VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma Haukka 2020-2023

Digitaalisen turvallisuuden arvioinnin nykytila ja kehittämisehdotukset -selvitys

Tuija Kuusisto
4.5.2021

VM:n asettama Haukka säädösvalmistelun koordinaatioryhmä - tehtävät

Selvitysraportti nykytilasta ja kehittämistarpeista

Toimikausi 1.9.2020 – 31.12.2021

1) Digitaalisen turvallisuuden arvioinnin menettelyjen ja rakenteiden kehittämistarpeiden selvittämisen tukeminen
2) Julkisen hallinnon digitaalisten palveluiden ja infrastruktuurin varautumisen ja valmiuden vaatimuksiin ja niiden arvioinnin menettelyjen ja rakenteiden kehittämistarpeiden selvittämisen tukeminen
3) Selvitystehtäviin liittyvien säädösten kuten lain viranomaisten tietojärjestelmien (1405/20119 ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011) mahdollisten uudistamistarpeiden selvittämisen tukeminen
4) Selvitysten perusteella tehtyihin johtopäätöksiin perustuvan mahdollisen säädösvalmistelun tukeminen

Haukka – säädösvalmistelun koordinaatioryhmä - jäsenet

- Niko Mäkilä VM
- Tuija Kuusisto VM
- Eeva Lantto VM
- Mika Tuikkanen VM
- Ari Uusikartano UM
- Taina Riihinen OM
- Kimmo Janhunen OM
- Kari Santalahti SM
- Harri Mäntylä PLM
- Sami Aalto OKM
- Laura Niemi OKM
- Jaana Merta MMM
- Erica Karppinen LVM
- Rauli Paananen LVM
- Teemupekka Virtanen STM
- Roni Kiviharju YM
- Tomi Marjamäki YM
- Ville Autero TEM
- Risto Suominen FINAS
- Jari Ylikoski Kuntaliitto
- Kari Nykänen Oulu
- Seppo Ruotsalainen Kuopio
- Tomi Kelo Traficom
- Johanna Erkkilä Traficom
- Mikko Pitkänen DVV
- Pia Satopää PV
- Petri Hakonen PV
- Jonna Ylikauppila Kela
- Pertti Nieminen Kela

Digitaalisen turvallisuuden nykytila ja kehittämisehdotukset selvitys - lausuntokierros

- Lausuntoaika 9.2. - 23.3.2021, asiakirjan päivitetty versio julkaistu lausuntopalvelussa 19.2.2021
- Lausuntoja 23 kpl
- Lausujat:
  - Innovaatiorahoituskeskus Business Finland
  - Turun kaupunki
  - Rajavartiolaitos
  - Imatran kaupunki
  - Suomen Erillisverkot Oy
  - Espoon kaupunki
  - sisäministeriö
  - valtiovarainministeriö
  - Valtion tieto- ja viestintätekniikkakeskus Valtori
  - Lääkealan turvallisuus- ja kehittämiskeskus Fimea
  - Geologian tutkimuskeskus
  - oikeusministeriö
  - Liikenne- ja viestintävirasto Traficom
  - Digi- ja väestötietovirasto
  - ulkoministeriö
  - KEHA-keskus
  - puolustusministeriö
  - työ- ja elinkeinoministeriö
  - Kuusamon kaupunki
  - sosiaali- ja terveysministeriö
  - Kansaneläkelaitos
  - Suomen Kuntaliitto ry
  - Liikenne- ja viestintäministeriö

