

16.2.2017

## **Viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit**

### *Tilaaajaorganisaation näkökulma*

#### **JOHDANTO**

Kansainvälisistä tietoturvaluokitusvelvoitteista, turvallisuusselvityksistä sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien<sup>1</sup> mukaan Viestintäviraston tehtäviin kuuluvat erilaiset tietojärjestelmien turvallisuusarvioinnit ja -hyväksynnit. Viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit sisältävät tilaaajaorganisaatiolta vaadittavia suoritteita. Tässä ohjeessa kuvataan arviointi- ja hyväksyntäprosessit tilaaajaorganisaation näkökulmasta. Kuvauksessa määritellään käytetyt termit, esitellään arvioinnin ja hyväksynnän edellytykset ja perittävien maksujen määräytyminen, esitellään tilaaajaorganisaatiolta vaadittavia suoritteita osana arviointi- tai hyväksyntäprosessia sekä määritellään hyväksynnän voimassaolon ehdot.

#### **MÄÄRITELMÄT**

"Hyväksynnällä/hyväksyntäprosessilla" (accreditation) tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen<sup>2</sup> antaa virallisen lausunnon siitä, että järjestelmä on hyväksytty käytettäväksi määritellyssä turvaluokassa, tiettyä turvallisuuden takaavaa toimintatapaa noudattaen käyttöympäristössään ja hyväksyttävällä riskitasolla, sen pohjalta, että hyväksytyt tekniset, fyysiset, organisatoriset ja menettelyyn liittyvät turvatoimet on toteutettu.

"Arvioinnilla/arviointiprosessilla" (assessment) tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen antaa virallisen lausunnon siitä, miltä osin järjestelmä täyttää siihen kohdistuvat vaatimukset. Arviointiprosessi on usein hyväksyntäprosessin osaprosessi.

"Tarkastuksella" (audit) tarkoitetaan riippumattoman tahon suorittamaa kohteen, sen toiminnan ja toiminnan tulosten yleensä määrääjain tapahtuvaa tutkimista sen selvittämiseksi, vastaako järjestelmä tai sen osa siihen kohdistuvia vaatimuksia.

<sup>1</sup> Laki kansainvälisistä tietoturvaluokitusvelvoitteista (588/2004). Turvallisuusselvityslaki (726/2014). Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvaluokituksen arvioinnista (1406/2011).

<sup>2</sup> Security Accreditation Authority (SAA), tässä Viestintäviraston NCSA-toiminto. Lisätietoa: Kansallisen turvallisuusviranomaisen ohje kansainvälisen turvallisuusluokituksen tietoaikain käsittelystä, [www.formin.finland.fi](http://www.formin.finland.fi) > Palvelut > Kansallinen turvallisuusviranomainen (NSA) > Kansainvälisen turvallisuusluokituksen tietoaikain käsittelyohje

## ARVIOINNIN JA HYVÄKSYNNÄN EDELLYTYKSET SEKÄ PERITTÄVÄT MAKSUT

Viestintäviraston suorittamat tietoturvaluusarvioinnit ja -hyväksynnät edellyttävät tilaajaorganisaatiolta perusteltua tarvetta käsitellä kansallista tai kansainvälistä salassa pidettävää tietoa. Arviointimenettelyn piiriin kuuluvat

- viranomaisen määräämisvallassa olevat tai hankittavaksi suunnittelemaat järjestelmät, joista viranomainen on tehnyt Viestintävirastolle arviointipyyntö (L 1406/2011<sup>3</sup>, L 10/2015<sup>4</sup>), ja
- valtiovarainministeriön pyynnöstä tehtävät selvitykset valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvaluusudun tasosta (L 1406/2011, L 10/2015).

Viestintäviraston hyväksyntämenettelyn piiriin kuuluvat

- valtionhallinnon toimijoiden järjestelmät siltä osin, kun ne liittyvät kansainvälisten tietoturvaluusvelvoitteiden täyttämiseen (L 588/2004<sup>5</sup>), ja
- kansalliseen tai kansainväliseen yritysturvaluuspalvelusprosessiin hakeutuneiden yritysten järjestelmät siltä osin, kun ne edellyttävät kansallisen tietoturvaluusviranomaisen (NCSA, National Communications Security Authority) hyväksyntää (L 588/2004) tai Viestintäviraston selvitystä vaatimustenmukaisuudesta (L 726/2014).

