tulosten selkeämmän tulkittavuuden varmistamiseksi. Kattavaa kuvaa arviointilain mukaisista arvioinneista tai ISO/IEC 27000 -sarjan sertifioinneista kunnissa ei ole saatavilla. Kuntaliiton arvion mukaan suuremmissa kunnissa sisäinen tarkastus on tehnyt laajojakin tietoturvallisuuden katselmointeja.

Arviointilaitosten arviointipalveluja käyttävät organisaatiot ovat kohdanneet haasteita arviointipalvelujen käytössä. Arviointien teettäminen on sekä hidasta että kallista ja arviointilaitosten vajaiden resurssien takia myös epävarmaa. Epävarmuutta lisää mahdollinen arviointikriteeristön päivittyminen ja arviointilaitosten puuttuvat akkreditoinnit uusille pätevyysalueille. Koska turvallisuusverkkoasetuksen ja valtiovarainministeriön määräyksen edellyttämiä ja asiakastietolain ja toisiolain edellyttämiä tietoturvallisuuden arviointeja toteuttaa vain kaksi toimijaa, on palvelujen käyttöön ottaminen pitkälti riippuvaa niiden resursseista ja aikatauluista mukaan lukien näihin liittyvät äkilliset muutokset. Järjestelmiä joudutaan myös arvioimaan muutostilanteissa uudelleen, eikä arviointilaitosten kapasiteetti nykyisellään mahdollista riittävän nopeaa etenemistä.

Liikenne- ja viestintävirastosta ja arviointilaitoksilta kerätyn palautteen perusteella julkisen hallinnon organisaatioiden pyytämien arviointien hitaus ja kustannukset voivat johtua ajoittain organisaation omasta toiminnasta, jos tietojärjestelmiä, prosesseja ja hallintakeinoja ei ole alun perin suunniteltu arvioinnissa käytettävän kriteeristön mukaisesti. Lisäksi arviointi hidastuu, jos haastateltavan henkilöstön sekä mahdollisten alihankkijoiden ajankäyttöä ei priorisoida arvioinnin hyväksi. Myös arvioinnissa havaittujen poikkeamien korjausten todentaminen lisää kustannuksia sekä viivästyttää arvioinnin päättämistä. Arviointitoimintaa varten arviointien toteuttajat ovat tehneet merkittäviä investointeja tiloihin, laitteistoihin, ohjelmistoihin ja osaamisen kehittämiseen sekä näiden vaatimustenmukaisuuden säännöllisiin auditointeihin.

Kuntakenttään ei tällä hetkellä kohdistu suoraan sellaisia lakisääteisiä yksilöityjä vaatimuksia, joiden perusteella kuntakentän toimijoiden tulisi hankkia arviointilaitosten tekemiä tietojärjestelmien vaatimustenmukaisuuden arviointeja. Kuntakentällä ei ole ollut merkittävää tarvetta käsitellä kansainvälistä turvallisuusluokiteltua tietoa. Se ei käsittele toiminnassaan merkittävässä määrin kansallista turvallisuusluokiteltua tietoa,

koska se ei ole tiedonhallintalain alaisen turvallisuusluokitteluasetuksen piirissä. Vertailtaessa valtionhallinnon ja hyvinvointialueiden toteuttamaan tiedonkäsittelyyn, kuntakentän tietojärjestelmät ja tiedonkäsittely on nähty kansallisen turvallisuuden ja yhteiskunnan toimivuuden näkökulmasta vähemmän kriittiseksi kuin muiden hallinnon tasojen toteuttama tietojenkäsittely. Kunnille siirtyvien TE-palveluiden tietojärjestelmien järjestämisestä vastaa KEHA-keskus keskitetysti. Tulevaisuudessa kuntakentällä voi olla tarvetta käsitellä enenevässä määrin salassa pidettävää tietoa tai kansallisesti ja kansainvälisesti turvallisuusluokiteltua tietoa viranomaisten välisessä tiedonvaihdossa. Kunnan toiminnassa tuotettujen tietojen, kuten valmiussuunnitelmien ja rakennetun ympäristön kriittistä infrastruktuuria koskevien paikkatietojen suojausvaatimukset voivat tiukentua tietoihin kohdistuvan kansallista turvallisuutta vaarantavan väärinkäytösriskin vuoksi.

Kuntien perustehtävien toteuttamisessa hyödynnettävien keskeisten tietojärjestelmien tarjoajat ovat usein suuria kansallisia tai kansainvälisiä palveluntoimittajia. Nämä tietojärjestelmät ovat enenevässä määrin luonteeltaan pilvipalveluita. Johtuen kuntien suhteessa pienestä koosta ja pienistä volyymeista, kunnilla ei välttämättä ole kaikissa tilanteissa merkittävää vaikuttamismahdollisuutta palveluntarjoajiin ja niiden palveluehtoihin. Tällöin kunta voi usein olla palvelun hankkijana tilanteessa, jossa tietojärjestelmäpalvelun voi saada käyttöön vain hyväksymällä myyjän sopimusehdot. Täten yksittäisen kuntatoimijan vaikutusmahdollisuudet hankittavan tietojärjestelmän vaatimuksiin voivat olla vähäiset. Samoin palveluna hankittavien tietojärjestelmien tietoturvallisuuden vaatimustenmukaisuuden arviointi voi olla haastavaa, ellei mahdotonta, yksittäiselle kunnalle. Tämän vuoksi kuntien tietoturvallisuuden kannalta olisi tärkeää, että olennaisten palveluntoimittajien tietoturvallisuusvaatimusten asettamisessa ja vaatimustenmukaisuuden arvioinnissa hyödynnettäisiin entistä enemmän kansallista yhteistyötä ja kansallisia ratkaisuja.

Kansainvälinen vertailu

Selvityksessä digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä (VM 2021) käsiteltiin arviointilainsäädäntöä, tarkastusjärjestelyjä, akkreditointikäytäntöjä, arviointikriteeristöjä, toiminnan organisoitumista ja toiminnassa käytettäviä standardeja Tanskassa, Ruotsissa, Virossa, Saksassa, Alankomaissa ja Singaporessa. Selvityksessä digitaalisen turvallisuudella tarkoitettiin riskienhallintaa, jatkuvuudenhallintaa ja varautumista, tietoturvallisuutta, kyberturvallisuutta ja tietosuojaa. Tieto kerättiin verrokkivaltioiden julkisista dokumenteista ja muista lähteistä. Tässä luvussa selvitystä on tuoreutettu ja täydennetty.

Useissa valtioissa Nato-sääntelyn toimintamalleja sovelletaan myös kansallisen turvallisuusluokitellun tiedon suojaamisessa. Siten Nato-sääntely on merkittävin yhtenevä kansainvälisten ja kansallisten turvallisuusluokiteltujen tietojen käsittelyyn liittyvä arviointisääntely. EU:n vaatimustenmukaisuuden arviointisääntely on Nato-sääntelyn kanssa pääsääntöisesti yhtenevää. EU-valtioiden käytäntöjä yhtenäistävät luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettu Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, jäljempänä *yleinen tietosuoja-asetus*, toimenpiteistä yhteisen korkeatasoisen kyberturvallisuuden varmistamiseksi koko unionissa annettu Euroopan parlamentin ja neuvoston direktiivi, jäljempänä *NIS2 tai NIS2-direktiivi*, sekä tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta annettu Euroopan parlamentin ja neuvoston asetus (EY) N:o 765/2008 ja kyberturvallisuusasetus (CSA).

Viron kansallisen turvallisuusluokitellun tiedon suojaamiseen kohdistuu samansuuntainen akkreditointimenettely kuin esimerkiksi EU:n ja Naton turvallisuusluokiteltuun tietoon. Virossa siis myös vain kansallista turvallisuusluokiteltua tietoa käsittelevät tietojärjestelmät läpikäyvät akkreditointiprosessin. Kansallista turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien suojaamisessa hyödynnetään samansuuntaisia vaatimuksia ja menettelyjä kuin esimerkiksi Naton turvallisuusluokitellun tiedon suojaamisessa.

Alankomaissa turvallisuusluokitellun tiedon suojaamisen arviointiin hyödynnetään ABDO-kehikkoa (https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019-english), joka on hyvin yhtenevä esimerkiksi Suomen Katakrin kanssa. Alankomaissa ABDO:n historia on puolustushallinnossa, mutta sen käyttö on viime vuosina laajentunut myös muualla Alankomaiden valtionhallintoon ja sen sidosryhmiin turvallisuusluokitellun tiedon suojaamisen arvioinneissa. Lähitulevaisuudessa ABRO:ksi nimettävä ja päivitettävä kehikko on tulossa sääntelymuutosten myötä selkeästi käytettäväksi sekä siviili- että puolustustoiminnassa.

Valtion virastojen ja kriittisen infrastruktuurin toimijoiden tietoturvallisuuden säännöllistä tarkastamista suositellaan kaikissa verrokkimaissa, mutta tarkastuksen toteutuskäytäntö vaihtelee. Säännöllistä arviointia edellytetään määrävälein Virossa, Saksassa ja Singaporessa, kun taas Tanskassa, Ruotsissa ja Alankomaissa määrävälein toteutettuja arviointeja ei edellytetä. Virossa ministeriöt, virastot sekä valtion tietoturvaan liittyvät rekisterinpitäjät ovat velvollisia suorittamaan arvioinnin suojausluokituksen mukaisesti kahden, kolmen tai neljän vuoden välein. Saksassa on säädetty, että kriittisen infrastruktuurin toimijoiden tulee kahden vuoden välein osoittaa palvelunsa täyttävän tietoturva-asetuksen (IT-SiG) vaatimukset auditointien, tutkimusten tai sertifikaattien avulla. Myös Singaporessa kyberturvallisuuslaki edellyttää kriittisen infrastruktuurin toimijoita suorittamaan tietoturvallisuusauditointia vähintään kerran vuodessa. Suomessa viranomaisten kansallisten tietoturvallisuuden arviointien hakeminen on vapaaehtoista, eikä laki velvoita säännöllisiin ulkopuolisen toimijan tekemiin arviointeihin. NIS2-direktiivin kansallista täytäntöönpanoa (HE 57/2024 vp) koskevassa tiedonhallintalain 4a luvussa ei säädetä tiedonhallintayksikölle velvollisuutta hankkia arviointeja. Valvovan viranomaisen mahdollisiin valvontakeinoihin kuuluu tarkastus, jossa valvoja voi käyttää apuna hyväksyttyä arviointilaitosta.

Yleisesti ottaen verrokkimaissa tunnustetaan ja hyväksytään kansainväliset digitaalisen turvallisuuden alueiden standardit. ISO/IEC 27001 -standardi on tunnustettu tietoturvan hallintajärjestelmien toteuttamisessa ja ISO/IEC 17021-1 -standardi asettaa vaatimuksia tietoturvallisuuden arviointilaitosten akkreditointiprosessiin. Tanskassa on erityisesti säädetty, että kaikkien valtion viranomaisten on noudettava ISO/IEC 27001 -standardia vuodesta 2014 lähtien. Joissakin maissa on myös kehitetty omia standardeja digitaalisen turvallisuuden varmistamiseksi. Saksassa on kehitetty tietoturvan hallintajärjestelmänä BSI IT-Grundschutz, joka kattaa tekniset ja organisatoriset sekä infrastruktuuriin ja henkilöstöön liittyvät näkökulmat. Viro on ottanut mallia Saksan IT-Grundschutzista ja laatinut oman E-ITS-standardinsa. Singaporessa on kehitetty monitasoinen pilviturvallisuusstandardi, MTCS, jossa määritetään kolme erilaista tietoturvasertifikaatin tasoa pilvipalvelujen pääasiallisille tuotantomalleille. Suomessa arviointilait antavat mahdollisuuden käyttää arvioinneissa useita erilaisia viitekehyksiä, mutta toistaiseksi ainoastaan Katakri ja ISO/IEC 27001 ovat arviointilaitoksille myönnettyjä pätevyysalueita.

Suomessa hyväksytyn arviointilaitoksen henkilöstöltä edellytetään osaamista ja koulutusta tai kokemusta, mutta henkilösertifiointia ei vaadita. Virossa asetus tietojärjestelmien turvatoimenpiteiden järjestämisestä edellyttää, että valtion turvallisuuden hallintajärjestelmän toteutuksen auditoinnissa tarkastajalla tulee olla voimassa olevat sertifikaatit. Tarkastajalla täytyy siis olla paikallisen ISACA:n myöntämä CISA-sertifikaatti (Certified Information Systems Auditor) sekä Yhdistyneen kuningaskunnan kansallisen standardointielimen (British Standards Institution, BSI) myöntämä ISO/IEC 27001 -sertifikaatti tai Saksan kyberturvallisuusviranomaisen (Bundesamt für Sicherheit in der Informationstechnik, BSI) myöntämä ISO/IEC 27001 IT-sertifikaatti.

Selvityksessä vain osasta verrokkivaltioita löydettiin tietoja julkisen hallinnon tietoturvallisuuden arviointilaitoksista tai niitä koskevista lainsäädännöistä. Esimerkiksi Tanskassa tietosuojaviranomaisella (Datatilsynet) on valtuudet valtion viranomaisten tietosuoja-arviointiin, ja Saksassa viranomaisten tietoturva-arviointia tukevat kyberturvallisuusviranomaisen (BSI) sertifioimat tietoturvapalveluntarjoajat. Verrokkivaltioiden valtiontalouden tarkastusviraston yleiseen tehtävään kuuluu valtion viranomaisten tietoturvajärjestelmien tarkastus. Vuoden 2021 selvityksessä ehdotetaan, että kansainväliseen vertailuun perustuen myös Suomessa tietojärjestelmiä ja palveluita arvioitaisiin säännöllisesti niiden elinkaaren aikana ja pidettäisiin huolta, että arvioinnissa käytettävät kriteerit olisivat linjassa kansainvälisten standardien kanssa.

VALTIONEUVOSTO
STATSRÅDET

2. Arviointitahot

Arviointien pyytäjät ja tarkoitus

Viranomaisille ei ole säädetty yleistä tietojärjestelmien ja tietoliikennejärjestelyjen vaatimustenmukaisuuden arviointivelvoitetta. NIS2-direktiivin täytäntöönpanossa kyberturvallisuusriskien hallinnan vaatimukset laajenevat julkishallinnon toimialalle. Direktiivin soveltamisalaan kuuluvien eri toimialojen vaatimukset säädetään pääosin uudessa yleislaissa kyberturvallisuuslaki (HE 57/2024 vp) ja julkishallinnon toimialan osalta vastaavat vaatimukset säädetään tiedonhallintalain 4 a luvussa. Luvun soveltamisalaa on rajattu tiedonhallintalain 3 §:ssä, eli sitä ei sovelleta kuntiin, opetus- ja koulutusalan toimijoihin, kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla toimiviin viranomaisiin eikä turvallisuusverkon palvelutuottajiin ja palvelujen käyttöön. Tiedonhallintalain 4a luvussa ei säädetä tiedonhallintayksikölle velvollisuutta hankkia arviointeja. Kyberturvallisuuslakia sovelletaan eräisiin kuntien kriittisen infrastruktuurin toimintoihin, esimerkiksi vesi- ja jätehuoltoon. Kyberturvallisuuslaissa ei myöskään velvoiteta tietoturvallisuuden arviointeihin.

NIS2-direktiivin toimeenpano on Suomessa toteutettu hajautetun mallin mukaisesti, jolloin sektoriviranomaiset valvovat sektorillaan olevia toimijoita. Lisäksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii kansallisena koordinaatiopisteenä. Valvovia viranomaisia ovat Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Lääkealan turvallisuus ja kehittämiskeskus ja Finanssivalvonta. Tiedonhallintalain 4 a luvun vaatimusten täyttymistä ohjaa ja valvoo Liikenne- ja viestintävirasto. Valvova viranomainen voi muun muassa pyytää selvityksiä tai tehdä tarkastuksen, jossa se voi käyttää avustajana hyväksyttyä arviointilaitosta, ja antaa päätöksen korjausvelvoitteista laissa tai NIS 2-direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamiseksi. Tarvittaessa viranomaisen tieto- ja tietoliikennejärjestelyjen riittävä taso voi siten tiedonhallintalain 4 a luvun soveltamisen piiriin kuuluvissa toiminnoissa tulla ratkaistavaksi viranomaisen valvontapäätöksellä.

Tiedonhallintalain 13 §:n perusteella vastuu tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta varmistumisesta kuuluu tiedonhallintayksikölle. Säännös painottaa tiedonhallintayksikön riskiarviointiin perustuvaa lähestymistapaa. Tiedonhallintalain 13 a §:ssä säädetään velvollisuus varmistaa viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys riittävällä testauksella säännöllisesti. Testauksia tai niitä tekeviä tahoja ei säännellä tarkemmin.

Tiedonhallintalain 13 §:n 5 momentin mukaan viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen. Arviointilain 3 §:ssä säädetään valtionhallinnon viranomaisille sallituista arviointien toteuttajista. Säännöksen mukaan valtionhallinnon viranomaiset saavat käyttää tietojärjestelmiensä ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnissa vain Liikenne- ja viestintävirastoa tai arviointilaitoslain mukaisesti hyväksyttyä tietoturvallisuuden arviointilaitosta. Säännös on sanamuodoltaan tiukka. Säännöksen rajoituksen laajuus on ollut tulkinnanvarainen ja aiheuttanut epäselvyyttä. Lain perustelujen mukaan (HE 45/2011 vp, s. 11) *säännöksellä varmistettaisiin, että valtionhallinnon viranomaiset käyttävät vain luotettavia ulkopuolisia tietoturvallisuuden arviointipalveluja*.

Arviointilaissa ei huomioida arvioitavan tietojärjestelmän riskitason tai järjestelmässä käsiteltävien tietojen luottamuksellisuus-, eheys- tai saatavuusvaatimusten vaikutusta siihen, millainen arviointitaho on riittävä: viranomainen, julkista hallintotehtävää hoitava arviointilaitos vai muu taho. VAHTI-ohjeessa 2/2014 oli tuotu esille myös muita kuin arviointilain mukaisia tietoturvallisuuden arviointimenettelyjä: *Viranomaiset voivat kuitenkin osana normaalia toiminnan kehittämistä tehdä itse sisäisiä arviointeja, itsearviointeja tai tietojärjestelmien teknistä testausta. Ohjattuja sisäisiä arviointeja ja itsearviointeja voidaan myös hankkia ulkopuolisilta palveluntuottajilta käyttäen esimerkiksi Valtorin kilpailuttamia ja tuottamia asiantuntijapalveluita.* Arviointilakiin nämä menettelyt eivät sisälly. Digitalisoidun julkisen palvelun tietoturvallisuudessa saattaa korostua tiedon luottamuksellisuus tai luottamuksellisuuden rinnalla tai jopa sijasta tiedon eheys ja saatavuus. Näin voi olla esimerkiksi terveystietojen hallinnassa tai kansalaisille suunnatussa kriisiviestinnässä.

Julkisen, salassa pidettävän ja kansallisen turvallisuusluokitellun tiedon suojaamisessa tiedonhallintayksiköt voivat tiedonhallintalain nojalla arvioida omia tietojenkäsittelyn ratkaisuja, tietojärjestelmiä ja niissä hyödynnettäviä teknologioita sekä päättää niiden jäännösriskin hyväksymisestä ja käyttöönottamisesta. Tämä koskee ratkaisuille hyväksyttäviä turvallisuusjärjestelyjä, mukaan lukien salausratkaisuja ja hajasäteilyltä suojautumista. EU:n ja Naton turvallisuusluokitellun tiedon käsittelyyn käytettävät tietojärjestelmät on turvallisuusääntöjen mukaan etukäteen akkreditoitava, ja myös tietyt osa-alueet tai elementit on etukäteen arvioitava ja hyväksyttävä. Akkreditointivelvoitteen tarkoitus on tälläkin tavoin varmistaa kansainvälisen turvallisuusluokitellun tiedon suojaaminen. Turvallisuusverkon palveluiden tietoturvallisuuden arvioinnissa on noudatettava turvallisuusverkkolain ja -asetuksen säännöksiä.

Kansainvälisten tietoturvallisuusvelvoitteiden arvioinnissa toimivaltaisista viranomaisista säädetään kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä ja yritysturvallisuusselvityksissä toimivaltaisista viranomaisista turvallisuusselvityslain 9 §:ssä. Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arviointi on kummassakin laissa säädetty Liikenne- ja viestintäviraston tehtäväksi. Näiden lakien nojalla toimivaltaiset viranomaiset voivat kuitenkin sopia tapauskohtaisesti tehtävistä toistensa lukuun ja tätä mahdollisuutta hyödynnetään jatkuvasti kulloinkin tarkoituksenmukaisella tavalla.

Tietoturvallisuuden vaatimustenmukaisuuden arvioinnin tarkoitus on tuottaa arvioinnin pyytäjälle objektiivista tietoa tietoturvallisuuden tilasta suhteessa käytettyyn arviointiperustaan. Arviointilain 4 §:n mukaan vaatimustenmukaisuuden arviointipyynnön Liikenne- ja viestintävirastolle voi tehdä vain viranomainen, jonka määräämisvallassa tai hankittavaksi suunniteltu tietojärjestelmä tai tietoliikennejärjestely on. Viranomaisen toimeksiannosta pyynnön voi tehdä myös se, joka tekee viranomaisen lukuun hankintoja tai tuottaa tietojenkäsittely- tai tietoliikennepalveluja tai hoitaa niiden järjestämiseen liittyviä palvelutehtäviä. Arviointipyynnön voi siis tehdä esimerkiksi yhteisiä palveluja tuottavat viranomaiset kuten Valtori, DVV tai toimialakohtaisia palveluita oikeusministeriön hallinnonalalle tuottava Oikeusrekisterikeskus sekä julkishallinnon yhteishankintayksikkö Hansel. Toisaalta esimerkiksi sidosyksikköasemassa olevat ICT-palveluyhtiöt eivät voi itse pyytää arviointia hyvinvointialueiden käyttöön tarkoitetulle palvelulle Liikenne- ja viestintävirastolta, mutta ne voivat pyytää arviointia hyväksytyltä arviointilaitokselta.

Arviointilain perusteella yritykset eivät voi esittää arviointipyyntöjä, joten pyyntöjä eivät voi tehdä esimerkiksi viranomaisille tietojärjestelmäpalveluita tarjoavat yritykset tai salaustuotteiden valmistajat. Kansainvälisissä

tietoturvallisuusvelvoitteissa EU-R- tai NR-tason tiedon sähköinen käsittely edellyttää aina järjestelmän akkreditointia. Yrityksellä ei välttämättä ole suomalaista viranomaiskumppania, vaan yritys voi saada mainitun turvallisuustason tietoja ulkomaiselta viranomaiselta tai yritykseltä. Näissä tilanteissa yritys voi kansainvälisistä tietoturvallisuusvelvoitteista annetun lain ja arviointilain valossa tehdä hyväksyntäpyynnön ja saada asian vireille Liikenne- ja viestintävirastossa. Korkeampien turvallisuusluokkien tietoja käsiteltäessä arviointi tehdään osana yritysturvallisuusselvitystä. Myös valmistajilta tulevien EU:n ja Naton turvallisuusluokitellun tiedon suojaamisessa käytettäväksi tarkoitettujen salaustuotteiden hyväksyntäpyyntöjä voidaan arvioida oikeudellisesti samalla tavalla. Sen sijaan kansallisen turvallisuusluokitellun tiedon suojaamisessa yritys ei voi saada lain perusteella asiaa käsittelyyn hallintoasiana. Liikenne- ja viestintävirasto tekee salaustuotearviointeja joko viranomaisen hakemuksesta tai virastosta säädetyn lain mukaisena julkisoikeudellisena sopimussuoritteena.

Arviointilaissa ei säädetä tarkemmin arviointia varten tarvittavista tiedoista. Laissa ei säädetä myöskään tarkemmin arvioinnin tai todistuksen hakemista varten tarvittavista tiedoista. Toisaalta viranomaisten välisten tai sisäisten arviointipyyntöjen sisältämistä tiedoista ei nähdä tarvetta säätää. Tulisi kuitenkin harkita sitä, että säädetäänkö salaustuotteen valmistajien tai TEMPEST-yritysten hakemukseen sisällytettävistä tiedoista.

Arviointilaitoslain 1 §:n mukaan lain tarkoitus on säätää *menettelystä, jonka avulla yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso*. Laissa ei kuitenkaan säädetä siitä, mitkä tahot arviointeja voivat hyväksytyiltä arviointilaitoksilta hankkia. Siten ei ole estettä sille, että viranomainen hankkii arvioinnin arviointilaitokselta.

Sote-alan säädöksiin on kirjattu lakisääteinen arviointivelvoite: hyväksytyltä arviointilaitokselta on hankittava arviointia koskeva todistus järjestelmien ja sovellusten luokittelun mukaisesti (THL määräys sosiaali- ja terveydenhuollon tietojärjestelmien ja hyvinvointisovellusten luokittelusta 4/2024). Arviointivelvollisuuden tarkoitus on suojata sote-palveluihin liittyviä asiakastietoja eli henkilötietoja. Sääntelyllä edellytetään suojaamiskyvystä kolmannen riippumattoman osapuolen todistusta, koska järjestelmiä ja sovelluksia tuottavien ja käyttävien organisaatioiden joukko voi olla laaja ja monimuotoinen. Asiakastietolaissa ja toisiolaissa säädetään myös todistuksen voimassaolosta, ylläpidosta ja peruuttamisesta.

Tarkempien turvallisuusratkaisujen, kuten salausratkaisujen ja hajasäteilysuojauksen arvioinnista ja hyväksynnästä ei ole säännöksiä. Nykyiset säännökset tukevat vain kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen liittyviä salaustuotteiden hyväksyntätehtäviä. Orpon hallituksen hallitusohjelmakirjauksen mukaan *salaustuotteiden hyväksyntäprosessia nopeutetaan, jotta kotimainen kyberteknologia saadaan nopeammin markkinoille. Suomi hankkii itselleen kansainvälisiä tietoturvahyväksyntöjä myöntävän maan aseman EU:ssa.*

Salaustuotteiden ja hajasäteilysuojausten arviointiin käytettävissä olevat viranomaisresurssit ovat niukat ja riittävän syvällistä osaamista on mahdollisesta rahoituksesta huolimatta saatavilla vähän. Tehokas osaamisresurssien käyttö ja päällekkäisen hyväksyntätoiminnan välttäminen sekä käytäntöjen yhtenäisyys valmistajien kannalta edellyttävät salaustuotteiden arviointi- ja hyväksyntätoiminnan kehittämistä viranomaisten yhteistyöhön perustuvalla mallilla. Tarkoituksenmukainen resurssointi ja viranomaistehtävien työnjako

näyttäisi edellyttävän tarkastelua koko valtionhallinnon tasolla ja mahdollisesti tehtävistä, yhteistyöstä ja kustannusten jakautumisesta säätämistä. Mittausten ja arvioinnin tarve on Nato-jäsenyyden myötä ruuhkautunut pahasti, mutta pitkällä tähtäimellä tarpeet ovat hallittavissa verraten vähäisellä henkilömäärällä.

Hyvinvointialueille, kunnille ja yrityksille, toisin kuin valtionhallinnon viranomaisille, ei ole yleisesti asetettu velvoitetta käyttää Liikenne- ja viestintäviraston hyväksymää tietoturvallisuuden arviointilaitosta, vaan ne voivat käyttää arvioinneissaan myös muita toimijoita. Luotettavan arvion saaminen tietoturvallisuustoimien tasosta saattaa kuitenkin olla yrityksille edellytyksenä tiettyihin hankkeisiin osallistumiselle. Tällöin kyseeseen voi tulla myös yritysturvallisuusselvityksen hakeminen suojelupoliisilta tai Pääesikunnalta, jolloin selvitetään laajemmin yrityksen kykyä käsitellä turvallisuusluokiteltua tietoa. Yritysturvallisuusselvitys voi sisältää myös yrityksen tietojärjestelmien tietoturvallisuuden tason selvittämisen. Arviointilaitoslaki ei koske niitä arviointitahoja, jotka eivät ole hakeneet Liikenne- ja viestintäviraston hyväksyntää. Arviointilaitostoiminnan kehittämisessä on hyvä ottaa huomioon myös yksityisen sektorin arviointitarpeet. Siten arvioidaan voitavan parantaa arviointipalvelujen saatavuutta myös julkiselle hallinnolle.

Yritykset eivät siis pääsääntöisesti voi itsenäisesti hankkia arviointilain tarkoittamaa tietoturvallisuuden vaatimuksenmukaisuuden arviointia Liikenne- ja viestintävirastolta. Arvioinnin hankkiminen on mahdollista, jos yritys toimii viranomaisen palveluntuottajaroolissa, arviointiin on turvallisuusselvityslaissa säädetty peruste tai yrityksellä on turvallisuusluokiteltuun sopimukseen perustuva tarve käsitellä kansainvälisen tietoturvallisuusvelvoitteen piiriin kuuluvaa tietoa. Palveluhankinnan osalta tilanne on ongelmallinen, koska viranomainen tekee palvelusopimuksen tietojärjestelmän toimittamisesta, jonka tietoturvallisuuden vaatimuksenmukaisuuden varmistaminen tapahtuu vasta sopimussuhteen perusteella. Etenkin räätälöitävien tai kokonaan uusien tietojärjestelmien hankinnassa saatetaan joutua tilanteeseen, jossa yritys on sitoutunut tietojärjestelmän toimittamiseen ja viranomaisen palvelu odottaa tätä tietojärjestelmää, mutta sen tietoturvallisuuden arvioinnissa havaitaankin merkittäviä puutteita.

Liikenne- ja viestintävirasto, Puolustusvoimat ja Valtori arviointien toteuttajina

Liikenne- ja viestintävirasto

Liikenne- ja viestintäviraston kyberturvallisuuskeskuksella on monipuolinen näkyvyys kansallisiin ja kansainvälisiin tietoturvallisuusvelvoitteisiin, turvallisuusluokitellun tiedon suojaamisen vaatimuksiin ja kyberturvallisuuden sääntelyyn ja uhkiin. Virasto on kerryttänyt osaamista tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden syvälliseen arviointiin ja teknisiin todentamismenetelmiin. Virastolla on kansainvälisten tehtävien takia osaamista salausratkaisuista, turvallisuuskriittisistä tuotteista ja hajasäteilystä. Virasto antaa erilaisiin tilanteisiin neuvontaa, jotta vältyttäisiin erityisesti arviointiprosessin alkuvaiheen ongelmilta eli esimerkiksi järjestelmäkuvaukset ja arvioinnin rajaukset tehtäisiin asianmukaisesti. Viranomaisyhteistyöllä ja tiedon jakamisella on pystytty vastaamaan arviointityön haasteisiin. Käytännön työn organisointi vaatii työpanosta sekä tarkastustyöhön osallistujilta että arvioinnin kohteelta ja sen palveluntuottajilta, jotta arviointi sujuu mahdollisimman hyvin.

Liikenne- ja viestintävirasto priorisoi arviointi-, todistus- ja selvityspyynnöt arviointilain 4 §:n 3 momentin mukaan käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattamisen sekä pyydettyjen toimenpiteiden merkityksen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen. Liikenne- ja viestintäviraston tietojärjestelmätarkastustoiminnan työmäärä on jatkanut kasvuaan. Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyvät tarpeet ovat lisääntyneet etenkin Nato-jäsenyyden myötä, mutta myös muiden tarpeiden vuoksi virasto priorisoi näitä pakollisiin akkreditointeihin liittyviä pyyntöjä. Liikenne- ja viestintävirasto priorisoi siis viranomaisten kansainvälisiin tietoturvallisuusvelvoitteisiin liittyviä pyyntöjä sekä myös kansallisen turvallisuusluokan I ja II tarpeisiin liittyviä pyyntöjä. Virasto ei juurikaan pysty resursoimaan kansallisen turvallisuusluokan III tai IV käsittelyn arviointiin.

Liikenne- ja viestintäviraston tehtävien priorisoinnin perusteilla on yhteys viranomaisten työnjakoon ja yhteistyöhön tietojärjestelmien tietoturvallisuuden ja sen osa-alueiden arvioinnissa. Kansainvälisten tietoturvallisuusvelvoitteiden viranomaistehtävissä kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 5 § mahdollistaa määrättyjen turvallisuusviranomaisten yhteistyön ja sopimisen tehtävän tai tehtäväkokonaisuuden hoitamisesta toisen turvallisuusviranomaisen lukuun, kun se on tarpeen tehtävien hoitamiseksi tarkoituksenmukaisesti taloudellisesti ja joutuisasti. Lain yhteistyö- ja delegointimahdollisuuksia on hyödynnetty aktiivisesti Puolustusvoimien operatiivisten järjestelmien Nato-hyväksynnöissä. Liikenne- ja viestintävirasto on suunnitellut Puolustusvoimien Naton turvallisuusluokitellun tiedon käsittelyyn tarvitsemien arviointien suoritusjärjestystä tiiviisti yhteistyössä Puolustusvoimien kanssa. Tarvetta olisi myös koko valtionhallinnon arviointitarpeiden tarkoituksenmukaisen järjestyksen koordinoinnille, jotta kaikki erityissuojattavaa tietoaineistoa käsittelevät viranomaiset saisivat vaikutusmahdollisuuden ja vastuuta Suomen kyvykkyydestä EU:n ja Naton turvallisuusluokitellun tiedon sähköisessä käsittelyssä. Priorisointiperusteiden tarkastelussa olisi huomioitava myös salaustuotteiden ja muiden turvallisuuskriittisten tuotteiden valmistajien arviointi- ja hyväksyntätarpeet. Ne liittyvät sekä viranomaisten turvallisuusluokitellun tiedon käsittelyn järjestelmätarpeisiin että yritysten kaupallisiin mahdollisuuksiin.

Liikenne- ja viestintäviraston tuotearvioinnit kohdistuvat salaustuotteisiin tai muihin turvallisuuskriittisiin tuotteisiin. Ne perustuvat Liikenne- ja viestintäviraston kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaiseen tehtävään toimia kansallisen turvallisuusviranomaisen asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. Salaustuotteilla varmistetaan tiedon luottamuksellisuus ja eheys erilaisilla salausmekanismeilla. Salaustuotteita ovat esimerkiksi VPN-tuotteet ja kiintolevyn tai massamuistin salausratkaisut. Salaustarpeet voivat liittyä esimerkiksi puheen ja tietoliikenteen salaamiseen langallisilla tai langattomilla yhteyksillä. Turvallisuuskriittiset tuotteet ovat muutoin tietojärjestelmien turvallisuuden kannalta keskeisiä komponentteja, kuten yhdyskäytävätuotteita tai tiedon tuhoamiseen käytettäviä ylikirjoitustuotteita.

Liikenne- ja viestintävirasto tekee tuotearviointeja ja -hyväksyntöjä EU:n ja Naton turvallisuusäännöissä ja käytännöissä määriteltyjen menettelyjen mukaisesti. Salaustuotteita arvioidaan turvallisuusluokitellun tiedon suojaamista varten. Eräissä tilanteissa kansallisella viranomaisella on toimivalta arvioida ja hyväksyä salausratkaisu ja eräissä tilanteissa hyväksyntä edellyttää lisäksi EU:n tai Naton turvallisuussääntöjen mukaisen toisen tahon arviointia (EU/488/2013 artikla 10 ja C-M (2002)49-REV1 liite F kohta 11). EU:n EU SEC-

RET- tai EU TOP SECRET -turvallisuusluokkien salaustuotteen hyväksyntä edellyttää jonkin EU:n niin sanotun AQUA-viranomaisen arviointia (SPE, second party evaluation). Myös tuotteen vieminen EU:n LACP-tuotelistalle edellyttää SPE-arviointia. Naton NATO SECRET- tai COSMIC TOP SECRET -turvallisuusluokan salaustuotteen hyväksyntä edellyttää Naton toimielimen SPE-arviointia. Kansallisen turvallisuusluokitellun tiedon suojaamisessa virasto tekee tuotearviointeja, joiden tarkoitus on tarjota tietoa viranomaisten riskiarvioon ja siten edistää mahdollisuutta hankkia tietojärjestelmiinsä riittävän turvallisia tuotteita.

Puolustusvoimat

Puolustusvoimien suuresta arviointitarpeesta huolimatta puolustushallintoon ei ole säädetty erikseen toimivaltaa arvioida ja hyväksyä tietojärjestelmiä ja salaustuotteita. Kansallisen turvallisuusluokitellun tiedon osalta arviointitoiminta perustuu tiedonhallintalaissa ja turvallisuusluokitteluasetuksessa säädettyihin tiedonhallintayksikön ja valtionhallinnon viranomaisen velvoitteisiin huolehtia tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta ja vaatimuksista. Lisäksi edellä mainitulla tavalla Nato-jäsenyyden ja lisääntyneen harjoitustoiminnan takia Liikenne- ja viestintäviraston kanssa on sovittu joidenkin arviointitehtävien siirtämisestä Puolustusvoimille kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 5 §:n perusteella. Liikenne- ja viestintäviraston kanssa on myös sovittu, että Puolustusvoimat hoitaa tiettyjä salausteknisen materiaalin jakeluun ja hallintaan liittyviä tehtäviä, joihin Puolustusvoimilla on toimivat menettelyt.

Puolustusvoimilla on oma toimintamallinsa ja kyvykkyydet tietojärjestelmien ja salaustuotteiden hyväksynnälle eri turvallisuusluokkiin. Tietojärjestelmien ja salaustuotteiden hyväksyntä turvallisuusluokkaan on Puolustusvoimissa eriytetty eri toimijalle kuin arviointien toteutus. Arviointi- ja hyväksymistoimintaa ei ole tällä hetkellä järjestetty riippumattomaksi ja itsenäiseksi toiminnoksi. Varsinaisen arviointi- ja hyväksymistoiminnan lisäksi Puolustusvoimien kybersietoisuuden ja tietoturvallisuuden varmistamisessa on tunnistettavissa ohjaus- ja valvontavastuita, elinjakson aikaista hallintaa sekä kehittämis- ja tutkimustyötä. Nämä tehtävät jakautuvat useille eri Puolustusvoimien toimijoille.

Puolustusvoimissa arviointi- ja hyväksymistoiminta sisältyy tietojärjestelmän elinkaaren aikaiseen kybersietoisuuden ylläpitoon ja arviointiin. Kybersietoisuus kuvaa joukon ja järjestelmän kykyä sietää kybertoimintaympäristön kautta tulevia uhkia. Sen tarkoituksena on tukea puolustusjärjestelmän operaatiovarmuuden takaamista suorituskykyjen suunnittelun, rakentamisen ja käytön aikana. Kybersietoisuus pitää sisällään tekniset tietoturvakontrollit ja ICT-varautumisen (muun muassa jatkuvuuden hallinnan ja toipumisen) sekä järjestelmän poikkeamien havainnoinnin ja niihin reagoinnin.

Puolustusvoimilla on myös pitkäaikainen kyvykkyys TEMPEST-mittauksiin. TEMPEST-mittauksia tehdään turvallisuusluokitellun tiedon sähköisen käsittelyn turvallisuuden varmistamiseksi mittaamalla sen hajasäteilyä. Puolustusvoimissa TEMPEST-mittauksia käytetään myös laajemmin osana tilaturvallisuutta ja tarkoitus on luoda kyvykkyydet liikkuvien kohteiden mittauksille materiaaliprojektien tukemiseksi. TEMPEST-mittauskyvykkyyttä on myös ulkoministeriöllä. Kansainvälisten tietoturvallisuusvelvoitteiden näkökulmasta Liikenne- ja viestintävirasto toimii Suomessa kansallisena TEMPEST-viranomaisena. Käytännössä siviili- ja puolustushallinnon organisaatioiden tarpeita ja vaatimusten soveltamista pyritään koordinoimaan tiiviissä yhteistyössä Puolustusvoimien, ulkoministeriön sekä Liikenne- ja viestintäviraston kesken. Kehittämistarpeita kansallisesti liittyy erityisesti laitemittauskyvykkyyksiin.

Valtion tieto- ja viestintätekniikkakeskus Valtori

Valtorin tuotteistettujen Tori- ja turvallisuusverkkolakien mukaisten palvelujen käyttöönotot toteutetaan määrämuotoisesti valtiovarainministeriön hallintamallien mukaisesti. Hallintamallien lisäksi Valtori ja valtiovarainministeriö ovat laatineet ja julkaisseet Tori- ja turvallisuusverkkolakien mukaisen toiminnan turvallisuuden hallintaan liittyviä ohjeita ja määräyksiä. Turvallisuusverkkoasetuksen perusteella turvallisuusverkon palvelun käyttöönotosta päättää valtiovarainministeriö ja turvallisuusverkkoon liitettävän tietojärjestelmän liittämisen hyväksyy turvallisuusverkon palvelujen tuottaja. Osana Tori- ja turvallisuusverkkolakien mukaisten palvelujen käyttöönottoa on palvelujen vaatimuksenmukaisuuden todentaminen. Todentaminen-käsite sisältää katselmoinnin, joka on Valtorin turvallisuusyksikön tietoturva-asiantuntijoiden suorittama; arvioinnin, joka on hyväksytyn arviointilaitoksen suorittama ja Katakri-viitekehyksen mukainen sekä tarkastuksen, joka on muun ulkoisen tahon suorittama ja valitulla viitekehyksellä toteutettu. Katselmoinnin suorittavat tietoturva-asiantuntijat ovat suorittaneet Katakri-pääauditoijakoulutuksen eivätkä osallistu kyseisen palvelun tietoturvallisuuden kehittämiseen.

Tori- ja turvallisuusverkkolakien mukaisten palvelujen toteuttamiseen ja arviointitoimintaan on rooleihin ja vastuisiin liittyviä erityiskysymyksiä. Valtori vastaa Tori- ja turvallisuusverkkolakien mukaisten palvelujen tietoturvallisuudesta ja varautumisesta. Lisäksi valtiovarainministeriö on antanut Valtoria turvallisuusverkon palvelujen tuottajana velvoittavia määräyksiä.