Raportin työstämisestä

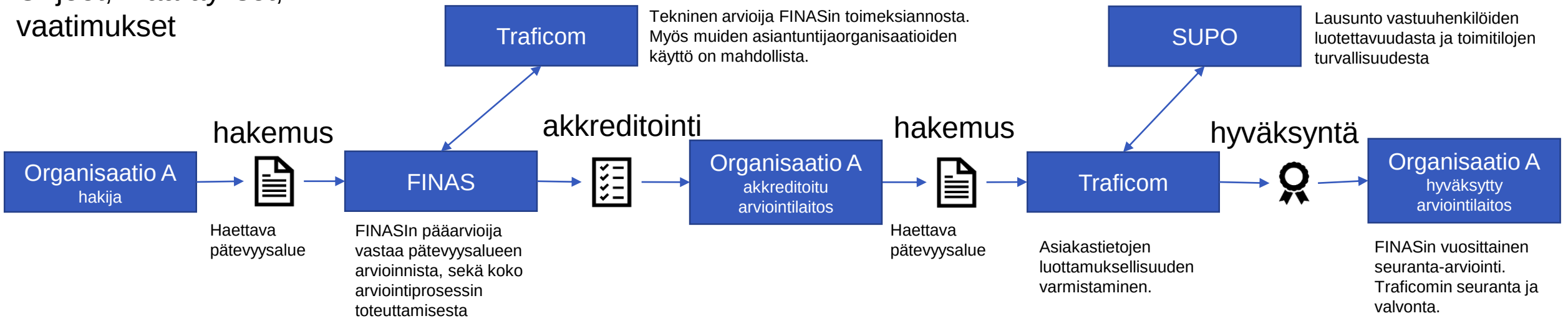
- VM:n, Traficomin ja FINASin yhteinen pienryhmä on tarkentanut arviointilaitoksen hyväksyntäprosessin, arviointitoiminnan ja resurssien nykytilakuvauksia
- Digitaalisen turvallisuuden arvioinnin nykytila- ja kehittämistarpeet - raporttia on muokattu lausuntopalautteen perusteella
- Raportti julkaistaan ja se tulee Julkisen hallinnon tietojärjestelmiä koskevan yleislainsäädännön tarkistamista valmistelevalle työryhmälle käyttöön

Tietoturvallisuuden arviointilaitoksen hyväksyntä

ISO/IEC 17021-1
ISO/IEC 27006

Arviointilaitosohje 210/2016 O (V8.2)
Katakri

Ohjeet, määräykset, vaatimukset



Keskeinen lainsäädäntö

920/2005 5 §
1405/2011 3 §

1405/2011 10 §

920/2005 6 §
1405/2011 5.1 § 1-3 k

920/2005 7 §

1405/2011 4 §
1405/2011 5.1 § 4-5 k
1405/2011 7 §
159/2007 19 j §

1405/2011 5.3 §

920/2005 8 §
1405/2011 6-8 §§
1405/2011 13 a §

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tietoturvallisuuden kansallinen arviointi (Traficom)

Traficomin ohje (3.9.2019)

Traficomin ohje (3.9.2019)
Katakri

Ohjeet, määräykset, vaatimukset

Nykytilan kuvauksessa on keskitytty kansallisiin arviointeihin. Kansainvälisistä tietoturvavelvotteista johtuvia tehtäviä ei ole kuvattu.