Viranomaisella on mahdollisuus hakea Viestintäviraston todistusta vaatimustenmukaisuudesta (L 1406/2011) myös arviointimenettelyn piiriin kuuluvista järjestelmistä. Organisaatiolta, joka on tilannut Viestintävirastolta tietojärjestelmän tietoturvaluusarvioinnin tai -hyväksynnän, peritään käytettyyn aikaan perustuva maksu<sup>6</sup>. Tilaajaorganisaatiolla on oikeus saada Viestintävirastolta arvio maksun suuruudesta ennen tilauksen tekoa.

## ARVIOINTI- JA HYVÄKSYNTÄPROSESSIEN KUVAUS

Arviointiprosessi koostuu kuudesta keskeisestä suoritteesta sekä näitä täydentävistä osasuoritteista. Hyväksyntäprosessiin kuuluu lisäksi seitsemäs suorite, sekä arviointiprosessin kanssa valtaosin yhteneväiset osasuoritteet. Tässä kuvataan kukin suorite sillä tarkkuudella, että tilaajaorganisaatio saa selkeän yleiskuvan siltä vaadittavista toimista. Arviointiprosessia on havainnollistettu kuvassa 1. Hyväksyntäprosessia on havainnollistettu kuvassa 2.

### 1. Arviointi-, todistus- tai hyväksyntäpyyntö Viestintävirastolle

Tilaajaorganisaatiolla on mahdollisuus hakea järjestelmälle Viestintäviraston arviointia, todistusta vaatimustenmukaisuudesta tai hyväksyntää. Haettaessa todistusta vaatimustenmukaisuudesta, pyyntö käsitellään hyväksyntää vastaavalla menettelyllä. Arviointi-, todistus- tai hyväksyntäpyyntö suositellaan lähetettäväksi vasta, kun tilaajaorganisaatiossa uskotaan, että arvioinnin kohde täyttää pääasiallisen arviointikriteeristön<sup>7</sup> vaatimukset.

Arviointi-, todistus- tai hyväksyntäpyynnöstä on käytävä ilmi:

- Järjestelmän nimi
- Lyhyt luonnehdinta järjestelmästä ja sen laajuudesta
- Käsitteleeekö järjestelmä kansallista, kansainvälistä vai sekä kansallista että kansainvälistä salassa pidettävää tietoa
- Korkein käsiteltävä turvaluokka
- Järjestelmän omistaja, rakentaja ja ylläpitäjä
- Järjestelmän tila: suunnitteilla / rakenteilla / valmis / käytössä
- Järjestelmään liittyvät ulkoiset tai sisäiset vaatimukset, sekä suunniteltu käyttöönottopäivä
- Yhteyshenkilön nimi ja yhteystiedot
- Laskutustiedot

Pyyntöön on Viestintävirastolta saatavissa esitötetty lomake<sup>8</sup>. Mikäli järjestelmään on tehty hyväksytyt arviointilaitoksen arviointi, pyydetään arviointilaitoksen raportti toimittamaan pyynnön liitteenä. Pyyntö on toimitettava kirjallisesti Viestintäviraston kirjaamoon osoitteeseen: Viestintävirasto / Kirjaamo, Tarkastukset ja hyväksynnät -ryhmä / Aki Tauriainen, Itämerenkatu 3A, PL 313, 00181 Helsinki.

<sup>3</sup> Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvaluusudun arvioinnista (1406/2011), <http://www.finlex.fi/fi/laki/alkup/2011/20111406>