Valtori arvioi Torilain mukaisten palvelujen arviointitarpeita yhdessä palveluita käyttävien tiedonhallintayksiköiden kanssa ja tilaa sen perusteella arviointeja. Turvallisuusverkkolain mukaisessa toiminnassa lähtökohtana on aina ulkoisen arvioinnin toteuttaminen, joskin palveluja voidaan ottaa käyttöön määräajaksi myös Valtorin itsearvioinnin tai katselmoinnin perusteella. Todentamisen tuloksia käsitellään Tori- tai Tuve-hallintamallin mukaisissa ryhmissä ennen käyttöönottopäätöstä. Lisäksi todentamisraportit ovat palvelujen käyttäjien saatavilla tiedonhallintayksikön päätöksentekoa varten. Valtori tekee Torilain mukaisiin palveluihin käyttöönottopäätöksen ja valtiovarainministeriö tekee turvallisuusverkkolain mukaisten turvallisuusverkon palvelujen käyttöönottopäätökset. Molemmat päätökset edellyttävät, että vaatimuksenmukaisuus on todennettu ja todentamisesta on saatavilla raportit riskiarvioineen. Torilain mukaisten palvelujen käyttöönottopäätöksessä todetaan myös palvelussa käsiteltävien tietojen korkein mahdollinen turvallisuusluokka: julkinen, salassa pidettävä, turvallisuusluokiteltu. Turvallisuusverkkolain mukaisessa käyttöönottopäätöksessä todetaan minkä kriteeristön ja turvallisuusluokan vaatimusten mukaisesti vaatimuksenmukaisuuden todentaminen on tehty. Jokainen kutakin yhteistä palvelua käyttävä tiedonhallintayksikkö vastaa palvelun käyttöönottoon liittyvästä riskipäätöksestä.

Turvallisuusverkkoasetuksen 10 §:n mukaisesti turvallisuusverkon palvelujen tuottajien eli Valtorin ja Suomen Erillisverkot Oy:n on *arvioitava ja todettava turvallisuusverkon palvelujen tietoturvallisuus- ja varautumisvaatimusten täyttyminen noudattaen* arviointilakia ja kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia. Valtiovarainministeriö on antanut turvallisuusverkkolain 14.4 §:n toimivallalla turvallisuusverkon palvelujen tuottajille määräyksen, jonka mukaisesti turvallisuusverkon palvelujen ja turvallisuusverkkoon liitettävien tietojärjestelmien vaatimuksenmukaisuuden arviointi tulee tehdä ennen palvelujen käyttöönottoa tai tietojärjestelmän liittämistä turvallisuusverkkoon. Turvallisuusverkkolain perusteella annettava määräys

on turvallisuusverkon palvelujen tuottajaa velvoittava. Kunkin tiedonhallintayksikön erikseen toteuttama turvallisuusverkkolain mukaisten palvelujen ja tuotteiden arviointi sekä käyttöönotto olisi yhteistyötä tehottomampaa.

Valtori on kehittänyt todentamisprosessiaan vuoden 2024 aikana. Käynnistyvä tarkastustoiminne on täydentänyt olemassa olevaa vaatimuksenmukaisuuden todentamisprosessia siten, että se tekee kohteena olevaan palveluun teknisen tarkastuksen arviointilaitoksen tapaan. Toiminta on käynnistetty tarkastustoimintana, koska se ei ole arviointilain tarkoittamaa arviointitoimintaa. Valtorin asiakkaiden eli tiedonhallintayksiköiden näkökulmasta on tärkeää, että vaatimuksenmukaisuuden todentaminen tapahtuu edelleen riippumattomasti ja objektiivisesti. Oman tarkastusyksikön perustamisella Valtorin järjestelmien arviointiin tavoitellaan ennakoitavuutta, joustavuutta ja sujuvuutta. Myös menosäästöjen arvioidaan olevan mittavat. Valtorissa tehdyn laskelman mukaan kahden henkilön rekrytoiminen tekemään tietojärjestelmien tarkastustoimintaa säästää vuositasolla noin 458 000 euroa verrattuna siihen, että palvelut ostettaisiin ulkopuolisilta arviointilaitoksilta. Tämä laskelma ei sisällä mahdollisia Valtorille ja sen asiakkaille tulevia säästöjä siitä, kun arviointitoimintaa saadaan joustavammaksi ja ennakoitavammaksi, ja kun riippuvuus ulkopuolisiin arviointilaitoksiin vähenee sekä tietojärjestelmiä saadaan helpommin ja nopeammin käyttöön.

Valtiovarainministeriö tulee osaltaan arvioimaan osana Tori- ja turvallisuusverkkolakien mukaisen toiminnan kehittämistä, onko turvallisuusverkon palvelujen arviointi ulkoisen arviointilaitoksen toimesta välttämätöntä vai olisi se jatkossa mahdollista toteuttaa esimerkiksi Valtorin ja Suomen Erillisverkot Oy:n yhteisenä tarkastustoimintana. Pohdittavaksi tulee jatkossa myös millä todentamismenettelyllä käyttäjät voivat liittää omia tietojärjestelmiään turvallisuusverkkoon.

Tori- ja turvallisuusverkkolakien tarkoittamien yhteisten tieto- ja viestintäteknisten palvelujen vaatimuksenmukaisuuden ja turvallisuuden arvioinnin ohjauksen näkökulmasta todentamismenettelyn puutteena on, että valtiovarainministeriön tai palvelutuottajan käyttöönottopäätös ei ole samalla tiedonhallintayksikön käyttöönotto- ja käyttöpäätös. Käyttöönotto- ja käyttöpäätöstä tehtäessä huomioon otettavia näkökulmia ovat palvelujen käyttäjien näkemykset ja käyttövelvoitteen vaikutus. Haasteena on, että osa palvelujen käyttäjistä kokee arviointiprosessin liian hitaaksi ja jäykäksi, koska heillä ei ole varsinaisia tiedonhallinnallisia vaatimuksia tietojärjestelmille. Näin ollen riskiperusteisesti näille tiedonhallintayksiköille tulisi harkita palvelukohtaisesti mahdollisuutta käyttöönottoon ja käyttöön tiedonhallintalain mukaiseen tiedonhallintayksikön riskiarvioon perustuen ilman vaatimustenmukaisuuden todentamista.

Tiedonhallintalaissa ei ole säädetty tiedonhallintayksiköiden yhteistoiminnasta tai tiedonvaihdosta arviointeja koskien. Tiedonhallintayksiköiden yhteisen ja yhtenäisen kannan muodostumista jäännösriskeistä ja sen mukaista päätöksentekoa ei ole kaikissa tilanteissa edistetty määrätietoisesti. Tämä menettely olisi kutienkin tehostanut yhteisten tieto- ja viestintäteknisten palvelujen arviointien hyödyntämistä ja palvelujen käyttöönottoa.

VALTIONEUVOSTO
STATSRÅDET

Arviointitehtävä julkisessa hallinnossa

Arviointi- ja hyväksyntäviranomaisen tai muun julkisessa hallinnossa toimivan organisaation henkilöstöllä tulee olla riittävä osaaminen, koulutus ja kokemus. Hyväksynnän antajan tulee pystyä ymmärtämään ja itsenäisesti arvioimaan tehtyjen arviointien ja tarkastusten kattavuus ja riittävyys. Kaikkiin arviointia julkisessa hallinnossa hoitaviin toimijoihin tulisi soveltaa yhtäläisiä, arviointitehtävän pätevyysalueista riippuvia osaamisvaatimuksia. Viranomaisella on hallintolain 8 §:n mukaan neuvontavelvollisuus. Viranomainen noudattaa toiminnassaan hallintolakia, julkisuuslakia ja muita hallinnon yleislakeja ja viranomaisessa työskentelevä henkilöstö hoitaa tehtäviä virkavastuulla.

Arviointia tehtävänä Liikenne- ja viestintävirastossa, Puolustusvoimissa ja Valtorissa arvioitaessa on huomioitava, että Naton ja EU:n turvallisuussäännöt mahdollistavat useamman SAA-viranomaisen perustamisen. Naton turvallisuussäännöt edellyttävät SAA-viranomaisen tehtävien ja vastuiden erottamista järjestelmän vastuuviranomaisen tehtävistä. Riippumattomuuden voidaan katsoa myös tarkoittavan sitä, että arviointitoiminta on riippumaton tietoteknisten palvelujen tuottamisesta, suunnittelusta, rakentamisesta, ylläpidosta ja tähän liittyvästä ohjauksesta ja valvonnasta. Kansainvälisten kumppanien on voitava luottaa siihen, että Suomi suojaa kumppaniensa turvallisuusluokiteltuja tietoja kansainvälisten tietoturvallisuusvelvoitteidensa mukaisesti.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan NSA ohjaa ja valvoo, että erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti. Lain 5 §:n yhteistoimintavelvoite korostaa turvallisuusviranomaisten tiedonvaihtoa ja yhteistyötä tietoturvallisuusvelvoitteiden asianmukaiseksi hoitamiseksi. EU ja Nato tekevät osaltaan tarkastuksia tietojensa käsittelystä tietyissä rajoissa. GSA-sopimuskumppaneilla on yleensä valtiosopimusten perusteella tietyissä rajoissa oikeus tarkastusvierailuihin Suomessa.

Mahdollinen arviointielimen tyyppi voisi nykyisin olla julkisen hallinnon toimijan sisäinen pätevä ja riippumaton tarkastusyksikkö muutoin kuin arviointilaitoslain nojalla. Tällöin haasteena on se, miten voidaan varmistaa riittävä pätevyys suorittaa arviointia ja arvioinnin tasalaatuisuus. Tämä on merkittävää toimijoiden välisen tiedonvaihdon vuoksi. Henkilötietojen, salassa pidettävien tietojen ja turvallisuusluokiteltujen tietojen vaihdon johdosta vaatimustenmukaisuuden arviointia ei pitäisi katsoa vain arviointitoimijoiden sisäisenä asiana. Toimijoilla on mahdollisesti erilaisia perusteita jäännösriskien hyväksymisessä. Lainsäädännön tulisi tukea toimijoiden keskinäistä luottamusta tietojen turvallisesta käsittelystä.

Arviointilaitoslain mukaiseksi arviointilaitokseksi voisi lain perustelujen valossa hakeutua muukin organisaatio kuin yritys. Jos jonkin julkisen hallinnon organisaation – kuten Valtorin – yksikkö hakisi arviointilaitoksen akkreditointia ja hyväksyntää, yksikön riippumattomuus tulisi arvioitavaksi osana FINASin akkreditointia. Tällaisessa tilanteessa voisi olla tarpeellista selkeyttää arviointiyksikön riippumattomuutta ja tehtäviä kyseistä toimijaa koskevassa sääntelyssä.

Arviointilaissa ei ole säädetty mahdollisuudesta käyttää julkisen hallinnon toimijoiden toteuttamissa vaatimustenmukaisuuden arvioinneissa alihankintaa, yksityisiä resursseja tai henkilöitä arviointien tukena. Julkisen hallinnon toimijoiden toteuttamissa arvioinneissa olisi tarve laajentaa resurssien käyttöä yksityisiltä

markkinoilta hankittuun henkilötyövoimaan, jota koskisivat samat pätevyysvaatimukset kuin viranomaisten henkilöstöäkin. Siten saataisiin Suomen osaamispotentiaali hyödynnettyä täysimääräisesti ja joustavasti ilman, että nämä henkilöresurssit olisivat virkasuhteessa arviointitoimijassa. Yksityisten henkilöresurssien hyödyntäminen on tarpeen järjestää siten, että vastuut ja toimeksiannon sisältö ovat selviä sekä arvioinnissa saatujen tietojen suojaamisesta varmistutaan. Markkinoilta hankittu arvioija voisi suorittaa arvioinnin ja laatia raportin asiakkaan ja arviointitoimijan tiloissa sekä näiden työvälineillä, jolloin varmistettaisiin, että tiedot eivät kasaudu arvioinnin kohdeorganisaation tai arviointitoimijan ulkopuolelle. Tämä toimintamalli mahdollistaisi sen, että arviointihenkilön työnantajan järjestelmiä, laitteita ja tiloja ei tarvitsisi tarkastaa. Arviointitehtävä voitaisiin harkita rajatusti tietyin edellytyksin annettavaksi myös muulle kuin viranomaiselle. Mikäli julkisena hallintotehtävänä hoidettavassa arvioinnissa halutaan luoda mahdollisuus hyödyntää muita kuin viranomaisia, tulee tehtävän hoitamisesta säätää lailla tai antaa valtuutussäännöksellä viranomaiselle oikeus siirtää julkisen hallintotehtävän hoitaminen sopimusperusteisesti.

Hyväksytyt arviointilaitokset

Arviointilaitoksilla on merkittävä rooli tietoturvallisuuden arviointipalvelujen tuottajina. Arviointilaitoslailla on pyritty edistämään viranomaisten ja yritysten tietoturvallisuutta luomalla valvonta viranomaisten ja yritysten tietoturvallisuutta arvioiville laitoksille. Lain tarkoituksena on antaa arviointilaitoksina toimiville yrityksille mahdollisuus osoittaa toimintansa tietoturvallisuuden taso ulkopuolisen ja luotettavan arvioinnin avulla. Arviointilaitokseksi voi hakeutua myös sellainen arviointilaitos, jonka asiakaskunta koostuu ensisijaisesti viranomaisista ja muista julkisen hallinnon toimijoista. Keskeisiin EU-säädöksiin liittyvien toimijoiden ja arviointielinten suhdetta kansallisen arviointilaitoslain mukaisiin hyväksyttyihin tietoturvallisuuden arviointilaitoksiin on käsitelty luvussa "Sovellettavasta EU:n sertifiointisääntelystä".

Hyväksymisprosessi

Arviointilaitoslaissa ei ole rajattu sitä, minkälaiset toimintayksiköt voivat toimia laissa tarkoitettuina arviointilaitoksina. Arviointilaitokseksi voi hakeutua yksityinen elinkeinonharjoittaja sekä organisaatiomuodosta riippumatta myös muu sellainen toimintayksikkö, joka tarjoaa arviointipalveluja julkiselle hallinnolle. Arviointilaitoslain 5 §:n mukaan toimintayksikön riippumattomuus olisi arvioitava FINASin akkreditoinnissa.

Hyväksytyn arviointilaitoksen toiminta on julkinen hallintotehtävä ja laitosten vastuuhenkilöiden luotettavuus selvitetään ennen hyväksyntää. Säännöksessä ei kuitenkaan huomioida työntekijöiden luotettavuutta.

Arviointilaitoslain 3 §:n mukaan arviointilaitos voi hakea Liikenne- ja viestintäviraston hyväksyntää. Arviointilaitoslain 5 §:n 1 momentin 1–3 kohtien mukaan *tietoturvallisuuden arviointilaitoksen hyväksymisen edellytyksenä on* muun ohessa, *että: 1) laitos on toiminnallisesti ja taloudellisesti riippumaton arvioinnin kohteesta; 2) laitoksen henkilökunnalla on hyvä tekninen ja ammatillinen koulutus sekä riittävän laaja-alainen kokemus toimintaan kuuluvissa tehtävissä; 3) laitoksella on toiminnan edellyttämät laitteet, välineet ja järjestelmät*. Laissa säädetään vain yksi mahdollinen menettely näiden riippumattomuus- ja pätevyysvaatimusten hyväksymiselle. Lain 5 §:n 2 momentin nojalla kyseisten vaatimusten täyttäminen on osoitettava

FINASin akkreditoinnilla. Liikenne- ja viestintäviraston hyväksyntäpäätös perustuu näiltä osin akkreditointitodistukseen.

Arviointilaitoslain 5 §:n 1 momentin 2 kohta edellyttää, että henkilökunnalla on hyvä tekninen ja ammatillinen koulutus ja 3 kohta, että laitoksella on toiminnan edellyttämät laitteet, välineet ja järjestelmät. Arviointilaitoslain 5 §:n 1 momentin 4 kohdan mukaan arviointilaitoksen hyväksynnän edellytyksenä on, että vastuuhenkilöiden luotettavuus ja tietojenkäsittelyn ja toimitilojen turvallisuus on selvitetty (*laitoksen vastuuhenkilöiden luotettavuus on varmistettu ja laitoksella on luotettavaksi arvioitu ja valvottu menetelmä, jonka avulla laitoksen toimitilojen ja tietojenkäsittelyn turvallisuus varmistetaan;*) Tietojenkäsittelyn ja toimitilojen turvallisuuden Liikenne- ja viestintävirasto selvittää tarkastuksella. Lisäksi virasto tarkistaa 5 §:n 1 momentin 5 kohdassa edellytetyt ohjeet laitoksen toimintaa ja sen seurantaa varten.

Arviomuistiossa Julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista (VM 2021:54) kohdassa 9.2.3 Arviointilaitosten hyväksyminen, hyväksyjä ja valvonta s. 103–104 todetaan seuraavaa: *Arviointilaitoslaissa säädetyt edellytykset arviointilaitoksen hyväksymiselle ovat hyvin yleisluontoiset. Tämä on johtanut siihen, että hyväksyntä perustuu suurelta osin Liikenne- ja viestintäviraston antamaan ohjeeseen tietoturvallisuuden arviointilaitoksille (Ohje 210/2016 O)* [Ohje päivitetty, ajantasainen versio 210/2022 O] *– eli ei sitovaan normistoon. Hyväksymisen edellytykset on koettu jossain määrin tulkinnanvaraisiksi. Lisäksi turvallisuusluokitellun tiedon käsittelyn tietoturvallisuuden arviointilaitoksen pätevyyttä hakeneilla ei välttämättä ole prosessin alkuvaiheessa ollut riittävää ymmärrystä edellytettävästä osaamisesta ja tällaisen osaamisen hankkiminen (henkilöstö, laitteistot, ohjelmistot) on osoittautunut aikaa vieväksi. Nämä syyt ovat osaltaan johtaneet myös siihen, että arviointilaitoksen hyväksyntäprosessit ovat olleet pitkiä eikä uusia arviointilaitoksia ole tullut markkinoille. – – Arviointilaitosten hyväksymistä koskevat vaatimukset on arviointilaitoslaissa säädetty yleisellä tasolla siten, ettei niiden perusteella voida muodostaa selkeää kokonaiskäsitystä siitä, mitkä ovat konkreettisia vaatimuksia arviointilaitoksille. Tältä osin sääntelyä voidaan pitää epätäsmällisenä, tulkinnanvaraisena ja puutteellisena. Sääntely jättää harkintavaltaa arviointilaitoksen hyväksyvälle viranomaiselle, jolloin tällaisten vaatimusten täyttämistä koskevat soveltamisohjeet voivat sisältää konkreettisia vaatimuksia, joiden tulisi olla lakitasoisia.* Tärkeää on kuitenkin valita tarkoituksenmukaisen sääntelyn taso ja huomioitava riittävä joustavuus arviointilaitoksille asetetuissa vaatimuksissa ja niiden hyväksymisessä.

Pätevyysalueet

Vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta annetun lain (920/2005) 7 §:n 3 momentin mukaan *akkreditointipäätöksessä määritellään arviointielimen akkreditoitu pätevyysalue ja vahvistetaan menettelytavat, joilla pätevyyttä pidetään yllä ja seurataan. Päätös voidaan antaa määräajaksi.* Jokainen arviointilaitoksen pätevyysalue edellyttää siten omaa arviointilaitoslain 5 §:n mukaista FINASin akkreditointia. Lain 8 §:n 1 momentin mukaan *akkreditointiyksikkö seuraa akkreditoimiensa arviointielinten pätevyyttä 7 §:n 3 momentissa tarkoitetussa päätöksessä vahvistamallaan tavalla*. Edelleen lain 9 §:ssä säädetään akkreditoinnin peruuttamisesta. Käytännössä FINAS seuraa pätevyyttä pääsääntöisesti kerran vuodessa tehtävillä määräaikaisarvioinneilla, jotka kohdistetaan eri kerroilla toiminnan eri osa-alueisiin. Itse akkreditointi tulee uusia neljän vuoden välein.

Kaikilla hyväksytyillä arviointilaitoksilla on arviointilaitoslain vakiintuneen soveltamiskäytännön mukaisesti peruspätevyytenä FINASin akkreditoima ja Liikenne- ja viestintäviraston hyväksymä pätevyys tehdä tietoturvallisuuden johtamisjärjestelmän ISO/IEC 27001 -standardin mukaisia sertifiointeja. Pääsääntöisesti näitä sertifiointeja tehdään kuitenkin käytännössä toimeksiannoissa muussa kuin hyväksytyn arviointilaitoksen roolissa ja vastuulla ja arviointilaitoslain valvonnan piirissä. Jos arviointilaitos tekisi toimeksiannosta ISO/IEC 27001 -standardiin perustuvia arviointeja ja sertifiointeja nimenomaisesti arviointilaitoslaissa säädetyssä julkisen hallintotehtävän roolissa, sertifioinnin myöntämisessä ja ylläpidossa tulisi tällöinkin noudattaa myös standardin vaatimuksia. Arviointilaitosrooli edellyttää arviointikohteen suojattavien tietojen käsittelyä asianmukaisesti suojatussa tietojenkäsittely-ympäristössä. Arviointilaitoksena toimimisen hyöty ISO27001-arvioinneissa on se, että asiakas saa luotettavan suojan tietojensa käsittelylle arviointilaitoksella. Muutoin kuin arviointilaitoksena toimittaessa tietojen suojaamisen käytännöt ovat sopimuksen varassa.

Suomen arviointiliiketoimintamarkkinat ovat pienet. Nykyisellään Liikenne- ja viestintäviraston hyväksynnän toimia tietoturvallisuuden arviointilaitoksena on saanut yhteensä neljä yritystä. Näistä kahdella on pätevyys tasoille TL IV KÄYTTÖ RAJOITETTU ja TL III LUOTTAMUKSELLINEN turvallisuusluokitellun tiedon käsittelyn arviointiin Katakrin mukaisesti. Viimeisimmät hyväksynnät arviointilaitoksiksi on tehty 7.11.2023 ja 10.3.2017 sekä aikaisemmin hyväksytyille arviointilaitoksille päätökset täydennetyiksi pätevyysalueiksi 27.6.2022 ja 8.7.2021. Arviointilaitokseksi pääsy on koettu hankalaksi. Toimijoilla on ollut vaikeuksia hakea arviointilaitoksen asemaa sujuvasti eli ilman merkittäviä viivästyksiä. Joiltakin osin arviointitoimijoiden laadussa on ollut haasteita.

Tietoturvallisuuden arviointilaitoksen pätevyyden akkreditointiin sisältyy yleensä näyttöarviointi, jonka avulla FINASin käyttämä asiantuntija arvioi arviointilaitoksen arviointipätevyyden riittävyyttä. Käytännössä on välttämätöntä, että pätevyysalueen arviointiperustasta on olemassa konkreettiset työohjeet ja ennalta määritelty perusteiden soveltamistapa, jotta arviointitoiminta on tasapuolista ja tasalaatuista. Julkri-kriteeristön osalta on haasteena ollut se, mikä taho määrittelisi kriteerien mukaisen riittävän käytännön ja sen, millaisilla menetelmillä arvioijan tulisi todentaa kriteerien toteutuminen. Tämän tahon edustajan tulisi myös pystyä toimimaan FINASin asiantuntijana, jos jokin yritys haluaisi hakea arviointilaitoslain mukaisesti hyväksytyn arviointilaitoksen pätevyyttä kriteeristöön. Yleisemminkin kriteeristöjen käyttöönottoa voisi helpottaa laatimalla kriteeristössä soveltamisesimerkkejä ja -kuvauksia ja määrittelemällä kriteeristössä edellytettävät todentamismenetelmät. Edellä kuvatuista syistä Julkria ei ole toimeenpantu arviointilaitosten pätevöitymisalueeksi, vaikka se täyttää kriteeristönä arviointilaitoslain 10 §:n edellytykset. Kriteeristöjen antamisen, ylläpidon ja soveltamistuen sääntelyä tulisi tarkastella ja arviointilaitosten pätevyysalueiden hyväksyntämenettelyjä arviointilaitoslaissa joustavoittaa. Näin parannettaisiin mahdollisuuksia saada käyttöön nykyistä laajemmin erilaisia kriteeristöjä arviointilaitosten pätevyysalueina.

Hyväksytyt arviointilaitokset sote-alan arvioinneissa

Arviointilaitoslakia säädettäessä ei ole ennakoitu, että jatkossa myös muualla lainsäädännössä eri viranomaisille tulisi tehtäviä arviointilaitosten hyväksyntään, ohjaukseen ja valvontaan liittyen. Asiakastietolain 3 §:n 24 kohdan mukaan *tietoturvallisuuden arviointilaitoksella tarkoitetaan tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitettua yritystä, yhteisöä tai viranomaista, jonka Liikenne- ja*

viestintävirasto on hyväksynyt. Toisiolain 3 §:n 20 kohdan mukaan *tietoturvallisuuden arviointilaitoksella tarkoitetaan sellaista yritystä, yhteisöä ja viranomaista, jonka Liikenne- ja viestintävirasto on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella arvioimaan sitä, täyttääkö tietojärjestelmä tietoturvallisuutta koskevat vaatimukset.*

Asiakastietolain säännöskohtaisten perustelujen mukaan (HE 246/2022 vp, s. 64) *arviointilaitoksella tulisi lisäksi olla hyvä asiantuntemus sosiaali- ja terveydenhuollon tietojärjestelmiä koskevista vaatimuksista, joista säädetään asiakastietolain 84 §:ssä ja sen nojalla. Tietoturvallisuuden arviointilaitoksen tehtävänä on tarkastaa, täyttääkö Kansaneläkelaitoksen ylläpitämiin valtakunnallisten tietojärjestelmäpalvelujen ja niihin välittömästi liitettäväksi suunniteltu tietojärjestelmä tietoturvaa ja siihen sisältyvää tietosuojaa koskevat olennaiset vaatimukset. Tietoturvallisuuden arviointilaitokseksi hakeudutaan erikseen. Arviointilaitoksen tulee täyttää tietoturvallisuuden arviointilaitoksista annetun lain 5 §:n ja asiakastietolain mukaiset vaatimukset.* Toisiolain yksityiskohtaisten perustelujen mukaan (HE 159/2017 vp, s. 95) *arviointilaitoksella tulisi lisäksi olla hyvä asiantuntemus toisiolain mukaisista tietoturvallista käyttöympäristöä koskevista tietoturvaedellytyksistä, joista säädetään lain 3 luvussa. Tietoturvallisuuden arviointilaitoksen tehtävänä on tarkastaa, täyttyvätkö tietoturvaa ja tietosuojaa koskevat vaatimukset toisiolain 20 §:n mukaisissa käyttöympäristöissä.*

Vaikka asiakastietolaissa ja toisiolaissa on asetettu lisävaatimuksia näiden lakien mukaisia arviointeja tekevälle arviointilaitokselle, ei kyseisissä laissa ole säädetty minkä viranomaisen tehtävänä on arvioida, että arviointilaitos täyttää vaatimukset ja voi tulla hyväksytyksi tekemään lakien mukaisia arviointitehtäviä. Arviointilaitoslain mukaiset tietoturvallisuuden arviointilaitosten hyväksyntä- ja valvontatehtävät kuuluvat Liikenne- ja viestintävirastolle. Lain tarkoituksena on ollut saattaa laitosten toiminta kokonaisuutena valvonnan piiriin. Asiakastietolain ja toisiolain toimeenpanon aikatauluun liittyvistä välttämättömyyssyistä Liikenne- ja viestintävirasto on todennut, että asiakastietolain ja toisiolain mukaisia arviointeja voivat tehdä sellaiset hyväksynnän saaneet tietoturvallisuuden arviointilaitokset, joiden pätevyysalueena on VAHTI tai Katakri. Näitä arviointilaitoksia on tällä hetkellä kaksi.

Hyvinvointialueiden näkökulmasta arviointilaitosten käyttö sotearvioinneissa vaatii sekä aikaa että resursseja niin järjestelmätoimittajan, pyytäjän kuin arviointitoimijankin puolelta. Hyvinvointialueet toimivat asiakas- ja potilastietojärjestelmien osalta siten, että arvioinnin tilaa tietojärjestelmätoimittaja ja sote-palvelujen järjestäjänä ja rekisterinpitäjänä hyvinvointialueilla on velvoite huolehtia järjestelmiensä lainmukaisuudesta. Haasteena nähdään, että ydintoiminnot, joita varten järjestelmiä hankitaan, eivät ole tietoisia kaikista laeista tai asetuksista, joita tulee noudattaa ja siten järjestelmän lainmukaisuuden valvonta on haasteellista alueilla. Rekisterinpitäjät tukeutuvat siis siihen, että käyttöön hankittu järjestelmä on käynyt läpi yhteistestauksen ja se on arvioitu arviointilaitoksen toimesta. Käytännössä kuitenkin osa käytössä olevista tietojärjestelmien versioista on vanhentuneita suhteessa vaatimuksiin.

Arviointilaitosten tekemät arvioinnit asiakastietolain näkökulmasta ovat kalliita, ja tämä vähentää toimittajien halua toteuttaa arviointeja sekä nostaa tietojärjestelmän arvioinnin pyytäjän kustannuksia välillisesti. On tärkeää, että lainsäädännön velvoittamiin vaatimustenmukaisuuden arviointeihin on käytettävissä oikea-aikai-

sesti ja ennen kaikkea kustannustehokkaasti riittävän laadukkaita arviointitoimijoita. Hyvinvointialueilla toteutetaan jonkin verran myös muuta tietoturvallisuuteen liittyvää arviointia erityisesti omien järjestelmäympäristöjen riskien kartoittamiseksi.

Hyväksyttyjen arviointilaitosten toteuttamat asiakastietolain ja toisiolain mukaiset tietojärjestelmissä ja lääkinnällisissä laitteissa tapahtuvan asiakastietojen käsittelyn tietoturvallisuuden arvioinnit liittyvät yhä enenevässä määrin tuotteiden tuotesertifiointeihin. Asiakastietolaissa on säädetty arviointilakeihin nojautuvasta tuotesertifioinnista. Sote-palvelujen tuotetasoisella riskiluokittelulla ja vaatimustenmukaisuuden arvioinnilla on pyritty välttämään samojen tietojärjestelmien toistuvaa arviointia ja korjausten tekemistä useissa eri käyttöympäristöissä. Tuotetasoisten arviointien on nähty alentavan kustannuksia verrattuna organisaatiokohtaisesti toteutettuihin tietojärjestelmien vaatimustenmukaisuuden arviointeihin, Sote-toimiala on esimerkki toimialasta, jossa toimivien tuotteiden kilpailu on selvästi entistä enemmän laajenemassa myös EU-tasoiseksi.

Todistus hyväksytystä vaatimustenmukaisuuden arvioinnista

Arviointilain 4 §:n mukaan Liikenne- ja viestintävirasto voi tehdä pyynnöstä tietojärjestelmän tai tietoliikennejärjestelyjen arvioinnin tietyillä arviointiperusteilla tai antaa pyynnöstä lain 8 §:n mukaisen todistuksen, jos arviointiperusteena olevat vaatimukset täyttyvät. Pelkästä arvioinnista syntyy pyytävälle viranomaiselle käytännössä arviointiraportti järjestelmän tietoturvallisuuden tilasta ja kohteena voi olla suppeakin joukko kriteerejä. Raportissa voidaan todeta lieviä tai vakaviakin poikkeamia.

Virasto hyödyntää arvioinneissa vakiintuneesti Katakria, jossa on hyvä valikoima tietoturvallisuuskriteerejä ja vakiintuneita toteutusesimerkkejä. Katakri on kansainvälisistä tietoturvavelvoitteista annettua lakia täsmentävä ja siinä on huomioitu muun muassa EU:n ja Naton Suomea sitovat tietoturvallisuusvaatimukset. Sitä voidaan käyttää työkaluna kansainvälisissä arvioinneissa ja turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen tai vastaavien suojattavien kohteiden arvioinneissa.

Arviointien tekijöiden ja pyytäjien näkökulmasta yksinomaan Katakri ei ole teknisten yksityiskohtien kannalta riittävä kriteeristö, ja Katakrissa viitataankin myös muihin ohjeisiin ja standardeihin. Arvioinneissa käytettävä osaaminen ja tietotaito perustuu yleisiin tietoturvallisuuden hyviin käytäntöihin ja niiden kehityksen seuraamiseen. Lisäksi huomioidaan kyberturvallisuusuhkien kehittyminen. Kaikkia teknisten osa-alueiden standardeja ei kannata yrittää ylläpitää yhdessä kriteeristössä. Katakri ei sovellu sellaisenaan pilviteknologioiden arviointiin. Liikenne- ja viestintävirasto ja Katakria soveltavat arviointilaitokset hyödyntävät Katakria täydentämään esimerkiksi sovellusturvallisuuden OWASP-viitekehyksiä, joihin myös viitataan Katakrissa (katso Katakrin kohta I-13).

Arviointilain 8 §:n mukaisen todistuksen Liikenne- ja viestintävirasto voi antaa pyynnöstä vain, jos vaatimukset täyttyvät: *todistukseen merkitään käytetyt arviointiperusteet sekä tiedot arvioinnin laajuudesta sekä tarvittaessa todistuksen voimassaoloajasta. Todistus voidaan antaa määräajaksi, jos siihen on erityinen syy.* Todistukseen liittyy myös laissa säädetty seuranta, joka perustuu lain 9 §:n mukaisesti todistuksen saajan

sitoumukseen tietoturvallisuustason säilyttämisestä ja velvollisuuteen ilmoittaa Liikenne- ja viestintävirastolle muutoksista, joilla on vaikutusta tietoturvallisuustasoon. Arviointilain 10 §:ssä säädetään todistuksen peruuttamisesta.

Varsinaiset arviointilain mukaan annetut todistukset ovat verraten harvinaisia. Tavallisemmin Liikenne- ja viestintävirasto on laatinut arviointiraportin, selvityksen Suojelupoliisille tai Pääesikunnalle osana yritysturvallisuusselvitystä tai hyväksyntälausunnon kansainvälisen tietoturvallisuusvelvoitteen mukaisesti. Arviointilaissa todistuksen hankkimista ei edellytetä, vaan viime kädessä vastuu tietojärjestelmien riittävästä suojaamisesta, riskienhallinnasta ja käyttöönottopäätöksistä on kullakin tiedonhallintayksiköllä. Arviointien pyytäjät ovat kokeneet mahdollisuutensa päättää jäännösriskien hyväksynnästä epäselväksi.

Arviointilaitoslain 9 §:n 3 momentin mukaan *hyväksytty tietoturvallisuuden arviointilaitos antaa selvitysten ja tarkastuksen perusteella todistuksen, jos arvioitavan kohteen toimitilat ja toiminta on selvityksen perustana olleiden arviointiperusteiden mukainen*. *Todistuksessa tulee yksilöidä arvioinnissa käytetyt tietoturvallisuuden arviointiperusteet ja arvioinnin laajuus.* Todistuksen ylläpidosta tai peruuttamisesta ei säädetä. Arviointilaitoslaissa ei säädetä myöskään arviointilaitoksen arviointiraportin antamisesta siinä tapauksessa, että kaikki vaatimukset eivät täyty tai toimeksiantaja tarvitsee vain arvioinnin ilman todistusta. Nimenomaisen sääntelyn puuttumisen ei ole soveltamiskäytännössä katsottu estävän arviointilaitoksia antamasta pelkkiä arviointiraportteja. Arviointilaitoslain perusteella arviointilaitosten antamat todistukset voidaan vain arvioinnin pyytäjän suostumuksella rekisteröidä turvallisuusselvitysrekisteriin. Rekisterin käyttöoikeudet ovat merkittävästi rajatut.

Arviointilain 8 a §:ssä säädetään mahdollisuudesta säätää valtioneuvoston asetuksella velvollisuudesta hankkia todistus valtionhallinnon viranomaisen määräysvallassa olevasta tietojärjestelmästä tai tietoliikennejärjestelystä, jossa käsitellään turvallisuusluokkaan I tai II kuuluviksi luokiteltuja asiakirjoja. Tätä säädösvaltuutta ei ole toistaiseksi käytetty, joten todistuksen pyytäminen kansallisen turvallisuusluokitellun tiedon käsittelyssä on arviointilaissa säädetty vapaaehtoiseksi. Todistuspyynnöt Liikenne- ja viestintävirastolle kansallisen turvallisuusluokitellun tiedon käsittelyssä ovat käytännössä harvinaisia.

Pilvipalvelut ovat uutta teknologiaa, joiden tietoturvallisuuden arviointi vaatii osaamista, joka on vasta hiljalleen kertymässä tiedonhallintayksiköissä. Säädettyjä vaatimuksia on pilvipalvelujen arvioinneissa tulkittu niiden tarkoitusta tiukemmin, mikä on johtanut tarpeettoman tiukkoihin arviointikriteereihin. Esimerkiksi viranomaiset nostavat usein esiin Tiedonhallintalautakunnan suosituksen Turvallisuusluokiteltavien asiakirjojen käsitellystä pilvipalveluissa (VM 2022:4) mukaisen näkemyksen, että käyttötapauskohtaisesti myös turvallisuusluokan IV tietojen käsittelyyn tarkoitetun tietojärjestelmän – erityisesti pilvipalvelun – käyttöönoton olisi hyvä perustua arviointilain mukaiseen arviointiin ja todistukseen. Toisten valtioiden lainsäädännön piirissä oleviin palveluihin kuten pilvipalveluihin voi hakea kansainvälistä yritysturvallisuusselvitystä (FSC, Facility Security Clearance). Se on kuitenkin pääsääntöisesti käytettävissä vasta turvallisuusluokasta III/CONFIDENTIAL lähtien. Liikenne- ja viestintäviraston tarkastustoimivallan voi katsoa koskevan vain Suomen lainkäyttövallan piiriin kuuluvaa toimintaa. Siten virastolla ei ole edellytyksiä tarkastaa ja arvioida toisen valtion lainkäyttövallan piiriin kuuluvaa toimintaa siten kuin todistuksen edellyttämä varmuus edellyttäisi. Arviointilaki ei velvoita viranomaisia hankkimaan arviointilain mukaista arviointia tai todistusta pilvipalvelujen

käytölle turvallisuusluokiteltavien tietojen käsittelyssä. Turvallisuusverkon palvelujen tietoturvallisuuden arviointivelvoitteesta on säädetty turvallisuusverkkoasetuksessa ja sitä tarkentavassa valtiovarainministeriön määräyksessä. Pilvipalvelun käyttöönoton riskiarvioinnin haasteet tiedonhallintayksiköissä ja epäselvät tulkinnat arviointisäännöksistä ovat ohjanneet teettämään vaatimustenmukaisuuden arviointeja varmuuden vuoksi ja myös tilanteissa, joissa riskiperusteisesti arvioituna niille ei olisi ollut tarvetta. Tämä on vaikuttanut siihen, että viranomaisten pilvipalvelujen käyttöönotot ovat voineet viivästyä tarpeettomasti.

EU:n ja Naton tietoturvallisuusvelvoitteiden mukaisista arvioinneista turvallisuussäännöissä edellytetty hyväksyntälausunto on arviointilain menettelyn valossa todistuksen luonteinen. Turvallisuusselvityslain mukaisissa yritysturvallisuusselvityksissä Liikenne- ja viestintävirasto tekee Suojelupoliisin tai Pääesikunnan pyynnöstä selvityksen tietojärjestelmän tietoturvallisuudesta. Tämäkin selvitys on todistuksen luonteinen sinä mielessä, että selvitys annetaan vain vaatimukset täyttävästä järjestelmästä, mutta itse yritysturvallisuusselvitystodistuksen antaa turvallisuusselvityslain mukaan Suojelupoliisi tai Pääesikunta ja kansainvälisten tietoturvallisuusvelvoitteiden tapauksessa ulkoministeriön kansallinen turvallisuusviranomainen. Yritysturvallisuusselvitystodistus voi siis liittyä joko kansallisiin tai kansainvälisiin tietoturvallisuusvelvoitteisiin.

EU:n ja Naton turvallisuussäännöissä yritysturvallisuusselvitystä ei edellytetä EU-R tai NR-tason tiedon käsittelyssä, mutta järjestelmien akkreditointi on pakollista näissäkin tilanteissa. Siten Liikenne- ja viestintävirasto arvioi järjestelmät ja antaa niistä hyväksyntälausunnon. Fyysisestä turvallisuudesta Liikenne- ja viestintävirasto pyytää tällöin kansainvälisistä tietoturvallisuusvelvoitteista annetun lain tehtäväjaon mukaisesti lausunnon Suojelupoliisilta tai Pääesikunnalta. Käytännössä Liikenne- ja viestintäviraston antama todistus on oikeudelliselta muodoltaan valituskelpoinen hallintopäätös hyväksynnästä, vaatimusten täyttymisestä tai hyväksyntälausunnosta.

Arkaluonteisten sosiaali- ja terveystietojen sähköiseen käsittelyyn liittyen asiakastietolaissa ja toisiolaissa säädetään eräistä vaatimuksista sekä velvollisuudesta hankkia tietoturvallisuuden arviointilaitoksen todistus tietoturvallisuusvaatimusten täyttymisestä. Arviointiperusteina käytetään Terveyden ja hyvinvoinnin laitoksen tai sosiaali- ja terveysalan tietolupaviranomaisen Findatan määräyksiä. Arviointilaitoksen on muodostettava arvioinnissa kanta siitä, täyttyvätkö vaatimukset riittävästi, sillä todistuksen voi näiden lakien ja arviointilaitoslain mukaan antaa vain, jos vaatimukset täyttyvät. Toimintojen ohjauksesta ja valvonnasta säädetään muutoin asiakastietolaissa ja toisiolaissa.

Terveyden ja hyvinvoinnin laitoksen määräykset pohjautuvat asiakastietolakiin. Niiden perusteella laadittavien tietoturvasuunnitelmien avulla sote-alan toimijoita ohjataan riittäviin ja yhdenmukaisiin tietoturva- ja tietosuojakäytäntöihin. Lisäksi tietojärjestelmiin ja hyvinvointisovelluksiin kohdistuvia olennaisia vaatimuksia yhdenmukaistetaan valtakunnallisesti. Olennaisten vaatimusten määräykset kohdistuvat ratkaisujen toiminnallisuuteen, yhteentoimivuuteen ja tietoturvallisuuteen. Määräykset ohjaavat myös asiakas- ja hyvinvointitietoja käsittelevien järjestelmien ja sovellusten sertifiointia eli niin sanottuja Kanta-sertifiointeja.