Keskeinen lainsäädäntö

906/2019 13 §
1406/2011 1-4 §§
1109/2015 9-10 §§

1406/2011 7 §

1406/2011 4 - 6 §§

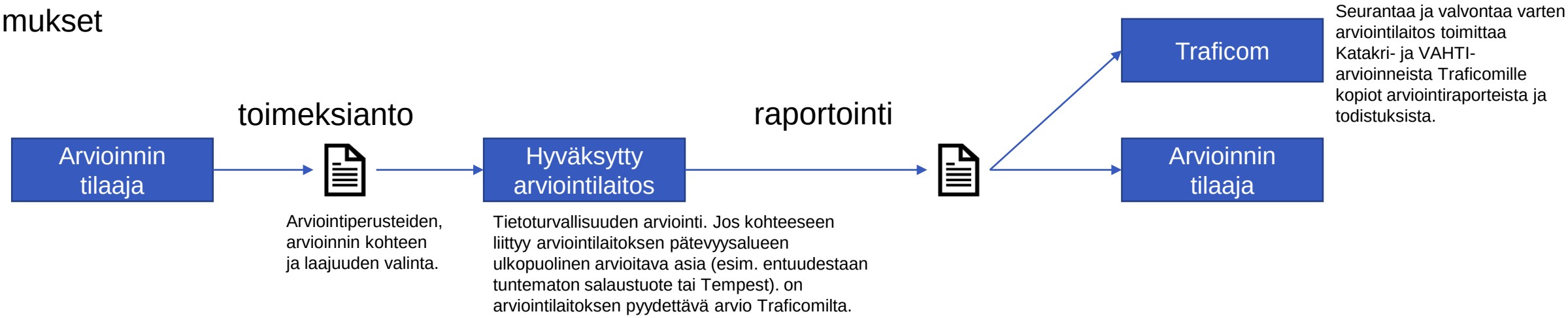
1406/2011 9-10 §§

Tietoturvallisuuden arviointi (arviointilaitos)

Arviointilaitokselle hyväksytty pätevyysalue
Arviointilaitosohje 210/2016 O (V8.2)

Arviointilaitosohje 210/2016 O (V8.2)

Ohjeet, määräykset, vaatimukset



Keskeinen lainsäädäntö

906/2019 13 §
1406/2011 2-3 §
159/2007 19 k §
552/2019 26 §
1109/2015 9-10 §§

1405/2011 10 §
1406/2011 8 a §

1405/2011 9.1 - 9.2 §
1405/2011 10 §

1405/2011 9.3 §
159/2007 19 k §
552/2019 26.2 §

1405/2011 6-8 §§
159/2007 19 g §
552/2019 29 §

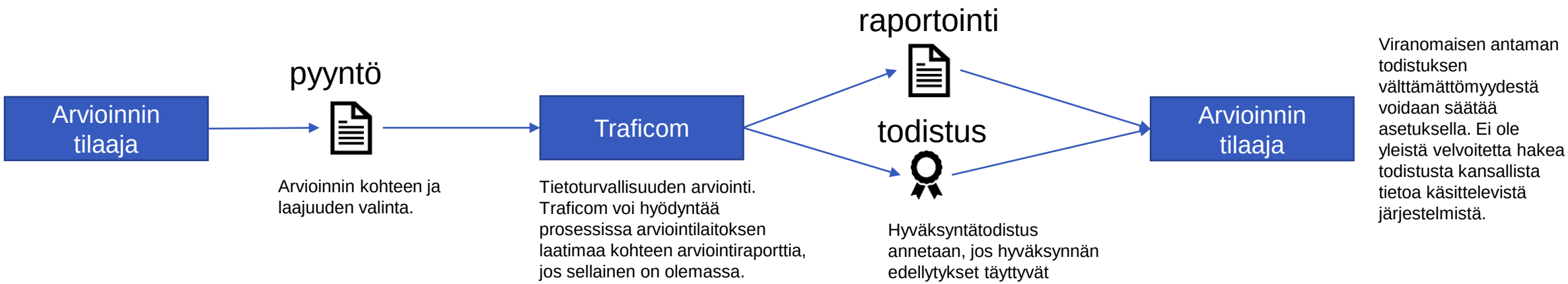
Tietoturvallisuuden kansallinen hyväksyntä (Traficom)

Traficomin ohje (3.9.2019)

Traficomin ohje (3.9.2019)
Katakri

Ohjeet, määräykset, vaatimukset

Nykytilan kuvauksessa on keskitytty kansallisiin arviointeihin. Kansainvälisistä tietoturvavelvotteista johtuvia tehtäviä ei ole kuvattu.