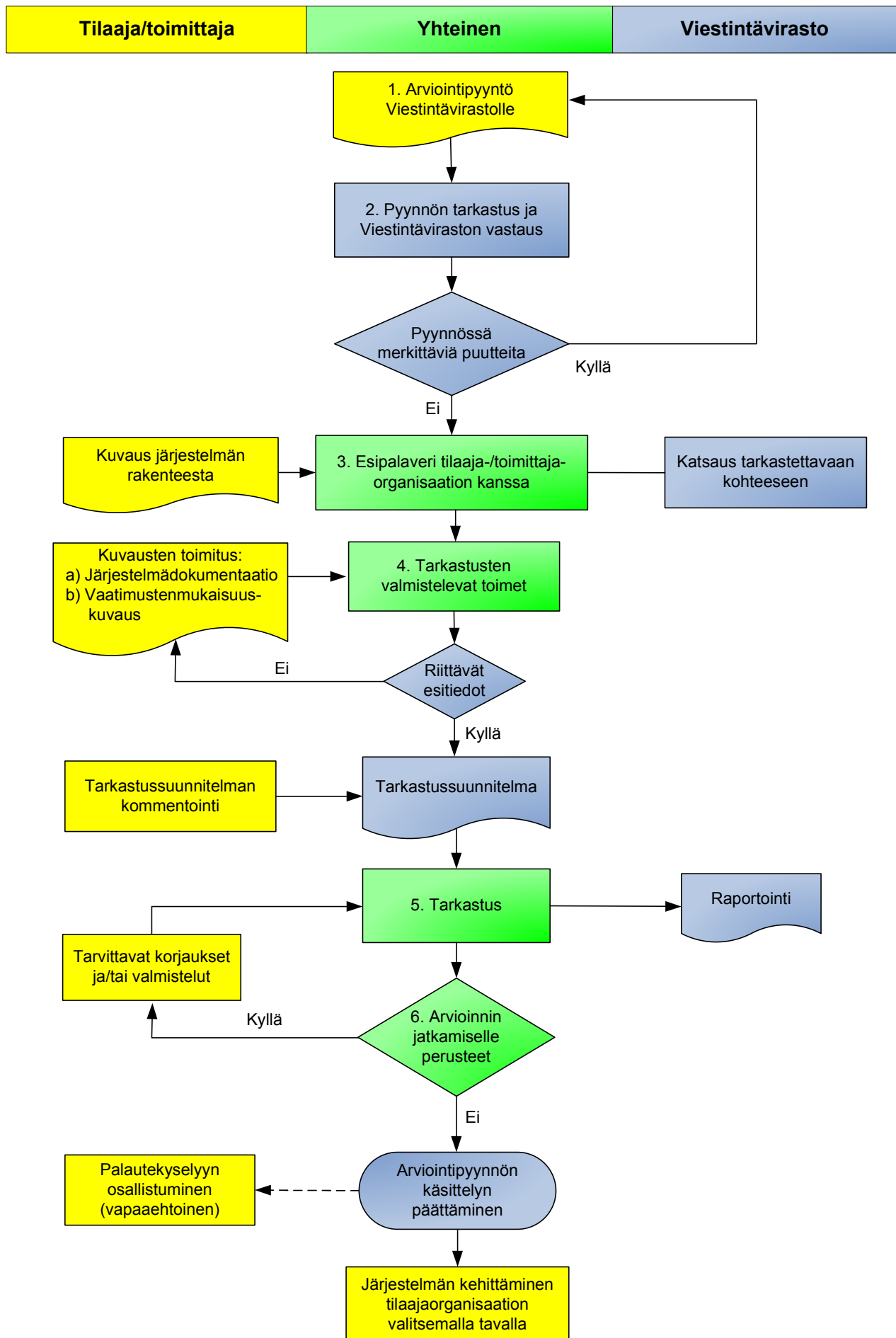
<sup>4</sup> Laki julkisen hallinnon turvaluusverkkotoiminnasta, <http://www.finlex.fi/fi/laki/alkup/2015/20150010>

<sup>5</sup> Laki kansainvälisistä tietoturvaluusvelvoitteista (588/2004), <http://www.finlex.fi/fi/laki/alkup/2004/20040588>