VALTIONEUVOSTO
STATSRÅDET

Itsearviointi

Sääntely ei sisällä tiedonhallintayksiköiden tai Tori- ja turvallisuusverkkolakien mukaisten yhteisten tieto- ja viestintäteknisten palvelujen tuottajien itse toteuttamaa vaatimuksenmukaisuuden todentamista eli itsearviointeja ja niihin liittyviä katselmointeja, tarkastuksia tai testauksia. Tiedonhallintayksiköt toteuttavat itsearviointeja soveltaessaan tiedonhallintalakiin perustuvaa riskienhallintavelvoitettaan. Itsearviointien toteuttamista tai hankkimista tietoturvallisuuspalvelujen tarjoajilta koskevia vaatimuksia ei ole säädetty. Viranomaisen tulee kuitenkin voida varmistaa järjestelmänsä turvajärjestelyihin perehtyvän yrityksen turvallisuus, tai ainakin huomioida tähän liittyvien riskien olemassaolo. Viranomaisen keinoja varmistua käyttämänsä yrityksen turvallisuudesta ovat muun muassa hyväksytyn tietoturvallisuuden arviointilaitoksen käyttäminen, yritysturvallisuusselvityksen edellyttäminen, yrityksen luottotietojen tarkastaminen ja sopimukselliset keinot.

Sääntely ei estä itsearviointien tai testausten toteuttamista. Niiden avulla tuetaan järjestelmien tietoturvallisuuden suunnittelua ja ylläpitoa merkittävästi. Itsearviointeja voisi selventää osana lain perusteluja tai ne voisi tarvittaessa listata säännöstasolla osana tiedonhallintayksikön toimenpiteitä. Tietoturvatestausta ja tietoturvatarkastuksia tarjoavat yritykset voidaan nähdä yhtenä arviointielintyyppinä. Ne voitaneen yleensä rinnastaa itsearviointiin, jolloin riittävän pätevyyden arviointi on palveluhankintaan liittyvä sopimusasia.

Kaupallisen toimijan julkinen hallintotehtävä tai viranomaisen tehtävän ulkoistaminen

Julkinen hallintotehtävä, hallinnon yleislait ja virkavastuu

Perustuslain 124 §:ssä säädetään, että julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle. Pykälän perusteluissa (PL, HE 1/1998, s. 179) todetaan, että julkisella hallintotehtävällä viitataan tässä yhteydessä verraten laajaan hallinnollisten tehtävien kokonaisuuteen, johon kuuluu esimerkiksi lakien toimeenpanoon sekä yksityisten henkilöiden ja yhteisöjen oikeuksia, velvollisuuksia ja etuja koskevaan päätöksentekoon liittyviä tehtäviä.

Tällä perusteella julkisen hallintotehtävän ulkoistaminen edellyttää aina lailla säätämistä. Kun viranomaistehtävä tulisi muun julkisen hallinnon toimijan kuin viranomaisen tai yksityisen yrityksen hoidettavaksi, tulee valvovalla viranomaisella myös olla säädettynä toimivalta ja riittävät edellytykset tehtävää hoitavan toimijan valvomiseksi. Valvonta on tärkeää, jotta eri toimijoiden tarjoamat palvelut olisivat keskenään yhtä laadukkaita ja sellaisia, mitä on edellytetty, kun tehtävä on päätetty ulkoistaa. Erityisesti tietoturvallisuuden arviointitehtävässä ei voida ajatella, että markkinoilla olisi yritys tai muu toimija, joka myöntäisi todistuksia kilpailijoitaan löysemmin vaatimuksin, sillä tämä rapauttaisi koko järjestelmän.

Arviointilaitoslain 13 §:ssä säädetään, että *hyväksytyn tietoturvallisuuden arviointilaitoksen on tässä laissa tarkoitettuja tehtäviä hoitaessaan noudatettava hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä kielilakia (423/2003)*. Hallituksen esityksessä (HE 45/2011 vp, s. 10) todetaan, että *tulkintaongelmien välttämiseksi mainittujen säädösten soveltamista ei ehdotuksen mukaan olisi sidottu julkisen hallintotehtävän hoitamiseen, vaan säädöksiä sovellettaisiin kaikkiin ehdotetun lain mukaisten tehtävien hoitamiseen*. Arviointilaitoslain perusteluissa ei suoraan mainita siitä, että tietoturvallisuuden arviointilaitokset toimivat julkisessa hallintotehtävässä. Kuitenkin hallituksen esityksen perusteluista käy ilmi, että on ajateltu ainakin osan tietoturvallisuuden arviointilaitosten työstä olevan julkisen hallintotehtävän hoitamista. Tätä käsitystä puoltaa myös se, että arviointilaitoslaissa on katsottu tarpeelliseksi ulottaa keskeiset hallinnon lait koskemaan myös tietoturvallisuuden arviointilaitoksia.

Ainakin arviointilaitosten todistusten antamista voidaan pitää julkisena hallintotehtävänä, sillä myönnetyllä todistuksella tietojärjestelmän omistaja tai haltija voi osoittaa täyttävänsä käytetyn kriteeristön mukaiset vaatimukset. Tämä vaikutus jää saavuttamatta, jos todistusta ei myönnetä. Ottaen huomioon, että Liikenne- ja viestintäviraston tekemänä pelkkä arviointikin ilman todistusta on ilman muuta viranomaisen toimintana julkinen hallintotehtävä ja hyväksytyn tietoturvallisuuden arviointilaitoksen tarkoitus on tuottaa vastaava luotettava arviointi, joten sitäkin voisi pitää julkisena hallintotehtävänä. Tätä tukisi julkisen hallintotehtävän laaja tulkinta perustuslain valossa.

Perustuslakivaliokunta on katsonut, että hallinnon yleislakeihin ei ole enää välttämätöntä viitata laissa (PeVL 13/2010 vp, PeVL 46/2002 vp, s. 10, PeVL 33/2004 vp, s. 7/II, PeVL 11/2006 vp, s. 3). Kuitenkin perustuslakivaliokunta on katsonut, että hallinnon yleislakeihin voidaan viitata säännöksissä, kunhan pykälässä luetellaan kattavasti sovellettavat hallinnon yleislait (PeVL 37/2010 vp). Arviointilaitoslaissa viittausta hallinnon yleislakeihin voidaan pitää tarpeellisena informatiivisuuden ja sääntelyn selkeyden kannalta. Nykyinen viittaus hallinnon yleislakeihin ei kuitenkaan ole tyhjentävä. Siihen olisi syytä lisätä ainakin viittaus tiedonhallintalakiin. Tiedonhallintalain 3 §:n 4 momentista on luettavissa, että sen nojalla tietoturvallisuuden arviointilaitosten tulee soveltaa tiedonhallintalain 4 lukua (tietoturvallisuus) sekä 25–28 §:ää julkista hallintotehtävää hoitaessaan. Hallinnon yleislakina on pidetty myös sähköisestä asioinnista viranomaistoiminnassa annettua lakia, johon näin ollen olisi tarpeen myös lisätä viittaus arviointilaitoslaissa. Jos arviointilaitosten päätöksistä säädettäisiin muutoksenhakuoikeus, tulisi viitata myös oikeudenkäynnistä hallintoasioissa annettuun lakiin.

Sen sijaan perustuslakivaliokunta on lausunnoissaan katsonut, että perustuslain 124 §:n mukainen julkisen hallintotehtävän ulkoistaminen virkamieskoneiston ulkopuolelle edellyttää nimenomaista virkarikosvastuun perustavaa laintasoista säännöstä (esim. PeVL 93/2022 vp, s. 4, PeVL 15/2019 vp, s. 4). Sellaista ei nykyisellään ole arviointilaitoslaissa. Sen enempää hallituksen esityksessä tai hallintovaliokunnan lausunnossa kuin liikenne- ja viestintävaliokunnan mietinnössäkään ei virkavastuuta ole mainittu. Perustuslakivaliokunnan nykyisin vakiintuneen tulkintakäytännön mukaan kyse on perustuslaista juontuvasta lain säätämisen edellytyksestä. Hallituksen esityksessä on nostettu esille se, että eduskunnan oikeusasiamiehen mukaan julkisen hallintotehtävän hoitamisessa tulee noudattaa kielilakia. Muita julkisen hallintotehtävän hoitamista koskevia lausuntoja ei sitä vastoin ole mainittu. Vaikuttaa olevan kyse siitä, että asiaa ei ole lainsäädäntöprosessin ajankohtana vielä osattu ottaa huomioon.

VALTIONEUVOSTO
STATSRÅDET

Hyväksyttyjen arviointilaitosten toimivalta

Arviointilaitoslailla on nykyisin säädetty muun kuin viranomaisen tekemästä riippumattomasta arvioinnista, jota viranomaiset voivat käyttää. Arviointilaitos voi pätevyytensä rajoissa arvioida tietojärjestelmiä, joissa käsitellään julkista, salassa pidettävää tai kansallista turvallisuusluokiteltua tai tietoturvallisuussopimuksen perusteella vastavuoroisen suojaamisen piirissä olevaa ulkomaista turvallisuusluokiteltua tietoa. Tällaisissa tietojärjestelmätarkastuksissa toimivaltaisia ovat siis sekä Liikenne- ja viestintävirasto että pääsääntöisesti sen hyväksymät tietoturvallisuuden arviointilaitokset.

Sen sijaan kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:ssä säädettyjen toimivaltaisten viranomaisten tehtävien valossa arviointilaitoksilla ei ole toimivaltaa arvioida erityissuojattavaa tietoaineistoa sisältäviä tietojärjestelmiä, joiden osalta kansainväliset tietoturvallisuusvelvoitteet eivät perustu vastavuoroiseen kansallisen sääntelyn soveltamiseen, vaan suoraan esimerkiksi EU:n tai Naton turvallisuussääntöihin. Samoin turvallisuusselvityslain nojalla annettava selvityksen tietojärjestämän tietoturvallisuuden tasosta on toimivaltainen tekemään vain Liikenne- ja viestintävirasto, joskin virasto voi turvallisuusselvityslain 35 §:n valossa huomioida arviointilaitoksen todistuksen.

Seuraavassa on tarkasteltu, olisiko toimivallan säätäminen arviointilaitoksille mahdollista EU:n turvallisuusluokitellun tiedon käsittelyn edellyttämissä arvioinneissa. EU:n neuvoston turvallisuussääntöjen EU/488/2013 Liitteen IV kohta 25 edellyttää, että jäsenvaltion salauslaitteiden hyväksyntäviranomaisen on arvioitava ja hyväksyttävä EU:n turvallisuusluokiteltujen tietojen suojaamisessa käytettävät salaustuotteet. Kohdan 46 mukaan *salauslaitteiden hyväksyntäviranomainen vastaa sen varmistamisesta, että salaustuotteet ovat kansallisten tai neuvoston salausperiaatteiden mukaisia. Se hyväksyy salaustuotteen, jolla EU:n turvallisuusluokitellut tiedot suojataan määrättyyn turvallisuusluokkaan asti tuotteen käyttöympäristössä. Jäsenvaltioiden osalta salauslaitteiden hyväksyntäviranomainen vastaa lisäksi salaustuotteiden arvioinnista.* Siten tällaisten EU:n salaustuotteiden arviointia ei ole nykysääntelyn voimassa ollessa mahdollista ulkoistaa viranomaiselta.

EU:n neuvoston turvallisuussääntöjen Liitteen IV kohta 48 näyttäisi mahdollistavan EU:n turvallisuusluokiteltua tietoa koskevan tietojärjestelmän tarkastamisen osittaisen ulkoistamisen, jolloin vain hyväksyntälausunnon antaminen jäisi viranomaiselle. EU:n neuvoston turvallisuussääntöjen Liitteen IV kohta 34 edellyttää, että liitettäessä viestintä- ja tietojärjestelmä toiseen tietotekniikkajärjestelmään on seuraavien perusvaatimusten täytyttävä: a) toimivaltaisten viranomaisten on todettava ja hyväksyttävä yhteen liittämistä koskevat toiminta- tai käyttövaatimukset; b) yhteen liittämisen on käytävä läpi riskinhallinta- ja hyväksyntäprosessi, ja se on hyväksytettävä toimivaltaisella turvallisuusjärjestelyt hyväksyvällä viranomaisella. Edellä mainitun kohdan 48 alakohtien e ja h valossa voisi olla mahdollista, että viranomainen asettaisi vaatimukset ja hyväksyisi riskinhallinta- ja hyväksyntäprosessin lopputuloksen, mutta tarkastustehtävä säädettäisiin arviointilaitokselle.

Vastaava tarkastelu tulisi tehdä myös Naton turvallisuussääntöjen osalta ja tarkastelussa täytyy huomioida se, että tietojärjestelmien akkreditointiin ja tuotteiden arviointiin liittyy yksityiskohtaisia sääntöjä rooleista ja menettelyistä. Ennakko-oletus on kuitenkin, että turvallisuusäännöt mahdollistavat teknisen testauksen ja

tarkastamisen ulkoistamisen, mutta eivät vastuun ulkoistamista SAA-, NCSA- tai NTA-viranomaistoiminnolta.

Salaustuotteiden tai muiden turvallisuuskriittisten tuotteiden arviointitehtävä voitaisiin harkita tietyin edellytyksin annettavaksi myös muulle kuin viranomaiselle. Mikäli julkisena hallintotehtävänä hoidettavassa tuotteiden arvioinnissa halutaan luoda mahdollisuus hyödyntää muita kuin viranomaisia, kuten VTT:tä tai evaluointilaboratoriota, tulee tehtävän hoitamisesta säätää lailla tai antaa valtuutussäännöksellä viranomaiselle oikeus siirtää julkisen hallintotehtävän hoitaminen sopimusperusteisesti. Vaihtoehtoisesti arviointitoiminnassa voitaisiin hyödyntää hyväksyttyjä arviointilaitoksia, mikä luonnollisesti edellyttäisi pätevyyttä. Ulkoistamisesta säätäminen on tärkeää salaustuoteinvestointeja tekevien yritysten oikeusvarmuuden näkökulmasta, mutta myös arviointitoiminnan markkinan toimivuuden näkökulmasta. Kun ulkoistaminen tehdään säädöspohjaisesti, arviointitaholle voidaan antaa selkeä ja itsenäinen rooli, joka tukee arviointitoiminnan nopeuttamisen tavoitetta. Kuten edellä on todettu EU:n osalta, ulkoistamista harkittaessa tulee kiinnittää huomiota myös siihen, miltä osin ulkoistaminen on kansainvälistä salaustuotehyväksyntää silmällä pitäen mahdollista.

Viranomaisyhteistyö arviointitoiminnassa

Turvallisuusselvityslaissa ja kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa viranomaistehtävät tiedon turvaamisen arvioinnissa jaetaan henkilöstö- ja toimitilaturvallisuuteen ja tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuteen. Yritysturvallisuus pitää tarvittaessa sisällään nämä kaikki osa-alueet. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan puolustusministeriö, Pääesikunta ja Suojelupoliisi toimivat kansallisen turvallisuusviranomaisen asiantuntijoina henkilöstö-, yritys- ja toimitilaturvallisuutta koskevissa asioissa sekä Liikenne- ja viestintävirasto tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa.

Ulkoministeriön kansallisen turvallisuusviranomaisen tehtävänä on ohjata ja valvoa, että kansainvälisten tietoturvallisuusvelvoitteiden mukaiset erityissuojattavat tietoaineistot suojataan ja niitä käsitellään asianmukaisesti. Turvallisuusselvityslain 9 §:n mukaan henkilöturvallisuusselvityksen ja yritysturvallisuusselvityksen tekemisestä päättää Suojelupoliisi tai Pääesikunta. Liikenne- ja viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen. Sekä kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa että turvallisuusselvityslaissa säädetään viranomaisten yhteistyöstä ja mahdollisuudesta sopia tapauskohtaisesti tehtävistä.

Arviointilaissa ei säädetä viranomaisten yhteistyöstä tai mahdollisuudesta sopia tehtävistä. Arviointilaitoslaissa ja myöhemmin voimaan tulleissa toisiolaissa sekä asiakastietolaissa ei ole säädetty viranomaisten yhteistyöstä, työnjaosta, tehtävien koordinoimisesta eikä tietojenvaihdosta. Viranomaisten yhteistyö voisi koskea esimerkiksi arviointilaitosohjeen valmistelua yhteistyönä. Tietyn arviointipätevyyden tai -kriteeristön substanssiviranomaisen (kuten THL laatimiensa määräysten käyttämisessä arviointikriteeristönä) roolia pätevyyden hyväksynnässä, ohjauksessa ja valvonnassa tulisi lisätä ja selkeyttää. Tähän soveltuvia lausunto-, päätös- ja yhteistyömenettelyjä tulisi tarkentaa. Kukin viranomainen voisi tällöin arviointitoiminnan kannalta keskittyä omiin ydintehtäviinsä. Yrityksen elinkeinotoimintaan kohdistuvan eri viranomaisten ohjauksen ja

valvonnan tehtävien ja toimivaltuuksien olisi oltava selkeät: Liikenne- ja viestintävirastolle ei ole säädetty oikeutta saada tietoja tietoturvallisuuden arviointilaitosten asiakkailta tai soteviranomaisilta eikä salassapitosääntelyn estämättä, eikä säädetty Liikenne- ja viestintäviraston tiedonsaantioikeudesta tai tiedonvaihdosta FINASin kanssa, eikä säädetty mahdollisista pätevyyden seurannan aikaisista poikkeamista ilmoittamisesta liikenne- ja viestintävirastolle.

Liikenne- ja viestintävirastolla ei ole toimivaltaa ohjata ja neuvoa sekä valvoa arviointilaitosten toimintaa niiltä osin, kun arviointitehtäviä suoritetaan muun kuin arviointilaitoslain mukaisesti - esimerkiksi sotelainsäädännön vaatimusten ja THL:n määräysten täyttymisestä arvioinnissa. Epäselvää on, missä määrin arviointilaitosten toiminnan asianmukaisuutta sekä velvoitteiden noudattamista valvotaan niissä tilanteissa, kun arviointilaitosten tehtävistä on säädetty asiakastietolaissa, toisiolaissa tai niiden nojalla ja onko sääntelyssä otettu huomioon riittävässä määrin arviointilaitosten valvonnan kannalta tarpeelliset tiedonsaanti- ja tarkastusoikeudet, sekä seuraamukset niiden tilanteiden varalta, mikäli velvoitteita ei ole noudatettu. Myös valvottavien kannalta lainsäädännöstä ei ilmene ja on todennäköisesti epäselvää, mikä viranomainen on missäkin tilanteessa toimivaltainen ja kenen puoleen tulisi kääntyä ohjausta ja neuvontaa varten.

3. Sovellettavasta EU:n sertifiointisääntelystä

Tässä luvussa tarkastellaan EU:n sisämarkkinoihin liittyvän sertifiointisääntelyn suhdetta kansalliseen viranomaisten tietojärjestelmien arvioinnin sääntelyyn. Jos kansallinen viranomaisen tietojärjestelmien tietoturvallisuuden arvioinnin sääntely olisi päällekkäistä EU:n sertifiointisääntelyn kanssa, päällekkäisyys rajoittaisi kansallista sääntelytoimivaltaa. Luvussa tarkastellaan sääntelyiden suhdetta myös siitä näkökulmasta, miten viranomaisen tietojärjestelmissä voi olla mahdollista hyödyntää EU:n sertifiointisääntelyn tuloksia.

Keskeisiä EU-säädöksiä

EU:ssa on hiljan annettu tai ollaan valmistelemassa useita säädöksiä eri palvelujen tai tuotteiden sertifioinnista: kyberturvallisuusasetus (CSA); Euroopan parlamentin ja neuvoston asetuksen (EU) 2024/2847 digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) n:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta, jäljempänä *kyberkestävyysasetus* tai *CRA*, Cyber Resilience Act; Euroopan parlamentin ja neuvoston asetus (EU) 910/2014 sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta ja Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183 asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta, jäljempänä *eIDAS-asetus*; ja Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta, jäljempänä *tekoälysäädös*, (*AIA, Artificial Intelligence Act*). Vaatimuksia sisältyy myös radiolaitedirektiiviin 2014/53/EU (*RED, Radio Equipment Directive*). Viittaukset kyberturvallisuusasetuksen (CSA) mukaiseen EU:n sisämarkkinoille tarjottavien tuotteiden ja palveluiden sertifiointiin ovat lisääntymässä EU-sääntelyssä. EU:n sertifiointisääntelyn toimeenpano on vielä monelta osin valmisteluvaiheessa.

Yleinen tietosuoja-asetus mahdollistaa käytännesäännöt ja sertifioinnit menettelynä osoittaa henkilötietojen käsittelyn vaatimustenmukaisuus. Yleisessä tietosuoja-asetuksessa tarkoitettuna kansallisena valvontaviranomaisena toimii tietosuojalain mukaan tietosuojavaltuutettu, joka on myös toimivaltainen akkreditoimaan yleisen tietosuoja-asetuksen mukaisen sertifiointielimen.

Kyberturvallisuusasetus (CSA)

Kyberturvallisuusasetuksen 1 artiklan mukaan asetuksen kohde on sisämarkkinoiden asianmukaisen toiminnan varmistaminen ja kyberturvallisuuden, kyberresilienssin ja luottamuksen korkea taso unionissa. Tässä tarkoituksessa asetuksessa vahvistetaan kehys kyberturvallisuuden sertifiointijärjestelmien perustamiselle tieto- ja viestintätekniikan tuotteille, palveluille ja prosesseille. Kehyksillä vältetään sisämarkkinoiden hajautuminen kyberturvallisuuden sertifiointijärjestelmien osalta. Asetus ei 2 artiklan 2 alakohdan mukaan rajoita jäsenvaltioiden toimivaltaa yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden alalla eikä yksittäistä valtiota koskevan rikosoikeuden toimissa.

Asetuksen 2 artiklan mukaan ’tieto- ja viestintätekniikan tuotteella’ tarkoitetaan mitä tahansa verkko- ja tietojärjestelmien elementtiä tai elementtien ryhmää; ’tieto- ja viestintätekniikan palvelulla’ mitä tahansa palvelua, jonka sisältönä on kokonaan tai pääasiassa tiedon välittäminen, tallentaminen, hakeminen tai käsittely verkko- ja tietojärjestelmien avulla ja ’tieto- ja viestintätekniikan prosessilla’ toimintaa, jonka tarkoituksena on suunnitella, kehittää, tarjota tai ylläpitää tieto- ja viestintätekniikan tuotetta tai palvelua. Määritelmät ovat laajoja, mutta käytännössä sertifioinnin mahdolliset kohteet määritellään sertifiointijärjestelmissä eli skeemoissa. Asetuksen 2 artiklan mukaan ’eurooppalaisella kyberturvallisuuden sertifiointijärjestelmällä’ tarkoitetaan unionin tasolla vahvistettuja kattavaa sellaisten sääntöjen, teknisten vaatimusten, standardien ja menettelyjen muodostamaa kokonaisuutta, joita sovelletaan tiettyjen tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointiin tai vaatimustenmukaisuuden arviointiin.

Ensimmäisenä sertifiointijärjestelmänä on vastikään komission täytäntöönpanosäädöksellä (EU) 2024/482 annettu EU:n Common Criteria -skeema (EUCC). Täytäntöönpanosäädöksen 2 artiklan mukaan arvioinnin kohteella (*TOE, Target of Evaluation*) tarkoitetaan tieto- tai viestintätekniikan tuotetta tai sen osaa taikka osana tieto- ja viestintätekniikan prosessia suojausprofiilia (*PP, Protection Profile*), jolle tehdään kyberturvallisuusarviointi EUCC-sertifikaatin saamiseksi. Skeema soveltuu esimerkiksi älykorttien ja tietoturvabokseilla varustettujen laitteiden sertifiointiin, ja tämän tyyppiset elementit soveltuvat esimerkiksi vahvan sähköisen allekirjoituksen luontivälineiden, sähköisesti luettavien matkustusasiakirjojen ja ajopiirtureiden sertifiointiin.

Kyberturvallisuusasetuksen skeemaksi valmistelussa ovat muun ohessa pilvipalveluita (EUCS, European Union Cloud Security) ja 5G-verkkoja koskevat sertifiointiskeemat. Mahdollisia tulevia työkohteita tarkastellaan komission kyberturvallisuussertifiointia koskevassa työohjelmassa (COMMISSION STAFF WORKING DOCUMENT Union Rolling Work Programme for European cybersecurity certification, SWD(2024) 7.2.2024). Siinä mainitaan eIDAS-asetuksen digitaalisen identiteetin lompakkosovellus (*European Digital Identity Wallets*) ja NIS2-direktiivin mukaiset tietoturvallisuuden hallintapalvelut (*Managed Security Services*), jotka voivat liittyä poikkeamien hallintaan, penetraatiotestaukseen, auditointiin ja konsultointiin.

Tarkasteltavina sertifiointialueina työohjelmassa mainitaan yleisesti CRA:n puitteissa tarvittavat skeemat ja teollisuuden automaatiojärjestelmät (*IACS, Industrial Automation Control Systems*). CRA-skeemat kattaisivat myös ennen CRA:n antamista tunnistetun tarpeen IoT-skeemalle (*Internet Of Things*). Tarkasteltavana mainitaan turvallisen kehityksen elinkaari (*SDL, Secure Development Lifecycle*), joka on tärkeä esimerkiksi ohjelmistokehityksessä ja haavoittuvuuksien hallinnassa. Edelleen työohjelmassa mainitaan erityisalueena salausmekanismit (*Cryptographic Mechanisms*) eli esimerkiksi salausalgoritmit, joita tarkastellaan kyberturvallisuusasetuksen mukaisen Euroopan kyberturvallisuuden sertifiointiryhmän (*ECCG, European Cyber Certification Group*) alatyöryhmässä.

Kyberturvallisuusasetuksen mukaisen sertifioinnin hakeminen on palvelun tai tuotteen tarjoajalle vapaaehtoista. Arviointi- ja sertifiointieliminä voivat toimia skeemassa määritellyn varmuustason mukaisesti kansallinen *kyberturvallisuussertifioinnin myöntävä viranomainen* tai skeemaan päteväksi akkreditoitu ja tarvittaessa kansallisen kyberturvallisuussertifioinnin myöntävän viranomaisen valtuuttama asetuksen (EY) N:o 765/2008 2 artiklan 13 alakohdassa määritelty *vaatimustenmukaisuuden arviointilaitos* (*CAB, Conformity Assessment Body*).

EUCC-skeeman täytäntöönpanosäädöksen 2 artiklassa puolestaan säädetään skeemakohtaisesti, että 'sertifiointielimellä' tarkoitetaan asetuksen vaatimustenmukaisuuden arviointilaitosta, joka toteuttaa sertifiointitoimia. Edelleen 'ITSEFillä' tarkoitetaan tietotekniikan turvallisuuden arviointilaitosta (*Information Technology Security Evaluation Facility*), joka on vaatimustenmukaisuuden arviointilaitos ja joka suorittaa arviointitehtäviä. EUCC-skeeman sertifiointitehtävissä vaatimustenmukaisuuden arviointilaitos voi siten olla joko tekniseen laboratoriotestaukseen akkreditoitu ITSEF tai sertifiointielin, joka tarkastaa testaustulokset ja antaa sertifioinnin.

Kyberkestävyyssäädös (CRA)

CRA annettiin 23.10.2024 ja sen voimaantuloon liittyy siirtymäaikoja. Liikenne- ja viestintäministeriön lainsäädäntöhanke asetuksen täytäntöönpanosta on käynnistetty toukokuussa 2024.

Asetuksella vahvistetaan säännöt digitaalisia elementtejä sisältävien tuotteiden asettamiselle saataville EU-markkinoilla, jotta tuotteiden kyberturvallisuus varmistetaan. CRA on horisontaalinen tuoteturvallisuusasetus, jonka vaatimusten toteutuminen taataan tulevaisuudessa osana CE-merkintää. Asetuksen mukaisten turvallisuusvaatimusten täyttyminen on jatkossa markkinoille pääsyn edellytys EU:ssa.

Asetuksen 2 artiklan mukaan sitä sovelletaan kaikkiin markkinoilla saataville asetettuihin digitaalisia elementtejä sisältäviin tuotteisiin, joiden käyttötarkoitus tai kohtuudella ennakoitavissa oleva käyttö sisältää suoran tai välillisen loogisen tai fyysisen datayhteyden johonkin laitteeseen tai verkkoon. Asetusta ei kuitenkaan 2 artiklan 7 alakohdan mukaan sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on kehitetty tai joita on muutettu yksinomaan kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, eikä tuotteisiin, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten.

Asetus koskee digitaalisen elementin sisältäviä laitteita tai ohjelmistoja, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon. Asetuksen 3 artiklan mukaan ”digitaalisia elementtejä sisältävällä tuotteella” tarkoitetaan ohjelmisto- tai laitteistotuotetta ja sen ratkaisuja datan etäkäsittelystä, mukaan lukien toisistaan erillään markkinoille saatettavat ohjelmisto- tai laitteistokomponentit. Tällaisia tuotteita ovat esimerkiksi turvakamerat, televisiot, lelut, kotitalousreitittimet, palomuurit sekä pelit, tekstin- ja kuvankäsittelyohjelmat. CRA ulottaa kyberturvallisuusvaatimukset myös esimerkiksi käyttöjärjestelmään, selaimiin, salasanan hallintaohjelmistoon sekä tiettyihin mikroprosessoreihin ja -ohjaimiin. Tällä tavalla kyberturvallisuutta parannetaan koko toimitusketjussa. Kyberkestävyyssäädöksessä huomioidaan IoT-laitteiden erityispiirteet. IoT-laitteisiin tyypillisesti liittyvä valmistajan vastuulla oleva hallintapalvelu eli datan etäkäsittelyratkaisu katsotaan osaksi tuotetta.

Pilvipalveluratkaisu tai siinä käytetty komponentti kuuluu asetuksen soveltamisalaan, jos se täyttää asetuksen määritelmän datan etäkäsittelyratkaisulle ja sen kehittäminen on tuotteen valmistajan vastuulla. Pilvipalveluratkaisu voi olla esimerkiksi etähallintayhteyksien luomiseen tarkoitettu komponentti. Pilvipalveluihin ja pilvipalvelumalleihin, kuten ohjelmistopalveluihin (SaaS), alustapalveluihin (PaaS) tai infrastruktuuripalveluihin (IaaS) tulee kyberturvallisuusvelvoitteita NIS 2 -direktiivistä.

VALTIONEUVOSTO
STATSRÅDET

Asetusta ei sovelleta lääkinnällisiin laitteisiin, tiettyihin ajoneuvoihin ja lentokoneisiin. Näihin sovelletaan tuotekohtaisessa sääntelyssä jo ennestään olevia kyberturvallisuusvaatimuksia.

CRA:n mukaisia arviointeja voivat tehdä tuoteryhmän kriittisyyden mukaan joko valmistaja itse, akkreditoitu *ilmoitettu laitos* (*Notified Body*) tai kyberturvallisuusasetuksen (CSA) mukainen *kyberturvallisuussertifoinnin myöntävä viranomainen*. CRA:n 27 artiklan 8 kohdan mukaan vaatimustenmukaisuuden voi osoittaa kokonaan tai osittain kyberturvallisuusasetuksen skeeman mukaisella sertifioinnilla, jos se kattaa CRA:n vaatimukset. CRA:ssa edellytetään 7 ja 8 artiklan tuotteilta erityistä vaatimustenmukaisuutta, joka tarkoittaa EU:n tyyppitarkastusmenettelyä, ilmoitetun laitoksen suorittamaa vaatimustenmukaisuuden arviointia tai korotetun tai korkean tason kyberturvallisuussertifiointia. Tämän vuoksi CRA:n kansallisessa toimeenpanossa kiinnitetään erityistä huomiota ilmoitettujen laitosten määrään kansallisesti markkinoille tulon pullonkauloilta välttymiseksi.

Radiolaitteet, RED

EU:n radiolaitedirektiivillä asetetaan vaatimukset erilaisille langattomasti radiotaajuuksilla toimiville laitteille. Radiolaitteen valmistajan on osoitettava radiolaitteen vaatimustenmukaisuus noudattaen jotakin radiolaitedirektiivin liitteissä II, III ja IV tarkoitetuista vaatimustenmukaisuuden arviointimenettelyistä (laki sähköisen viestinnän palveluista 917/2014 255.4 §). Mikäli valmistaja ei suorita itse radiolaitteen vaatimustenmukaisuuden arviointia, valmistaja voi käyttää arvioinnissaan *ilmoitettua laitosta*.

Komission delegoidussa asetuksella (EU) 2022/30 tietyille RED:n soveltamisalaan kuuluville laitteille, kuten internetiin liitettäville laitteille, leluille, lastenhoitoon liittyville laitteille ja päälle puettaville laitteille, asetetaan tietoturvallisuusvaatimuksia direktiivin 3 artiklan 3 kohdan alakohtien d, e ja f mukaisesti. Komissio on siirtänyt asetuksella (EU) 2023/2444 siirtymäaikaa tietoturvavaatimusten soveltamiselle, jotta teknisten standardien valmisteluun saadaan enemmän aikaa. EU-markkinoille saatettavien radiolaitteiden tulee olla tietoturvavaatimusten mukaisia 1.8.2025 alkaen.

eIDAS-asetus

Työryhmän työhön kuuluu myös arvioida lainsäädäntöä, joka liittyy hyväksyttyjen luottamuspalvelujen arviointiin sekä rajat ylittävään käyttöön ilmoitettujen sähköisen tunnistamisen menetelmien arviointiin. Asetusta sovelletaan myös kansallisten vahvan sähköisen tunnistuksen menetelmien ilmoittamiseen ja vastavuoroiseen tunnustamiseen. Jatkossa asetus koskisi myös eurooppalaisia lompakkosovelluksia, joille asetus asettaisi yhteiset vaatimukset.

Asetuksen 3 artiklan 16 alakohdan mukaan ”luottamuspalvelulla” tarkoitetaan sähköistä palvelua, jota yleensä tarjotaan vastiketta vastaan ja joka koostuu mistä tahansa seuraavista:
a) sähköisten allekirjoitusten varmenteiden, sähköisten leimojen varmenteiden, verkkosivustojen todentamisen varmenteiden tai muiden luottamuspalvelujen tarjoamista koskevien varmenteiden myöntäminen;
b) sähköisten allekirjoitusten varmenteiden, sähköisten leimojen varmenteiden, verkkosivustojen todentamisen varmenteiden tai muiden luottamuspalvelujen tarjoamista koskevien varmenteiden validointi;

c) sähköisten allekirjoitusten tai sähköisten leimojen luominen;
d) sähköisten allekirjoitusten tai sähköisten leimojen validointi;
e) sähköisten allekirjoitusten, sähköisten leimojen, sähköisten allekirjoitusten varmenteiden tai sähköisten leimojen varmenteiden säilyttäminen;
f) sähköisen allekirjoituksen etäluontivälineiden tai sähköisen leiman etäluontivälineiden hallinnointi;
g) sähköisten attribuuttitodistusten myöntäminen;
h) sähköisten attribuuttitodistusten validointi;
i) sähköisten aikaleimojen luominen;
j) sähköisten aikaleimojen validointi;
k) sähköisten rekisteröityjen jakelupalvelujen tarjoaminen;
l) sähköisten rekisteröityjen jakelupalvelujen kautta toimitettujen tietojen ja niihin liittyvien todisteiden validointi;
m) sähköisten tietojen ja sähköisten asiakirjojen sähköinen arkistointi;
n) sähköisten tietojen tallentaminen sähköiseen tilikirjaan;”

Asetuksen 3 artiklan mukaan ’hyväksytyllä luottamuspalvelun tarjoajalla’ tarkoitetaan luottamuspalvelun tarjoajaa, joka tarjoaa yhtä tai useampaa hyväksyttyä luottamuspalvelua ja jolle valvontaelin on myöntänyt hyväksytyn aseman. ’Hyväksytyllä luottamuspalvelulla’ tarkoitetaan luottamuspalvelua, joka täyttää tässä asetuksessa säädetyt sovellettavat vaatimukset.

Luottamuspalvelujen vaatimuksenmukaisuutta ja jatkossa myös ilmoitettavien kansallisten tunnistusjärjestelmien sekä lompakkosovellusten vaatimustenmukaisuutta voivat arvioida tuotteiden kaupan pitämiseen liittyvää akkreditointia ja markkinavalvontaa koskevista vaatimuksista ja neuvoston asetuksen (ETY) N:o 339/93 kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa tarkoitetut vaatimustenmukaisuuden arviointilaitokset. Mainitusta arvioinnista on nykyisin säädetty vahvasta sähköisestä tunnistamisesta ja luottamuspalveluista annetussa laissa (617/2009). Tarkoitus on, että lompakkosovelluksen vaatimustenmukaisuus osoitettaisiin tämän sijaan ainakin kyberturvallisuuden kannalta merkityksellisin osin kyberturvallisuusasetuksen (CSA) mukaisella sertifioinnilla, sitten kun tällainen sertifiointijärjestelmä olisi aikanaan saatavilla. Ennen sertifiointijärjestelmän valmistumista arviointiperusteet tulee asetuksen mukaan määritellä kansallisesti.

Luottamuspalveluiden hyväksytty (*Qualified*) asema edellyttää vaatimustenmukaisuuden arvioinnin lisäksi kansallisen valvontaviranomaisen hyväksyntää. Hyväksytyt luottamuspalvelut listataan Komission ylläpitämään luotettuun luetteloon (*Trusted List*). NIS2-direktiivin 24 artiklan 1 kohdan mukaan jäsenvaltioiden on kannustettava keskeisiä ja tärkeitä toimijoita käyttämään hyväksyttyjä luottamuspalveluja. Tähän ei liity direktiivissä tai kansallisesti lainsäädäntötoimia.

Tekoälysäädös, AIA

EU:n tekoälysäädös tuli voimaan 1.8.2024. Asetus pannaan täytäntöön vaiheittain eri siirtymäaikojen mukaisesti ja se sisältää eri määräaikoja jäsenvaltioille. Ellei muuta ole säädetty, asetuksen soveltaminen alkaa 24 kuukautta voimaantulon jälkeen.

Asetuksen tarkoitus on parantaa sisämarkkinoiden toimintaa ja edistää ihmiskeskeisen ja luotettavan tekoälyn käyttöönottoa, samalla kun varmistetaan terveyden, turvallisuuden, perusoikeuskirjassa vahvistettujen perusoikeuksien, mukaan lukien demokratian, oikeusvaltion ja ympäristön korkeatasoinen suojelu, tekoälyjärjestelmien haitallisilta vaikutuksilta unionissa, ja tukea innovointia.

Asetus säätelee tekoälyjärjestelmiä niiden aiheuttamien riskien perusteella. Erittäin haitalliset tekoälyn käyttötavat kielletään ja tietyille korkeariskiseksi luokiteltaville tekoälyjärjestelmille asetetaan tiukennettuja vaatimuksia. Työ- ja elinkeinoministeriö on sidosryhmätilaisuuden esityksessään 6.11.2024 tiivistänyt suuririskisiä tekoälyjärjestelmiä koskevat velvoitteet seuraavasti: Suuririskisen tekoälyjärjestelmän tarjoajan on varmistettava, että markkinoille tuotava järjestelmä on tekoälyasetuksen vaatimusten mukainen. Suuririskisten tekoälyjärjestelmien maahantuojien, jakelijoiden ja valtuutettujen edustajien on osana arvoketjua huolehdittava esimerkiksi asianmukaisesta dokumentaatiosta ja siitä, että järjestelmässä on CE-merkintä. Suuririskisen tekoälyjärjestelmän käyttöönottajan on ennen kaikkea huolehdittava asianmukaisesta ihmisvalvonnasta ja siitä, että syöttötiedot ovat merkityksellisiä ja riittävän edustavia. Eri toimijoilla on myös velvollisuus ilmoittaa eteenpäin havaituista häiriöistä, poikkeamista tai vaaratilanteista.

Asetuksessa vahvistetaan muun muassa yhdenmukaistetut säännöt tekoälyjärjestelmien markkinoille saattamiselle, käyttöönotolle ja käytölle unionissa. Asetusta sovelletaan myös tekoälyjärjestelmien käyttöönottajiin ja näillä tarkoitetaan asetuksen 3 artiklan 4 alakohdan mukaan luonnollista tai oikeushenkilöä, viranomaista, virastoa tai muuta tahoa, joka käyttää valvonnassaan olevaa tekoälyjärjestelmää, paitsi jos tekoälyjärjestelmää käytetään henkilökohtaisessa muussa kuin ammattitoiminnassa.

Asetusta ei sen 2 artiklan 3 kohdan mukaan sovelleta aloihin, jotka eivät kuulu unionin oikeuden soveltamisalaan, eikä se missään tapauksessa vaikuta kansalliseen turvallisuuteen liittyvään jäsenvaltioiden toimivaltaan riippumatta siitä, minkä tyyppisiä tahoja jäsenvaltiot ovat valtuuttaneet suorittamaan näihin toimivaltuuksiin liittyviä tehtäviä. Asetusta ei sovelleta tekoälyjärjestelmiin, jos ja siltä osin kuin ne saatetaan markkinoille, otetaan käyttöön tai niitä käytetään muutettuina tai muuttamattomina yksinomaan sotilaallisia, puolustuksen tai kansallisen turvallisuuden tarkoituksia varten, riippumatta kyseisiä toimia toteuttavan toimijan tyypistä. Asetusta ei myöskään sovelleta tekoälyjärjestelmiin, joita ei saateta markkinoille tai oteta käyttöön unionissa, jos tuotosta käytetään unionissa yksinomaan sotilaallisia, puolustuksen tai kansallisen turvallisuuden tarkoituksia varten, riippumatta kyseisiä toimia toteuttavan toimijan tyypistä.