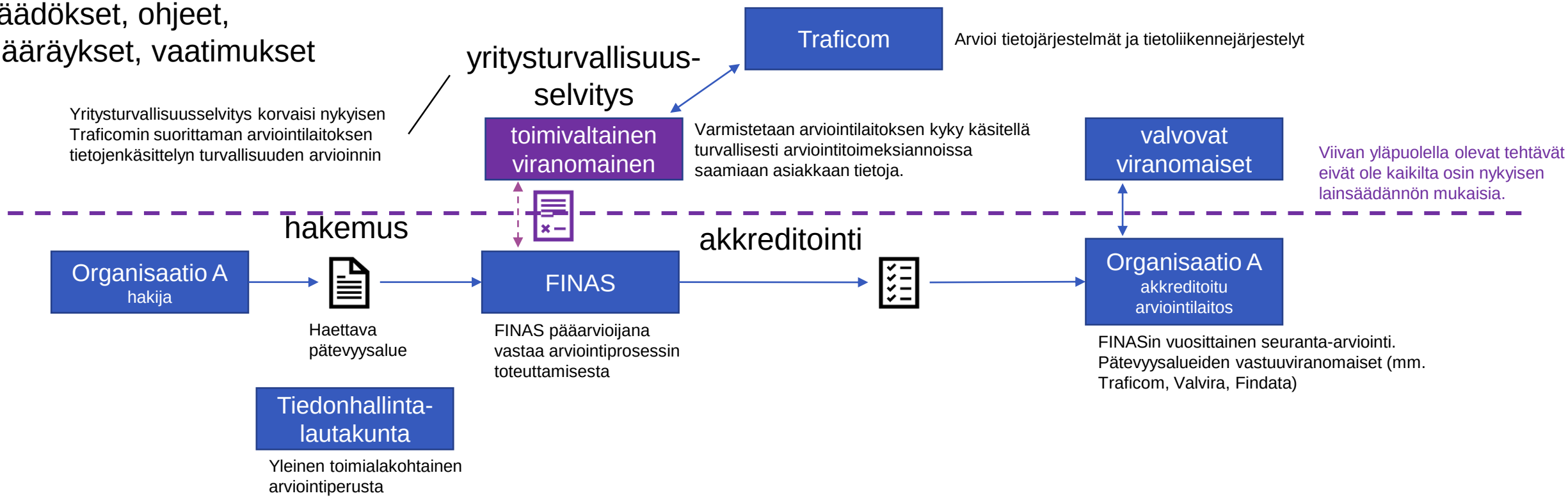
Keskeinen lainsäädäntö

906/2019 13 § 1406/2011 1-4 §§ 1406/2011 8 a § 1109/2015 10 §	1406/2011 4-7 §§ 726/2014 9 §	1406/2011 8 §	1406/2011 9-10 §§

Tietoturvallisuuden arviointilaitoksen hyväksyntä, tavoitetila

ISO/IEC 17021-1
ISO/IEC 27006
726/2014 5 luku

Säädökset, ohjeet, määräykset, vaatimukset



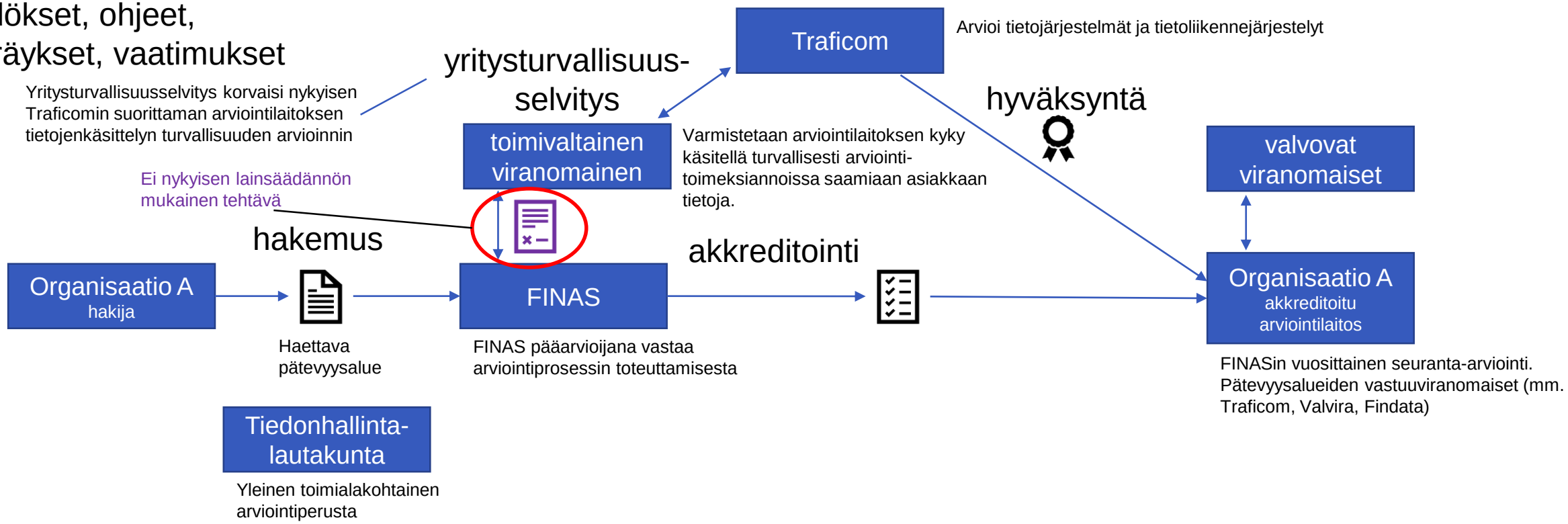
Menettely, kun haettava pätevyysalue kattaa julkisia tai salassa pidettäviä, luokittelemattomia tietojen käsittelevät tietojärjestelmät ja tietoliikennejärjestelyt