Asetus edellyttää, että suuririskisille tekoälyjärjestelmille tulee tehdä vaatimustenmukaisuuden arviointi ennen kuin ne saatetaan markkinoille tai otetaan käyttöön. Asetuksen mukaan ”vaatimustenmukaisuuden arviointilaitoksella” tarkoitetaan tahoa, joka suorittaa kolmantena osapuolena vaatimustenmukaisuuden arviointitoimia, kuten testausta, sertifiointia ja tarkastuksia ja ”ilmoitetulla laitoksella” vaatimustenmukaisuuden arviointilaitosta, joka on ilmoitettu tämän asetuksen ja muun asiaankuuluvan unionin yhdenmukaistamislainsäädännön mukaisesti. CRA:n 12 artiklan mukaan suuririskisissä tekoälyjärjestelmissä kyberturvallisuuden vaatimustenmukaisuuden arvioinnissa olisi noudatettava CRA:ssa asetettua arviointimenettelyä.

Tekoälyn hyödyntäminen on merkittävä tavoite julkisessa hallinnossa. Tekoälysäädös vaatinee jatkossa ISO/IEC 42001 -standardin käyttöönottoa harmonisoituna joko ISO 9001:n tai ISO 13485:n kanssa.

Viranomainen sertifioinnin kohteena tai hyödyntäjänä

NIS2-direktiivin perusteella ei säädetä viranomaisen tietojärjestelmän tai muidenkaan sääntelyn tarkoittamien toimijoiden tietoturvallisuuden arviointimenettelyistä. NIS2-direktiivi sisältää kuitenkin mahdollisuuden vaatia kyberturvallisuusasetuksen (CSA) mukaisesti sertifioitujen tuotteiden ja -palvelujen käyttöä taikka sertifioinnin hankkimista.

NIS2-direktiivin 24 artiklan 1 kohdan mukaan jäsenvaltio voi vaatia riskienhallintavelvoitteen vaatimusten noudattamisen osoittamiseksi, että keskeiset ja tärkeät toimijat käyttävät TVT-tuotteita, TVT-palveluja ja TVT-prosesseja, jotka on sertifioitu EU:n kyberturvallisuusasetuksen 49 artiklan nojalla hyväksyttyjen eurooppalaisten kyberturvallisuuden sertifiointijärjestelmien mukaisesti. Lain kansallisessa täytäntöönpanossa on käytetty kansallista liikkumavaraa ja velvoitteista ei ole ehdotettu säädettäväksi.

NIS2-direktiivin 24 artiklan 2 kohdan nojalla puolestaan Euroopan Komissiolla on toimivalta antaa delegoituja säädöksiä, joilla täydennetään direktiiviä täsmentämällä, mitä keskeisten ja tärkeiden toimijoiden luokkia on vaadittava käyttämään tiettyjä sertifioituja TVT-tuotteita, TVT-palveluja ja TVT-prosesseja tai hankkimaan sertifiointi kyberturvallisuusasetuksen 49 artiklan nojalla hyväksytyn eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän mukaisesti. Tällaisia delegoituja säädöksiä annetaan, kun on havaittu, että kyberturvallisuus ei ole riittävän korkealla tasolla, ja niissä säädetään täytäntöönpanokaudesta. Komission delegoitu säädös koskisi toteutuessaan NIS2-direktiivin soveltamisalaan Suomessa kuuluvia toimijoita sillä toimialalla, jolle komissio säätäisi velvoitteen.

NIS2-direktiivin 24 artiklan sääntely ei kuitenkaan vaikuta soveltuvan EU:n jäsenvaltioiden julkishallinnon keskeisten tai tärkeisiin toimijoiden tietojärjestelmien ja tietoliikennejärjestelyjen kokonaisuuksiin, vaikka julkishallinnon toimijoita ei ole ennalta suljettu pois artiklan ja Komission säädöstoimivallan piiristä. Ensinnäkin kyberturvallisuusasetuksen sertifiointijärjestelmien kohteena ovat tuotteet tai palvelut, joita tarjotaan sisämarkkinoilla ja tähän tavoitteeseen soveltuu huonosti sertifiointikehyksen laatiminen monimuotoisille julkisen hallinnon tietojärjestelmille ja tietoliikennejärjestelyille, joita ei ole tarkoitus tarjota markkinoille. Julkishallinnon kyberturvallisuutta EU:ssa on sertifiointivaatimusten sijaan pyritty kehittämään ulottamalla myös julkishallinnon tärkeisiin ja keskeisiin toimijoihin NIS2-direktiivin sääntely viestintäverkko- ja tietojärjestelmien kyberturvallisuusriskien hallinnasta eli kyberturvallisuusvaatimuksista. Toiseksi on huomattava, että NIS2-direktiivin 7 artiklassa kyberturvallisuussertifiointiin liittyvät vaatimukset julkisissa TVT-tuotteiden ja -palvelujen hankinnoissa kuuluvat kansallisen kyberturvallisuusstrategian alaan, mikä voisi olla ristiriidassa sen kanssa, että Komissio velvoittaisi jäsenvaltioiden julkishallinnon toimialan hankkimaan vain sertifioituja TVT-tuotteita tai -palveluita, saati sertifioimaan omat tietojärjestelmänsä. Kolmanneksi Komission sääntelytoimivaltaan vaikuttaa se, että NIS2-direktiivin 24 artiklan 2 kohdan mukaan ennen tällaisten delegoitujen säädösten hyväksymistä komissio tekee vaikutustenarvioinnin ja toteuttaa kuulemisia kyberturvallisuusasetuksen 56 artiklan mukaisesti ja Euroopan Parlamentilla ja Neuvostolla on NIS2-direktiivin 38 artiklan mukaan toimivalta vastustaa delegoitua säädöstä.

NIS2-direktiivin täytäntöönpanon myötä tietynlaiset tietoturvapalvelut tulevat kyberturvallisuuden riskienhallintavaatimusten ja valvonnan piiriin. Kyseiseen sääntelyyn ei kuitenkaan lähtökohtaisesti liity vaatimustenmukaisuuden arviointia tai arviointipätevyyden toteamista, vaan tietyntyyppisille tietoturvapalveluille yleisesti säädetyt kyberturvallisuusvaatimukset ja niiden valvonta. Kuten edellä kyberturvallisuusasetuksen kohdalla todettiin, Komission kyberturvallisuusasetuksen työohjelmassa mainitaan NIS2-direktiivin mukaiset tietoturvallisuuden hallintapalvelut (*Managed Security Services*), jotka voivat liittyä poikkeamien hallintaan, penetraatiotestaukseen, auditointiin ja konsultointiin. Siten on mahdollista, että tällaisten palveluiden sertifiointijärjestelmän valmistelu tulee käynnistymään ja sertifiointijärjestelmän laatiminen antaisi myös edellytykset Komissiolle harkita sertifioinnin hakemisen velvollisuuden säätämistä tietoturvallisuuden hallintapalveluille.

Sertifioinnilla ja sertifikaatilla tarkoitetaan EU-sääntelyssä yleisesti ottaen tiettyjen säädettyjen arviointielimien tietyille tuotteille, palveluille tai prosesseille tarkkarajaisesti säädettyjen vaatimusten perusteella tekemää arviointia ja arvioinnin tulosten perusteella annettuja sertifikaatteja, joiden tarkoitus on osoittaa EU:n sisämarkkinoilla tuotteen, palvelun tai prosessin ominaisuudet. Kyberturvallisuusasetuksen 2 artiklan 11 kohdan mukaan ’eurooppalaisella kyberturvallisuussertifikaatilla’ tarkoitetaan asiaa koskevan elimen myöntämää asiakirjaa, jolla todistetaan, että tietty tieto- ja viestintätekniikan tuote, palvelu tai prosessi on arvioitu eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä vahvistettujen erityisten turvallisuusvaatimusten mukaiseksi. Viranomaisten tietojärjestelmien tietoturvallisuuden ja varautumisen kansallinen arviointisääntely kohdistuu viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman tietojärjestelmän tai tietoliikennejärjestelyn tietoturvallisuuden ja varautumisen tapauskohtaiseen arviointiin, ei siis markkinoilla yleisesti tarjottavien tuotteiden, palveluiden tai prosessien vaatimuksiin.

Edetessään EU:n sertifiointisääntelyn voi odottaa tarjoavan tukea myös viranomaisten järjestelmien suunnitteluun sekä tietoturvallisuuden ja varautumisen ylläpitoon, kun järjestelmissä käytetään sellaisia markkinoilla tarjolla olevia palveluita ja tuotteita, jolla on jonkin jäsenvaltion viranomaisen tai akkreditoidun arviointitahon antama sertifiointi. Yksittäisten elementtien sertifioinnit eivät toki poista sitä tosiseikkaa, että tietojärjestelmä koostuu aina tapauskohtaisesti rakennetusta tietoteknisestä kokonaisuudesta ja yksittäisten elementtien sertifiointi ei takaa näiden kokonaisuuksien tietoturvallisuutta. Kyberturvallisuusasetuksen johdantokappaleessa (77) todetaan, että vaatimustenmukaisuuden arviointi ja sertifiointi eivät sinänsä takaa, että sertifioidut tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit ovat kyberturvallisia. Ne ovat pikemminkin menettelyjä ja teknisiä menetelmiä, jotka todistavat, että tieto- ja viestintätekniikan tuotteet, palvelut ja prosessit on testattu ja että ne täyttävät tietyt kyberturvallisuusvaatimukset, jotka on vahvistettu muualla, esimerkiksi teknisissä standardeissa. Siten viranomaisen tietojärjestelmän suunnittelussa ja arvioinnissa voidaan hyödyntää EU-sääntelyn mukaisesti myönnettyjä sertifikaatteja ja sertifioituja tuotteita, palveluita tai prosesseja siltä osin, kun ne kattavat viranomaisen riskiarvioon tai säädettyihin vaatimuksiin perustuvat tarpeet. Tuotesertifiointien hyödyntämisen mahdollisuus julkisen hallinnon tietojärjestelmien teknisessä, fyysisessä ja osin hallinnollisessa vaatimustenmukaisuuden arvioinnissa olisi otettava nykyistä paremmin jatkossa huomioon. Arviointien ja sertifiointien automatisointimahdollisuuksia tutkitaan.

Salaustuotteiden ja turvallisuuskriittisten tuotteiden arviointi

Tässä raportissa tarkastellaan salaustuotteiden, muiden turvallisuuskriittisten tuotteiden ja TEMPEST-tuotteiden tai -mittauspalveluiden arviointi- ja hyväksyntätarpeita, tehtäviä ja toimivaltuuksia.

Kyberturvallisuusasetus ei asetuksen 2 artiklan 2 alakohdan mukaan rajoita jäsenvaltioiden toimivaltaa yleisen turvallisuuden, puolustuksen ja kansallisen turvallisuuden alalla eikä yksittäistä valtiota koskevan rikosoikeuden toimissa. Asetuksen johdantokappaleen (94) loppuosassa todetaan seuraavaa: Jäsenvaltioita ei kuitenkaan tulisi estää hyväksymästä tai pitämästä voimassa kansallisia kyberturvallisuussertifiointijärjestelmiä kansallisen turvallisuuden nimissä. Jäsenvaltioiden olisi toimitettava komissiolle ja Euroopan kyberturvallisuuden sertifiointiryhmälle tieto aikomuksestaan laatia uusia kansallisia kyberturvallisuuden sertifiointijärjestelmiä. Komission ja Euroopan kyberturvallisuuden sertifiointiryhmän olisi arvioitava uuden kansallisen kyberturvallisuuden sertifiointijärjestelmän vaikutuksia sisämarkkinoiden moitteettomaan toimintaan ja sitä, olisiko strategisesti asianmukaista pyytää käyttämään sen sijaan eurooppalaista kyberturvallisuuden sertifiointijärjestelmää. Asetuksen 2 artiklan mukaan ’kansallisella kyberturvallisuuden sertifiointijärjestelmällä’ tarkoitetaan kansallisen viranomaisen kehittämiä ja käyttöön ottamaa sellaisten kattavaa sääntöjen, teknisten vaatimusten, standardien ja menettelyjen kokonaisuutta, joita sovelletaan kyseisen erityisen järjestelmän kattamien tieto- ja viestintätekniikan tuotteiden, palvelujen ja prosessien sertifiointiin tai vaatimustenmukaisuuden arviointiin.

CRA:ta ei sovelleta digitaalisia elementtejä sisältäviin tuotteisiin, jotka on kehitetty tai joita on muutettu yksinomaan kansalliseen turvallisuuteen tai puolustukseen liittyviin tarkoituksiin, eikä tuotteisiin, jotka on erityisesti suunniteltu turvallisuusluokiteltujen tietojen käsittelyä varten.

Salaustuotteiden, turvallisuuskriittisten tuotteiden ja TEMPEST-tuotteiden ja -mittauspalveluiden arviointi- ja hyväksyntätarpeet liittyvät ennen kaikkea kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseen erityissuojattavien tietoaineistojen sähköisessä käsittelyssä ja kansallisen turvallisuusluokitellun tiedon sähköisen käsittelyn suojaamiseen. Turvallisuusluokittelun perusteiden voi yleisesti katsoa liittyvän kansalliseen turvallisuuteen ja joissain tapauksissa nimenomaisesti esimerkiksi varautumiseen tai puolustukseen. Siten EU:n sisämarkkinoita koskeva sertifiointisääntely ei näyttäisi estävän vaatimusten ja arviointimenettelyjen asettamista näihin tarkoituksiin kansallisen sääntelyn mukaisesti ja kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti. Arvioinnissa ja viranomaisen tietojärjestelmässä voidaan toki tällöinkin hyödyntää EU:n markkinoilla saatavilla olevia sertifioituja ja CE-merkittyjä tuotteita ja ohjelmistoja siltä osin, kun niiden turvallisuus vastaa tarpeita. CE-merkinnällä valmistaja vakuuttaa, että laite täyttää säädöksen (RED, AIA, CRA) olennaiset vaatimukset. CE-merkintä tulee olla sekä tuotteessa että sen pakkauksessa. Merkinnän kiinnittää valmistaja. CE-merkintä ei ole viranomaisen tai muun tahon myöntämä.

Arviointielimet

Arviointielinten sääntelyn näkökulmasta EU:n sertifiointisääntelyyn liittyvät kyberturvallisuusasetuksen (CSA) mukaiset vaatimustenmukaisuuden arviointilaitokset sekä kyberkestävyyssäädöksen (CRA) mukaiset

ilmoitetut laitokset. Näihin säädöksiin liittyy myös korkean tason sertifikaatit myöntävä kansallinen sertifiointiviranomainen, joka on sähköisen viestinnän palveluista annetun lain nojalla Liikenne- ja viestintävirasto. Nämä arviointi- ja sertifiointitehtävät liittyvät EU-sääntelyn mukaisesti tarkkarajaisesti määriteltyihin tuotteisiin ja palveluihin. Sertifikaatit on tarkoitettu markkinoilla julkisiksi tuotteiden tai palveluiden hankkijoita varten.

Arviointilaitoslain mukaan hyväksyttyjen arviointilaitosten tehtävänä on lain 9 §:n mukaan tarkastaa arvioinnin kohteen toimitilat ja selvittää, onko arvioinnin kohteen toiminnassa asianmukaisella tavalla toteutettu lain 10 §:ssä tarkoitetut tietoturvallisuutta koskevat vaatimukset, jotka on otettu selvityksen perustaksi (tietoturvallisuuden arviointiperusteet). Arviointiperusteet voivat liittyä sellaiseen 10 §:n mukaiseen säädökseen, ohjeeseen tai standardiin, johon arviointilaitos on saanut akkreditoidun pätevyyden. Käytännössä arviointilaitosten tarve ja pätevyydet liittyvät vaihteleviin tietojärjestelmäkokonaisuuksiin samalla tavalla kuin arviointilain mukaiset Liikenne- ja viestintäviraston arviointitehtävät. Arviointilaitoksen toimeksiannosta laatima arviointiraportti tai todistus ei ole julkinen, vaan todistuksen voi merkitä turvallisuusselvitysrekisrekisteriinkin vain kohteen suostumuksella. EU:n sertifiointisääntelyihin verrattuna yhteistä hyväksytyille tietoturvallisuuden arviointilaitoksille on se, että niiden pätevyyden akkreditoinnissa hyödynnetään kansallisen akkreditointiyksikön FINASin akkreditointia. Sen sijaan arviointilaitoslain mukaiset arvioinnin kohdealueet ja arvioinnin tuloksen tarkoitus eroavat EU:n sertifiointisääntelystä.

VALTIONEUVOSTO
STATSRÅDET

4. Vaatimusten sääntely ja vähimmäistason määrittäminen

Vaatimusten sääntelyn nykytila

Tässä luvussa käsitellään viranomaisten tietojärjestelmille ja eräille muille tietojärjestelmille säädettyjä vaatimuksia. Vaatimustenmukaisuuden arviointi edellyttää, että on olemassa säädetyt tai muutoin määritellyt vaatimukset, joihin arvioinnin kohdetta verrataan. Säädetyt vaatimukset ovat usein niin yleisluonteisia, että käytännön arviointityöhön on tarpeen laatia yksityiskohtaisia työkaluja, kuten kriteeristöjä ja soveltamisohjeita.

Julkisen hallinnon viranomaisten tietojärjestelmien tietoturvallisuusvaatimuksista säädetään tiedonhallintalaissa. Lakia sovelletaan tältä osin laajasti viranomaisten ja julkista hallintotehtävää hoitaviin yhteisöihin. Lain 4 luvussa säädetään 13 §:ssä tiedonhallintayksikön velvollisuudesta selvittää olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittaa tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Lain 13 a §:ssä edellytetään myös toiminnan jatkuvuuteen kohdistuvien riskien selvittämistä ja jatkuvuudesta huolehtimista valmiussuunnittelulla ja häiriötilanteiden toiminnan etukäteisvalmistelulla.

Valtionhallinnon turvallisuusluokitellun tiedon käsittelyyn liittyviä tietoturvallisuustoimenpiteitä tarkennetaan turvallisuusluokitteluasetuksessa. Tarkennukset koskevat tietojärjestelmille ja tietoliikennejärjestelyille asetettuja vaatimuksia. Asetuksen 11 §:ssä huomioidaan nimenomaisesti myös tietoturvallisuuden erityiset osa-alueet: salausratkaisujen riittävä turvallisuus ja hajasäteilysuojaus eli TEMPEST. Kansainvälisissä tietoturvallisuusvelvoitteissa näihin osa-alueisiin liittyy tarkasti määriteltyjä vaatimuksia.

Eräiden viranomaisten tai julkista hallintotehtävää hoitavien yksiköiden tai viranomaisille tarkoitettujen tietojärjestelmien vaatimuksista säädetään tarkemmin niitä koskevissa erityislaeissa. Torilaissa säädetään Valtorista ja sen velvoitteista ja ohjauksesta. Lain 2 §:ssä säädetään, että yhteisten palvelujen on täytettävä tarpeen mukaiset tietoturvallisuutta ja varautumista koskevat vaatimukset. Toriasetuksessa tarkennetaan palvelujen sisältöä ja asiakkaiden ja Valtorin yhteistyötä asiakasneuvottelukunnassa. Siinä säädetään Valtorin raportointivelvollisuus toimintansa turvallisuudesta ja tietoturvallisuudesta sekä ilmoitusvelvollisuus niihin liittyvistä poikkeamista valtiovarainministeriölle tai sen osoittamalle viranomaiselle. Yhteisten tieto- ja viestintäteknisten palvelujen tietoturvallisuuden vaatimukset määritetään yksityiskohtaisemmin yhdessä palveluita käyttävien tiedonhallintayksiköiden kanssa.

Turvallisuusverkkotoiminnan vaatimuksia on asetettu turvallisuusverkkoasetuksessa ja valtiovarainministeriö voi turvallisuusverkkolain 14 §:n mukaan tarkentaa vaatimuksia määräyksillä. Ministeriö voi myös suorittaa palvelutuotannon varautumista, turvallisuutta ja laatua koskevia ennakollisia tarkastuksia ja arviointeja. Tietojärjestelmien tietoturvallisuuden vaatimukset määrittyvät turvallisuusverkossa yksityiskohtaisemmin valtiovarainministeriön ohjaus- ja valvontamenettelyissä.

Hyvinvointialueiden tietoturvallisuusvaatimukset koostuvat yleislakien lisäksi tiedonhallintalain, asiakastietolain, toisiolain, lääkinnällisten laitteiden, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta annetun Euroopan parlamentin ja neuvoston asetuksen (EU 2017/745) ja NIS2:n muodostamasta kokonaisuudesta. Hyvinvointialueet kuuluvat NIS2-direktiivin piirissä sekä julkishallinnon että terveydenhuollon alaan ja ne voivat lisäksi olla lääkinnällisten laitteiden valmistajia. Lisäksi sosiaali- ja terveydenhuollon järjestämisestä annetussa laissa on säädetty valmiuteen ja varautumiseen liittyvistä asioista ja tässä yhteydessä myös tietojen käyttämisestä. Jatkossa hyvinvointialueita tulee koskemaan myös sosiaali- ja terveydenhuollon data-avaruus (EHDS) ja sen sääntely.

EU:n NIS2-direktiivin täytäntöönpanossa kyberturvallisuusriskien hallinnan vaatimukset laajenevat julkishallinnon toimialalle. Direktiivin soveltamisalaan kuuluvien eri toimialojen vaatimukset säädetään pääosin uudessa yleislaissa kyberturvallisuuslaki (HE 57/2024 vp) ja julkishallinnon osalta vastaavat vaatimukset säädetään tiedonhallintalain 4 a luvussa. Luvun soveltamisalaa on rajattu tiedonhallintalain 3 §:ssä, eli sitä ei sovelleta kuntiin, opetus- ja koulutusalan toimijoihin, kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla toimiviin viranomaisiin eikä turvallisuusverkon palvelutuottajiin ja palvelujen käyttöön. Kyberturvallisuuslakia sovelletaan eräisiin kuntien kriittisen infrastruktuurin toimintoihin, esimerkiksi vesi- ja jätehuoltoon. Vaatimukset ovat pitkälti samansuuntaisia kuin tiedonhallintalain 4 luvussa säädetyt tietoturvallisuusvaatimukset, mutta ne on eritelty yksityiskohtaisemmin.

Suomessa toimitaan hajautetun mallin mukaisesti, jolloin sektoriviranomaiset valvovat sektorillaan olevia toimijoita. Lisäksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimii kansallisena koordinaatiopisteenä. Valvovia viranomaisia ovat Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Lääkealan turvallisuus ja kehittämiskeskus ja Finanssivalvonta. Tiedonhallintalain 4 a luvun vaatimusten täyttymistä ohjaa ja valvoo Liikenne- ja viestintävirasto. Valvova viranomainen voi muun muassa pyytää selvityksiä tai tehdä tarkastuksen, jossa se voi käyttää avustajana hyväksyttyä arviointilaitosta, ja antaa päätöksen korjausvelvoitteista laissa tai NIS 2-direktiivin nojalla annetuissa säännöksissä säädettyjen velvollisuuksien noudattamiseksi. Tarvittaessa viranomaisen tieto- ja tietoliikennejärjestelyjen riittävä taso voi siten tiedonhallintalain 4 a luvun soveltamisen piiriin kuuluvissa toiminnoissa tulla ratkaistavaksi viranomaisen valvontapäätöksellä.

Henkilötietojen käsittelyn tietoturvallisuusvaatimuksia säännellään yleisessä tietosuoja-asetuksessa ja tietosuojalaissa (1050/2018). Yleisen tietosuoja-asetuksen 32 artiklassa säädetään käsittelyn tietoturvallisuudesta ja riskeistä, jotka käsittelyn turvallisuudessa on huomioitava. Henkilötietojen käsittelyn tietoturvallisuuden riittävyydestä vastaa rekisterinpitäjä. Tietosuojan vaikutusarvioinneissa käsitellään henkilötietojen suojaukseen vaadittavia tietoturvallisuustoimenpiteitä ja siten ne ovat osa vaatimustenmukaisuuden arviointia. Yleisessä tietosuoja-asetuksessa tarkoitettuna kansallisena valvontaviranomaisena toimii tietosuojalain mukaan tietosuojavaltuutettu ja tarvittaessa riittävä taso voi tulla ratkaistavaksi tietosuojavaltuutetun valvontapäätöksellä.

Kansainväliset tietoturvavelvoitteet, EU ja Nato

Viranomaisten ja niille palveluita tuottavien yritysten kansainvälisten tietoturvallisuusvelvoitteiden vuoksi erityissuojattavan aineiston käsittelystä säädetään kansainvälisistä tietoturvallisuusvelvoitteissa annetussa laissa. Kansainväliset tietoturvallisuusvelvoitteet liittyvät aina turvallisuusluokitellun aineiston käsittelyyn. Kun kansainväliset tietoturvallisuusvelvoitteet perustuvat valtioiden kahden- tai monenvälisiin tietoturvallisuussopimuksiin (GSA, General Security Agreement), muista valtioista saatujen turvallisuusluokiteltujen tietojen suojaamisvaatimukset perustuvat pääsääntöisesti vastavuoroisuusperiaatteen mukaisesti turvallisuusluokan mukaisiin kansallisiin vaatimuksiin. Tietoturvallisuussopimuksen mukaisesti turvallisuusluokitellun tiedon sähköiseen siirtämiseen valtioiden välillä voi liittyä toimivaltaisen viranomaisen tehtäviä tietoturvallisuuden tarkastamisesta, joka voi ulottua tiedonsiirtoyhteyden kansalliseen päätepisteeseen. Olennainen osa tietoturvallisuusvaatimuksia on molemmille osapuolille riittävän salausratkaisun sopiminen ja sen hallinnan turvallisuus. Järjestelyihin voi tapauskohtaisesti liittyä valtioiden osapuolten hyväksyntälautakunta, jossa jäsenenä ovat ainakin tietojärjestelmien arvioinnista vastaavat viranomaiset. Kansallisen taustajärjestelmän tietoturvallisuus kuuluu Suomessa tiedonhallintalain mukaisesti tiedonhallintayksikön vastuulle, eikä siihen liity arviointivelvollisuutta.

Euroopan unionin ja Naton turvallisuusluokitellun tiedon käsittelyn vaatimukset puolestaan määritellään näiden organisaatioiden turvallisuussäännöstöissä: Euroopan unionin neuvoston turvallisuussäännöt EU/488/2013 ja niitä tarkentavat periaatteet ja suuntaviivat sekä Naton asiakirja C-M(2002)49-REV1 ja sitä tarkentavat direktiivit ja ohjeet. Naton asiakirja ja sen suomennos löytyvät hallituksen esityksestä HE 4/2023 vp (Hallituksen esitys eduskunnalle tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdyn sopimuksen ja turvallisuussääntöjen hyväksymiseksi ja voimaansaattamiseksi sekä Suomen ja Pohjois-Atlantin liiton kesken vaihdettavan turvallisuusluokitellun tiedon suojaamiseksi tehdyn hallinnollisen järjestelyn ja Pohjois-Atlantin liiton kanssa tehdyn tietoturvallisuussopimuksen irtisanomiseksi). Tarkentavat periaatteet ja ohjeet ovat sekä EU:n että Naton säännöstöissä pääosin jakelurajoitettuja (EU LIMITE, NATO UNCLASSIFIED) tai turvallisuusluokiteltuja ja siten jaettavissa vain tahoille, joilla on tietoon tehtävään perustuva käyttötarve. Vaatimuksista on järjestelmien suunnittelun ja arvioinnin tueksi laadittu kansallinen ohje *Katakri – Tietoturvallisuuden arviointityökalu viranomaisille* ja sen liite IV, *Naton turvallisuusluokitellun tiedon suojaaminen*. EU:n ja Naton turvallisuussääntöjen vaatimuksissa korostetaan kaikille järjestelmille yhteisten riskien ohella erityisesti järjestelmäkohtaisten riskien ja toimenpiteiden tunnistamista ja järjestelmäkohtaisen vaatimusmäärittelyn merkitystä.

Kaikki EU:n ja Naton turvallisuusluokitellun tiedon käsittelyyn käytettävät tietojärjestelmät on turvallisuusääntöjen mukaan akkreditoitava, eli niiden vaatimustenmukaisuus tulee arvioida ja toimivaltaisen viranomaisen (SAA, Security Accreditation Authority) tulee antaa asiasta hyväksyntälausunto. Toimivaltainen viranomainen on Suomessa kansainvälisistä tietoturvallisuusvelvoitteista annetun lain 4 §:n mukaisesti Liikenne- ja viestintävirasto, joka toimii kansallisen turvallisuusviranomaisen asiantuntijana tieto- ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. Liikenne- ja viestintävirasto vastaa turvallisuussäännöissä yksilöidyistä tietojärjestelmätarkastus-, hajasäteilysuojaus- eli TEMPEST- ja salaustuotteiden sekä muiden turvallisuuskriittisten tuotteiden arviointi- ja hyväksyntätehtävistä. Järjestelmien käyttöönottopäätöksestä ja hyväksyntälausunnossa todettujen jäännösriskien hyväksynnästä vastaa kansallisen järjestelmän haltijaviranomainen tai EU:n tai Naton toimittaman järjestelmän hyväksyntälautakunta.

Vaatimustenhallinnan ongelmia

Riskienhallinnan tarkoitus on tavoitteiden saavuttamiseen liittyvän epävarmuuden hallinta. Tiedonhallintalain 13§:ssä on sovellettu riskienhallintaa asettamalla tiedonhallintayksiköille velvoitteet tietojenkäsittelyyn kohdistuvien olennaisten riskien selvittämisestä ja tietoturvallisuustoimenpiteiden mitoittamisesta riskiarvioinnin mukaisesti. Riskienhallintaan kuuluu riskien arviointi, tietoturvallisuustoimenpiteiden suunnittelu tunnistettujen riskien perusteella, jäännösriskien hyväksyminen sekä tietoturvallisuustoimenpiteiden toteuttaminen. Riskienhallinnan tulee olla jatkuvaa ja suunnitelmien toteutumista sekä toteutettujen tietoturvallisuustoimenpiteiden vaikuttavuutta tulee arvioida säännöllisesti. Tietoturvallisuustoimenpiteiden eli riskien hallintakeinojen valinta perustuu riskien merkityksen arviointiin.

Tiedonhallintayksiköt voivat hyödyntää tietojärjestelmien vaatimustenmukaisuuden arviointia osana tietojenkäsittelyn riskien selvittämistä ja tietoturvallisuustoimenpiteiden mitoittamista. Tiedonhallintayksiköiden sääntely ja ohjeistus on vanhentunutta koskien sitä, millä menettelyllä kunkin tietojärjestelmän vaatimustenmukaisuus tulisi riskiperustaisesti valiten arvioida, kuka olisi kokonaistaloudellisesti edullisin arvioinnin toteuttava toimija ja mitä kriteerejä arvioinnissa tulisi kokonaistaloudellisuuden ja turvallisuuden näkökulmista käyttää ja miten arvioinneista huolehdittaisiin tehokkaasti ja riittävä turvallisuustaso varmistaen tietojärjestelmän elinkaaren ajan. Viranomaisen toteuttaman arvioinnin ja hyväksytyn arviointilaitoksen toteuttaman arvioinnin rinnalle ei nykytilassa ole selkeästi tunnistettu itsearviointia. Arviointimenettelyn valinnassa ei ole ohjattu huomioimaan arvioitavassa kohteessa käsiteltävien tietojen luottamuksellisuus-, eheys-, saatavuus-, ja jatkuvuudenhallintavaatimuksia sekä tarkoituksenmukaiseen tuotantotapaan kohdistuvia vaatimuksia.

Arviointilaissa ei huomioida myöskään eritasoisia arviointeja. Yhteiskunnan, kansallisen turvallisuuden ja varautumisen kannalta kriittisten viranomaisten kohteiden arvioinneissa on tarkoituksenmukaista rajata arviointien toteuttaminen jatkossakin vain viranomaisvastuulla toimiville tai julkista hallintotehtävää hoitaville toimijoille. Organisaation ohjeiden mukaisesti organisaatiossa sisäisesti toteutetut itsearvioinnit (ohjattu sisäinen arviointi) ja itsearviointi ulkopuoliselta palveluntuottajalta -menettelyt tarvitsevat selkeyttämistä esimerkiksi sen suhteen, miten ne eroavat hyväksytyn arviointilaitoksen tekemistä arvioinneista.

Tiedonhallintayksikön tietojärjestelmien suunnittelussa ja arvioinnissa asettamien vaatimusten valinnan tulisi perustua tiedonhallintayksikön toimintaympäristön riskien hallinnan kautta valituille riskien hallintakeinoille. Arviointilait eivät kuitenkaan ohjaa riskiperustaisuuden huomioimiseen vaatimusten asettamisessa. Arviointikriteeristöt voivat tukea riskien huomioimista vaatimuksia ja arviointikriteerejä asetettaessa, sillä niitä valmisteltaessa on yleensä pyritty huomioimaan keskeisiä toimintaympäristön riskejä ja valitsemaan kriteerejä riskien arvioinnin perusteella. Riskienhallintaa tulisi arviointitoiminnassa soveltaa myös kriteerien täyttymisen arvioinnissa sekä jäännösriskien arvioinnissa ja hallinnassa. Arviointilait eivät huomioi riskienhallintaa näilläkään arviointitoiminnan alueilla, vaikkakin etenkin mahdollisuus laatia arviointiraportti todistuksen asemasta painottaa selkeästi juuri arvioinnin pyytäjän riskienhallintaa.

Vaatimusten sääntely sisältää tietojärjestelmien suunnittelulle ja ylläpidolle teknologianeutraalit reunaehdot. Teknologioiden ja uhkien jatkuvan muuttumisen vuoksi täydellistä tietoturvallisuutta ei ole mahdollista toteuttaa merkittävilläkään panostuksilla. Tietoturvallisuuden ylläpito edellyttää tietoturvauhkien ja -riskien ar-

viointia, tietojärjestelmän tosiasiallisen toteutuksen tarkastelua ja riittävien toimenpiteiden toteuttamista riskien vähentämiseksi ja jäljelle jäävän jäännösriskin arviointia ja hyväksymistä. Turvallisuusluokitellun tiedon käsittelyyn liittyvät erityisvaatimukset tai muut säädetyt yksityiskohtaiset vaatimukset määrittelevät vähimmäistoimenpiteitä, jotka asettavat hyväksyttävän riskinsiedon vähimmäistason.

Kansalliset säädökset antavat tiedonhallintayksikölle mahdollisuuden arvioida tietoon kohdistuvia uhkia toisistaan poikkeavalla tavalla ja perustaa hallintakeinot tekemäänsä riskiarvioon. Toisaalta tällä halutaan välttää ylimitoitetut hallintakeinot, mutta toisaalta tämä voi aiheuttaa tilanteita, joissa eri viranomaisten omistamat, mutta samantyyppistä tietoa sisältävät tietojärjestelmät suojataan toisistaan poikkeavalla tavalla. Yhteistä uhkaymmärrystä pyritään kehittämään esimerkiksi tiedonvaihtoverkostoilla. EU:n turvasääntö (liite II, kohta 3) puolestaan edellyttää, että fyysisten turvatoimien valinnan on perustuttava toimivaltaisten viranomaisten tekemään uhka-arvioon. Lisäksi EU:n turvasäännössä (liite IV, kohta 5) mainitaan, että toimivaltaisten viranomaisten on tarkasteltava viestintä- ja tietojärjestelmiin mahdollisesti kohdistuvia uhkia ja pidettävä yllä ajantasaisia ja tarkkoja uhka-arvioita, jotka perustuvat ajankohtaiseen toimintaympäristöön. Näin ollen toimivaltaisella viranomaisella on erilainen rooli kansallisen turvallisuusluokitellun tiedon kuin EU:n turvallisuusluokitellun tietoaineiston suojaamisen osalta.

Haasteita voi siis aiheuttaa se, että samoja tietojärjestelmiä olisi usein tarvetta käyttää sellaisten tietoryhmien käsittelyyn tai toimintaan, joihin liittyy erilaisia vaatimuksia. Esimerkiksi kansallista turvallisuusluokiteltua ja EU:n ja Naton turvallisuusluokiteltua tietoa käsiteltäessä on muodostettava käsitys vaatimusten kokonaisuudesta ja eri luovuttajien tietojen suojaamisesta toisiinsa nähden. Näiden vaatimusten muodostaminen ja niiden mukaisten järjestelmien suunnittelu on haasteellista. Tietojärjestelmiä voi myös olla tarve liittää yhteen tai hyödyntää niissä yhteisiä tai ulkoisia elementtejä. Tietyn säädös- ja vaatimuskehikon piiriin kuuluvan järjestelmän toteutuksen teknisen kokonaisuuden ja rajauksen tunnistaminen voi olla työlästä.

Edelleen eri sääntelykehikoiden mukaiset roolit arvioinnissa ja päätöksenteossa voivat olla epäselviä. Tietojärjestelmälle tai sen elementille, kuten salausratkaisulle tai hajasäteilysuojauksille, tehdyn arvioinnin ja tiedonhallintayksikön päätösvallan ja -vastuun suhde ei aina ole tiedonhallintayksiköille selkeä. Kansainvälisiin tietoturvallisuusvelvoitteisiin kuuluvan akkreditoinnin pakollisuus on omiaan aiheuttamaan epäselvyyttä päätösvallasta.

Riittävä tiedon laatu on asianmukaisen asiankäsittelyn ja lainmukaisen hallintoasian käsittelyn edellytys. Tiedonhallintayksiköiden tulisi huomioida, että tietovarannot ovat myös tietojärjestelmiä ja niiden vaatimustenmukaisuutta on arvioitava. Erityisesti automaattisen päätöksenteon tietojärjestelmien tietovarantojen laatua, vastuita ja käyttöä on arvioitava tiedonhallintayksiköissä jatkossa yhä tarkemmin. Tässä asiakirjassa ei arvioida tietosisältöjen laadun arviointia tai sen kehittämistarpeita.

Kansallisella tasolla tietojärjestelmien yhteisessä todentamisessa ja hyväksymisessä on ollut haasteita. Lainsäädäntö ei ole luonut kattavia edellytyksiä yhteisesti tai laajasti käytettyjen ratkaisujen, sovellusten ja palvelujen vaatimustenmukaisuuden todentamiseksi ja valvomiseksi yhdessä ja koordinoidusti, yhdellä kertaa, yli hallinnonala- ja -tasorajojen.

Kuntien näkökulmasta lainsäädännön tulisi olla mahdollisuuksien mukaan paremminkin mahdollistavaa kuin velvoittavaa sekä kevyttä kuin yksityiskohtaista. Lainsäädäntö ei ole riittävästi tukenut sitä, ettei turhia ja tehottomia päällekkäisyyksiä pääsisi syntymään kansainvälisen ja kansallisen tason välillä tai toimialojen tai hallinnon tasojen välillä.

Puolustusvoimien tietojärjestelmien määrä on suuri jakautuen yhteisiin järjestelmiin, puolustushaarojen ja toimialojen eritasoisiin ratkaisuihin sekä edelleen aselajien järjestelmiin. Puolustusvoimien sotilaallisen puolustuksen tehtävien toteuttamista tukevat tiedustelu-, valvonta- ja johtamisjärjestelmien tulee olla toimintavarmoja ja tietoturvallisia kaikissa valmiustiloissa. Operatiivisissa ympäristöissä tulee pystyä käsittelemään turvallisuusluokkien III ja II tietoa. Tietoon ja järjestelmiin kohdistuu salausvaatimuksia, jotka edellyttävät salausavainten hallinnan ja jakelun viiveetöntä toimintaa. Puolustusvoimien normaaliolojen toimintaan liittyy kiinteästi alueellisen koskemattomuuden valvonnan ja turvaamisen sekä valmiuden ylläpidon lisäksi laaja harjoitustoiminta. Puolustushaarakohtaisiin ratkaisuihin liittyy lähes aina liikuteltavuus ja käyttö kenttäolosuhteissa. Tämä tarkoittaa käyttöpaikkojen sijoittamista ajoneuvoihin, aluksiin, lentokoneisiin tai erilaisiin kontti- ja telttaratkaisuihin. Lainsäädännöstä tulevia ja arviointikriteereihin sisällytettyjä vaatimuksia tulee soveltaa ja tulkita siten, että huomioidaan Puolustusvoimien toiminnan erityispiirteet.

Arvioitavien vaatimusten sisältö

Tässä luvussa tarkastellaan sitä, minkä luonteisia substanssivaatimuksia arvioinnit voivat koskea. Erityisesti tarkastellaan tietoturvallisuuden ja toiminnan jatkuvuuden ja varautumisen suhdetta, sekä eräitä tietoturvallisuuden teknisiä osa-alueita. Vaatimusten ryhmittely ja sisältö vaihtelevat sovellettavien säädösten sekä niitä tarkentavien kriteeristöjen perusteella.

Arviointilaissa tai arviointilaitoslaissa ei määritellä, mitä *tietoturvallisuudella* tarkoitetaan. Arviointilain ja arviointilaitoslain perusteluissa (HE 45/2011 vp) viitataan kansainvälisiin tietoturvallisuusvelvoitteisiin, mistä voinee päätellä, että tietoturvallisuudella on tarkoitettu samoja tavoitteita kuin esimerkiksi EU:n sääntelyssä. Tietoturvallisuudella tarkoitetaan yleisemminkin sääntelyssä varsin yhdenmukaisesti tiedon luottamuksellisuutta, eheyttä ja käytettävyyttä/saatavuutta (*confidentiality, integrity, availability*). Erityisesti kansainvälisissä säädöksissä vaadittuihin tavoitteisiin lisätään yhä useammin tiedon alkuperä (*authenticity*) ja kiistämättömyys (*non-repudiation*), joiden sinänsä voi katsoa sisältyvän tiedon eheyteen. Tiedonhallintalaissa puolestaan säädetään *tietoturvallisuustoimenpiteistä,* joilla tarkoitetaan tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä. Tietoturvallisuusvaatimuksissa ja niiden arvioinnissa on vakiintuneesti painotettu tiedon luottamuksellisuutta ja eheyttä, kun suojan kohteena ovat turvallisuusluokitellut tiedot. Painotus johtuu siitä, että turvallisuusluokittelun perusta on arvio siitä, kuinka vakavaa vahinkoa tiedon oikeudeton paljastuminen aiheuttaisi.

Tiedonhallintalakiin on vuonna 2023 lisätty tietoturvallisuutta koskevaan 4 lukuun säännös 13 a § varautumisesta häiriötilanteisiin ja toiminnan jatkuvuudesta mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa. Tietoturvallisuuden määritelmä sisältää luottamuksellisuuden lisäksi myös tietojen eheyden ja saatavuuden. Tietoturvallisuuden vaatimus-

tenmukaisuuden arvioinnin voidaan siten katsoa kattavan myös jatkuvuuden arvioinnin. *Tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvien olennaisten riskien* selvittämisessä on huomioitava myös tietojen käytettävyyteen ja saatavuuteen liittyvät vaatimukset näkökulmat. Toiminnan jatkuvuus ja varautuminen voivat kattaa monenlaisia toimenpiteitä kuten tärkeiden toimintojen tunnistamista, teknisten komponenttien kahdentamista, resurssien ja toimintojen ja toimitusketjujen tarkastelua ja hallintaa ja toiminnan varajärjestelyjä vakavissa häiriötilanteissa tai poikkeusoloissa.

NIS2-direktiivin myötä osalle julkishallinnon toimialan toimijoista säädetään nyt eduskuntakäsittelyssä olevassa tiedonhallintalain 4 a luvussa velvoitteet kyberturvallisuusriskien hallintatoimenpiteisiin. Organisaation on tunnistettava viestintäverkkoihin ja tietojärjestelmiin ja niiden fyysiseen ympäristöön kohdistuvat riskit kaikki vaaratekijät huomioivan lähestymistavan mukaisesti. Se tarkoittaa verkko- ja tietojärjestelmien ja näiden järjestelmien fyysisen ympäristön suojaamista sellaisilta tapahtumilta kuin varkaus, tulipalo, tulva, televiestintä- tai sähkökatko, luvaton fyysinen pääsy tai muu vahingoittaminen tai häirintä. Tässä sääntelyssä edellytetään myös toimitusketjujen turvallisuudesta huolehtimista, johon voi liittyä sekä luottamuksellisuuden että saatavuuden riskinhallinta.

Luottamuksellisuutta ja eheyttä suojaavista teknisistä tietoturvallisuustoimenpiteistä on olemassa vakiintunutta teknistä tietoa ja prosesseja haavoittuvuuksien ja uhkien huomioimiseksi. Tietoturvallisuussääntelyssä tiedonhallintalaissa, tietoturvallisuusasetuksessa ja kansainvälisissä tietoturvallisuusvelvoitteissa eritellään myös niitä teknisen tietoturvallisuuden osatekijöitä, jotka vaikuttavat luottamuksellisuuteen ja eheyteen. Käytettävyys/saatavuus viranomaisen tietoturvallisuuden osa-alueena ei ole ollut samalla tavalla keskiössä, vaan toimintavarmuuden toimenpiteet ovat pikemminkin osa organisaatiokohtaista toiminnan ja sen laadun varmistamista.

Vaatimustenmukaisuuden arviointi koskee nykytilassa tyypillisesti teknisen tietoturvallisuuden ja luottamuksellisuuden ja eheyden arviointia sekä tilanteesta riippuen tilaturvallisuuden ja henkilöstöturvallisuuden arviointia. Arviointeja olisi tarve laajentaa koskemaan varautumista, toiminnan jatkuvuudenhallintaa sekä tietosuojaa. Tulee varmistaa tietojen suojaaminen eli turvallisuus-, jatkuvuus-, käytettävyys-, yksityisyydensuoja- ja uusiokäyttövaatimukset. Toiminnan jatkuvuuden ja varautumisen arvioinnin haasteena on se, että yleispäteviä vaatimuksia ei ole saatavilla sillä tasolla, että ne mahdollistaisivat minkä tahansa organisaation toiminnan jatkuvuuden ja varautumisen tason riippumattoman arvioinnin. Julkrissa on varautumisen ja jatkuvuudenhallinnan (VAR) osa-alue. Se koostuu normaaliolojen varautumista ja jatkuvuudenhallintaa koskevista kriteereistä. Myös Katakri 2020:n kohdassa T-06 on käsitelty jatkuvuutta.

Viranomaisen toiminnan jatkuvuuden ja varautumisen riittävän tason määrittely edellyttää viranomaisen toimintojen tärkeys- tai kriittisyysluokittelua ja toimintoihin vaikuttavien riskien, tieto- ja tietoliikennejärjestelyjen sekä muiden resurssien tunnistamista. Vakaviin häiriötilanteisiin ja poikkeusoloihin varautuminen edellyttää myös varajärjestelyjen suunnittelua. Viranomaisen toiminnan jatkuvuuden riippumattomaan ulkoiseen arviointiin on luotu tarkistuslistoja ja kriteereitä, joilla voi ainakin muodollisella tasolla todeta varmistusten tai suunnitelmien olemassaolon. Sisällöllinen jatkuvuuden ja varautumisen riittävyyden arviointi edellyttää kuitenkin organisaation omaa tietoa. Tällainen tieto on turvallisuusluokitteluasetuksen soveltamisalalla turvallisuusluokiteltavaa. Se voi olla myös luonteeltaan pysyvämpää kuin tietojärjestelmien tekniset toimenpiteet.

Tiedon kertymistä ulkoisille arviointitahoille tulee punnita soveltuvin osin kansallisen turvallisuuden näkökulmasta. Usean arvioinnin aikana arviointitaholle kerääntyvän viranomaisten tietomassan turvallisuusluokitus voi muodostua korkeaksi.

Tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden toteuttamisessa tunnistetaan kansallisessa ja kansainvälisten tietoturvallisuusvelvoitteiden sääntelyssä erityisiä teknisiä osa-alueita, joiden vaatimuksista ja arvioinnista kansainvälisissä tietoturvallisuusvelvoitteissa määrätään nimenomaisesti. Turvallisuusluokitteluasetuksen 11 §:ssä säädetään tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset. Säännöksessä edellytetään muun ohessa, että käytetyt salausratkaisut ovat tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltyjen asiakirjojen turvallisuusluokka huomioon ottaen riittävän turvallisia ja että käsiteltäessä turvallisuusluokan I–III asiakirjoja sähköisesti on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. EU:n ja Naton turvallisuusäännöissä on vaatimuksia ja velvoitteita salausratkaisujen ja hajasäteilysuojauksen (TEMPEST) arvioinnille sekä eräiden muiden turvallisuuskriittisten tuotteiden arviointiin. Myös valtioiden kahden- tai monenvälisissä tietoturvallisuussopimuksissa valtioiden välisissä sähköisissä tiedonsiirtoyhteyksissä salausratkaisuista sopiminen on keskeinen sopimusmääräys ja -käytäntö.

Tietojärjestelmien tietoturvallisuusvaatimuksiin liittyy myös järjestelmän muutostenhallinta ja tekninen jatkuva seuranta mukaan lukien poikkeamien havainnointi ja niihin reagoiminen. Tämä mahdollistaa haavoittuvuuksien hallinnan ja tietoturvallisuuden jatkuvan ylläpidon ja todentamisen. Nykytilassa teknisen jatkuvan seurannan velvoittavuutta ei tarkenneta tiedonhallintalain yleisissä vaatimuksissa. Lain 4a lukuun ehdotettu sääntely sisältää tällaisia vaatimuksia (18 c § Toimenpiteet kyberturvallisuutta koskevien riskien hallinnassa). Tiedonhallintayksikön teknistä seurantaa tukee esimerkiksi Liikenne- ja viestintäviraston kyberturvallisuuskeskuksen Hyöky-palvelu. Teknisen seurannan perusteina ovat tietojärjestelmälle asetetut vaatimukset. Teknisen seurannan rinnalla on toteutettava säännölliset hallinnolliset, tekniset ja toimitila-arvioinnit.

Arviointi- ja todentamismenetelmät, arviointien tehokkuus ja käytännön toteutettavuus

Tässä luvussa käsitellään arviointien käytännön toimeenpanoon liittyviä menettelyjä. Menettelyt eivät pääosin ole säädäntötason asioita, mutta niiden toimivuudella on oleellinen merkitys arviointien sujuvuudelle ja tehokkuudelle ja välillisesti myös arvioinnin kustannuksille. Siksi on tärkeää huomioida, miten arviointitoimintaa voidaan soveltuvin osin tehostaa ja sen ohjausta tukea menettelyjä yhtenäistämällä. Huomioon tulisi ottaa myös viranomaisyhteistyön edistäminen sääntelyn keinoilla.

Luvussa tarkastellaan arvioinnin työkaluja eli kriteeristöjä ja arviointimenetelmiä. Teknisissä arvioinneissa arviointimenetelmistä käytetään usein myös termiä todennusmenetelmä tai tarkastusmenetelmä. Arviointia koskevassa sääntelyssä ja sen toimeenpanossa olisi hyvä tarkastella, kuinka voitaisiin välttää tarpeettomasti päällekkäisten kriteeristöjen laatiminen.

Kriteeristöt, arviointi- ja todentamismenetelmät

Arviointilain 7 §:ssä ja arviointilaitoslain 10 §:ssä säädetään arviointiperusteista, joita Liikenne- ja viestintävirasto tai hyväksytty tietoturvallisuuden arviointilaitos voivat käyttää arvioinnissa. Säännökset ovat varsin joustavia ja siten aikaa kestäviä, mutta niihin olisi kuitenkin tarpeen tehdä joitain tarkistuksia. Arviointilaissa kuvattujen arviointiperusteiden luettelo mahdollistaa laajasti eri arviointiperusteiden käyttämisen. Tiettyjen viranomaisten, kuten valtiovarainministeriön ja kansallinen turvallisuusviranomaisen ohjeiden mainitsemisen sijaan yleisesti viranomaisen ohjeet säädösten soveltamisesta voisi olla riittävä ja yleispätevämpi määrittely. Viranomaisten tulisi varmistua ohjeistuksen yhdenmukaisuudesta ja yhtenäisyydestä.

Arviointilaissa ja kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa ei ole yksilöity arvioinnin työkaluna käytettäviä arviointikriteeristöjä arviointien pyytäjien näkökulmasta riittävän yksityiskohtaisesti. Arviointilaissa ei säädetä, kenen toimivallassa on päättää mitä arviointiperustetta minkäkin tietojärjestelmän kansallisessa arvioinnissa käytetään. Sekä tiedonhallintalain vaatimukset että arviointikriteeristöt kuten Katakri koetaan tulkinnanvaraisiksi. Olisi arvioitava, tarvitaanko lakia alemman asteista sääntelyä tietojärjestelmän vaatimuksista, esimerkiksi tiedonhallintalain vaatimusten täsmentämistä asetuksella. Arviointikriteeristöjen tulkinnanvaraisuutta voi vähentää soveltamisesimerkeillä, mutta tietotekniikan luonteen ja toteutusten monimuotoisuuden ja joustavuuden takia tulkinnanvaraa on väistämättä.

Olisi huomioitava, että eräillä tietoturvallisuuden osa-alueilla tarkat arviointikriteerit voi olla tarpeen pitää salassa, tai vähintäänkin on varmistuttava siitä, että arvioinnin pyytäjällä on tosiasiallinen ja legitiimi syy saada ne tietoonsa. Tällaisia osa-alueita voivat olla esimerkiksi salaustuotteiden ja hajasäteilysuojausten yksityiskohtaiset arviointiperusteet.

Käytännössä säännösten puitteissa on Liikenne- ja viestintäviraston sekä arviointilaitosten toteuttamissa arvioinneissa taannoin sovellettu VAHTI-ohjeita ja sovelletaan jatkuvasti Katakria. Kansainvälisten tietoturvallisuusvelvoitteiden arvioinneissa sovelletaan Katakrin ohella tarvittaessa myös EU:n tai Naton turvallisuussäännöstöihin sisältyviä periaate- ja ohjeasiakirjoja. Sote-alan arvioinneissa, joista säädetään asiakastietolaissa ja toisiolaissa, arviointilaitosten on sovellettava viranomaisten eli terveyden ja hyvinvoinnin laitoksen ja Findatan määräyksiä.

Katakri on laadittu viranomaisten ja elinkeinoelämän yhteistyönä ja siihen on koottu keskeiset kansallisen ja kansainvälisen turvallisuusluokitellun tiedon suojaamiseen kohdistuvat turvallisuusluokkien IV, III ja II vaatimukset. Katakri on kansainvälisistä tietoturvavelvoitteista annettua lakia täsmentävä ja siinä on huomioitu muun muassa EU:n ja Naton Suomea sitovat tietoturvallisuusvaatimukset. Sitä on käytettävä kansainvälisissä arvioinneissa ja sitä voidaan käyttää turvallisuusluokiteltavia tietoja käsittelevien kansallisten tietojärjestelmien ja tietoliikenneratkaisujen tai vastaavien suojattavien kohteiden arvioinneissa. Katakria käytetään Katakri-julkaisun liitteessä kaksi kuvatuissa turvallisuusselvityslain ja viranomaisten tietojärjestelmien arviointien käyttötapauksissa. Sinänsä turvallisuusluokitellun tiedon käsittelyssä huomioitavien tietoteknisten suojaamistoimien tarve ei välttämättä eroa olennaisesti, olipa tieto lähtöisin Suomesta, EU:sta tai Natosta ja lähtökohtana tulee olla kansallisen tiedon suojaaminen vähintään yhtä hyvin kuin EU:n tai Naton. Katakri ei sisällä julkisten tai salassa pidettävien tietojen arviointiin kohdennettuja arviointikriteerejä.

Julkrin käyttäminen kansallisissa muiden kuin hyväksyttyjen arviointilaitosten tekemissä todentamisissa on alkanut. Julkrin suunnittelun lähtökohtana oli arviointikriteeristön asettaminen käyttötapauskohtaisesti riskiperusteisesti. Julkri sisältää Katakrin kriteeristön lukuun ottamatta EU:n ja Naton turvallisuusluokitellun tiedon suojaamisen vaatimuksia. Julkriin on kerätty myös julkisten ja salassa pidettävien tietojen, turvallisuusluokkaa I olevien tietojen sekä tietojen eheyden ja saatavuuden ja jatkuvuudenhallinnan arviointikriteerejä. Sitä voidaan käyttää apuna arvioitaessa tiedonhallintalaissa, turvallisuusluokitteluasetuksessa sekä osin myös tietosuoja-asetuksessa säädettyjen tietoturvallisuutta koskevien vaatimusten täyttymistä. Julkrissa yhdistetään tietoturvallisuuden ja tietosuojan kriteeristöt. Tämä on hyvä lähtökohta ja siitä on suositeltavaa pitää kiinni jatkossakin. Tavoitteena tulisi olla, ettei tietoturvallisuuden ja tietosuojan osa-alueilla synny osin päällekkäistä ja yhteensovittamatonta sääntelyä tai sääntelyn toimeenpanoon liittyviä määräyksiä tai ohjeistuksia.

Valtori on valmistelemassa Julkrin käyttöä tukevaa ohjeistusta ja DVV ylläpitää Julkri-työkaluja. Nykyisin arviointitoiminnassa ei käytetä ainoastaan tiettyjä kriteeristöjä, vaan arvioitavan tietojärjestelmän perusteella valittuja kriteereitä ja tarkistuslistoja. Merkittävää on sisäänrakennettu turvallisuus ja kokonaisuuden hallinta. Tarvitaan hyviä esimerkkejä arviointikriteerien vaatimusten saavuttamisesta. Valtorissa valmisteilla oleva Julkrin käyttöä tukeva ohjeistus sekä DVV:n toteuttama Julkri-työkalujen kehittäminen pyrkivät vastaamaan näihin haasteisiin. Julkri-työkaluihin on täydennetty mahdollisuus organisaatiokohtaisesti lisätä kriteerejä ja niihin on lisätty NIS2-direktiivin vaatimukset Liikenne- ja viestintäviraston valmisteilla olevan suosituksen mukaisesti. Julkri-työkaluihin on täydennetty käyttötapauksia ja niistä onkin kehittymässä myös käyttötapauspankki.

Tietojärjestelmien ja palvelujen vaatimustenmukaisuus tulisi arvioida säädettyjen vaatimusten tai niitä tarkentavista kriteeristöistä tai standardeista riskiperusteisesti valittujen kriteerien avulla. Laissa säädetyt mahdolliset arviointiperusteet voivat olla yksityiskohtaisuudeltaan varsin eritasoisia. Käytännön arviointitehtävissä on kuitenkin välttämätöntä olla käytettävissä konkreettiset työohjeet ja ennalta määritelty perusteiden soveltamistapa, jotta arviointitoiminta on tasapuolista ja tasalaatuista.

Liikenne- ja viestintävirasto on laatinut omien arviointikäytäntöjensä dokumentoimiseksi ja arviointilaitosten ohjaamiseksi ohjeen todentamismenetelmistä. Ne on julkaistu osana viraston ohjetta Liikenne- ja viestintävirasto Traficomin ohje tietojärjestelmien arviointi- ja hyväksyntäprosesseista (dnro TRAFICOM/1061/09.04.00/2023 15.5.2023) ja arviointilaitosohjetta 210/2022 O (dnro 153/602/2016, 22.6.2022). Hallinnollisia todentamismenetelmiä ovat esimerkiksi haastattelu ja dokumentaation tarkastelu ja teknisiä todentamismenetelmiä ovat esimerkiksi järjestelmäkonfiguraatioiden tarkastelu ja passiivinen tai aktiivinen rajapinta-analyysi.

Vertailun vuoksi EU:n kyberturvallisuusasetuksen (EU) 881/2019 52 artiklassa säädetään sertifioinnin eri varmuustasoilla – perustaso, korotettu taso ja korkea taso – edellytettävistä arviointimenetelmistä. Asetuksessa säädetään myös, että eurooppalaisessa kyberturvallisuuden sertifiointijärjestelmässä voidaan määritellä useita arviointitasoja käytettävien arviointimenetelmien tiukkuuden ja kattavuuden mukaan.

Perustasolla on vähintään arvioitava tekniset asiakirjat. Korotetulla varmuustasolla arviointitoimiin on sisällyttävä vähintään seuraavat toimet: tarkastelu, jolla osoitetaan, että julkisesti tiedossa olevia haavoittuvuuksia ei ole, ja testaus, jolla osoitetaan, että kyseiset tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit toteuttavat välttämättömän turvallisuustoiminnon oikein. Korkealla varmuustasolla arviointitoimiin on sisällyttävä vähintään seuraavat: tarkastelu, jolla osoitetaan, että julkisesti tiedossa olevia haavoittuvuuksia ei ole; testaus, jolla osoitetaan, että kyseiset tieto- ja viestintätekniikan tuotteet, palvelut tai prosessit toteuttavat uusimman tekniikan mukaiset välttämättömät turvallisuustoiminnot oikein; ja arviointi penetraatiotestauksen avulla kyseisten prosessien, tuotteiden tai palvelujen kyvystä vastustaa kyvykkäitä hyökkääjiä.

Kansallisesta sääntelystä poiketen EU:n ja Naton turvallisuussäännöstöissä otetaan kantaa arviointikriteereiden määrittelyyn. Naton turvallisuussääntöjen C-M(2002)49-REV1 Liitteen F kohdassa 2.2. säädetään tietojärjestelmien ja tietoliikennejärjestelyjen turvallisuustavoitteista. Ne rakentuvat vähimmäistoimenpiteistä, joiden tiedetään vaikuttavan kaikkiin järjestelmiin ja tietoa tukeviin järjestelmäpalveluihin ja resursseihin sekä järjestelmän tai sen olosuhteiden järjestelmäkohtaisiin riskeihin liittyvistä toimenpiteistä.

Akkreditointia tarkentavissa alemman tasoisissa ohjeissa määritellään järjestelmäkohtaisten turvallisuusvaatimusmäärittelyjen (SSRS, System-specific Security Requirements Statement) laatiminen osaksi järjestelmän suunnittelu- ja arviointiprosessia. Liikenne- ja viestintävirasto on laatinut malleja SSRS:n ja muun dokumentaation laatimiseen. Järjestelmäkohtaisten vaatimusten räätälöinnissä voi hyödyntää Naton direktiivejä tai Katakria, johon on laadittu täydentävä liite helpottamaan Naton turvallisuussääntöjen soveltamista.

Naton turvallisuussääntöjen mukainen akkreditointiprosessi perustuu järjestelmän haltijan ja akkreditointiviranomaisen eli Liikenne- ja viestintäviraston vaiheittaiseen yhteistyöhön siten, että virasto arvioi joka vaiheessa suunnitelmien ja vaatimusten etenemistä. Jos suunnittelu ja arviointi pystytään toteuttamaan tämän prosessin mukaan, itse arviointivaiheessa tarvittava todentaminen on sujuvaa. Prosessin mukaisia hyväksyntälausuntoja on jo annettu ja käytäntö on osoittanut, että toimintamalli palvelee järjestelmäkohtaista riskiperusteista suunnittelua ja arviointia.

EU:n neuvoston turvallisuussääntöjen EU/488/2013 5 artiklan mukaan *EU:n turvallisuusluokiteltuihin tietoihin kohdistuvia riskejä on hallittava prosessina* ja *turvatoimet EU:n turvallisuusluokiteltujen tietojen suojaamiseksi koko niiden elinkaaren ajan on suhteutettava erityisesti tietojen tai aineistojen turvallisuusluokitukseen, muotoon ja määrään, EU:n turvallisuusluokiteltujen tietojen sijoitustilojen sijaintiin ja rakentamiseen sekä paikallisesti arvioituun vihamielisen ja/tai rikollisen toiminnan uhkaan, vakoilu, sabotaasi ja terrorismi mukaan luettuina.* EU:n turvallisuussääntöjen liitteen IV 48 kohdasta ilmenee järjestelmäkohtaisten turvavaatimusten kuuluminen osaksi akkreditointiprosessia. Niiden laatiminen on ollut vakiintunut menettely etenkin EU:n toimittamissa järjestelmissä ja Liikenne- ja viestintävirasto ohjaa myös kansallisten EU:n turvallisuusluokitellun tiedon käsittelyyn suunniteltavien järjestelmien suunnittelu- ja arviointiprosessia tähän toimintamalliin.

Järjestelmäkohtaisen vaatimusmäärittelyn mallin soveltuvuutta ja edistämistä on tarkoitus tukea myös muissa arvioinneissa kuten yritysturvallisuusselvityksiin liittyvissä selvityksissä ja kansallista turvallisuusluokiteltua tietoa käsittelevissä järjestelmissä. Toimintamallin edistämiseen voi yhdistää harkinnan Liikenne-

ja viestintäviraston neuvonnan lisäämisestä siten, että järjestelmän haltija saisi tukea suunnittelussa ja sittemmin arvioinnissa tarkoituksenmukaisista rajauksista ja kriteereistä. Tällöin järjestelmän arvioitavuuden kypsyys voisi parantua ja olla nykyistä helpommin myös arviointilaitoksen tehtävissä. Neuvonnan lisääminen edellyttäisi tehtävän tunnistamista arviointilaissa. Nykyisellään neuvonta ja sen maksullisuus todetaan Liikenne ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista annetussa liikenne- ja viestintäministeriön asetuksessa 1190/2023. Asetuksen 3 §:n 7 kohdan mukaan *luokiteltua tietoa käsittelevien tietojärjestelmien suunnitteluun liittyvä neuvontapalvelu on omakustannusarvon mukaisena julkisoikeudellisena suoritteena maksullinen*. 4 §:n 3 momentin mukaan *Liikenne- ja viestintävirasto voi periä suoritteen omakustannusarvoa vastaavan hinnan silloin, kun sillä on valtion maksuperustelain 7 §:n 2 momentissa tarkoitettu tosiasiallinen yksinoikeus palvelun tuottamiseen. Muut sähköisen viestinnän palvelut hinnoitellaan liiketaloudellisin perustein.* Kaikilla viranomaisilla on kuitenkin hallintolain 8 §:n mukainen neuvontavelvollisuus toimivaltansa rajoissa. Viranomaisten yhteistyövelvoite tukisi mahdollisimman yhdenmukaista neuvontaa. Maksullisuus riippuu siitä, kuuluuko asia maksuperusteasetuksen mukaiseen toimintaan. Sääntelyn näkökulma on viranomaisen resurssien käyttö.

Tietoturvallisuuden arvioinneissa on olennaista todentaa hallintakeinon toimivuus, esimerkiksi ettei sovellus mahdollista väärien syötteiden antamista tai että verkkopalomuurin säännöt on määritelty ja toiminnassa. Varautuminen koostuu erilaisten toimintaa haittaavien skenaarioiden tunnistamisesta ja niihin varautumisesta, joka yleensä tarkoittaa sopimuksiin, suunnitelmiin, redundanttisuuteen sekä varmistuksiin perustuvaa toimintaa. Tällaisen toiminnan aito todentaminen edellyttäisi joko aitoa kriisitilannetta tai sen simulointia esimerkiksi kyberhäiriöharjoituksessa tai yksittäisen häiriötilanteen testaamista, kuten datakeskuksen niin sanotulla blackout-testillä. Varautumisen arviointitoiminta poikkeaa luonteeltaan tyypillisestä tietoturvallisuuden arvioinnista, jossa tutustutaan dokumentaatioon ja tietojärjestelmään, haastatellaan ihmisiä sekä otantaan perustuen todennetaan, että dokumentaatiosta ja haastatteluin saadut tiedot vastaavat tietojärjestelmässä tehtyjä havaintoja ja testejä. Varautumisen perustasoa voi arvioida silti suunnitelmien ja muun dokumentaation sekä sopimusten ja haastatteluiden perusteella.

Arviointikriteeristöjen haasteita

Kriteeristöjen laatimista ja niiden mukaisissa arvioinneissa edellytettäviä arviointi-/todentamismenetelmiä ei säännellä eikä esimerkiksi keskeisistä arviointikriteeristöille asetettavista vaatimuksia ole säädetty. Arviointikriteeristöjen vastuut ja toimijoiden roolit eivät ole kaikilta osin selkeästi määritellyt. Organisaatiot eivät välttämättä tiedä, kuka vastaa arviointikriteeristöjen päivittämisestä ja ylläpidosta. Arviointikriteeristöjen soveltamisohjeet eivät ole olleet kokonaisuudessaan selkeitä ja riittävän yksiselitteisiä.

Toimintaympäristön muuttuessa kriteeristöjä on tarve ylläpitää jatkuvasti. Arviointikriteeristöt eivät ole olleet ajan tasalla koko elinkaarensa ajan. Niitä ei ole päivitetty kaikilta osin säännöllisesti vastaamaan muuttuneita uhkia ja teknologisia kehityksiä. Arviointikriteeristöjen päivitysprosessit eivät ole olleet selkeitä ja tehokkaita.

Arviointikriteeristöt ovat paikoitellen liian yleisiä, jotta ne ohjaisivat riittävästi teknisiä ratkaisuja. Esimerkiksi tietoturvallisuusvaatimukset voivat liittyä salaukseen, fyysiseen suojaamiseen ja muihin teknisiin seikkoihin. Näiden kriteerien tulisi olla mahdollisimman selkeitä ja konkreettisia.

Kun kriteeristön taustalla vaikuttaa jokin säädös, kriteeristön soveltamisen ohjaamiseen ja valvontaan voi liittyä jonkin viranomaisen toimivaltaa. Sinänsä lienee tarkoituksenmukaista säilyttää arviointiperusteiden soveltaminen sääntelyn toimeenpanoon liittyvänä toimintana ilman tarkempaa sääntelyä.

Arviointitoiminnan tavoitteena on nostaa ja yhdenmukaistaa tietoturvallisuuden tasoa toimijakentässä EU:n laajuisesti ja kansallisesti. Merkittäviä tekijöitä tämän onnistumisessa olisivat yhdenmukaiset tai vähintään yhteensopivat tiedon luokittelukäytännöt ja toisaalta yhtenevät tai vähintään yhteensopivat vaatimustenmukaisuuden todentamisen käytännöt. Lainsäädännöllä sekä sen toimeenpanon yhteydessä tulisi varmistaa riittävällä tasolla edellytykset tiedon luokittelun ja vaatimustenmukaisuuden todentamisen yhdenmukaisuuteen.

Tietojärjestelmän toteutukseen ja arviointiin valitut kriteerit tulisi nykyistä laajemmin asettaa tietojärjestelmäkohtaisesti: yhteiset vähimmäisvaatimukset ja lisäksi tietojärjestelmän käyttötarkoituksen, toteutustavan ja järjestelmään liittyvät erityiset uhkat huomioivat täydentävät kriteerit. Kriteerien tulisi vastata tietojen suojaamisen riskeihin ja uhkiin kunkin tietojärjestelmän käyttötarkoitus ja tiedon luokittelu huomioiden. Yhteisille palveluille on haastavaa asettaa yhteisesti hyväksyttävissä olevaa riskitasoa: riskien toteutumisen vaikutukset ovat erilaisia kullekin toimijalle.

Pitkään hyödynnetyssä Teknisen ICT-ympäristön tietoturvataso-ohjeessa (Vahti 2012) käytettiin tietojen luottamuksellisuuden näkökulmasta jäsennystä eri tietoturvatasoihin: perustaso, korotettu taso ja korkein taso. Eri luokkien tietojärjestelmille asetettiin erilaiset tietoturvallisuusvaatimukset. Tietoturvatasojen käyttö on mahdollistanut samantyyppisesti suojattujen tietojärjestelmien yhteen liitettävyyden ja digitalisaatiolla tavoiteltavien hyötyjen ulosmittaamisen. Riskiperusteiset hallintakeinot ilman täsmällisempää ja yhdenmukaistavaa jäsennystä saattavat jättää toisiinsa liitettyjen tietojärjestelmien kokonaisuuteen heikkouksia ja haavoittuvuuksia, sillä kukin tiedonhallintayksikkö arvioi riskejä omista näkökulmistaan. Riskiperustaisten hallintakeinojen käyttöönoton jälkeen ei ole ollut yhtenäistä tietoturvallisuuden tasoa salassa pidettävän tiedon käsittelyyn. Salassa pidettävän tiedon tietoturvallisuuskontrollit toteutetaan riskiperusteisesti eikä riskiarviointi ja sen mukaisesti toteutetut tietoturvallisuuskontrollit eri toimijoiden välillä ole välttämättä samanlaisia. Erot turvallisuuskontrolleissa voivat kasvattaa tietojen jakamisesta eri viranomaisten välillä syntyviä riskejä.

Riskiperustaisten hallintakeinojen haasteiden johdosta tietojärjestelmien tietoturvallisuusvaatimusten suunnittelussa ja arvioinnissa tulisi hyödyntää vaatimusten asettamisten ja arviointien toteuttamisen käyttötapauksia. Julkri on kriteeristö, joka tukee käyttötapausten avulla vaatimusten asettamista riskiperustaisesti. Käyttötapauksista löytyy tietoa siitä, mitä kriteerejä on perusteltua valita vaatimustenmukaisuuden arviointiin. Käyttötapausten laaja hyödyntäminen yhtenäistäisi saman käyttötapauksen tietojärjestelmien vaatimustenmukaisuutta ja siten tukisi saman käyttötapauksen tietojärjestelmien välistä turvattua tietojenvaihtoa. Käyttötapauksia tulisi hyödyntää etenkin salassa pidettäviä ja julkisia tietoja käsittelevien tietojärjestelmien suunnittelussa ja arvioinnissa. Käyttötapausten koordinointi ja laadunvalvonta olisi vastuutettava.

Katakrin kansainvälisen turvallisuusluokitellun tiedon arviointiin tarkoitettuja kriteerejä on käytetty myös kansallisissa vähäriskisten kohteiden arvioinneissa. Tämän voidaan arvioida olevan ongelmallista. Julkisia tietoja käsittelevien kansallisten tietojärjestelmien vaatimustenmukaisuuden arviointia varten tarvitaan myös

yleiskäyttöisiä vähäriskisten tietojärjestelmien arviointikriteerejä. Käyttötapausten vaikutus käytettäviin arviointikriteereihin tulee ottaa huomioon. Vähäriskisten kohteiden arvioinneissa tulisi siirtyä selkeämmin käyttämään käyttötapauskohtaisesti riskiarvioinnin perusteella asetettuja kriteerejä.

Viime vuosina kuntakentän näkökulmasta haasteena on ollut useat eri vaatimuskriteeristöt, esimerkiksi VAHTI, Katakri, Pitukri ja Julkri, joiden voimassaolosta ja soveltamisalasta sekä keskinäisistä suhteista ei ole ollut selkeää kuvaa. Tällaisen muodostaminen ja selkeän lainsäädännön tulkinnan ja kriteeristöpohjan ylläpitäminen kuuluu kansallisille viranomaisille osana lainsäädäntöä ja sen toimeenpanoa. Kunnat voivat tukea kansallisia viranomaisia tässä työssä. Kuitenkin myös riittävä joustovara ja vaihtoehtoisten toteutusmallien ja kriteeristöjen mahdollistaminen on tärkeää, jotta arviointijärjestelyt voivat elää ajassa ja vastata nopeasti toimintaympäristön muutoksiin.

Esimerkiksi pilvipalvelujen arviointiin liittyen joillakin julkisen hallinnon toimijoilla on voinut olla se käsitys, että riskien hallinnan vuoksi olisi hyvä, että globaali pilvipalvelu täyttäisi kansainvälisen turvallisuusluokitellun tiedon käsittelyn vaatimukset. Arvioinneissa on pyydetty käyttämään Katakria. Yhtenä syynä tähän on ollut se, että muitakaan arviointikriteeristöjä kuin Katakri ei ole ollut arviointilaitoslain mukaisissa arviointilaitosten arvioinneissa käytettävissä. Lainsäädäntö ei tätä edellytä. Julkisen hallinnon ohjausta ja ohjeistusta pilvipalvelujen vaatimustenmukaisuuden arvioinnin osalta on tarve parantaa.

Etätyöstä on tullut keskeinen työn tekemisen muoto. Jatkossakin on arvioitava vaatimusten toteutuminen myös etätyössä, jotta salassa pidettävän ja turvallisuusluokkaan IV kuuluvan tiedon käsittely olisi vaatimusten mukaista.

Arvioinnin käytännön haasteita

Arvioinnin hankkimista ja arviointiprosessin sujuvuutta voivat käytännössä hankaloittaa muun muassa järjestelmän tai vaatimusten riittävän tuntemisen puutteet, dokumentaation puutteet, järjestelmän kehitysvaihe tai monitoimijaympäristöön liittyvät tekijät. Arviointia tilattaessa on otettava huomioon tietojärjestelmäsuunnitelmassa asetettujen vaatimusten toteuttamisen realistisuus. Arviointi muodostuu usein kalliiksi, jos vaatimustenmukainen tietojärjestelmä ei ole toteutettavissa. Haasteeksi on nähty se, että arvioinnin pyytäjä ei voi asettaa hintarajoitusta arvioinnin toteutukselle.

Arviointiliiketoiminnassa ei ole toimivia markkinoita, jotka hillitsisivät arviointitoiminnan hintoja. Arviointien kysynnän on pitkään tunnistettu olevan suurempaa kuin arviointipalvelujen tarjonta, mutta arviointipalvelujen tarjonta ei ole kasvanut. Hyväksyttyjen arviointilaitosten resurssipula ja henkilövaihdokset aiheuttavat jo sovittujen arviointien peruuttamisia ja siirtymisiä, millä on laajat seurannaisvaikutukset tietojärjestelmien ja palveluiden kehittämiselle ja käyttöönottojen etenemiselle. Toteutettujen vaatimustenmukaisuuden arviointien tuloksia voidaan nykyisin hyödyntää salassapitosäännösten takia muissa arvioinneissa ainoastaan arviointitietojen vastuuorganisaation luvalla.

Arviointeja tilaavat tahot näkevät vaatimustenmukaisuuden arviointien haasteiksi sen, että arvioinnit ovat jatkuvaa ja kuormittavaa tekemistä ja arviointien uusimisen perusteet ovat epäselvät, esimerkiksi ei ole

määritelty mikä on merkittävä muutos. Kaikki arviointeja tilaavat tahot eivät ole olleet tietoisia siitä, että merkittävien muutosten määrittely tehdään järjestelmäkohtaisesti järjestelmäkohtaisiin riskeihin pohjautuen. Salausratkaisut ovat voimassa vain kolme vuotta, ja alustaympäristöjen riippuvuuksien vuoksi arvioinnit pitää uusia kolmen vuoden välein tilanteissa, joissa käytetään salausratkaisuja, joiden elinkaaren kestävästä luotettavuudesta ei ole saatavilla riittävästi näyttöä.

Arviointeja tilaavat tahot eivät aina tunnista sitä, että arviointilaitoksille asetetut vaatimukset (ISO 17021) kieltävät osallistumisen toimintaan, joka *vaarantaa heidän toimintansa ja päätöstensä riippumattomuuden ja puolueettomuuden*. Arvioijat eivät standardin mukaisesti saa etenkään osallistua tarkastamiensa kohteiden *suunnitteluun, valmistamiseen, toimittamiseen, asentamiseen, hankintaan, omistamiseen, käyttöön tai huoltoon*. Käytännössä tiedonhallintayksiköt hankkivat tietoturvallisuuden asiantuntijapalveluita itsearviointien tueksi tietojärjestelmien elinkaaren eri vaiheissa. Toisin kuin arviointilaitokset, arviointiviranomaiset voivat neuvoa arvioinnin kohdetta vaatimuksenmukaisuuden täyttymisessä.

Teknologioiden nopea muutos ja tietojärjestelmien ketterä kehittäminen edellyttävät ylläpitämään ja arvioimaan vaatimustenmukaisuuden toteutumista jatkuvasti. Tietojärjestelmän elinkaaren tietyissä vaiheissa tehdyt ulkoiset arvioinnit eivät voi olla riittävä tapa varmistaa jatkuvaa vaatimustenmukaisuutta, vaan järjestelmästä vastaavan organisaation on ylläpidettävä tietoturvallisuutta ja vaatimustenmukaisuutta esimerkiksi huolellisella muutostenhallinnalla ja poikkeamien havainnoinnilla sekä niihin reagoimisella. Siten on tarpeen tarkastella kokonaisuutena tiedonhallintayksikön tietoturvallisuusvelvoitteita. Toimintaympäristöstä tuleva paine voi aiheuttaa tarvetta varmistaa yksittäisen järjestelmän tietoturvallisuuden tasoa arvioinnin avulla nykyisiä käytänteitä nopeammassa aikataulussa. Vasta Nato-arviointien myötä on syntymässä malli, jossa tekninen arviointi huomioidaan ketterästi jo järjestelmän kehittämisestä lähtien. Yleisesti tarvetta on toteuttaa vaatimustenmukaisuuden arviointeja eri laajuisina: esimerkiksi ketterästi arvioidaan tietojärjestelmään kehitetyn toiminnon vaatimustenmukaisuutta, mutta samalla ei välttämättä arvioida laajempaa kokonaisuutta. Laajempi arviointi toteutetaan tietojärjestelmän myöhemmässä elinkaaren vaiheessa.

Arvioinnit pitäisi tehdä ennen käyttöönottoa, mutta arvioinnissa käydään läpi ylläpitovaiheen asioita (esimerkiksi vuosikellon mukainen toiminta), joita ei vielä ole käyttöönotettu. Vaatimustenmukaisuuden arviointiin ei sisälly vaikutuksia toimintaympäristöön, kustannuksiin tai tiloihin arvioivaa vaikutustenarviointia, joka paremmin soveltuukin tiedonhallintayksikön tehtäväksi. Hansel on kilpailuttanut tietoturvallisuuden arviointilaitosten palveluja koskevan dynaamisen puitejärjestelyn. Siihen ei sisälly itsearviointeina toteutettavat kaupallisten yritysten suorittamat nykytilan arvioinnit vaatimuksiin nähden, joita voi hankkia tiedonhallinnan ja digiturvallisuuden asiantuntijapalveluiden dynaamisen hankintajärjestelyn kautta.

Tietojärjestelmän arvioinnin edellytyksiä ei useinkaan selvitetä riittävästi ennen arviointia. Moniviranomaisympäristössä tai monitoimijaympäristössä arvioinnin sujuvaa hankkimista ja toteuttamista vaikeuttavat teknisesti laajat ympäristöt, osapuolten vastuiden ja päätösvallan määrittelyyn liittyvät epäselvyydet ja se, että arviointiprosessin edistämisvastuu voi olla hajaantunut tai etäällä käytännön tarpeista. Kansallisissa, riskiperustaisissa vaatimustenmukaisuuden arvioinneissa keskeinen merkitys on tietojärjestelmän tuotantoketjun asettamien rajoitusten huomioimisella. Esimerkiksi kansallisesti salassa pidettävän tai julkisen tiedon käsittelyssä käytettävän, globaalissa tuotantoketjussa tuotetun pilvipalvelun arviointiin on valittava arviointi-

menettely ja -kriteeristö siten, että arviointi on mahdollista toteuttaa. Huomioon on otettava globaaliin tuotantoketjuun osallistuvien toimijoiden toimintavaltioiden lainsäädännön asettamat vaatimukset ja rajoitukset sekä mahdollisuus arvioida palvelun tietoturvallisuutta myös palvelun tarjoamista koskevien sopimusten perusteella.