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tietoturvallisuuden arviointilaitoksen hyväksyntä, tavoitetila

ISO/IEC 17021-1
ISO/IEC 27006
726/2014 5 luku

Säädökset, ohjeet, määräykset, vaatimukset



Menettely, kun haettava pätevyysalue kattaa <u>turvaluokiteltujen tai kansalliseen turvallisuuteen</u> liittyviä tietoja käsittelevät tietojärjestelmät ja tietoliikennejärjestelyt

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kehittämisehdotukset 1

- Digitaalisen turvallisuuden näkökulmasta tärkeimmät toiminnan jatkuvuuden ja varautumisen vaatimukset sisällytettäisiin tiedonhallintaa koskeviin säädöksiin.
- Arviointeja laajennettaisiin tietoturvallisuuden arvioinnista myös toiminnan jatkuvuuden ja varautumisen arvioitiin. Arviointien nopeuttamiseksi ja resurssien käytön tehostamiseksi julkista tai luokittelematonta sekä salassa pidettävää tietoa käsittelevien palvelujen arviointien tulisi olla pääasiallisesti akkreditoitujen kaupallisten arviointilaitosten tehtävänä. Tämän vuoksi on tarpeen varmistaa, että kansallisen akkreditointiyksikkö FINAS arvioi tietoturvallisuuden lisäksi myös toiminnan jatkuvuuden ja varautumisen arviointilaitosten pätevyyksiä määrävälein. FINAS voisi kuten nykyisinkin käyttää muita viranomaisia akkreditointiprosessissa käytettävien toimialakohtaisten vaatimusten määrityksessä ja pätevyyden arvioinnissa.
- FINAS päättäessään akkreditoitavien arviointilaitosten toimialakohtaisista arviointiperusteista kuulisi Tiedonhallintalautakuntaa yleisten tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen vähimmäisvaatimuksista.
- FINAS akkreditoisi kaupallisia tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitoksia hakijan hakemuksessa esittämille pätevyysalueille. Mahdolliset kilpailuoikeudelliset syyt erottaa kaupallisten arviointilaitosten ja viranomaisten arviointitehtävien pätevyysalueet selvitettäisiin.

Kehittämisehdotukset 2

- FINAS ylläpitäisi kuvausta mahdollisista arviointilaitosten pätevyysalueista. Pätevyysalueet voivat kattaa turvallisuusluokitteluasetuksen turvallisuusluokan IV ja III sekä salassa pidettäviä ja julkisia tietoja käsittelevien järjestelmien tietoteknisen turvallisuuden arvioinnin, arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen ja henkilöstöturvallisuus) arvioinnin sekä korkeintaan turvallisuusluokan TL III toiminnan jatkuvuuden ja varautumisen järjestelyjen arvioinnin.
- Säädettäisiin, että arviointilaitoksen akkreditointi- ja hyväksyntäprosessin osana arviointilaitoksesta toteutettaisiin turvallisuusselvityslain (726/2014) mukainen yritysturvallisuusselvitys, jolla mm. varmistettaisiin arviointilaitoksen kyvykkyys asiakkaiden tietojen käsittelyssä kuten salassa pidettävien tietojen suojaamisessa. Yritysturvallisuusselvitys korvaisi nykyisen Traficomin suorittaman arviointilaitoksen tietojenkäsittelyn turvallisuuden arvioinnin. Turvallisuusselvityslain mukaisesti jatkossakin henkilöturvallisuusselvityksen ja yritysturvallisuusselvityksen tekemisestä päättää suojelupoliisi, jollei turvallisuusselvityksen laatimisesta päätä pääesikunta. Liikenne- ja viestintävirasto laatii yritysturvallisuusselvityksen osana tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden tasoa koskevan selvityksen.
- Julkisia tai salassa pidettäviä tietoja käsittelevien palvelujen arviointilaitosten hyväksyntäprosessia yksinkertaistettaisiin ja nopeutettaisiin keventämällä tilaturvallisuusvaatimuksia ja tiedon suojaamiskyvyn vaatimuksia. Selvitettäisiin, että voitaisiinko erityisesti julkisia tai salassa pidettäviä tietoja käsittelevien palvelujen arviointilaitoksiksi hakevien osalta poistaa Arviointilain (1405/2011) 5§:n 1 mom. 5 kohdan vaatimus vaarantamatta arviointitoiminnan laadukkuutta.
- Traficomille säädettäisiin tehtäviksi tietoturvallisuuden lisäksi myös toiminnan jatkuvuuden ja varautumisen arviointi. Traficom on ehdottanut, että Traficomin arvioinnit sisältäisivät arvioitavaan tietojärjestelmään liittyvän turvallisuusjohtamisen (hallinnollinen ja henkilöstöturvallisuus) ja tietoteknisen turvallisuuden arvioinnin: salaustuotteet (CAA), tietojärjestelmät sekä tietoliikennejärjestelyt (SAA).

Kehittämisehdotukset 3

- Säädettäisiin valtiovarainministeriön ja liikenne- ja viestintäministeriön tiiviinä yhteistyönä toteuttamasta Traficomin arviointilaitosten akkreditointiin ja hyväksyntään sekä arviointitoimintaan liittyvästä ohjausmallista.
- Tiedonhallintayksikön ja sen itselleen tilaaman fyysisen turvallisuuden arvioinnista liittyen tietoturvallisuuden tai toiminnan jatkuvuuden tai varautumisen arviointiin säädettäisiin kansallisella tasolla, esimerkiksi Suojelupoliisin tehtäväksi.
- Puolustusvoimat on ehdottanut, että lakiin 1406/2011 säädettäisiin myös puolustusvoimat toimivaltaiseksi viranomaiseksi viranomaisarviointiin vastuualueenaan maanpuolustukseen liittyvä TL IV – TL I turvallisuusluokan tietotekninen arviointi: salaustuotteet (CAA), tietojärjestelmät sekä tietoliikennejärjestelyt (SAA). Toimivalta kattaisi edellä mainittujen kokonaisuuksien auditoinnin (arvioinnin) ja hyväksynnän (akkreditoinnin). Tämä edellyttäisi muutoksia myös turvallisuusselvityslakiin.
- Puolustusvoimat on ehdottanut, että puolustusvoimille säädettäisiin tehtäviksi tietoturvallisuuden lisäksi myös toiminnan jatkuvuuden ja varautumisen arviointi maanpuolustukseen liittyvien TL IV – TL I turvallisuusluokan salaustuotteiden, tietojärjestelmien sekä tietoliikennejärjestelyiden osalta.
- Sääntelyssä vahvennettaisiin tiedonhallintalailla tiedonhallintayksiköille asetettuja vaatimuksia ja asetettaisiin selkeä vaatimus sekä tiedonhallintayksikön toteuttamille itsearvioinneille että ulkopuolisille arvioinneille. Vaatimus ulkopuolisen arvioinnin tai todistuksen hankkimisesta säädettäisiin velvoittavaksi riskiarvioinnin perusteella niin, että se koskisi kriittisimpiä järjestelmiä ja toimintoja sekä korkeimpien turvallisuusluokkien järjestelmiä. Tässä yhteydessä arvioitaisiin vahvennetun sääntelyn kustannusvaikutuksia, joita on kuvattu myös tässä asiakirjassa. Säännöksissä ja ohjeistuksessa tulisi huomioida myös itsearviointi sekä kevyempi, konsultoiva tietojärjestelmien tarkastus, jonka voisi suorittaa muukin kuin akkreditoitu arviointilaitos.