Joissain tapauksissa arviointipyynnön sisältö voi jäädä epäselväksi ja arvioinnin kohteesta voi puuttua tarpeellisia asioita. Tällöin Liikenne- ja viestintävirasto on joutunut pyytämään lisäselvityksiä. Epäselvyydet ovat voineet myös liittyä siihen, että arviointipyynnön tai -hankinnan pyytäjä ei tunne arvioinnin kohdetta riittävästi tai hän ei ole saanut koottua tarpeellisia tietoja palveluntuottajalta. Erityisesti moniviranomaisympäristöihin kohdistuvissa arvioinneissa on myös havaittu, että arvioinnin pyytäjällä ei ole näkyvyyttä eikä käytännön vaikutusmahdollisuuksia kaikkiin tietojärjestelmän suojauksiin oleellisesti vaikuttaviin tietojärjestelmäosiin. Epäselvät pyynnöt ja tilanteet hidastavat prosessia. Lisäksi osapuolilla voi olla haasteita määritellä pyynnön sisältöä ja kohdetta myöhemminkin tehtävän edetessä ja eriäviä näkemyksiä voi olla pahimmillaan jopa arvioinnin loppuvaiheessa.

Vaikka arviointipyyntöä suunniteltaessa ja laadittaessa olisi käytettävissä järjestelmän hyvä tuntemus, arvioinnin kohteen tekninen rajaaminen aiheuttaa tyypillisesti ainakin jonkin verran haasteita. Hyväksyntäprosessin päätavoitteena on varmistua siitä, että tietojärjestelmässä saavutetaan turvallisuusluokitelluille tiedoille riskeihin nähden riittävä suojaamisen taso ja että sitä ylläpidetään tietojärjestelmän elinkaaren ajan. Tämä edellyttää sitä, että arvioinnin rajaukseen sisällytetään sellaiset tietojärjestelmän osat, jotka oleellisesti vaikuttavat tietojärjestelmässä käsiteltävän turvallisuusluokitellun tiedon suojaamiseen. Esimerkiksi tietojärjestelmän päätelaitteet, käyttöpisteet sekä ylläpitoon käytettävät hallintaratkaisut on lähes poikkeuksetta perusteltua sisällyttää hyväksyntälausuntoon tähtäävän tietojärjestelmäarviointiin. Toisinaan arvioinnin pyytäjä ei tunne tietojärjestelmää tai tunnista sen turvallisuuteen vaikuttavia tekijöitä sillä tarkkuudella, että olisi pystynyt tunnistamaan kaikkia tietojen suojaamiseen olennaisesti vaikuttavia tietojärjestelmän osia. Toisinaan onkin havaittu, että hyväksyntäprosessissa välttämättömän rajauksen kattavuus ei ole vastannut arvioinnin pyytäjällä ollutta ennakkokäsitystä tietojärjestelmäarvioinnin laajuudesta. Tilanteissa, joissa tavoitteena ei ole kansainvälisiin tietoturvallisuusvelvoitteisiin perustuva hyväksyntälausunto tai todistus vaatimustenmukaisuudesta, tietojärjestelmäarviointien rajauksessa on huomattavasti enemmän liikkumavaraa ja se perustuu tyypillisesti tiukemmin vain arvioinnin pyytäjän kuvaamiin tietojärjestelmäosiin ja toiminnallisuuksiin.

Arvioinnin sujuvuutta voi hankaloittaa myös järjestelmää koskevan dokumentaation puute tai keskeneräisyys, arvioinnissa havaittujen poikkeamien korjaamisen hitaus ja korjausten toimivuuden todentaminen sekä käytännön tarkastusten organisointi. Joskus omaakaan toimintaa varten ei ole laadittu riittävää dokumentaatiota ja sen puuttuminen hankaloittaa arvioinnin suunnittelua ja toteutusta. Dokumentaation tuottaminen arviointia varten voi viivästyttää arviointia merkittävästi. Ikävimmillään arviointityössä on tullut vastaan tilanteita, joissa arviointisuunnitelman laatimista on viivästyttänyt se, että arvioinnin pyytäjä ei pysty kuvaamaan järjestelmää edes ylätasoisesti eikä järjestelmästä ole saatavilla ajantasaisia kuvauksiakaan. Järjestelmän keskeneräisyys ei estä sujuvaa arviointia vaiheittain, jos se tapahtuu suunnitelmallisesti hallittuina osakokonaisuuksina. Jos sen sijaan suunnitelmia joudutaan kehittämisen aikana olennaisesti muuttamaan, vaiheittainen arviointi voi muuttua tehottomaksi, koska jo arvioituja osuuksia voidaan joutua muuttamaan ja

arvioimaan uudestaan. Erityisesti laajoissa ympäristöissä ja järjestelmissä voi muodostua ongelmaksi hahmottaa kokonaisuus ja mahdollisten erikseen tehtyjen arviointien kokonaiskuva.

Joissakin laajoissa monitoimijaympäristöissä on havaittu, että arviointien tilaajilla ei ole aina ollut riittävää kokonaiskuvaa tietojärjestelmän suojauksien osakokonaisuuksien aikaisemmista arvioinneista tai niissä havaittujen puutteiden korjaamisen tilanteesta. Organisaatioiden nopeus arvioinnissa havaittujen poikkeamien korjaamisessa vaihtelee merkittävästi, tunneista kuukausiin tai jopa vuosiin. Tähän vaikuttaa luonnollisesti korjauksen edellyttämien toimenpiteiden laajuus ja mahdollisen palveluntarjoajan kyvykkyys, mutta kokemuksen perusteella poikkeamiin reagointiin ja arvioinnin etenemiseen vaikuttaa myös se, onko organisaatiolla elinkeinotoimintaan, järjestelmän käyttöönoton tarpeeseen tai muuhun syyhyn liittyvää välitöntä painetta ja kannustinta. Joskus korjaamista hidastaa vastahakoisuus muuttaa vakiintunutta toimintamallia, joka on arvioinnissa osoittautunut turvattomaksi. Arviointiprosessissa voi myös tulla vastaan arkisia arviointityön organisoinnin kömmähdyksiä, kun tarkastuksessa eivät ole paikalla tarvittavat henkilöt.

Liikenne- ja viestintävirasto on havainnut, että organisaatioiden ennakointivalmius järjestelmiin tarvittavien salaustuotteiden valinnassa vaihtelee. Pääsääntöisesti salausratkaisujen valintaan kiinnitetään nykyään hyvin huomiota jo tietojärjestelmän suunnitteluvaiheessa ja ne valitaan jo ennakolta arvioitujen ja riittävän turvallisiksi todettujen salaustuotteiden listoilta. Toisinaan kuitenkin salausratkaisujen luotettavuuteen ei kiinnitetä riittävästi huomiota tietojärjestelmän suunnitteluvaiheessa ja puutteet tulevat esille vasta tietojärjestelmän arviointivaiheessa. Tällöin salausratkaisun arviointi voi viivästyttää tietojärjestelmän arviointihanketta merkittävästi. Viiveitä voi aiheutua muun muassa siitä, että salausratkaisun valmistaja ei ole halukas tuotteensa arviointiin tai että arvioinnissa havaitaan tuotteesta oleellisia turvallisuuspuutteita, joiden korjaaminen on hidasta. Kansainvälisiin tietoturvallisuusvelvoitteisiin liittyy myös valmistusta ja elinkaaren kestävää suojaamista koskevia vaatimuksia, joita kaikki tuotteet eivät täytä. On myös huomioitava, että kaikkiin käyttötapauksiin ei ole aina saatavilla valmiiksi arvioituja ja turvallisiksi todettuja salausratkaisuja esimerkiksi siksi, että vallitseva suojauskäytäntö on fyysinen suojaaminen. Tämä tulisi pystyä tunnistamaan jo tietojärjestelmien suunnitteluvaiheessa korvaavien suojausten toteuttamiseksi.

Arviointi- tai hyväksyntäpyynnöstä ei aina olla yhteydessä Liikenne- ja viestintävirastoon riittävän ajoissa, jotta virasto voisi huomioida arvioinnin tehtäviensä priorisoinnissa ja aikataulutuksessa tai neuvoa kääntymään arviointilaitoksen puoleen tai muutoin edistää asiakkaan tavoitteiden saavuttamista. Viime hetkellä tehtyjä pyyntöjä ei yleensä ole mahdollista tehdä pyytäjän suunnittelemassa aikataulussa.

Liikenne- ja viestintävirastolle on tullut vastaan myös tilanteita, joissa arvioinnin kohde ja palvelutoimittaja ovat keskenään sopineet ehdoksi Liikenne- ja viestintäviraston tekemän arvioinnin tai hyväksynnän eli todistuksen ottamatta huomioon sitä, että viraston tekemään arviointiin ei ole arviointilain perusteella subjektiivista oikeutta vaan virasto on joutunut priorisoimaan tehtäviään. Tällöin arvioinnin aikataulu tai tekijä voi olla toisenlainen kuin pyytäjä on suunnitellut tai mihin se on sopimuksessaan sitoutunut.

Arvioitavan järjestelmän teknisen tuntemuksen ja rajauksen lisäksi tietoturvallisuusvaatimusten tuntemus voi olla riittämätöntä. Vaatimusten tuntemiseen liittyy erityisesti tietoisuus uhkista ja riskeistä, joilta suojautumiseksi vaatimukset on laadittu. Toimenpiteet tulee luonnollisesti myös osata suhteuttaa turvallisuusluok-

kaan ja tiedon tai järjestelmän vaarantumisen aiheuttamaan vahinkoon. Liikenne- ja viestintävirasto on havainnut, että riskiarviossa ei aina osata tunnistaa etevän hyökkääjän hyökkäyspotentiaalia. Näin ollen organisaation riskinottokyky ja riskinottohalukkuus voivat osoittautua perusteettomiksi.

Salaustuotteiden, hajasäteilysuojausten ja TEMPEST-tuotteiden arvioinnit

Liikenne- ja viestintäviraston tuotearvioinnin kohteena voi olla kokonaan uusi salaustuote itsenäisenä kokonaisuutena, tuotteen muutos tai tiettyyn järjestelmään tai käyttötapaukseen viranomaisen hankittavaksi harkitsema tuote. Arviointien kesto vaihtelee. Kun Liikenne- ja viestintävirasto on vaatimusten mukaisesti mukana tuotteen kehittämisen prosessissa, arvioinnin kestoon vaikuttaa luonnollisesti myös valmistajan kehitystyön nopeus.

Arvioinnissa salaustuotteen toteutusmekanismeja arvioidaan kansainvälisten tai kansallisten vaatimusten mukaan, jotka määräytyvät turvallisuusluokan ja riskien perusteella. Vaatimukset voivat kohdistua esimerkiksi algoritmeihin ja niiden vahvuuksiin tai tuotteen turvalliseen toteutukseen, kuten ohjelmistoturvallisuuteen. Vaatimusten täyttymisen todentamisessa käytetään erilaisia menetelmiä, kuten dokumentaation tarkastusta, testaamista ja lähdekoodin tarkastelua. Arvioinnissa voi olla tarpeen huomioida valmistajan ja toimitusketjun alkuperänä ja tuotteen valmistusympäristö.

Voimassa olevassa sääntelyssä ei määritellä, millä edellytyksillä valmistaja voi saada salaustuotteensa toimivaltaisen viranomaisen arvioitavaksi, miten yrityksen taustat selvitetään ja millä edellytyksillä yritys voi saada tuotteelleen viranomaisen hyväksynnän. Ennustettavan sääntelyn puuttuminen on omiaan luomaan epävarmuutta valmistajien investointien suunnittelulle ja osaamisen kehittämiselle. Salaustuotteiden suunnittelu ja valmistus edellyttää yrityksiltä investointihalukkuutta ja riskinottokykyä sekä riittävää saatavilla olevaa osaamista työmarkkinoilla. Sääntelyn keinoilla yritystoimintaa voidaan tukea sääntelykehikolla, joka tarjoaa ennakoitavuutta ja tukee yrityksiä niiden investointipäätöksissä. Salaustuotteiden arviointi ja hyväksyntä myös muiden kuin kansainvälisten tietoturvallisuusvelvoitteiden osalta edellyttäisi siten sääntelyä.

Hajasäteilysuojausten toteutus ja arviointi jakautuu teknisesti tila- ja vyöhykeperusteisiin ja laiteperusteisiin. Tila- ja vyöhyketoteutuksissa yhteistyö Liikenne- ja viestintäviraston ja keskeisten viranomaisten välillä on tiivistä. Viranomaisten arvion mukaan hajasäteilysuojauksen vaatimustenmukaisuuden arvioinneissa tarvittavassa mittaustoiminnassa ei ole edellytyksiä yritystoiminnan mahdollistamiselle. Tämä johtuu mittaustoiminnan volyymeista ja osaamisvaatimuksista sekä suojaustarpeisiin ja -toteutuksiin liittyvien tietojen turvallisuusluokituksesta. Yritystoiminnan mahdollisuuksia arvioitaessa on erityisesti tilamittausten osalta huomioitava, että mittausta toteuttavan yrityksen kotimaisuudesta ja luotettavuudesta tulee olla mahdollista varmistua.

TEMPEST-suojattujen laitteiden valmistus on yritystoimintaa. EU:n ja Naton turvallisuussääntöjen mukaan toimivaltainen TEMPEST-viranomainen voisi hyväksyä yrityksiä, joilla olisi esimerkiksi kyvykkyys valmistaa ja mitata vaatimukset täyttäviä laitteita. Yritysten hyväksyntä ja valvonta näyttäisi edellyttävän viranomaistoimivaltuuksien tarkentamista kansallisessa lainsäädännössä. Asiaa tarkastellaan seuraavassa erikseen

kansallisen turvallisuusluokitellun tiedon ja EU:n tai Naton turvallisuusluokitellun tiedon suojaamisessa sekä julkisen hallintotehtävän ulkoistamisen näkökulmasta.

Kansallisen tiedon suojaamisessa TEMPEST-tehtävät ovat osa Liikenne- ja viestintäviraston arviointilain mukaista tietojärjestelmien arviointitehtävää ja kullakin tiedonhallintayksiköllä osa tiedonhallintalain mukaista tehtävää huolehtia järjestelmiensä tietoturvallisuudesta. Viranomaiset voivat pyynnöstä avustaa toisiaan hallintolain 10 §:n mukaisesti toimivaltansa puitteissa. TEMPEST-tehtäviä tai yritysten akkreditointia TEMPEST-tehtäviin ei ole nimenomaisesti säädetty eikä siten myöskään Liikenne- ja viestintäviraston arviointitehtävän ulkoistamiselle yrityksille ole sääntelypohjaa. Arviointilaitoslain perusteella arviointilaitoksen akkreditointi olisi mahdollinen edellyttäen, että saatavilla on jokin lain 10 §:n mukainen arviointikriteeristö, johon laitos voi hakea pätevyyden FINASin akkreditoinnilla ja Liikenne- ja viestintäviraston hyväksynnällä.

EU:n ja Naton turvallisuussäännöissä on nimenomaiset säännökset yritysten akkreditoinnista erilaisiin TEMPEST-tehtäviin kuten suunnitteluun, laitevalmistukseen ja mittauksiin. Yritykset ovat esittäneet asiasta neuvontapyyntöjä Liikenne- ja viestintävirastolle. EU:n ja Naton säännöt eroavat asiassa jonkin verran. Yrityksen TEMPEST-akkreditointi edellyttäisi kansallisesti mahdollisesti FINASin akkreditointia (pätevyyden osoittamista) soveltuvien standardien mukaisesti (esimerkiksi ISO 17025, ISO 9001) tai kansallisten vaatimusten mukaisesti (requirements of a national equivalent agreed by the NTA). Akkreditointia olisi pidettävä yllä, mikä FINASin sääntelyn ja käytännön mukaisesti edellyttää vuosittaista osittaista määräaikaistarkastelua ja neljän vuoden välein akkreditoinnin täyttä uusimista. EU:n ja Naton turvallisuussääntöjen ja standardien lisäksi tarvittaisiin Liikenne- ja viestintäviraston alustavan arvion mukaan joitakin kansallisia tarkennuksia.

Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain säännös viranomaisten tehtävistä on yleisluonteinen. Liikenne- ja viestintäviraston tehtäväksi on säädetty toimia NSA:n asiantuntijana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuutta koskevissa asioissa. EU:n ja Naton turvallisuussäännöissä edellytetyn TEMPEST-viranomaisen tehtävän (NTA, National TEMPEST Authority) on katsottu sisältyvän tähän tehtävään. EU:n ja Naton turvallisuussäännöissä yritysten akkreditointi sekä niiden seuranta ja valvonta ovat kansallisen TEMPEST-viranomaisen tehtäviä. Yritysten akkreditointiin liittyvät tehtävät ja viranomaisen toimivalta laatia akkreditoinnin vaatimusten kansallisia täydennyksiä edellyttäisi kansallisen sääntelyn täydentämistä. Elinkeinotoiminnan sääntelyn täytyy olla ennakoitavaa, joten vaatimusten tulisi perustua sitoviin säädöksiin. Myös akkreditoitujen yritysten valvontatoimivaltuuksien mahdollista kansallista sääntelypohjaa olisi tarkasteltava. EU:n ja Naton turvallisuussäännöissä TEMPEST-viranomaisen toimivaltuudet yritysten ohjauksessa ja valvonnassa mahdollistavat laajan tapauskohtaisen harkinnan ja toimenpiteet. Turvallisuussäännöissä korostetaan NTA:n vastuuta (The NTA is fully responsible for the accreditation given to the accredited TEMPEST company.) Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa ei ole säädetty NTA:n valvontatehtävistä. Suomessa elinkeinotoiminnan valvontasääntelyltä edellytetään tarkkarajaisuutta.

EU:n turvallisuussääntöjen periaateasiakirjassa IASP7 määritellään seuraavasti: The TA may delegate activities under his responsibility, for example supervision, consultancy or the role of approval authority, to another official, such as a Security Officer or TEMPEST expert, as appropriate. Julkisen vallan käyttöä ei voi

VALTIONEUVOSTO
STATSRÅDET

Suomessa delegoida yksityiselle. Valvonta (supervision) on selvästi julkisen vallan käyttöä. Julkisen hallintotehtävän voi PL 124 §:n mukaan tietyillä edellytyksillä antaa muulle kuin viranomaiselle säätämällä siitä lailla. Joltain osin IASP 7:ssä todettuja viranomaisen tehtäviä voisi olla mahdollista ulkoistaa yritykselle julkisena hallintotehtävänä. Olisi tarpeen analysoida, voiko akkreditoidun TEMPEST-yrityksen toiminta olla joissain tapauksissa, kuten mittaukset, joita viranomainen käyttää kolmannen osapuolen järjestelmän hyväksynnän perusteena, julkisen hallintotehtävän luonteista vai onko yritystoiminta luonteeltaan palvelua, johon on toimiluvan luonteinen hyväksyntä.

VALTIONEUVOSTO
STATSRÅDET

5. Arviointien toteuttajien valvonta

Arviointilaitosten valvonnan nykytilanne

Arviointilaitoslain 8 §:n mukaan arviointilaitoksella on velvollisuus ilmoittaa toimintaansa koskevista muutoksista Liikenne- ja viestintävirastolle eli esimerkiksi akkreditointitodistuksen muutoksista tai voimassaolon lakkaamisesta. Laissa ei ole kuitenkaan säädetty Liikenne- ja viestintäviraston tiedonsaantioikeudesta tai tiedonvaihdosta FINASin kanssa ja FINAS näkee akkreditoinnin valvontaan liittyvien tietojen luovuttamisen hyväksyntää valvovalle viranomaiselle akkreditoinnin luottamuksellisuutta edellyttävän luonteen vastaisena. Laissa ei säädetä myöskään mahdollisista pätevyyden seurannan aikaisista poikkeamista ilmoittamisesta Liikenne- ja viestintävirastolle.

Liikenne- ja viestintäviraston on arviointilaitoslain 4 §:n mukaan varattava suojelupoliisille tilaisuus lausua toimitiloista, joten niistä arvion voi tehdä suojelupolisiin päätöksen mukaan joko se itse tai liikenne- ja viestintävirasto. Vastuuhenkilöiden luotettavuuden Liikenne- ja viestintävirasto varmistaa pyytämällä suojelupoliisilta kaupparekisteriin merkityistä henkilöistä turvallisuusselvityksen. Sen sijaan työntekijöiden luotettavuuden selvittäminen ei kuulu laissa Liikenne- ja viestintävirastolle säädettyihin tehtäviin. Myöskään arviointilaitoksen mahdollisuudesta tai velvollisuudesta hankkia henkilöstöstä turvallisuusselvitystä ei ole säädetty.

Arviointilaitoksen luotettavuuteen liittyvät vaatimukset ovat väljiä. Arviointilaitoslain 7 §:n mukaan V*iestintävirastolla ja sen toimeksiannosta toimivalla asiantuntijalla on myös oikeus tarkastaa hyväksyntää hakeneen tai hyväksytyn tietoturvallisuuden arviointilaitoksen tilat sekä sen käytössä olevat menetelmät.* Arviointilaitoslaissa tukeudutaan nykyisellään osittain turvallisuusselvityslain työnjakoon ja säädetään lain 4 §:ssä Liikenne- ja viestintävirastolle velvollisuus varata suojelupoliisille mahdollisuus lausua arviointilaitoksen vastuuhenkilöistä ja toimitiloista. Valvontaviranomainen on arviointilaitoksen omien ilmoitusten varassa, eikä pysty valvomaan esim. omistuksen siirtymistä ulkomaille.

Arviointilaitoslain 9 §:n mukaan *arviointilaitoksen on saamaansa tietoturvallisuuden arviointitehtävää suorittaessaan noudatettava huolellisuutta.* Liikenne- ja viestintävirasto valvoo, että hyväksytty tietoturvallisuuden arviointilaitos hoitaa tehtäviään huolellisesti ja asianmukaisesti ja että arviointilaitos täyttää toimintaansa koskevat, sekä arviointilaitoksen hyväksynnälle asetetut vaatimukset. Arviointilaitoksen hyväksymistä koskevaan Liikenne- ja viestintäviraston päätökseen voidaan lain 5 §:n 4 momentin mukaan lisäksi sisällyttää arviointilaitoksen pätevyysaluetta, valvontaa sekä sellaisia toimintaa koskevia rajoituksia ja ehtoja, jotka ovat tarpeen arviointilaitoksen tehtävien asianmukaisen hoidon varmistamiseksi.

Arviointilaitoksen hyväksynnän ehtona arviointilaitoksia on hyväksyntäpäätöksissä velvoitettu noudattamaan toiminnassaan kulloinkin voimassa olevaa Liikenne- ja viestintäviraston tietoturvallisuuden arviointilaitoksia koskevaa ohjeistusta. Ohjeistuksella tarkoitetaan varsinkin arviointilaitosten yksityiskohtaisemman neuvonnan ja ohjauksen tarpeisiin koottua Liikenne- ja viestintäviraston julkaisemaa arviointilaitosohjetta (Ohje tietoturvallisuuden arviointilaitoksille). Arviointilaitosohjeeseen kootaan Liikenne- ja viestintäviraston neuvonta-, ohjaus- ja valvontatyössä muodostuneet linjaukset lain soveltamisessa.

Arviointilaitoslain 13 §:n mukaan *hyväksytyn tietoturvallisuuden arviointilaitoksen on kaikkia kyseisessä laissa tarkoitettuja tehtäviä hoitaessaan noudatettava myös hallintolakia (434/2003), viranomaisten toiminnan julkisuudesta annettua lakia (621/1999) sekä kielilakia (423/2003)*.

Arviointilaitoslain mukaisesti Liikenne- ja viestintävirasto valvoo hyväksyttyjä arviointilaitoksia. Toimivaltaan voidaan katsoa kuuluvan hallinnon yleislakien noudattamisen ohjauksen ja valvonnan, sillä laitoksen asianmukaiset ohjeet toimintaansa varten kuuluvat 5 §:n mukaan Liikenne- ja viestintäviraston selvitysvastuun piiriin laitoksen hyväksynnässä. Arviointilaitoksen oman tietojenkäsittelyn turvallisuus ja toimitilaturvallisuus kuuluvat myös viraston valvonnan alaan. Liikenne- ja viestintäviraston toimivaltaan tai tiedonsaantioikeuden piiriin arviointilaitoslain nojalla eivät kuulu arviointilaitosten toimeksiantosuhteiden ehdot mukaan lukien hinnoittelu. Valvonta ei siten kata esimerkiksi arviointilaitosten toiminnan markkinaseurantaa. Virastolla ei ole laissa säädettyä oikeutta tiedonsaantiin arviointilaitosten asiakkailta salassapitosäännösten estämättä.

Valvontatehtäviä varten arviointilaitoslain 8 §:ssä on säädetty arviointilaitoksen tiedonanto- ja ilmoitusvelvollisuudesta. Arviointilaitoksen on ilmoitettava Liikenne- ja viestintävirastolle sellaisesta toimintaansa koskevasta muutoksesta, jolla on merkitystä laitosta koskevien velvoitteiden kannalta. Liikenne- ja viestintävirastolla on oikeus pyynnöstä saada arviointilaitokselta ne tiedot, jotka ovat tarpeen sen valvomiseksi, että laitos täyttää toimintaansa koskevat vaatimukset. Ilmoitusvelvollisuuteen liittyvistä menettelyistä ja viraston pyytämistä tiedoista on tarkemmin ohjeistettu arviointilaitosohjeessa. Liikenne- ja viestintävirastolle ei ole säädetty oikeutta saada tietoja tietoturvallisuuden arviointilaitosten asiakkailta tai soteviranomaisilta eikä salassapitosääntelyn estämättä.

Liikenne- ja viestintävirasto valvoo käytännössä tietoturvallisuuden arviointilaitosten toimintaa seuraamalla arviointilaitosten arvioinneistaan säännöllisesti toimittamia raportteja, sekä pyytämällä lisäselvityksiä havaittuaan asian tai saatuaan tiedon, jolla voi olla merkitystä arviointilaitosten toiminnan asianmukaisuuteen tai velvoitteiden noudattamiseen. Liikenne- ja viestintäviraston arviointilaitosten ohjaus- ja neuvontatehtäviin liittyvät käytännössä säännölliset tapaamiset arviointilaitosten kanssa, joihin kutsutaan kaikki hyväksynnän saaneet ja hyväksyntää hakemassa olevat arviointilaitokset. Tällä hetkellä näitä tapaamisia pyritään järjestämään noin neljä kertaa vuodessa. Myös kahdenväliset tapaamiset ovat luonnollisesti mahdollisia tarvittaessa.

Mikäli arviointilaitos toimii tai laiminlyö velvoitteitaan tavalla, joka edellyttäisi arviointilaitoksen toimintaan puuttumista, tulee Liikenne- ja viestintäviraston arviointilain 6 §:n perusteella kehottaa arviointilaitosta korjaamaan puute määräajassa. Mikäli puutetta ei korjata voi Liikenne- ja viestintävirasto peruuttaa arviointilaitoksen hyväksymisen. Hyväksymisen peruuttamiselle on asetettu suhteellisen korkea kynnys, sillä pykälätekstin mukaan arviointilaitoksen tulee toimia olennaisesti tai jatkuvasti säännösten vastaisesti. Hyväksynnän peruuttaminen on mahdollista myös, jos arviointilaitos ei enää täytä hyväksymiselle asetettuja vaatimuksia. Arviointilaitoslain esitöissä (HE 45/2011 vp, s. 14) on viitattu perustuslakivaliokunnan ratkaisukäytäntöön, jonka mukaan valiokunta on katsonut sääntelyn oikeasuhtaisuuden kannalta välttämättömäksi sitoa luvan peruuttamismahdollisuus vakaviin tai olennaisiin rikkomuksiin tai laiminlyönteihin sekä siihen, että luvanhaltijalle mahdollisesti annetut huomautukset tai varoitukset eivät ole johtaneet toiminnassa esiintyneiden puutteiden korjaamiseen.

Hyväksynnän peruuttamista ei voi tehdä erikseen arviointilaitoksen eri pätevyysalueiden osalta, vaan nykyisen sääntelyn perusteella arviointilaitos menettää oikeuden toimia hyväksyttynä tietoturvallisuuden arviointilaitoksena. Ei siis niin että hyväksynnän peruuttaminen koskisi esimerkiksi vain hyväksyntää tehdä asiakastietolain tai toisiolain mukaisia arviointeja, tai että arviointilaitoksen arviointitoimintaa voisi rajoittaa tarvittaessa määräajaksi.

Arviointilaitosten tekemän arviointityön tulisi pitkälle vastata viranomaisen tekemää vastaavaa arviointia. Siksi tulisi kiinnittää huomiota siihen, että hyväksyttyjen arviointilaitosten toimintaan olisi riittävät ja tehokkaat keinot puuttua ongelmatilanteissa ja että säännösten vastaisesta toiminnasta olisi odotettavissa oikeasuhtaiset seuraamukset. Laissa valvonnan toimivaltuudet ovat pistemäiset ja mahdolliset seuraamukset ovat joustamattomat.

Julkisen hallinnon arviointitoiminnan tilannekuva

Arviointilain ja arviointilaitoslain perusteluissa (HE 45/2011 vp) todetaan ohjauksesta valtionhallinnon kannalta seuraavaa: *Tarkoituksena on, että valtionhallinnon tietojärjestelmien ja tietoliikenteen tietoturvallisuuden mahdollisimman tehokkaaksi kehittämiseksi sekä niiden arviointimenettelyn tarkoituksenmukaiseksi toteuttamiseksi Viestintävirasto, valtiovarainministeriö, liikenne- ja viestintäministeriö sekä muut hallinnonalat ovat tiiviissä yhteistyössä. Tässä yhteistyössä voidaan käyttää ja edelleen kehittää jo nykyisin hyvin toimivaa ja kattavaa Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden kehittämis-, ohjaus- ja yhteistyötä. Lisäksi Viestintäviraston tulosohjausta lakiehdotuksen mukaisissa uusissa tehtävissä on tarkoitus toteuttaa valtiovarainministeriön ja liikenne- ja viestintäministeriön tiiviinä yhteistyönä.* Kuvattua ohjausmallia ei ole toteutettu. VAHTI-johtoryhmästä ei nykyisin ole sääntelyä ja se toimii DVV:n asettamana.

Arviointilain 4 §:n 1 momentin 3 kohdan mukaan Liikenne- ja viestintäviraston tehtävänä on *viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden edistämiseksi ja varmistamiseksi tehdä valtiovarainministeriön pyynnöstä selvityksiä valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta*. Säännöksen perustelujen mukaan tämä liittyy tarpeeseen saada yleistä tietoa tietoturvallisuuslainsäädännön täytäntöönpanosta. Näistä selvityksistä säädetään lain 5 §:ssä, jonka mukaan *selvitys voi koskea valtionhallinnon viranomaisten tietojärjestelmien tai tietoliikennejärjestelyjen yleistä tietoturvallisuuden tasoa* ja selvityksen tarkoitus on *valtionhallinnon tietoturvallisuudesta annettujen säännösten täytäntöönpanon seuraaminen ja kehittäminen*. Edelleen 5 §:n mukaan *selvityksen piiriin tulevat tietojärjestelmät voidaan määritellä tietojärjestelmien käyttötarkoituksen, niihin talletettavien tietojen laadun tai muun vastaavan yleisen tekijän mukaan*. Lain perustelujen mukaan *kysymys ei siten olisi yksittäisen tietojärjestelmän valvontaluonteisesta arvioinnista eikä arvioinnissa selvitettäisi tietojärjestelmään talletettuja tietoja tai niiden tallettamisen perusteita*. Arviointilain 6 §:n nojalla Liikenne- ja viestintävirastolla on *oikeus sen estämättä, mitä tietojen salassapidosta säädetään, saada käyttöönsä Viestintäviraston arvioitavana tai selvityksen kohteena olevaa tietojärjestelmää tai tietoliikennejärjestelyjä koskevat tiedot* ja 5 §:n nojalla *virasto voi salassapitosäännösten estämättä sisällyttää valtiovarainministeriölle antamaansa arvioon sellaisia tietoja, jotka ovat välttämättömiä arvioinnin tarkoituksen toteuttamiseksi*.

VALTIONEUVOSTO
STATSRÅDET

Arviointilain 5 §:n mukaisia selvityksiä valtiovarainministeriön toimeksiannosta on toteutettu harvoin. Valtiovarainministeriössä kuitenkin arvioidaan, että jatkossakin on tarve sille, että valtiovarainministeriö voi tehdä selvityspyynnön. Arviointilain 12 §:n mukaan a*sian vireille saattajalta Viestintäviraston arvioinnista, todistuksen antamisesta ja selvityksestä perittävistä maksuista säädetään valtion maksuperustelaissa (150/1992) ja sen nojalla*. Nykyisin valtiovarainministeriö on ohjannut yhteisten palvelujen tuottajia toteuttamaan vaatimustenmukaisuuden arviointeja. Jatkossa voi olla tarve ohjata myös toimialasidonnaisten palvelujen arviointien toteuttamista.

Valtiovarainministeriön työjärjestyksestä annetun valtiovarainministeriön asetuksen (359/2023) 21 §:n 11 kohdan mukaan valtiovarainministeriön tehtäviin kuuluu julkisen hallinnon tietoturvallisuuden yleistä kehittämistä ja valtionhallinnon tietoturvallisuuden ohjausta koskevien asioiden valmistelu. Valtiovarainministeriöllä ei ole käytettävissä otsikkotason tietoja julkisen hallinnon tietojärjestelmien vaatimustenmukaisuuden arvioinneista julkisen hallinnon tietoturvallisuuden yleistä kehittämistä varten.

VALTIONEUVOSTO
STATSRÅDET

6. Kehittämisehdotukset

Keskeiset kehittämisehdotukset priorisoituina ovat:

1) **Parannetaan arviointien saatavuutta ja viranomaisyhteistyötä tarkistamalla viranomaisten arviointitehtäviä.**

2) **Parannetaan salaustuotteiden valmistajien, TEMPEST-tuotteiden valmistajien ja arviointilaitosten elinkeinotoiminnan edellytyksiä.**

3) **Sujuvoitetaan arviointimenettelyjä riskiperusteisesti sekä selkeytetään ja täydennetään arviointiperusteita.**

Arviointitoiminnan termien määrittely tulisi sisällyttää säädösvalmisteluun. Termien määrittelyn ehdotus on liitteenä 2. Arviointi-termiä ehdotetaan yläkäsitteeksi ja sen rinnalla voi tarvittaessa käyttää termiä vaatimustenmukaisuuden arviointi ottaen kuitenkin huomioon termin merkitys eri EU-säädöksissä. Säädöksissä tulee käyttää arviointisääntelyn yleisiä termejä ja verrata niitä esimerkiksi pätevyyslain termeihin ja EU-säädöksiin, kuten kyberturvallisuusasetukseen.

Sääntelyn yhtenäistämiseksi tulisi tarkastella, miltä osin kehittämisehdotukset kuuluvat tiedonhallintayksikön velvoitteina tiedonhallintalakiin tai arviointilakiin ja mitkä riippumatonta arviointitoimintaa koskevina arviointilakiin ja arviointilaitoksia koskevina arviointilaitoslakiin. Kehittämisehdotusten yhteensovittaminen kansainvälisistä turvallisuusvelvoitteista annetun lain ja turvallisuusselvityslain kanssa tulee huomioida. Siten varmistetaan toimintaympäristön muutosten vaatima seuranta ja säännösten säännöllinen ajantasaistaminen sekä kansainvälisten säännösten riittävä huomiointi.

Kehittämisehdotusten tarkempi kuvaus on seuraavissa alaluvuissa.

I Parannetaan arviointien saatavuutta ja viranomaisyhteistyötä

- **Puolustushallintoon voitaisiin säätää itsenäinen ja riippumaton arviointi- ja hyväksyntäviranomainen, jolla olisi toimivalta puolustusvoimien omien järjestelmien osalta, mukaan lukien oikeus hyväksyä edellä mainittuja tietojärjestelmiä kansainvälisten tietoturvallisuusvelvoitteiden perusteella.** Puolustushallinnossa tehdyn selvitysryhmän raportin (Puolustusvoimien tietojärjestelmien ja salausratkaisujen arvioinnin ja hyväksynnän nykytila ja kehittäminen) keskeinen johtopäätös on, että Puolustusvoimien tietojärjestelmien ja salaustuotteiden arviointi- ja hyväksyntätoiminta tulee järjestää niin, että se vastaa merkittävästi lisääntynyttä tarvetta sekä ottaa huomioon Puolustusvoimien toiminnan erityispiirteet. Puolustusvoimilla on jo olemassa sisäiset menettelyt arviointi- ja hyväksymistoimintaan ja erilaisia kyvykkyyksiä, jotka yhdessä toiminnan kehittämisen

kanssa luovat pohjan toimivallasta säätämiselle. Puolustushallinnon sisäisellä arviointi- ja hyväksyntäviranomaisella ja sen riittävällä resursoinnilla voitaisiin vastata lisääntyneisiin arviointitarpeisiin sekä huomioida arviointitoiminnassa sotilaallisen puolustuksen tehtäviin ja tietojenkäsittely-ympäristöön perustuvat erityispiirteet. Puolustushallinnon sisäisen arviointi- ja hyväksyntäviranomaisen toimivalta ja tehtävät olisivat tarkoituksenmukaista rajata Puolustusvoimien omiin tietojärjestelmiin, jotta selkeä tehtävänjako säilyy Liikenne- ja viestintäviraston kanssa ja vältetään päällekkäisyydet.

- *Kohdesäädös:* arviointilaki, laki kansainvälisistä tietoturvallisuusvelvoitteista. Puolustushallinnon arviointiviranomaisen tarkemmasta sijainnista ja organisoinnista voidaan säätää erikseen asetuksella tai puolustushallinnon omassa sääntelyssä.
- *Hallinnollinen ja yritysten taakka:* Puolustusvoimien itsenäinen arviointi- ja hyväksymistoiminta edellyttää merkittävää lisäresursointia. Keventää Liikenne- ja viestintäviraston hallinnollista taakkaa, kun Puolustusvoimat kykenee itse joustavammin arvioimaan ja hyväksymään omat tietojärjestelmät myös kansainväliseen käyttöön. Yritysten taakkaan tällä ei arvioida olevan vaikutuksia.
- *Resurssi-/kustannusvaikutukset:* käsitellään luvussa 7.

- **Valtorille voitaisiin säätää itsenäinen ja riippumaton arviointi- ja hyväksyntäviranomainen, jonka tehtävänä olisi Valtorin palveluiden sekä niihin liitettävien tietojärjestelmien vaatimustenmukaisuuden arviointi.** Valtorin arviointitoimintaa voitaisiin jatkossa hyödyntää käytettävissä olevien resurssien puitteissa laajemminkin yhteisiin tieto- ja viestintäteknisiin palveluihin liitettävien asiakkaiden tietojärjestelmien vaatimustenmukaisuuden arvioinnissa. Arviointilain päivityksen mahdollistaessa Valtorin palveluluetteloon voitaisiin liittää Valtorin maksullinen arviointipalvelu, joka toisi kaivattuja lisäresursseja arviointilaitoksien arviointitoiminnan rinnalle. Tämä palvelu koskisi Valtorin palveluihin liitettävien tietojärjestelmien arviointia. Arviointiviranomaisen organisointi ja asiakasyhteistoiminta järjestettäisiin siten, että arviointitoiminnan riippumattomuus olisi turvattu. Valtori käyttäisi arviointitoiminnassa käytössä olevia viitekehyksiä ja arviointiperusteita kuten Katakri 2020 ja Julkri.
  - *Kohdesäädös:* arviointilaki. Valtorin arviointiviranomaisen tarkemmasta sijainnista ja organisoinnista voidaan säätää erikseen Torilaissa.
  - *Hallinnollinen ja yritysten taakka:* Keventää Valtorin hallinnollista taakkaa, koska tietojärjestelmien vaatimustenmukaisuuden arviointien arvioidaan sujuvoituvan ja toteuttamisen olevan edullisempaa.
  - *Resurssi-/kustannusvaikutukset:* käsitellään luvussa 7.

- Valtionhallinnon yhteisten tieto- ja viestintäteknisten palveluiden **käyttöönotto- ja käyttöpäätösten** tiedonhallintayksiköille aiheutuvan hallinnollisen kuorman vähentämistä tulisi edistää myös säädöksin nykyisin jo hyvin toimivan vapaaehtoisen yhteistyön rinnalle. Esimerkiksi Valtorin asiakkaiden muodostama hyväksyntälautakunta, asiakasneuvottelukunta tai muu jo toimiva yhteistyöryhmä voisi tehdä kunkin yhteisen tieto- ja viestintäteknisen palvelun käyttöönotto- ja käyttöpäätöksen, joka perustuisi vaatimustenmukaisuuden arvioinnin pohjalta tehtyyn jäännösriskiarvioon ja hyväksyntälautakunnan käyttöönottoa ja käyttöä puoltavaan yksimieliseen näkemykseen. Tällöin tiedonhallintayksikkökohtaisista käyttöpäätöksistä voitaisiin luopua. Rekisterinpitäjä tekisi kuitenkin käyttöpäätöksen tietosuoja-asioita koskien. Hyväksyntälautakunnasta säätäminen muuttaisi tiedonhallintalakiin

säädettyä vastuunjakoa ja yksimielisen päätöksen voidaan katsoa tarkoittavan lähes samaa hallinnollista kuormaa isoissa tiedonhallintayksiköissä kuten virastoissa kuin kunkin tiedonhallintayksikön erikseen tekemän päätöksen. Päätös palvelun vaatimustenmukaisuudesta kuitenkin yhtenäistyisi tiedonhallintayksiköiden välillä.

- *Kohdesäädös:* tiedonhallintalaki.
- *Hallinnollinen ja yritysten taakka:* Keventää asiakasorganisaatioiden hallinnollista taakkaa, koska kunkin asiakasorganisaation ei enää tarvitse tehdä erikseen palveluiden käyttöönotto- ja käyttöpäätöksiä.
- *Resurssi-/kustannusvaikutukset:* hallinnollisen taakan keventymisen arvioidaan pienentävän resurssi- ja kustannusvaatimuksia.