Kehittämisehdotukset 4

- Säädettäisiin selkeämmin arviointien tilaamisesta, mm. yhteishankintayksiköiden ja yhteisten palvelujen osalta. Viranomaiset ja yhteisöt voisivat tilata arviointeja tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen akkreditoiduilta arviointilaitoksilta niiden pätevyysalueilta ja niiden määrittämillä kustannuksilla. Toimeksiannon yhteydessä tilaaja määrittäisi arvioinnin kohteen ja arviointiperustan tai arviointiperusta määräytyy säädösten perusteella. Vaatimustenmukaisuustodistus kuitenkin myönnettäisiin kuten nykyisinkin ainoastaan käytettäessä pätevyysalueen mukaista arviointiperustaa (esimerkiksi tiedonhallintalautakunnan antama kriteeristö tai Katakri).
- Säädettäisiin, että arviointitehtävää hoitavan viranomaisen ja arviointilaitoksen tulisi ilmoittaa tilaajalle arvio tai tarjous arvioinnin kestosta ja kustannuksista kuukauden kuluessa arvioinnin tai arviointitarjouksen pyytämisestä siinä määritettyä arvioinnin kohdetta vastaavasti.
- Tiedonhallintalautakunta valmistelisi julkisen hallinnon tietoturvallisuuden arviointikriteeristön ottaen huomioon myös toiminnan varautumisen ja jatkuvuudenhallinnan asettamat vaatimukset.
- Tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen vaatimustenmukaisuuden arvioinnin tilaajan olisi osoitettava säännöllisillä seuranta-arvioinneilla palvelun turvallisuuden tason ylläpitäminen ja parantaminen. Tähän liittyvistä seuranta- ja valvontamenettelyistä säädettäisiin ainakin tiedonhallintalain soveltamisalan osalta.
- Säädetään, että tiedonhallintayksiköt, mahdollisesti yhteistoiminnassa, arvioisivat tieto- ja viestintäteknisten palveluita tuottavien alihankkijoidensa tietoturvaa koskevia vastuita ja velvoitteita. Lähtökohtana on, että kriittisille palveluille asetetaan palvelukohtaisesti turvallisuus- ja toimintavarmuusvaatimukset ja palvelujen vaatimuksenmukaisuus arvioidaan hyväksytyn arviointityökalun kriteerien mukaisesti arviointityökalun määräytyessä kunkin palvelun luonteen perusteella (esim. Tiedonhallintalaissa (906/2019) säädetyt vaatimukset, ISO 27001, Katakri TL IV -tason vaatimukset).
- Kaupallisten tietoturvallisuuden, toiminnan jatkuvuuden ja varautumisen arviointilaitosten valvonnan sääntelyä kehitettäisiin siten, että kyseisen pätevyysalueen valvontaan osallistuisivat Traficomin lisäksi myös muut pätevyysalueen vastuuviranomaiset koordinoidusti.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kiitos

Tuija Kuusisto
etunimi.sukunimi@vm.fi