- **Liikenne- ja viestintäviraston arviointitehtävien säädettyjä priorisointiperusteita tulisi entisestään tarkentaa** ja kohdentaa tehtäviä selkeämmin kansainvälisen tietoturvallisuusvelvoitteen mukaisesti luokiteltua erityssuojattavaa tietoa ja turvallisuusluokkiin I ja II kuuluvaa tietoa käsittelevien järjestelmien sekä salaustuotteiden ja turvallisuuskriittisten tuotteiden arviointitoimintaan. Priorisoinnissa tulisi huomioida myös arvioinnin *yleinen merkitys tietoturvallisuuden varmistamiseksi julkishallinnossa taikka yhteiskunnan elintärkeiden toimintojen tai erittäin tärkeiden yksityisten etujen suojaamisessa*/suomalaisten turvallisuuskriittisten ja salaustuotteiden tarjonnassa *ja kohteiden yhdenvertainen kohtelu* (kursivoidut ilmaisut lainattu turvallisuusselvityslain 10 §:stä). Viraston **neuvontatehtävä** tietoturvallisuuden arvioinnissa tulisi todeta maksuasetuksen lisäksi myös viraston lakisääteisissä tehtävissä. Virastolle tulisi säätää arviointia tekevien viranomaisten yhteistyössä **koordinoiva** rooli.
  - *Kohdesäädös:* arviointilaki (tehtävät ja priorisointi lain 4 §)
  - *Hallinnollinen ja yritysten taakka:* Priorisointiperusteiden tarkastelun ja tarkentamisen arvioidaan vähentävän hallinnollista ja yritysten taakkaa, kun Liikenne- ja viestintäviraston tehtävät selkeytyisivät.
  - *Resurssi-/kustannusvaikutukset:* Tehtävien sääntelyllä ei nähdä olevan olennaisia resurssi- tai kustannusvaikutuksia, vaan sääntely liittyisi lähinnä olemassa olevien resurssien kohdentamiseen. Arviointi- ja neuvontatehtävät on säädetty maksullisiksi.

- **Säädettäessä arviointi- ja hyväksyntäviranomaisesta on tärkeää organisoida se riippumattomaksi ja itsenäiseksi toimijaksi**, ilman arvioitavan organisaation mahdollisuutta vaikuttaa sen työhön. Viranomaisen kansallisen tai kansainvälisen arviointitehtävän sääntelyssä tulisi huomioida ainakin:
  - Selkeä tehtävän säätäminen ja toimiala ja olisiko tehtävänä tarjota arviointia yleisesti vai tehdä viranomaisen omien järjestelmien arviointia. Huomioitava myös yrityksen mahdollisuus hakea vaatimustenmukaisuuden arviointia viranomaiselta.
  - Työnjako muiden viranomaisten kanssa mm. toimitilojen, henkilöstöturvallisuuden, yritysturvallisuuden ja tietoturvallisuuden teknisten erityisalueiden suhteen.
  - Viranomaisyhteistyö- ja koordinointivelvollisuudet, jotta varmistetaan yhtenäinen soveltaminen muun hallinnon kanssa ja tunnistetaan toisiinsa liittyvät tapaukset.
  - Toisen riippumattoman ja pätevän arviointitahon arvioinnin hyväksi lukeminen.
  - Arvioinnin hallintomenettely, valitusoikeus sekä ohjaus ja valvonta.

- Riippumattomuuden ja pätevyyden varmistamisen menettelyt.
- Tarvittavien resurssien varmistaminen.
    - *Kohdesäädös:* arviointilaki
    - *Hallinnollinen ja yritysten taakka:* Organisoinnin riippumattomaksi ja itsenäiseksi toimijaksi arvioidaan pitkällä tähtäimellä vähentävän hallinollista taakkaa, koska arviointi- ja hyväksyntäviranomaisen suhde muuhun organisaatioon olisi selkeä.
    - *Resurssi-/kustannusvaikutukset:* käsitellään luvussa 7.

- **Viranomaisarviointien resurssien varmistamiseksi säädettäisiin mahdollisuus joustavasti käyttää yksityisiä resursseja tai henkilöitä viranomaisarviointien tukena.** Uudet viranomaisarviointitehtävät edellyttävät toimivallan lisäksi riittäviä resursseja. Osaavien resurssien niukkuuden takia viranomaisten voi olla vaikea saada palkattua henkilöitä suoraan virkatehtäviin. Arviointilaissa tulisi siten mahdollistaa henkilöresurssien hankkiminen yksityisilta markkinoilta. Henkilöresurssien pätevyysvaatimukset olisivat samat kuin arviointiviranomaisilla. Sääntely mahdollistaisi erilaiset tavat hyödyntää yksityisiä henkilöresursseja:
    - Yksityisten henkilöresurssien ostaminen ja hyödyntäminen viranomaisen johdon ja valvonnan alaisuudessa ja virkavastuulla. Toimivat viranomaisen tiloissa ja henkilöturvallisuusselvitys on riittävä.
    - Tietyn rajatun arvioinnin osan kuten järjestelmän tekniset tarkastukset/todentamiset ulkoistaminen yksityiselle toimijalle. Tämä vaatii yritysturvallisuusselvityksen, jos tietoa käsitellään kyseisen yrityksen tiloissa.
        - *Kohdesäädös:* arviointilaki, laki kansainvälisistä tietoturvallisuusvelvoitteista
        - *Hallinnollinen ja yritysten taakka:* Hallinnollisen taakan arvioidaan keventyvän, koska viranomaisten arviointitoiminnassa olisi joustavasti mahdollista käyttää viranomaisiin rekrytoitavan henkilöstön ohella myös yksityisen sektorin toimijoita.
        - *Resurssi-/kustannusvaikutukset:* ei merkittäviä resurssi-/kustannusvaikutuksia.

- Viranomaisten tehokkaan ja tarkoituksenmukaisen toiminnan turvaamiseksi säädettäisiin myös arviointitehtävistä vastaavien **viranomaisten yhteistyöstä ja mahdollisuudesta tehtävien jakamiseen**. Sääntelyn tulisi edistää arviointiresurssien joustavaa käyttöä yhdessä sovittujen priorisointien mukaisesti, yhdenmukaista vaatimusten tulkintaa, osaamisen jakamista, sujuvaa tiedonvaihtoa ja yhteistä tilannekuvaa julkishallinnon arviointitarpeista. Tiedonjako viranomaisten kesken suoritetuista arvioinneista siten että vältetään päällekkäiset arvioinnit.
    - *Kohdesäädös:* arviointilaki, laki kansainvälisistä tietoturvallisuusvelvoitteista
    - *Hallinnollinen ja yritysten taakka:* Hallinnollinen taakka kevenee, koska viranomaisten yhteistoiminnan arvioidaan sujuvoituvan ja arvioinneissa käytettävissä olevan tietopohjan parantuvan sekä päällekkäisten vaatimustenmukaisuuden arviointien vähentyvän.
    - *Resurssi-/kustannusvaikutukset:* ei merkittäviä resurssi-/kustannusvaikutuksia.

- Nykyistä yleispiirteistä sääntelyä kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa ja arviointilaissa tulisi tarkentaa ja samalla ottaa huomioon myös **salaustuotteiden hyväksyntään, TEMPEST-yritysten akkreditointiin, salausteknisen materiaalin jakeluun ja hallintaan sekä**

TEMPEST-mittauksiin liittyvät tehtävät Liikenne- ja viestintävirastossa ja puolustushallinnon arviointiviranomaisessa. Hajasäteilysuojausten arviointien tarkoituksenmukainen resurssointi ja viranomaistehtävien työnjako näyttäisi edellyttävän tarkastelua koko valtionhallinnon tasolla ja mahdollisesti tehtävistä, yhteistyöstä ja kustannusten jakautumisesta säätämistä.

- *Kohdesäädös:* laki kansainvälisistä tietoturvallisuusvelvoitteista, arviointilaki, turvallisuusselvityslaki
- *Hallinnollinen ja yritysten taakka:* Sääntelyn selkeyttämisen voi arvioida vähentävän hallinnollista taakkaa; kansainvälisten tietoturvallisuusvelvoitteiden vuoksi kyseiset toiminnot tulee joka tapauksessa toteuttaa. Yritysvaikutuksia käsitellään jäljempänä.
- *Resurssi-/kustannusvaikutukset:* käsitellään luvussa 7.

II Parannetaan elinkeinotoiminnan edellytyksiä

Salaustuotteet ja turvallisuuskriittiset tuotteet

- **Tuotearvioinnin sääntelykehikon** avulla Suomi voi luoda salaustuote-ekosysteemin pelisäännöt ja varmistua yritysten viranomaistoimintaan kohdistamien oikeutettujen odotusten toteutumisesta ja oikeusvarmuudesta investointeihin kannustavalla tavalla. Sääntely on tarpeen myös viranomaisresurssien tarkoituksenmukaiseksi kohdentamiseksi ja priorisointien mahdollistamiseksi, mikä puolestaan tukee arviointitoiminnan ennakoitavuutta. Viranomaishyväksyntä tarvitaan, jos salaustuotetta on tarkoitus käyttää EU:n tai Naton turvallisuusluokiteltua tietoa käsittelevissä järjestelmissä. Turvallisuusluokitellun tiedon suojaamiseen tarkoitettujen tuotteiden osalta salaustuotehyväksyntä on usein käytännön edellytys kansainvälisille salaustuotteiden markkinoille pääsemiseksi. Toimivaltaisen viranomaisen arviointi- ja hyväksyntäpäätöksillä on siten vaikutuksia yrityksen oikeuksiin ja etuihin ja asiakasviranomaisten mahdollisuuksiin hankkia puolueettomasti arvioituja tuotteita. Valmistajilla tulisikin myös olla mahdollisuus hakea itse arviointia tai hyväksyntää viranomaiselta, mikä ei arviointilain mukaan nykyään ole mahdollista. Salaustuotteiden lisäksi sääntelyssä olisi hyvä huomioida myös muut turvallisuuskriittiset tuotteet (SEP, Security Enforcing Products), joiden arviointia ja hyväksyntöjä edellytetään jo esimerkiksi EU:n ja Naton turvallisuusluokitellun tiedon suojaamiseen liittyvässä sääntelyssä. Muita turvallisuuskriittisiä tuotteita ovat esimerkiksi yhdyskäytävätuotteet sekä TEMPEST-suojaamiseen liittyvät ratkaisut.
- Tuotearvioinnin sääntelyssä tulisi ottaa huomioon, **millä edellytyksin yrityksen salaustuote tai turvallisuuskriittinen tuote voidaan ottaa arvioitavaksi**, miten yrityksen taustat selvitetään ja millä edellytyksillä yritys voi saada tuotteelleen viranomaisen hyväksynnän. Edellytyksissä on hyvä ottaa huomioon valmistuksen alkuperään liittyvät ulkomaiseen vaikuttamiseen liittyvät seikat. Salaustuotteiden ja tarvittaessa muiden turvallisuuskriittisten tuotteiden valmistajien tuotteiden sääntelyssä tulisi edellyttää yritysturvallisuusselvitystä, sillä näillä tuotteilla ja niiden valmistusprosessilla on keskeinen merkitys turvallisuusluokitellun tiedon suojaamisessa. Sääntelyn on mahdollistettava sujuva jatkumo kansallisen turvallisluokitellun tiedon suojaamisen arvioinnista EU:n ja Naton vaatimusten mukaiseen arviointiin. Tuotekehityksessä on kustannustehokkuuden takia voitava ottaa huomioon sekä EU:n että Naton vaatimukset salaustuotteille ja näiden käyttötarkoitusten eriyttämi-

nen vaatimusten edellyttämällä tavalla. Tällöin on huomioitava EU:n ja Naton turvallisuusvaatimuksia kuvaavien dokumenttien turvallisuusluokittelu, joiden käsittely edellyttää, että yritykselle ja sen työntekijöille voidaan myöntää käsittelyoikeudet (FSC/PSC:t) EUn/Naton turvallisuusluokiteltuihin aineistoihin. Viranomaistoiminnan näkökulmasta on tärkeää, että toimivallasta ja tehtävistä on säädetty selkeästi laissa sellaisten tilanteiden varalle, jossa tuotetta ei voida ottaa arvioitavaksi tai sille ei voida myöntää hyväksyntää.

- Sääntelyssä olisi hyvä luoda viranomaiselle tehtävät ja toimivaltuudet, jotta suomalaisten yritysten **akkreditointi** olisi mahdollista **TEMPEST-tuotteiden valmistajiksi**. EU:n ja Naton turvallisuusääntöjen mukaan on kansallisesti mahdollista akkreditoida eli hyväksyä erilaisten TEMPEST-tuotteiden valmistajia tai mittauspalveluita. Akkreditointi edellyttää tiettyjen yleisten standardien mukaista toimintaa ja kykyä tuottaa yksityiskohtaisten TEMPEST-vaatimusten mukaisia tuotteita tai palveluita. TEMPEST-mittausten parissa toimivat viranomaiset arvioivat, ettei tilamittauspalveluiden yritystoiminnalle ole viranomaiskysynnän kannalta edellytyksiä, mutta laite- ja tuotevalmistuksessa yritystoiminta voisi olla mahdollista. TEMPEST-yritysten akkreditointi edellyttäisi turvallisuusääntöjen valossa tavanomaista viranomaishyväksyntää ja -valvontaa merkittävästi tiiviimpää ja operatiivisempaa seurantaa ja ohjausta sekä toiminnan yksityiskohtaisten vaatimusten muutoksia.
- Tuotearvioinnin sääntelykehikolla voitaisiin myös selkiyttää **viranomaisten roolia viranomaisten yhteisissä salaustuotehankinnoissa**, jotta arvioitavat tuotteet vastaavat mahdollisimman hyvin eri viranomaisten tarpeisiin. Tuotteiden valmistuksen edistäminen edellyttää usein asiakasviranomaisen myötävaikutusta ja tiivistä kolmikantayhteistyötä arviointiviranomaisen kanssa.
    - *Kohdesäädös:* arviointilaki
    - *Hallinnollinen ja yritysten taakka:* Tuotearvioinnin sääntelykehikon luominen vähentäisi hallinnon taakkaa, kun tehtävien ja toimivaltuuksien tulkinnanvarainen perusta selkeytyisi. Yritysten taakka vähenisi, sillä selkeä sääntelykehikko helpottaisi niiden toiminnan ja investointien suunnittelua ja viranomaisarvioinnin ennakoitavuutta.
    - *Resurssi-/kustannusvaikutukset:* Sääntelykehikon luominen tukisi sekä viranomaisen että yritysten resurssien suuntaamista itse valmistukseen ja arviointiin, kun reunaehdot ja prosessit olisivat nykyistä selkeämpiä.

Arviointilaitokset

- Arviointilaitoslakia voitaisiin muuttaa siten, että säänneltäisiin **arviointilaitosten vaatimuksia ja pätevyyttä selkeästi ja modulaarisesti**. Tällöin arviointilaitoshyväksynnän ja valvonnan piiriin pääsemisen kynnys madaltuisi nykyisestä ja erilaisia tai tiukempia vaatimuksia edellyttävät pätevyysalueet määriteltäisiin tarkoituksenmukaisina lisäkokonaisuuksina. Arviointilaitosten arvioinnin kohteet ja niiden riskit vaihtelevat merkittävästi ja siksi myös arviointitoiminnan pätevyysvaatimuksia ja pätevyyden hakemus- ja hyväksyntämenettelyjä olisi perusteltua porrastaa. Joustavoittamalla sääntelyä voitaisiin edistää kriteeristöjen saamista tuotantoon nykyistä laajemmin. Tekninen todentamisosaaminen olisi yksi pätevyysalue, jolloin hallinnolliset arvioinnit (kuten ISO/IEC 27001 voi olla) olisivat edelleen mahdollisia ilman teknisen testaamisen pätevyysvaatimusta.
- Pääsääntöisesti FINASin akkreditoimat pätevyysalueet ovat tarkasti kuvattuja ns. yksilöityjä pätevyysalueita (englanniksi fixed scope). Kaikkiin lisäpätevyyksiin ei tarvitsisi hakea FINASin yksilöidyn

pätevyysalueen akkreditointia vaan voitaisiin harkita EU-säädöksistä tuttua selvitystä kyseisen pätevyysalueen arviointikriteeristön antaneelle viranomaiselle, mikä ei sisällä varsinaista pätevyysalueen akkreditointia.

- *Kohdesäädös:* arviointilaitoslaki
- *Hallinnollinen ja yritysten taakka:* Pätevyyden hyväksyntämenettelyjen modularisoiminen ja selkiyttäminen keventäisi yritysten taakkaa.
- *Resurssi-/kustannusvaikutukset:* Yritysten taakan keventyminen alentaisi yritysten kustannuksia.

- Edellytettäisiin turvallisuusselvityslain mukaista **yritysturvallisuusselvitystä** ainakin sellaisten arviointilaitosten hyväksynnässä, jotka hakevat pätevyyttä turvallisuusluokitellun tiedon suojaamisen arviointiin. Valvontaviranomainen on yrityksen omien ilmoitusten varassa, eikä pysty valvomaan esimerkiksi omistuksen siirtymistä ulkomaille. Yritysturvallisuusselvitys toisi yritykset suojelupoliisin seurannan piiriin. Suojelupoliisin seuranta perustuu tehdyn sitoumuksen ilmoitusvelvollisuuksiin sekä yrityksen vastuuhenkilöiden turvallisuusselvitysten nuhteettomuusseurantaan. Omistajuuden seurannasta, vaatimuksista sekä riskien vähentämisen keinoista voitaisiin säätää tarkemminkin. Arviointilaitokselta edellytettäisiin sitä, että se on Suomessa rekisteröity oikeushenkilö.
  - *Kohdesäädös:* arviointilaitoslaki, turvallisuusselvityslaki
  - *Hallinnollinen ja yritysten taakka:* Yritysturvallisuusselvitysten tekeminen voisi jossain määrin lisätä suojelupoliisin hallinnollista taakkaa, mutta keventää hyväksyttyjä arviointilaitoksia käyttävien viranomaisten taakkaa.
  - *Resurssi-/kustannusvaikutukset:* Vaikuttaisi jonkin verran suojelupoliisin resursseihin.

- **Arviointilaitokselle ja sen palveluksessa olevalle arvioitsijalle asetettaisiin nykyistä tarkemmat yksilöidyt vaatimukset**, joita voidaan lakitasoiseen sääntelyyn perustuen valvoa. **Alihankinnan reunaehdoista säädettäisiin**. Alihankintaa ei voisi käyttää osaamispuutteiden kompensoimiseen, vaan työvoiman lisäämiseen. **Valvontatoimivaltuuksia olisi hyvä tarkentaa** ja harkita lakiin lisättäväksi hyväksynnän peruuttamista kevyempiä seuraamuksia.
  - *Kohdesäädös:* arviointilaitoslaki
  - *Hallinnollinen ja yritysten taakka:* yritysten taakan voi arvioida pienenevän, kun vaatimukset, alihankinnan reunaehdot ja valvontatoimivaltuudet olisivat selkeät.
  - *Resurssi-/kustannusvaikutukset:* ei tunnistettuja merkittäviä resurssi- tai kustannusvaikutuksia, sääntelyn selkeyttäminen ja ennustettavuus tehostaa valvontaviranomaisen toimintaa.

- Arviointilaitoksen julkiseen hallintotehtävään kuuluvien **hallinnon yleislakien luetteloa ja soveltamisen laajuutta** olisi tarkasteltava. Laissa tulisi ottaa virkavastuukysymys huomioon. Lisäksi tulisi lainkirjoittajan oppaan ohjeiden (LKO 12.12 Virkavastuu) mukaisesti lisätä viittaus vahingonkorvauslakiin.
- Säännöksen voisi muotoilla esimerkiksi turvallisuusverkkolain 20 §:ää mukaillen seuraavasti: *Arviointilaitoksen palveluksessa olevaan henkilöön sovelletaan rikosoikeudellista virkavastuuta koskevia säännöksiä hänen suorittaessaan arviointiin liittyviä tehtäviä. Vahingonkorvausvastuusta säädetään vahingonkorvauslaissa (412/1974).*
  - *Kohdesäädös:* arviointilaitoslaki

- *Hallinnollinen ja yritysten taakka:* ei vaikutusta.
- *Resurssi-/kustannusvaikutukset:* ei vaikutusta.

- **Eri viranomaisten tehtäviä ja toimivaltaa arviointilaitosten hyväksynnässä ja valvonnassa selkeytettäisiin ja kohdennettaisiin tarkoituksenmukaisesti**. Tällöin voisi olla useampia viranomaisia, joilla olisi oman toimialansa asioissa selkeä ja perusteltu toimivalta päättää arviointilaitoksen pätevyysalueen hyväksynnästä ja suorittaa pätevyysvaatimusten noudattamista koskevaa valvontaa. Liikenne- ja viestintäviraston rinnalle voisi tulla muita vastuuviranomaisia, jotka määrittyisivät sen perusteella, minkä viranomaisen toimivaltaan pätevyyden perusteet muutenkin kuuluisivat. **Tietyn arviointipätevyyden tai -kriteeristön antaneen tai osoittaneen substanssiviranomaisen** (kuten terveyden- ja hyvinvoinnin laitos) **roolia pätevyyden hyväksynnässä, ohjauksessa ja valvonnassa lisättäisiin ja selkiytettäisiin**. Koordinaation turvaamiseksi tähän soveltuvia viranomaisten välisiä **lausunto-, päätös- ja yhteistyömenettelyjä tarkennettaisiin**. Liikenne- ja viestintäviraston ohjaustehtävät arvioinneissa kohdistuisivat kansallisesti ja kansainvälisesti turvallisuusluokitellun tiedon suojaamisen vaatimuksiin, teknisiin todentamismenetelmiin sekä salaustuotteisiin, turvallisuuskriittisiin tuotteisiin ja hajasäteilyyn, joissa virasto voi tukea arviointilaitoksia, sekä arviointilaitoslain puitteissa viranomaisyhteistyön koordinointi.
  - *Kohdesäädös:* arviointilaitoslaki
  - *Hallinnollinen ja yritysten taakka:* Muiden hyväksyntämenettelyjen mahdollistaminen edellyttäisi kullekin pätevyydelle vastuuviranomaista, jonka hallinnollista taakkaa pätevyyden arviointi, hyväksyntä ja valvontaan osallistuminen lisäisi. Liikenne- ja viestintävirastolle modulaarisesta mallista aiheutuisi ainakin jonkin verran kokonaisuuden ja viranomaisyhteistyön koordinointitehtäviä. Yritysten taakan voi arvioida pienenevän, kun kulloinkin vastuullinen viranomainen on selvillä.
  - *Resurssi-/kustannusvaikutukset:* Vaikutus arviointikriteeristöstä vastaavan viranomaisen mahdollisiin lisäresurssitarpeisiin riippuu pätevyyttä hakevien arviointilaitosten määrästä ja siitä, voiko viranomainen käyttää samoja resursseja kuin kriteeristön laatimisessa ja muussa toimialansa ohjauksessa ja valvonnassa.

- Sääntelyn kehittämisessä voitaisiin harkita ja selvittää **arviointilaitosten toiminnan mahdollistamista ainakin RESTRICTED-tasolla** (EU-R ja NR). Arviointilaitosten tehtävä voisi liittyä vain tarkastamiseen tai testaamiseen määriteltäviin pätevyyksiin, SAA-viranomaisen vastuuta hyväksyntälausunnosta ei voi ulkoistaa arviointilaitokselle.
  - *Kohdesäädös:* arviointilaitoslaki ja kansainvälisistä tietoturvallisuusvelvoitteista annettu laki
  - *Hallinnollinen ja yritysten taakka:* Arviointilaitostoimintaa harjoittaville yrityksille tämä edellyttäisi pätevyyden hankkimista ja yritysturvallisuusselvitystä sekä laitosten oman tiedonkäsittelyn akkreditointia, ja tarjoaisi toisaalta liiketoimintamahdollisuuksia. Arviointilaitoksen ja sen tietojenkäsittelyn hyväksyntään liittyvät tehtävät eivät yritysturvallisuusselvitystä lukuun ottamatta juurikaan eroaisi nykyisistä TL IV tai TL III -Katakri-pätevyyteen liittyvistä hallinnollisista tehtävistä.
  - *Resurssi-/kustannusvaikutukset:* EU-R- ja NR-tietoa käsittelevien tietojärjestelmien arviointien tekemiseen saataisiin lisää resursseja, mikä vähentäisi näiden arviointien odotusaikaa ja siten säästäisi kustannuksia.

VALTIONEUVOSTO
STATSRÅDET

III Sujuvoitetaan arviointimenettelyjä

Arviointiprosessi

- Selkiytettäisiin tietohallintalain 13§ velvoitteita tiedonhallintayksiköille **tarkentamalla velvoitetta tietojärjestelmien vaatimustenmukaisuuden arvioinnista** osana tietojenkäsittelyn riskien selvittämistä ja tietoturvallisuustoimenpiteiden mitoittamista. Tiedonhallintayksiköiden tulisi arvioida millä menettelyllä kunkin tietojärjestelmän vaatimustenmukaisuus arvioidaan, kuka on arvioinnin toteuttava toimija ja mitä vaatimuksia ja kriteerejä arvioinnissa käytetään ja miten arvioinneista huolehditaan tietojärjestelmän elinkaaren ajan.
- Sääntelyssä voisi joko tiedonhallintalain 4 luvussa tai arviointilain 3 §:ssä tunnistaa seikkoja, joita viranomaisen tulee punnita harkitessaan vaatimusten arvioinnin menettelyä ja arvioinnin tekijää. Tätä punnitsemista voi luonnehtia myös tietojärjestelmään liittyvien riskien ja valittavaan arviointitahoon ja -tapaan liittyväksi arvioimiseksi.
- Tiedonhallintayksikkö valitsisi arviointimenettelyn riskiperustaisesti. Mahdollisia arviointimenettelyjä olisivat **viranomaisen toteuttama arviointi, hyväksytyn arviointilaitoksen toteuttama arviointi tai itsearviointi**. Arviointimenettelyn valinnassa tulisi huomioida arvioitavassa kohteessa käsiteltävien tietojen luottamuksellisuus-, eheys-, saatavuus-, ja jatkuvuudenhallintavaatimukset sekä tarkoituksenmukaiseen tuotantotapaan kohdistuvat vaatimukset.
- **Kansalliseen turvallisuuteen liittyvien tai turvallisuusluokiteltuja tietoja** käsittelevien tietojärjestelmien arvioinneissa voisi olla velvoite hankkia riippumaton arviointi arviointiviranomaiselta tai hyväksytyltä arviointilaitokselta.
- Selkeytettäisiin arviointilain 3 §:ssä, milloin itsearviointi on mahdollista/suositeltua tai velvoitettua.
    - **Itsearvioinnin** voisi organisaatio tehdä itse tai itsearvioinnin tukena voitaisiin käyttää sopimusperusteisesti kaupallista toimijaa tai organisaation ulkopuolisia osaavia henkilöresursseja tai hyväksyttyä arviointilaitosta.
    - Itsearviointi olisi pääsääntöinen suositeltu tai velvoitettu menettely **salassa pidettävää tai julkista tietoa käsitteleville vähäriskisiksi** arvioiduille tietojärjestelmille. Jos tiedonhallintayksikkö päättää hankkia ulkopuolisen arvioinnin itsearvioinnin sijaan, niin salassa pidettäviä ja julkisia tietoja käsittelevien tietojärjestelmien arvioinneissa voisi käyttää hyväksyttyä arviointilaitosta tai riippumatonta viranomaista.
    - **Salassa pidettäviä ja julkisia tietoja käsittelevien korkeariskisten tietojärjestelmien** arvioinneissa tulisi käyttää hyväksyttyä arviointilaitosta tai riippumatonta viranomaista.
- Sääntelyn olisi oltava viranomaisen kannalta **joustavaa** ja mahdollistettava tapauskohtainen harkinta.
    - Sääntelyn ulottamista ainoastaan **valtion ja hyvinvointialueiden** tiedonhallintayksiköihin harkittaisiin. Kuntien näkökulmasta yksittäisten, laajasti käytettyjen tietojärjestelmien ja niiden toimittajien yhteisarvointien parempaa mahdollistamista edistettäisiin erityisesti kustannusten jakamisen ja arvioinnissa tehtyjen havaintojen jakamisen sääntelyn osalta.
- Taustaksi itsearvioinnin teettämiselle: Yritysten saadessa tietoa viranomaisten järjestelmien turvallisuusjärjestelyistä tulee hankinnan yhteydessä ennakolta varmistua olemassa olevan sääntelyn mukaisesti, että **tietojen salassapidosta ja suojaamisesta huolehditaan** asianmukaisesti. Tarvittaessa turvallisuusselvityslain mahdollistaessa yrityksestä voidaan pyytää yritysturvallisuusselvitys tai

henkilöturvallisuusselvityksiä tai tehdä turvallisuussopimus, jotta tietojärjestelmien turvallisuusjärjestelyihin liittyviä tietoja ei päätyisi toimijoille, joiden turvallisuutta ei ole arvioitu ja joiden toimintaan, yrityskulttuuriin tai esimerkiksi omistuspohjaan liittyy ehkä ennakoimattomiakin riskejä. Tärkeää on varmistua viranomaisten turvallisuusjärjestelyjä koskevien tietojen käsittelyn turvallisuudesta.

- *Kohdesäädös:* arviointilaki, mahdollisesti tiedonhallintalaki, turvallisuusluokitteluasetus
- *Hallinnollinen ja yritysten taakka:* Korkeimpien turvallisuusluokkien tietojärjestelmien vaatimustenmukaisuuden arvioinnit toteutuvat jo nykytilassa vähintään kaupallisten toimijoiden tukemina itsearviointeina, joten kyse ei olisi uusista tehtävistä. Niissä tiedonhallintayksiköissä, joissa ei ole kattavasti arvioitu tietojärjestelmien ja palveluiden vaatimustenmukaisuuden toteutumista hallinnollinen taakka kasvaa, mutta toisaalta arviointien toteuttamisen arvioidaan pienentävän tietoturvallisuuden häiriö- ja poikkeamatilanteiden hallinnan hallinnollista taakkaa ja sitä kautta tietojärjestelmien elinkaarikustannuksia.
- *Resurssi-/kustannusvaikutukset:* ei merkittäviä vaikutuksia. Salassa pidettäviä ja julkisia tietoja käsittelevien tietojärjestelmien ulkopuolisten arviointien teettäminen hyväksytyissä arviointilaitoksissa toisi uusia liiketoimintamahdollisuuksia arviointilaitoksille mutta voi samalla lisätä kustannuksia.

- Korostettaisiin nykyistä selkeämmin tiedonhallintalain 13 §:n mukaista tiedonhallintayksikön vastuuta sekä **riskiperustaista käyttöpäätöksen tekoa** muun muassa jäännösriskiarvion perusteella**.** Selkeytetään sitä, että riippumattoman arvioinnin tehtävä on tuottaa tiedonhallintayksiköllle laadukasta ja luotettavaa tietoa tietojärjestelmän tilasta ja mahdollisista riskeistä, jotta tiedonhallintayksikkö voi tehdä päätöksen tietojärjestelmän käytöstä.
- Huomioidaan kansallisen turvallisuusluokittelun, turvallisuusselvityslain ja kansainvälisten tietoturvallisuusvelvoitteiden vaikutus siihen, kuinka kattava arviointi on tehtävä ja millainen tehtävä arvioinnista annettavalla arviointiraportilla, todistuksella, lausunnolla tai hyväksyntälausunnolla on eri säädösten mukaisissa arvioinneissa eli millainen liikkumavara tiedonhallintayksiköllä on riskipäätöksissään.
- Osana tiedonhallintayksikön vastuun ja arviointitahon roolien selkeyttämistä **harkitaan todistus -instrumentista luopumista** arviointilaissa kansallisen tiedon osalta ja säädetään arvioinnin rajausten ja jäännösriskien sisältymisestä arviointiraporttiin tai hyväksyntälausuntoon. Mahdollinen todistuksen poistaminen *arviointilaitoslaista* edellyttää tarkempaa vaikuttavuuden arviointia muun muassa sote-arviointien kannalta.
  - *Kohdesäädös:* arviointilaki, arviointilaitoslaki, mahdollisesti tiedonhallintalaki
  - *Hallinnollinen ja yritysten taakka:* Keventää hallinnollista taakkaa, koska tietojärjestelmästä vastuussa olevan tahon jäännösriskipäätös mahdollistaisi nykyistä selkeämmin tietojärjestelmien käyttöönoton.
  - *Resurssi-/kustannusvaikutukset:* Hallinnollisen taakan keventymisen arvioidaan pienentävän kustannuksia.

- **Säädettäisiin arviointiin valittavien kriteerien asettamisesta tietojärjestelmäkohtaisesti.** Vaatimukset tulisi tunnistaa jo tietojärjestelmän suunnitteluvaiheesta lähtien**,** jolloin arviointivaiheessa

vältetään ennakoimattomat vaatimukset ja on riittävää todentaa alusta lähtien määriteltyjen vaatimusten toteuttaminen.

- Vaatimuksissa tulisi huomioida mahdolliset säädetyt vaatimukset, yleiset kaikille tietojärjestelmille yhteiset tietoturvallisuuden vähimmäisvaatimukset ja lisäksi tietojärjestelmän käyttötarkoitukseen ja tekniseen toteutukseen liittyvät erityiset uhkat ja riskit huomioivat täydentävät vaatimukset. Kansallisen tiedon käsittelyssä tietojärjestelmien vaatimusten ja arviointikriteerien asettamisessa voidaan hyödyntää käyttötapauksia.
- Tiedonhallintayksiköitä ei edellytettäisi käyttämään tiettyjä vaatimuksia kansallisen arvioinnin hankkimiseksi, vaan ne voisivat edelleen käyttää harkintaansa saatavilla olevien kriteeristöjen ja arviointitahojen puitteissa.
    - *Kohdesäädös:* arviointilaki, mahdollisesti tiedonhallintalaki
    - *Hallinnollinen ja yritysten taakka:* Tietojärjestelmäkohtaisen vaatimusmäärittelyn arvioidaan siirtävän tietojärjestelmän tilaajan ja tarjoajan taakkaa suunnittelun alkuvaiheeseen, mutta puolestaan vähentävän sitä arviointivaiheessa.
    - *Resurssi-/kustannusvaikutukset:* ei merkittäviä vaikutuksia.

- **Arvioinnissa käytettävistä todentamismenetelmistä eli tarkastusmenetelmistä säädettäisiin ylätasolla.** Nämä soveltuisivat samalla myös arviointilaissa arviointiviranomaisen osaamisvaatimuksiksi. Arvioinnissa tulisi käyttää useampaa menetelmää, ellei ole erityistä syytä käyttää vain yhtä menetelmää. Todentamismenetelmiä ovat esimerkiksi haastattelut, dokumentaation tarkastelu, tietojärjestelmien asetusten tarkastelu ja muut erilaiset teknisesti tehtävät havainnoinnit sekä mahdollinen toimitilatarkastelu.
- Arvioinnissa hyödynnettävään dokumentaatioon voi sisältyä myös esimerkiksi sertifikaatteja kuten nykyäänkin. Teknisessä, fyysisessä ja osin hallinnollisessa tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden arvioinnissa huomioidaan siten tuotesertifiointien hyödyntämisen mahdollisuudet siltä osin kuin sertifiointi kattaa viranomaisen turvallisuusvaatimukset.
- Sääntely tarjoaisi välineitä arviointipätevyyden määrittelyyn ja arvioinnin hankintaan sekä edistäisi arviointien tasalaatuisuutta. Sääntely olisi teknologianeutraalia.
- Arviointitoiminnan automatisoitumista edistettäisiin, kun menetelmät kypsyvät.
- Arviointimenettelyistä säätämisen tarkoituksenmukainen säädöstaso tulisi arvioida. Liikenne- ja viestintävirastolle tulisi säätää määräyksenantovaltuus koskien arviointilaitosten toimintaa, jotta tarvittaessa olisi mahdollista tarkentaa vaatimuksia tai menettelyjä ennakoitavasti ja sitovasti kuten vaatimus teknisen todentamisen osaamisesta. Viranomaisella tulisi olla oikeus harkita tarkoituksenmukainen ohjausinstrumentti, joka voi olla myös ohje tai suositus, joka ei ole oikeudellisesti sitova.
    - *Kohdesäädös:* arviointilaitoslaki, arviointilaki
    - *Hallinnollinen ja yritysten taakka:* Keventää hallinnollista ja yritysten taakkaa, koska sääntelyllä olisi mahdollista luoda yhtenäinen työkalupakki, joka tehostaisi arviointilaitosten ohjausta, arviointitoiminnan suunnittelua ja toteuttamista. Itsearvioinneissa useamman todentamismenetelmän käyttäminen voi lisätä hallinnollista taakkaa, jos aikaisemmin itsearvioinneissa on käytetty vain yhtä todentamismenetelmää, mitä ei voi pitää hyvänä käytäntönä.
    - *Resurssi-/kustannusvaikutukset:* hallinnollisen ja yritysten taakan keventymisen arvioidaan pienentävän kustannuksia.

Arviointikriteeristöt

- **Keskeisistä viranomaisten antamien arviointikriteeristöjen vaatimuksista säädettäisiin**. Kullekin arviointikriteeristölle tulisi määritellä vastuutaho eli kriteeristön antava viranomainen sekä kriteeristöön liittyvän ohjeistuksen ja työkalujen ylläpitäjät, selkeärajainen käyttötarkoitus, soveltamiskohde, elinkaari ja suhde muihin kriteeristöihin. Selkeytettäisiin että viranomaiset voivat antaa tai osoittaa arviointikriteeristöjä ja säädettäisiin kriteeristöjä antavien viranomaisten ja kriteeristöjen käyttäjien koordinaatiosta, jotta vältetään tarpeettomat päällekkäisyydet.
- Käyttötapausten koordinointi ja laadunvalvonta olisi vastuutettava.
    - *Kohdesäädös:* arviointilaki
    - *Hallinnollinen ja yritysten taakka:* Keventää hallinnollista ja yritysten taakkaa, koska kansallisissa vaatimustenmukaisuuden arvioinneissa käytettyjen kriteerien arvioidaan selkeytyvän ja siten tehostavan arviointien toteuttamista.
    - *Resurssi-/kustannusvaikutukset:* hallinnollisen ja yritysten taakan keventymisen arvioidaan pienentävän kustannuksia.

Arvioinnin voimassaolo

- Arviointilaissa ja erityisesti arviointilaitoslaissa olisi **selkeytettävä arviointien voimassaolon perusteita, uusimistiheyttä sekä todistusten ylläpitoa ja voimassaoloa koskevia reunaehtoja**. Voimassaolosta voisi säätää esimerkiksi määräaikaisuudesta pääsääntönä sekä määrärajan enimmäispituuden tai seikat, jotka määräajan asettamisessa tulee huomioida. Toimintaympäristö muuttuu nopeasti ja tietojärjestelmät käyvät elinkaarensa aikana läpi useita muutoksia. Arviointi kuvaa vain tietyn ajankohdan tilannetta ja arvioinnin kohteen määrittelystä riippuen tietoturvallisuuden hallintajärjestelmää.
- Voimassaolosta on erityissäännöksiä kansainvälisissä tietoturvallisuusvelvoitteissa tai kansallisissa säädöksissä ja voimassaolo täytyy tarvittaessa voida yhteensovittaa tarkoituksenmukaisesti niihin.
- Voimassaoloon liittyy myös muutostenhallinta ja muutosten arviointi, jos niillä on vaikutusta todistuksen mukaiseen tietoturvallisuuden tasoon. Todistusten ylläpidon sääntelymallissa on kuitenkin huomioitava, että siitä voi aiheutua kustannuksia.
    - *Kohdesäädös:* arviointilaki, arviointilaitoslaki
    - *Hallinnollinen ja yritysten taakka:* Arviointien voimassaolon perusteiden ja uusimistiheyden selkeyttämisen arvioidaan keventävän hallinnollista ja yritysten taakkaa.
    - *Resurssi-/kustannusvaikutukset:* hallinnollisen ja yritysten taakan keventymisen arvioidaan pienentävän kustannuksia.

- Arviointien voimassaolon sääntelyssä huomioitaisiin, että **teknisen tietoturvallisuuden, tilaturvallisuuden ja tietoturvallisuuden hallintajärjestelmän/hallinnollisen arvioinnin voimassaolo voisivat erota toisistaan**. Tilaturvallisuuden ja hallintajärjestelmän riskit eivät välttämättä edellytä yhtä tiheää arviointia kuin teknisen tietoturvallisuuden. Arvioinnin kohteen laajuus olisi mahdollista määritellä tapauskohtaisesti.
    - *Kohdesäädös:* arviointilaki

- *Hallinnollinen ja yritysten taakka:* Keventää hallinnollista ja yritysten taakkaa, koska fyysisten ja hallinnollisten vaatimustenmukaisuuden arviointien arvioidaan vähentyvän.
- *Resurssi-/kustannusvaikutukset:* hallinnollisen ja yritysten taakan keventymisen arvioidaan pienentävän kustannuksia.

Tiedonhallintayksiköiden velvoitteet

- Säännöksillä **tarkennettaisiin tiedonhallintayksikön velvollisuuksia tietojärjestelmien poikkeamien havainnoinnissa ja niihin reagoimisessa** eli jatkuvassa teknisessä seurannassa. Nämä tuottavat jatkuvaa tietoa tietojärjestelmän tietoturvallisuuden tasosta, mikä vähentää tarvetta usein tehtäville ulkopuolisille vaatimustenmukaisuuden arvioinneille. Huomioitava jo lain 4 a luvussa oleva tähän liittyvä sääntely eli tarkennukset sikäli kuin 4 a:ta ei sovelleta. Tiedonhallintalakiin tai kansainvälisistä tietoturvavelvoitteista annettuun lakiin tulisi myös harkita lisättäväksi erityissuojattavan aineiston käsittelyyn liittyvien tietoturvapoikkeamien ilmoitusvelvollisuus NSA:lle niissä tapauksissa, joissa muun muassa Naton turvasäännöt sitä edellyttävät.
  - *Kohdesäädös:* tiedonhallintalaki, kansainvälisistä tietoturvallisuusvelvoitteista annettu laki
  - *Hallinnollinen ja yritysten taakka:* Teknisen seurannan velvoitteiden kasvattaminen voi lisätä niiden tiedonhallintayksiköiden hallinnollista taakkaa, joilla ei vielä ole käytössä teknistä seurantaa. Toisaalta tekninen seuranta vähentää tietoturvapoikkeamista aiheutuvaa työtä. Tekninen seuranta myös keventää hallinnollista taakkaa, koska kansallisten vaatimustenmukaisuuden arviointien vaatiman henkilötyömäärän arvioidaan pienenevän.
  - *Resurssi-/kustannusvaikutukset:* hallinnollisen taakan keventymisen arvioidaan pienentävän kustannuksia.

Tiedonhallintayksiköiden viestintä arvioinneista julkiselle hallinnolle

- Arviointia pyytävä tiedonhallintayksikkö tuottaisi **tiedot arvioinneista otsikkotasolla** yhteiseen pääsyltään rajattuun paikkaan. Otsikkotason tiedot olisivat saatavilla koko julkiselle hallinnolle päällekkäisten arviointien välttämiseksi huomioiden erityisesti hyvinvointialueiden ja kuntien tarpeet. Tämä mahdollistaisi hyvinvointialueille ja kunnille jo toteutettujen arviointien hyödyntämisen mahdollisuuden esimerkiksi palvelujen käyttöönotoissa ja käytössä. Otsikkotasoinen tieto arvioinneista ja soveltuvin osin arviointien tulokset olisivat saatavilla valtiovarainministeriölle.
- Tietoja arvioinneista kirjattaisiin julkisuuslain salassapito- ja vaitiolovelvollisuuksien estämättä muuten paitsi silloin kun niitä koskevat muusta lainsäädännöstä tulevat salassapitovelvoitteet kuten puolustus- ja turvallisuushankinnat sekä kansainvälisistä turvallisuusvelvoitteista annetun lain mukaiset hankkeet.
  - *Kohdesäädös:* arviointilaki, arviointilaitoslaki
  - *Hallinnollinen ja yritysten taakka:* Keventää hallinnollista taakkaa, koska päällekkäisten kansallisten vaatimistenmukaisuuden arviointien arvioidaan vähentyvän.
  - *Resurssi-/kustannusvaikutukset:* hallinnollisen taakan keventymisen arvioidaan pienentävän kustannuksia.

VALTIONEUVOSTO
STATSRÅDET

7. Arviointisäännösten kehittämisen pääasialliset vaikutukset

Arviointilakien ajantasaistamisen voidaan arvioida lisäävän tuottavuutta julkisen hallinnon tietojärjestelmien elinkaarikustannusten kasvun hillitsemisen ja häiriönsietokyvyn parantumisen kautta. Yleisesti arvioidaan, että tietojärjestelmän elinkaaren alusta lähtien toteutettava säännöllinen tietoturvallisuuden ja varautumisen vaatimustenmukaisuuden täyttymisen arviointi todentaa tietojärjestelmän tietoturvakontrollien toimivuuden ja parantaa järjestelmän häiriönsietokykyä ja siten vähentää järjestelmän elinkaarikustannuksia. Häiriösietokyvyn parantumisella tavoitellaan nopeampaa ja parempaa toipumista erilaisista tietoturvaloukkaustilanteista ja mahdollisten tietovuotojen sekä aineellisten ja aineettomien omaisuuksien menetysten minimoimista. Toimintaympäristön muutosten johdosta on vaatimustenmukaisuuden arvioinnin lisäksi esille noussut kasvava tarve arvioida tietojärjestelmien ja tiedon elinkaaren aikaista kyberresilienssiä ja mahdollisuuksia puolustaa tietojärjestelmiä ja tietoa tietoturvaloukkauksia ja –hyökkäyksiä vastaan.

Tietojärjestelmien vaatimustenmukaisuuden hallinnollista ja yritysten taakkaa keventämällä olisi mahdollisuus merkittävästi tehostaa arviointitoimintaa ja kasvattaa sen vaikuttavuutta tieto- ja kyberturvallisuuden varmistamisessa. **Arviointien saatavuuden ja viranomaisyhteistyön parantamiseksi toteutettavien viranomaisten arviointitehtävien tarkistamisen** vaikutuksia hallinnolliseen ja yritysten taakkaan on arvioitu kehittämisehdotusten yhteydessä.

Puolustusvoimille kehittämisehdotus tuo mukanaan merkittäviä muutoksia. Liikenne- ja viestintävirasto on perinteisesti ollut merkittävällä panoksella mukana Puolustusvoimien tietojärjestelmien arvioinnissa ja hyväksymisessä, mikä on korostunut kansainvälisen toiminnan lisääntyessä. Nyt tavoitellun muutoksen seurauksena merkittävä osa näistä arvioinneista ja hyväksynnöistä siirtyy Puolustusvoimille. Muutoksen vaikutus rahoituksessa on alusta alkaen miljoonan euron luokassa vuositasolla ja sen arvioidaan kasvavan yli kaksinkertaiseksi kuluvan vuosikymmenen loppuun mennessä. Itsenäisen arviointikyvykkyyden rakentamisessa Puolustusvoimat tarvitsee vähintään 20 henkilötyövuoden lisäkohdennuksen.

Valtorin arviointiyksikön perustamisen vaikutuksena viraston kustannusten arvioidaan vähenevän, huomioiden myös arviointiyksikön perustamisen kustannukset. Luvussa 1 kuvatusti yhden vaatimustenmukaisuuden arvioinnin hinta on keskimäärin yhteensä 60 000–70 000 euroa/arviointi, joista ulkoisen arvioinnin osuus on keskimäärin 30 000–40 000 euroa. Luvussa 2 todetusti Valtorissa tehdyn laskelman mukaan kahden henkilön rekrytoiminen tekemään tietojärjestelmien tarkastustoimintaa säästää vuositasolla noin 458 000 euroa verrattuna siihen, että palvelut ostettaisiin ulkopuolisilta arviointilaitoksilta. Tämä laskelma ei sisällä mahdollisia Valtorille ja sen asiakkaille tulevia säästöjä siitä, kun arviointitoimintaa saadaan joustavammaksi ja ennakoitavammaksi. Kun riippuvuus ulkopuolisiin arviointilaitoksiin vähenee, niin tietojärjestelmiä on mahdollista saada helpommin ja nopeammin käyttöön. Riskinä voidaan nähdä, että jos Valtori ei pysty järjestämään riittävästi resursseja riippumattomiin arviointitehtäviin, niin nopeutta voidaan hakea heikentämällä laatua, jolloin tietoturvallisuuden arviointien tavoite ei täyttyisi.

VALTIONEUVOSTO
STATSRÅDET

Valtorin arviointitoiminnan kokonaishenkilömäärätarve riippuu Valtorin palvelutarjonnan laajuudesta, arviointipalvelun laajuudesta ja arviointien toteuttamismenettelyistä, sekä tässä raportissa kuvattujen arviointimenettelyjä koskevien kehittämisehdotusten toteuttamisesta. Tavoitetilassa Valtorille arviointitoiminnasta aiheutuvat kustannukset laskevat suhteessa arvioitavien kohteiden määrään.

Viranomaisten näkemyksen ja kokemuksen mukaan tällä hetkellä hyväksytyillä arviointilaitoksilla on niin runsaasti kysyntää arvioinneille, että ne eivät pysty tarjoamaan arviointipalveluja kysyntää vastaavasti. Arviointilaitosten liiketoimintaan ei siten ainakaan nykyisen kaltaisessa tilanteessa olisi juurikaan vaikutusta sillä, että Valtorin tilaukset niiltä vähenisivät. Arviointilaitostoimintaa koskevien kehittämisehdotusten toteuttamisen johdosta on kuitenkin mahdollista, että arviointilaitosten määrä kasvaisi joidenkin vuosien kuluessa. Arviointilaitosten liiketoimintaan kohdistuvia vaikutuksia tulevaisuudessa voidaan arvioida sen perusteella, mitä Valtori on viime vuosina käyttänyt yksityisiin arviointipalveluihin vuosittain. Kolmen vuoden jaksolla elokuusta 2021 elokuuhun 2024 Valtori on teettänyt yhteisten tieto- ja viestintäteknisten palvelujen ja turvallisuusverkon palveluihin 73 todentamista ja keskimäärin niistä on maksettu arviointilaitoksille 35 000 euroa. Yhteensä niihin on käytetty kolmen vuoden ajanjaksolla siis noin 2 600 000 euroa eli vuosittain noin 850 000 euroa. Tämän euromääräisen arvon vähennettynä henkilöstökuluilla ja muilla kuluilla, joita arviointipalvelun tuottamisesta yritykselle koituu, voidaan katsoa olevan vaikutus yritysten liikevoittoon tulevaisuudessa. Tavoitetilassa Valtorilla olisi, kehittämisehdotusten mukaisesti, jatkossakin mahdollisuus joustavasti käyttää yksityisiä resursseja tai henkilöitä tietoturvallisuuden ja varautumisen arviointien tukena.

Vuonna 2023 kahden arviointilaitoksen liikevaihdot olivat yhteensä noin 6 miljoonaa euroa liikevoiton ollessa yhteensä noin 1,8 miljoonaa euroa. Arviointilaitosten edustajilta saadun palautteen perusteella vain osa edellä mainitusta liikevaihdosta perustuisi julkisen hallinnon hankkimiin arviointipalveluihin. Arviointilaitosten palautteessa korostetaan, että arviointimarkkinat ovat pienet. Pääasiassa yritysten tilaamien sote-alan tietojenkäsittelyn tietoturvallisuuden arviointien markkinoiden koko on noin 2 miljoonaa euroa. Sote-toimialalla nähdään tärkeäksi, että arviointilaitoksilla on osaamista ja ymmärrystä myös toimialan tai aihealueen ja siinä toimivien erityyppisten järjestelmien ja organisaatioiden tiedonhallinnan ympäristöstä, yleisestä tilanteesta ja kehittämissuunnista. Vaatimustenvastaisuuden kustannukset ja seuraukset voivat riskien toteutumisen kautta olla myös vakavia paitsi tietosuojanäkökulmasta myös terveydellisesti, esimerkiksi tapaus Vastaamo. Vaatimustenvastaisuuden riskien toteutumisesta olisi kenties hyvä jatkovalmistelussa esittää skenaarioita. Nykyisessä uhkaympäristössä erityisesti vaatimustason yleistä heikentämistä tulisi välttää.

Viranomaisten ja yritysten tilaamien turvallisuusluokiteltujen tietojen käsittelyn tietoturvallisuuden arviointien markkinoiden koko on samoin noin 2 miljoonaa euroa. Tästä Valtorin osuus on noin 850 000 euroa. Puolustusvoimissa on tarvittaessa hankittu turvallisuusluokkien III ja IV tietoja käsittelevien tietojärjestelmien arviointeja ostopalveluina markkinoilta. Arviointilaitosten edustajat ovat ilmaisseet huolensa liiketoimintamahdollisuuksien heikentymisestä Puolustusvoimille ja Valtorille suunnitellun arviointiviranomaistehtävän johdosta. On esitetty arvioita, että jos Puolustusvoimien ja Valtorin tilaukset arviointilaitoksille päättyvät, niin arviointitoiminta ei ole enää houkuttelevaa liiketoimintaa. Toisaalta nämä tilaukset ovat korkeintaan ainoastaan noin kolmasosa koko arviointitoiminnan nykyisistä markkinoista.

Arviointitoiminnan ja -palvelujen kysynnän ennakoidaan edelleen kasvavan tulevaisuudessa toimintaympäristön ja EU-sääntelyn muutosten johdosta. EU-sääntelyn mukainen sertifiointitoiminta myös avaa suomalaisille yrityksille mahdollisuuksia EU:n laajuiseen sertifiointipalvelujen tarjoamiseen. Lisäksi EU-R ja Nato R-luokiteltujen tietojärjestelmien arviointien mahdollistaminen arviointilaitoksille lisäisi arviointilaitosten liiketoimintamahdollisuuksia.

Arviointilaitokset ovat palautteessaan tuoneet esille, että henkilöstön rekrytointi julkisen hallinnon turvallisuusluokiteltujen tietojen käsittelyn tietoturvallisuuden arviointitehtäviin on haastavaa. Suomessa on rajallisesti teknisesti tarpeeksi kyvykkäitä henkilöitä. Työtä ei myöskään pääsääntöisesti voi tehdä etätyönä, mikä laskee sen houkuttelevuutta. Haastavana nähdään myös se, että viranomainen itse arvioisi omaa toimintaansa. Itsenäisen ja riippumattoman toimijan vaatimusten saavuttaminen ei välttämättä ole myöskään mahdollista toimijalle, joka itse tuottaa tieto- ja viestintäteknisiä palveluita, joita julkinen hallinto on velvoitettu käyttämään.

Liikenne- ja viestintäviraston tehtävien sääntelyllä ei pääosin nähdä olevan olennaisia resurssi- tai kustannusvaikutuksia, vaan sääntely liittyisi lähinnä olemassa olevien resurssien kohdentamiseen. Viraston arviointi- ja neuvontatehtävät on säädetty maksullisiksi. Viranomaisarvioinneille säädettäväksi ehdotetulla mahdollisuudella käyttää joustavasti yksityisiä resursseja tai henkilöitä viranomaisarviointien tukena ei katsota olevan merkittäviä kustannusvaikutuksia. Myöskään viranomaisten yhteistyöllä ja mahdollisuudella tehtävien jakamiseen ei katsota olevan kustannusvaikutuksia.

Liikenne- ja viestintäviraston ja puolustushallinnon arviointiviranomaisen tehtävät salaustuotteiden hyväksyntään, TEMPEST-yritysten akkreditointiin, salausteknisen materiaalin jakeluun ja hallintaan sekä TEMPEST-mittauksiin katsotaan välttämättömiksi toteuttaa kansainvälisten tietoturvallisuusvelvoitteiden johdosta. Toimivaltaisten viranomaisten kannalta salausteknisen materiaalin hallinnan sääntelystä ei aiheudu resurssi- tai kustannusvaikutuksia, vaan mahdolliset vaikutukset seuraavat operatiivisten tarpeiden kasvusta. Samoin TEMPEST- vyöhyke- ja tilamittauksiin liittyisi nähtävissä oleviin operatiivisiin tarpeisiin vastaamiseksi viranomaisten arvion mukaan vähäistä henkilöresurssien lisäystä. Etenkin salaustuotteiden arviointiin, TEMPEST-laitemittauksiin ja TEMPEST-yritysten akkreditointiin liittyy vaikutuksia, joita olisi arvioitava tarkemmin.

Myöskään salaustuotearviointeihin ja TEMPEST-laitteiden arviointeihin liittyvät resurssitarpeet eivät aiheudu sääntelyn luomisesta ja selkeyttämisestä, vaan siitä, kuinka vahvaa panostusta arviointien nopeuttamiseen ja sujuvuuteen tavoitellaan suomalaisen teollisuuden tukemiseksi tai viranomaisten arviointitarpeisiin vastaamiseksi. Tehtäviin liittyy yleisesti ottaen laboratorio- ja henkilöresurssien tarve, jonka taso riippuu myös valittavista toteutusmalleista. AQUA-kyvykkyys edellyttäisi myös vastavuoroisia suoritteita toisten jäsenvaltioiden tuotteille. TEMPEST-yritysten akkreditointi olisi puolestaan kokonaan uusi tehtävä, joka edellyttäisi hyväksyntä- ja valvontaprosessien määrittelyä ja toteuttamista. TEMPEST-kyvykkyyksillä voi olla liityntä myös salaus- ja turvallisuuskriittisten tuotteiden arviointiin.

Salaustuotteiden valmistajien, TEMPEST-tuotteiden valmistajien ja arviointilaitosten elinkeinotoiminnan edellytysten parantamisen ennakoitavalla sääntelyllä on arvioitu vähentävän yritysten hallinnollista taakkaa ja useimmissa kehittämisehdotuksissa myös keventävän hallinnollista taakkaa ja parantavan

liiketoimintamahdollisuuksia. Samoin arviointilaitosten toiminnan mahdollistamisen ainakin RESTRICTED-tasolla (EU-R ja NR) arvioidaan tuovan arviointilaitoksille lisää liiketoimintamahdollisuuksia. Yritysten ja hallinnollisen taakan keventymisen johdosta kehittämisehdotusten arvioidaan myös pääsääntöisesti pienentävän kustannuksia.

Arviointimenettelyjen riskiperusteista sujuvoittamista sekä arviointiperusteiden selkeyttämistä ja täydentämistä koskevien kehittämisehdotusten on arvioitu keventävän hallinnollista taakkaa ja useimpien ehdotusten myös yritysten taakkaa. Kehittämisehdotusten resurssi-/kustannusvaikutuksia on arvioitu kehittämisehdotuskohtaisesti. Kehittämisehdotusten on arvioitu olevan joko kustannusneutraaleja tai vähentävän kustannuksia. Kehittämisehdotusten lähtökohtana on arviointimenettelyjen ja niissä käytettävien vaatimusten ja arviointikriteeristöjen selkiyttäminen huomioiden riskiperustaisuus. Tavoitteena ei ole kansallisin toimenpitein vaatia tietojärjestelmien tuottajilta nykyistä tukevampia tietoturvatoimenpiteitä vaan selkiyttää vaatimuksia ja kohdentaa niitä riskiperustaisesti.

Kunnissa toteutettavan vaatimustenmukaisuuden arvioinnin nykytilaa ei tunneta tarkasti, joten kunnille kehittämisehdotuksista mahdollisesti aiheutuvan uuden hallinnollisen taakan tai kustannusten arvioinnissa on epävarmuutta. Toisaalta kansallista salassa pidettävää ja julkista tietoa käsittelevien tietojärjestelmien vaatimustenmukaisuuden arviointimenettely on tarkoitus säätää valittavaksi riskiperustaisesti, jolloin itsearviointi tai tuettu itsearviointi muodostuisi kunnissa pääsääntöiseksi arviointimenettelyksi. Mahdollistava ja kuntien erityispiirteet huomioiva uusi arviointitoimintaan liittyvä lainsäädäntö voisi tukea kuntien tietoturvatyötä ja niiden tietoturvallisuuden tason nostamista kustannustehokkaalla tavalla.

VALTIONEUVOSTO
STATSRÅDET

Lähdeaineisto

Asiakirjat

Digi- ja väestötietovirasto (2024) Digitaalisen turvallisuuden riskienhallintaopas.

Liikenne- ja viestintävirasto (2022) Liikenne- ja viestintäviraston (Traficom) valtiovarainministeriölle laatima muistio arviointilaitostoiminnan kehittämisen sääntelystä 18.11.2022.

Liikenne- ja viestintävirasto (2022) Ohje tietoturvallisuuden arviointilaitoksille (Ohje 210/2022 O)

Puolustushallinto (2024) TLIV Puolustusvoimien tietojärjestelmien ja salausratkaisujen arvioinnin ja hyväksynnän nykytila ja kehittäminen.

Tiedonhallintalautakunta (VM 2022:4) Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa.

Tiedonhallintalautakunta (VM 2024:19) Suositus tietoturvallisuuden vähimmäisvaatimuksista.

Valtioneuvosto (2021) Valtioneuvoston periaatepäätös 10.6.2021 tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla (Titukri).

Valtioneuvoston kanslia (2024:11) Suomen kyberturvallisuusstrategia 2024–2035.

Valtiovarainministeriö (2021) Selvitys digitaalisen turvallisuuden kansainvälisestä arviointilainsäädännöstä.

Valtiovarainministeriö (2021) Selvitys digitaalisen turvallisuuden arviointitoiminnan nykytilasta ja kehitystarpeista.

Valtiovarainministeriö (2021:54) Arviomuistio julkisen hallinnon tietojärjestelmien sääntelyn nykytilasta ja kehittämistarpeista.

Valtiovarainministeriö (2023:54) Riskienhallinnan käsikirja valtionhallinnon toimijoille.

Lait

Kielilaki (423/2003)

Laki julkisen hallinnon tiedonhallinnasta (906/2019) (tiedonhallintalaki)

Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) (turvallisuusverkkolaki)

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

Laki oikeudenkäynnistä hallintoasioissa (808/2019)

Laki sosiaali- ja terveydenhuollon asiakastietojen käsittelystä (703/2023) (asiakastietolaki)

Laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) (toisiolaki)

Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)

Laki tietoturvallisuuden arviointilaitoksista (1405/2011) (arviointilaitoslaki)

Laki vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta (920/2005)

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013) (Torilaki)

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) (arviointilaki)

Turvallisuusselvityslaki (726/2014)

Laki Euroopan unionin edun vuoksi vaihdettujen turvallisuusluokiteltujen tietojen suojaamisesta neuvostossa kokoontuneiden Euroopan unionin jäsenvaltioiden välillä tehdyn sopimuksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta (SopS 76/2015)

Laki tietoturvallisuudesta Pohjois-Atlantin sopimuksen osapuolten välillä tehdystä sopimuksesta ja turvallisuussäännöistä (907/2023, SopS 55/2024)

Security within the North Atlantic Treaty Organization (Naton asiakirja C-M(2002)49-REV1)

Asetukset

Liikenne- ja viestintäministeriön asetus Liikenne ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista (1190/2023)

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) (turvallisuusluokitteluasetus)

Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014)

VALTIONEUVOSTO
STATSRÅDET

Valtioneuvoston asetus julkisen hallinnon turvallisuusverkkotoiminnasta (1109/2015) (turvallisuusverkko-asetus)

Valtiovarainministeriön asetus valtiovarainministeriön työjärjestyksestä (359/2023)

EU-säädökset

Neuvoston päätös, annettu 23 päivänä syyskuuta 2013, EU:n turvallisuusluokiteltujen tietojen suojaamista koskevista turvallisuussäännöistä (2013/488/EU)

Euroopan parlamentin ja neuvoston direktiivi 2014/53/EU, annettu 16 päivänä huhtikuuta 2014, radiolaitteiden asettamista saataville markkinoilla koskevan jäsenvaltioiden lainsäädännön yhdenmukaistamisesta ja direktiivin 1999/5/EY kumoamisesta

Euroopan parlamentin ja neuvoston asetus (EU) N:o 910/2014, annettu 23 päivänä heinäkuuta 2014, sähköisestä tunnistamisesta ja sähköisiin transaktioihin liittyvistä luottamuspalveluista sisämarkkinoilla ja direktiivin 1999/93/EY kumoamisesta ja Euroopan parlamentin ja neuvoston asetus (EU) 2024/1183, annettu 11 päivänä huhtikuuta 2024, asetuksen (EU) N:o 910/2014 muuttamisesta eurooppalaisen digitaalisen identiteetin kehyksen vahvistamisen osalta (eIDAS-asetus)

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

Euroopan parlamentin ja neuvoston asetus (EU) 2017/745, annettu 5 päivänä huhtikuuta 2017, lääkinnällisistä laitteista, direktiivin 2001/83/EY, asetuksen (EY) N:o 178/2002 ja asetuksen (EY) N:o 1223/2009 muuttamisesta sekä neuvoston direktiivien 90/385/ETY ja 93/42/ETY kumoamisesta

Euroopan parlamentin ja neuvoston asetus (EU) 2019/881, annettu 17 päivänä huhtikuuta 2019, Euroopan unionin kyberturvallisuusvirasto ENISAsta ja tieto- ja viestintätekniikan kyberturvallisuussertifioinnista sekä asetuksen (EU) N:o 526/2013 kumoamisesta (kyberturvallisuusasetus)

Komission delegoitu asetus (EU) 2022/30, annettu 29 päivänä lokakuuta 2021, Euroopan parlamentin ja neuvoston direktiivin 2014/53/EU täydentämisestä sen 3 artiklan 3 kohdan d, e ja f alakohdassa tarkoitettujen olennaisten vaatimusten soveltamisen osalta.

Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555, annettu 14 päivänä joulukuuta 2022, toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (NIS2-direktiivi)

VALTIONEUVOSTO
STATSRÅDET

Komission täytäntöönpanoasetus (EU) 2024/482, annettu 31 päivänä tammikuuta 2024, Euroopan parlamentin ja neuvoston asetuksen (EU) 2019/881 soveltamissäännöistä siltä osin kuin on kyse yhteisiin kriteereihin perustuvan eurooppalaisen kyberturvallisuuden sertifiointijärjestelmän (EUCC) hyväksymisestä.

Euroopan parlamentin ja neuvoston asetus (EU) 2024/2847, annettu 23 päivänä lokakuuta 2024, digitaalisia elementtejä sisältävien tuotteiden horisontaalisista kyberturvallisuusvaatimuksista ja asetusten (EU) n:o 168/2013 ja (EU) 2019/1020 ja direktiivin (EU) 2020/1828 muuttamisesta (kyberkestävyyssäädös CRA)

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös)

VALTIONEUVOSTO
STATSRÅDET

Liite 1 Työryhmän ja sihteeristön jäsenet

Tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän jäsenet:

- tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö, puheenjohtaja
- neuvotteleva virkamies Mika Kuronen, valtiovarainministeriö, varapuheenjohtaja
- toimialajohtaja Max Hamberg, valtioneuvoston kanslia, varajäsen johtava asiantuntija Jan Seuri
- tietoturvatarkastaja Mika Pullinen, ulkoministeriö
- lakimies Ville Salmi, ulkoministeriö, Kansallinen turvallisuusviranomainen
- johtava asiantuntija Kimmo Janhunen, oikeusministeriö
- turvallisuuspäällikkö Kari Santalahti, sisäministeriö, varajäsen johtava asiantuntija Ismo Parviainen
- neuvotteleva virkamies Jukka-Pekka Virtanen, puolustusministeriö
- johtava tietohallintoasiantuntija Mika Tuikkanen, maa- ja metsätalousministeriö, varajäsen erityisasiantuntija Hanna Majurinen, 2. varajäsen erityisasiantuntija Ari Mannonen
- valtion kyberturvallisuusjohtaja Rauli Paananen, liikenne- ja viestintäministeriö
- erityisasiantuntija Lars Dolk, liikenne- ja viestintäministeriö, varajäsen hallitusneuvos Mari Starck 23.11.2024 alkaen
- erityisasiantuntija Teemupekka Virtanen, sosiaali- ja terveysministeriö
- johtava asiantuntija Tanja Karvonen, työ- ja elinkeinoministeriö, varajäsen erityisasiantuntija Kimmo Kuusela
- IT-erityisasiantuntija Lauri Karppinen, Tietosuojavaltuutetun toimisto
- yksikönpäällikkö Sonja Marjamäki-Ruuskanen, Valtion tieto- ja viestintätekniikkakeskus Valtori, varajäsen ryhmäpäällikkö Mika Raappana, 2. varajäsen johtava asiantuntija Jyrki Siivola
- erityisasiantuntija Riina Seulasaari, Digi- ja väestötietovirasto, 23.11.2024 saakka
- riskienhallintapäällikkö Pekka Ristimäki, Digi- ja väestötietovirasto, 23.11.2024 alkaen
- johtava asiantuntija Anne Lohtander, Liikenne- ja viestintävirasto, varajäsen osastopäällikkö Johanna Erkkilä 16.9.2024 alkaen
- osastoinsinööri Tuomas Munnukka, Puolustusvoimat, varajäsen everstiluutnantti Kimmo Tarvainen
- erityisasiantuntija Hanna Menna, Hyvinvointialueyhtiö Hyvil Oy, varajäsen erityisasiantuntija Marjo Orava
- erityisasiantuntija Martti Setälä, Kuntaliitto

Tietojärjestelmien vaatimustenmukaisuuden arvioinnin ajantasaistamisen ja tehostamisen työryhmän sihteeristön jäsenet:

- tietohallintoneuvos Tuija Kuusisto, valtiovarainministeriö, puheenjohtaja
- neuvotteleva virkamies Mika Kuronen, valtiovarainministeriö, varapuheenjohtaja
- hankeassistentti Eeli Pakkala, valtiovarainministeriö, 30.11.2024 saakka
- hankeassistentti Katariina Rantala, valtiovarainministeriö, 11.12. alkaen

- erityisasiantuntija Lars Dolk, liikenne- ja viestintäministeriö
- hallitussihteeri Tuomas Hyvärinen, puolustusministeriö
- erityisasiantuntija Anna-Minna Lukkala, sisäministeriö, varajäsen erityisasiantuntija Ella Karvonen 12.6.2024 saakka
- lakimies Jussi Rissanen ja johtava asiantuntija Anne Lohtander, Liikenne- ja viestintävirasto
- tekninen tietoturvajohtaja Pasi Koljonen, Puolustusvoimat
- yksikönpäällikkö Sonja Marjamäki-Ruuskanen, Valtion tieto- ja viestintätekniikkakeskus Valtori
- erityisasiantuntija Hanna Heikkinen, Digi- ja väestötietovirasto.

Työryhmän ja sihteeristön työtä ovat tukeneet neuvotteleva virkamies Niko Mäkilä, lainsäädäntöneuvos Eeva Lantto, tietohallintoneuvos Isamaria Mäkinen, neuvotteleva virkamies Emilia Laitala, erityisasiantuntija Laura Kolinen, neuvotteleva virkamies Santtu Viiman ja korkeakouluharjoittelija Tomas Juutinen valtiovarainministeriöstä.

Liite 2 Käsitteet, termit ja lyhenteet

Ohessa on kuvattu keskeisiä tietojärjestelmien vaatimustenmukaisuuden arviointiin liittyviä käsitteitä ja määritelmiä. Tässä raportissa arvioinnilla on tarkoitettu vaatimustenmukaisuuden arviointia. Raportissa termiä *auditointi* on käytetty termin vaatimustenmukaisuuden arviointi synonyyminä.

Akkreditointi. Termillä voidaan tarkoittaa a) arviointilaitoksen tai sen pätevyysalueen hyväksyntää tai b) arvioitavan järjestelmän hyväksyntää.

1. *'akkreditoinnilla' tarkoitetaan kansallisen akkreditointielimen antamaa todistusta siitä, että vaatimustenmukaisuuden arviointilaitos täyttää tiettyä vaatimustenmukaisuuden arviointia koskevat, yhdenmukaistetuilla standardeilla vahvistetut vaatimukset, ja tarvittaessa muut vaatimukset, mukaan luettuna ne, jotka on vahvistettu asiaa koskevissa alakohtaisissa ohjelmissa;* ((EY) N:o 765/2008 2 artiklan 10 alakohta).

2. "*Arviointielimen pätevyyden toteamista yhdenmukaisten kansainvälisten tai eurooppalaisten arviointiperusteiden mukaisesti*" (laki vaatimustenmukaisuuden arviointipalvelujen pätevyyden toteamisesta 920/2005, 4 §).

3. Kansainvälisistä tietoturvallisuusvelvoitteista annetun lain (588/2014) mukaisten kansainvälisiin tietoturvallisuusvaatimuksiin liittyvien menettelyjen yhteydessä termillä akkreditointi tarkoitetaan esimerkiksi tietojärjestelmän vaatimustenmukaisuuden arvioinnin perusteella tehtävää hyväksyntää.

AQUA-viranomainen. Appropriately Qualified Authority -viranomainen. EU:n jäsenvaltion asianmukaisesti pätevä viranomainen. Sen on oltava jäsenvaltion salauslaitteiden hyväksyntäviranomainen, joka on neuvoston vahvistamin perustein hyväksytty suorittamaan EU:n turvallisuusluokiteltujen tietojen suojaamiseen tarkoitettujen salaustuotteiden toinen arviointi.

Arviointi. Yleiskäsite, joka voi tarkoittaa esimerkiksi vaatimustenmukaisuuden arviointia, auditointia tai sertifiointia.

Auditointi. Riippumaton selvitys siitä, täyttääkö auditoitava kohde sille asetetut vaatimukset.

CISA. Certified Information Systems Auditor. IASACAn (ks. alempaa) yksityishenkilöille myöntämä sertifiointi IT-järjestelmien auditointiin.

Crypto Approval Authority (CAA). Salauslaitteiden hyväksyntäviranomainen. Vastaa sen varmistamisesta, että salaustuotteet ovat kansallisten tai Euroopan unionin neuvoston salausperiaatteiden mukaisia.

Hyväksyy salaustuotteen, jolla EU:n turvallisuusluokitellut tiedot suojataan määrättyyn turvallisuusluokkaan asti tuotteen käyttöympäristössä. Jäsenvaltioiden osalta salauslaitteiden hyväksyntäviranomainen vastaa lisäksi salaustuotteiden arvioinnista.

Crypto Distribution Authority (CDA) / National Distribution Authority (NDA). Vastaa kansainvälisen salausteknisen materiaalin jakeluverkon hallinnasta Suomessa.

General Security Agreement (GSA). Kansainvälinen tietoturvallisuussopimus.

Hyväksytty arviointilaitos. Liikenne- ja viestintäviraston hyväksymä tietoturvallisuuden arviointilaitos (arviointilaitoslaki 5 §).

Ilmoitettu laitos. (Notified Body). Suomen viranomaisen nimeämä ja Euroopan komissiolle ilmoitettu Suomeen sijoittautunut laitos, jonka tehtävänä on tarjota tuotteiden vaatimustenmukaisuuden arviointipalveluja sovellettaessa unionin yhdenmukaistamislainsäädäntöön perustuvaa kansallista lainsäädäntöä. (Laki eräitä tuoteryhmiä koskevista ilmoitetuista laitoksista 278/2016). Vaatimustenmukaisuuden arviointilaitos, joka on nimetty 43 artiklan ja unionin muun asiaankuuluvan yhdenmukaistamislainsäädännön mukaisesti (kyberkestävyyssäädös)

ISACA. Kansainvälinen, hyvän tiedonhallintatavan kehittämiseen keskittynyt yhdistys. Myöntää mm. CISA-sertifikaatteja (ks. ylempää)

ITSEF (Information Technology Security Evaluation Facility). Tietotekniikan turvallisuuden arviointilaitos, joka on asetuksen (EY) N:o 765/2008 2 artiklan 13 kohdassa määritelty vaatimustenmukaisuuden arviointilaitos ja joka suorittaa arviointitehtäviä (komission täytäntöönpanoasetus EUCC-sertifiointijärjestelmän hyväksymisestä)

Julkri. Tiedonhallintalautakunnan suositus Julkisen hallinnon tietoturvallisuuden arviointikriteeristöstä (Julkri): Suositus ja kriteeristö (VM 2022:43 ja päivitys VM 2023:46) sekä Julkriin perustuva suositus tietoturvallisuudesta hankinnoissa (VM 2023:57).

Katakri. Kansallinen turvallisuusauditointikriteeristö Katakri. NSA:n julkaisu Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille sekä Katakri 2020 – Liite IV: Naton turvallisuusluokitellun tiedon suojaaminen.

Käyttötapaus. Käyttötapaus arvioinneissa sisältää tiedon arvioinnin tilaajasta eli siitä kuka on valinnut käyttötapaukseen sisällytetyt kriteerit tai kuka käyttää (aikaisemmin määritettyä) kriteeristöä; mikä on arviointimenettely eli miten valittuja kriteereitä tai kriteeristöä käytetään, esimerkiksi itsearviointiin; sekä minkä tavoitteen saavuttamiseksi valittuja kriteerejä tai kriteeristöä käytetään, esimerkiksi a) salassa pidettävien ja turvallisuusluokkaa IV olevien tietojen käsittely pilvipalvelussa ja turvallisuusluokkaa III olevien tietojen käsittely on-premise tai b) esimerkiksi riittävä varmuus kohteen soveltuvuudesta TL III -tiedon suojaamiseksi.

LACP. List of Approved Cryptographic Products. EU:n turvallisuusluokitellun tiedon käsittelyyn hyväksyttyjen salaustuotteiden lista.

National CIS-Security Authority (NCSA, CIS, Communications and Information System). Naton turvallisuussäännöstön mukainen kansallinen viestintä- ja tietojärjestelmien turvallisuusviranomainen.

National TEMPEST Authority (NTA). TEMPEST-viranomainen. Vastaa siitä, että viestintä- ja tietojärjestelmät ovat TEMPEST-periaatteiden ja -suuntaviivojen mukaisia. Hyväksyy TEMPEST-vastatoimet laitteistoille ja tuotteille, joilla EU:n tai Naton turvallisuusluokitellut tiedot suojataan määrättyyn turvallisuusluokkaan asti tuotteen käyttöympäristössä.

OWASP. Open Worldwide Application Security Project. Voittoa tavoittelematon järjestö, joka julkaisee muun ohessa järjestelmien tietoturvallisuuteen liittyviä asiakirjoja ja ohjeita.

Pitukri. Pilvipalveluiden turvallisuuden arviointikriteeristö Pitukri. Traficomin julkaisuja 13/2020.

Security Accreditation Authority (SAA). Turvallisuusjärjestelyjen hyväksyntäviranomainen. Vastaa viestintä- ja tietojärjestelmien turvallisuusjärjestelyjen arvioinnista ja hyväksynnästä. Varmistaa, että järjestelmä noudattaa turvallisuusperiaatteita ja suuntaviivoja sekä antaa lausunnon järjestelmän hyväksymisestä. Määrittelee turvallisuushyväksyntästrategian ja tarkistaa turvatoimien täytäntöönpanon.

Sertifiointi. Arviointikohteen vaatimustenmukaisuuden vahvistaminen, usein akkreditoinnin synonyymi (perustuu SFS standardiin). Prosessi, jossa tietty tuote, palvelu tai prosessi arvioidaan ja todetaan noudattavan tiettyjä turvallisuusvaatimuksia joko eurooppalaisella tai kansallisella tasolla, ja joka voi johtaa eurooppalaiseen kyberturvallisuussertifikaattiin (perustuu kyberturvallisuusasetukseen (CSA).

Second Party Evaluation (SPE). AQUA-viranomaisen (ks. ylempää) tekemä ulkopuolinen arviointi. Edellytys salaustuotteiden hyväksymiselle EU:ssa.

System-specific Security Requirements Statement (SSRS). EU:n turvallisuusluokiteltua tietoa käsittelevän järjestelmän pohjalta laadittu asiakirja, josta selviää, mitä järjestelmältä edellytetään ollakseen tietoturvallinen omaan käyttötarkoitukseensa.

TEMPEST. Telecommunications Electronics Material Protected from Emanating Spurious Transmissions. Vaarantavaan hajasäteilyyn kohdistuvat tarkastukset, tutkimukset, kontrollointi, tiedustelu-uhkaa vastaan suoritettavat vastatoimet ja vaarantavaa hajasäteilyä vaimentavat toimet.

Tietoturvallisuus. Tietoaineistojen saatavuus, eheys ja luottamuksellisuus sekä niiden varmistaminen hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä.

Todentaminen. Valtorilla on käytössä ylätason terminä todentaminen. Tämä jakautuu Valtorin asiantuntijoiden itse suorittamaan katselmointiin, arviointilaitoksen suorittamaan arviointiin ja ulkoisen tahon suorittamaan tarkastukseen.

Todistus. Liikenne- ja viestintäviraston pyynnöstä antama hallintopäätös arviointiperusteeksi otetut tietoturvallisuutta koskevat vaatimukset täyttävästä tietojärjestelmästä tai tietoliikennejärjestelystä (arviointilaki 7 § ja 8 §). Hyväksytyn arviointilaitoksen selvityksen ja tarkastuksen perusteella antama todistus siitä, että arvioitavan kohteen toimitilat ja toiminta ovat selvityksen perustana olleiden arviointiperusteiden mukaiset (arviointilaitoslaki 9 §). Hyväksytyn arviointilaitoksen tietoturvallisuuden arviointia koskeva todistus, jonka arviointilaitos antaa, jos tietojärjestelmä tai hyvinvointisovellus täyttää tietoturvallisuutta koskevat olennaiset vaatimukset (asiakastietolaki 87 §). Hyväksytyn arviointilaitoksen arviointia koskeva todistus, jos käyttöympäristö täyttää sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain mukaiset tietoturvallisuusvaatimukset (toisiolaki 26 §).

Vaatimustenmukaisuuden arviointi. Tietojärjestelmän katselmointi tai todentaminen, jonka perusteella todetaan, täyttääkö kohde säädetyt vaatimukset. Vaatimustenmukaisuuden arviointi toteutetaan säädettyjä vaatimuksia vastaan itsearviointina tai viranomaistehtävänä tai sen voi toteuttaa hyväksytty arviointilaitos. Vaatimustenmukaisuuden arviointi voi olla arviointilain tarkoittama arviointi. EU:n kyberturvallisuusasetuksen mukaan vaatimustenmukaisuuden arvioinnilla tarkoitetaan prosessia sen arvioimiseksi, ovatko tuotteelle, prosessille, palvelulle, järjestelmälle, henkilölle tai elimelle asetetut määritellyt vaatimukset täyttyneet. Lain 920/2005 mukaan vaatimustenmukaisuuden arviointi tarkoittaa akkreditointia, testausta, kalibrointia, sertifiointia, tarkastusta ja niihin rinnastettavaa toimintaa. Lähteet: vrt. CSA artikla 2 kohta 17) ’vaatimustenmukaisuuden arvioinnilla’ asetuksen (EY) N:o 765/2008 2 artiklan 12 alakohdassa määriteltyä vaatimustenmukaisuuden arviointia; → (EY) N:o 765/2008 2 artiklan 12) ’vaatimustenmukaisuuden arvioinnilla’ tarkoitetaan prosessia sen arvioimiseksi, ovatko tuotteelle, prosessille, palvelulle, järjestelmälle, henkilölle tai elimelle asetetut määritellyt vaatimukset täyttyneet; Vrt. laki 920/2005 1) vaatimustenmukaisuuden arviointi akkreditointia, testausta, kalibrointia, sertifiointia, tarkastusta ja niihin rinnastettavaa toimintaa.

Vaatimuksenmukaisuuden arviointilaitos (Conformity Assessment Body). Asetuksen (EY) N:o 765/2008 2 artiklan 13 alakohdassa määritelty vaatimustenmukaisuuden arviointilaitos (kyberturvallisuusasetus, eIDAS-asetus, kyberkestävyyssäädös). Taho, joka suorittaa kolmantena osapuolena vaatimustenmukaisuuden arviointitoimia, kuten testausta, sertifiointia ja tarkastuksia (tekoälysäädös). Elin, joka suorittaa vaatimustenmukaisuuden arviointitoimia kuten kalibrointia, testausta, sertifiointia ja tarkastuksia (asetus EY N:o 765/2008 2 artiklan kohta 13).