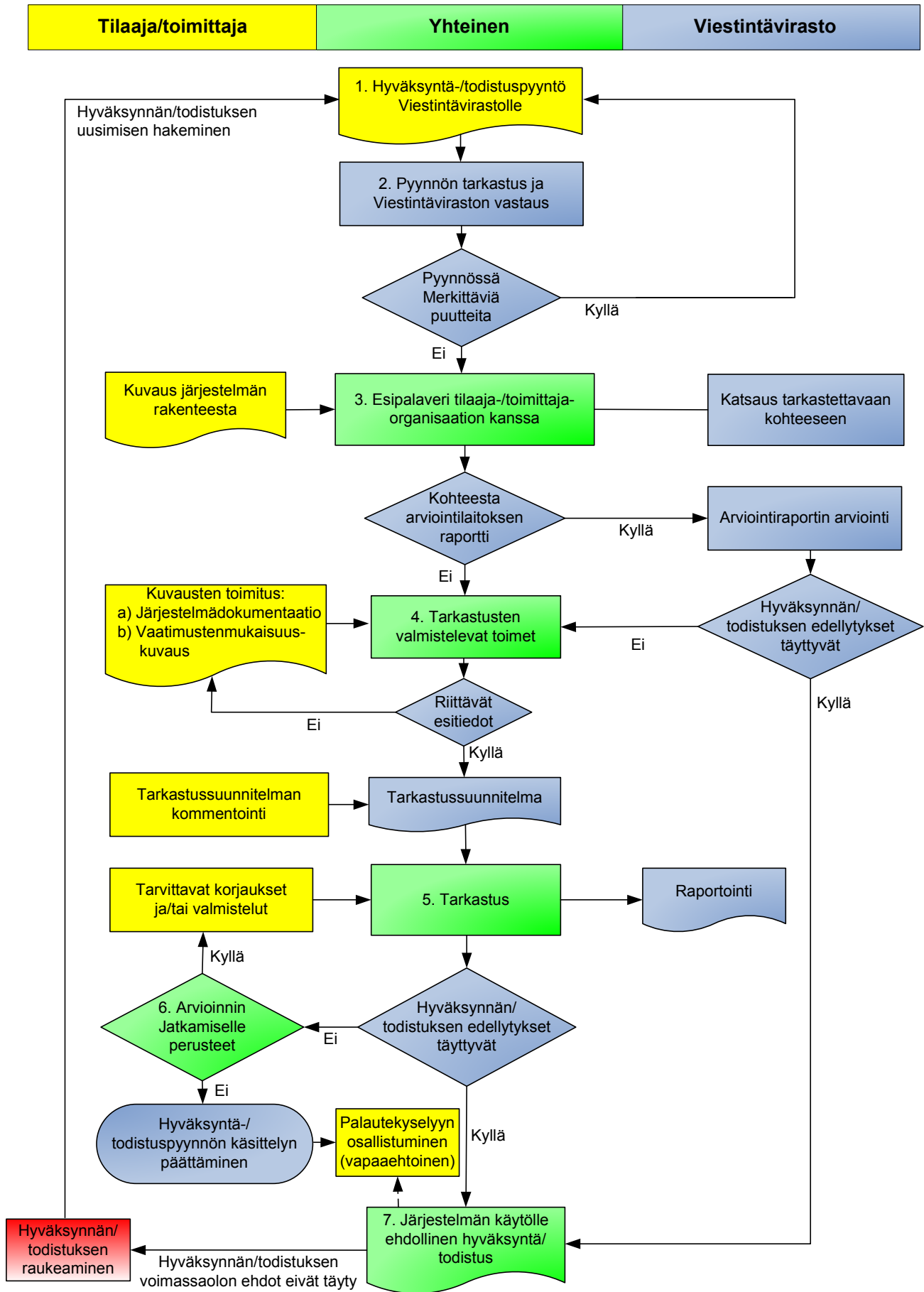
<sup>6</sup> Valtion maksuperustelaki (150/1992), <http://www.finlex.fi/fi/laki/ajantasa/1992/19920150>.

<sup>7</sup> [www.defmin.fi/katakri](http://www.defmin.fi/katakri); [www.ncsa.fi](http://www.ncsa.fi) > Asiakirjat > Työkalu tietoturvaluusudun arviointiin

<sup>8</sup> [www.ncsa.fi](http://www.ncsa.fi) > Asiakirjat > Pyyntö tietojärjestelmän tietoturvaluusudun hyväksynnälle/-arviointiin



**Kuva 1. Arviointiprosessi.**



**Kuva 2. Hyväksyntäprosessi.**

## 2. Viestintäviraston vastaus

Viestintävirasto pyrkii antamaan vastauksensa kahden viikon kuluessa pyynnön saapumisesta. Mikäli pyynnöstä ilmenee, että edellytyksiä arviointi- tai hyväksyntäprosessin aloittamiseen ei ole, pyyntö palautetaan täydennettäväksi. Arviointi- tai hyväksyntäprosessin aloittamisen edellytysten täytyessä Viestintäviraston vastauksesta selviää:

- Ehdotus esipalaverin ajaksi
- Esipalaveriin tilaajaorganisaatiolta vaadittavat dokumentit

## 3. Esipalaveri tilaajaorganisaation kanssa

Esipalaverin tavoitteena on saada yleiskuva tarkastuksen kohteena olevasta tietojärjestelmästä, sekä saavuttaa yhtenevä ymmärrys arviointi- tai hyväksyntäprosessin käytännön toimista. Esipalaveri pidetään lähtökohtaisesti seuraavien toimijoiden kesken:

- Tarkastajat (Viestintäviraston järjestelmätarkastuksen edustajat)
- Järjestelmän omistaja
- Järjestelmän rakentaja
- Järjestelmän ylläpitäjä

Esipalaverissa Viestintävirastolle luovutetaan<sup>9</sup> mahdollisuuksien mukaan seuraavat dokumentit:

- Kuvaus järjestelmän rakenteesta<sup>10</sup>
- Tiedot mahdollisista aikaisemmista tarkastuksista, arvioinneista ja/tai hyväksynnöistä raportteineen
- Järjestelmäkohtaiset erityisvaatimukset<sup>11</sup>

Viestintävirastolla on mahdollisuus myöntää järjestelmälle todistus tai hyväksyntä pohjautuen hyväksytyyn arviointilaitoksen suorittamaan arviointiin (L 1405/2011<sup>12</sup>). Myöntämisen keskeisinä ehtoina ovat tehtyjen tarkastusten rajausten yhteneväisyydet haettavan todistuksen tai hyväksynnän rajauksiin sekä toimitettujen arviointiraporttien tietojen riittävyys. Todistusta tai hyväksyntää varten Viestintävirasto suorittaa tarvittaessa tarkentavia arviointeja tai pyytää tilaajaorganisaatiolta lisäselvitystä sen varmistamiseksi, että hyväksynnän kohde täyttää soveltuvat tietoturvaluusvaatimukset.

## 4. Tarkastusten valmistelevat toimet

Viestintävirasto laatii osana tarkastusten valmistelevia toimiaan tarkastussuunnitelmaluonnoksen, jossa kuvataan yleistasolla kyseisen järjestelmän tarkastamiseen liittyvät asiakokonaisuudet ja tarkastusten aikataulus. Tilaajaorganisaatiolle annetaan mahdollisuus kommentoida tarkastussuunnitelmaa. Suunnitelma viimeistellään yhteistyössä tilaajaorganisaation kanssa.

Tilaajaorganisaatiota edellytetään toimittamaan tarkastussuunnitteluun seuraavat tiedot:

- Kuvaus järjestelmän rakenteesta ja toimintaperiaatteista (järjestelmädokumentaatio)
- Kuvaus järjestelmän vaatimustenmukaisuuden nykytilasta (itsearviointi)

Kuvauksista tulee selvittää järjestelmän rakenne, toimintaperiaatteet ja suojaamiskäytännöt. Kuvauksen tulee olla sellaisella tarkkuudella, että niiden avulla pystytään suunnittelemaan järjestelmän tarkastuskokonaisuudet ja räätälöimään tarkastuksessa käytetyt työkalut tarkastuskohteen mukaisesti. Kuvaukseen vaatimustenmukaisuuden nykytilasta on Viestintävirastolta saatavissa esitäytetty lomake<sup>13</sup>. Arviointi- tai hyväksyntäprosessi päätetään, mikäli edellytetyt kuvauksia ei toimiteta 6 kuukauden kuluessa esipalaverista lukien.

<sup>9</sup> Viestintävirastolla ja sen lukuun toimivilla asiantuntijoilla on oikeus saada nähtäville tai käyttöönsä ne tiedot, jotka ovat tarpeen tarkastusten suorittamista varten. Virastolla on lisäksi oikeus päästä tarkastuksen kohteen toimitiloihin. Tiedonsaantioikeudesta ja pääsystä toimitiloihin säädetään viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvaluusuden arvioinnista annetun lain (1406/2011) 6 §:ssä ja kansainvälisistä tietoturvaluusuvetoitteista annetun lain (588/2004) 16 §:ssä. Viestintävirasto ja virastossa toimivat ovat velvollisia noudattamaan lakia viranomaisten toiminnan julkisuudesta (621/1999). Julkisuuslaissa säädetään muun muassa salassa pidettävien tietojen koskevasta vaihtoluvelvollisuudesta ja hyväksikäyttökiellosta (julkisuuslaki 22 § ja 23 §), joiden rikkomisesta säädetään rikoslaisa (julkisuuslaki 35 §). Viestintäviraston tulee lisäksi noudattaa julkisuuslain 18 §:n mukaista hyvää tiedonhallintatapaa ja asetusta tietoturvaluusudesta valtiorhallinnossa, jossa säädetään asiakirjojen käsittelyssä noudatettavista tietoturvaluusuvetoitteista.

<sup>10</sup> Esimerkiksi verkkokuvat ja listaukset järjestelmäkomponenteista käyttöjärjestelmiseen.

<sup>11</sup> Turvaluokiteltujen tietojen omistajat asettavat usein järjestelmän käyttöluvan ehdoksi järjestelmäkohtaisen turvaluusuvetoite määrällisen (SSRS, System-Specific Security Requirements Statement) täyttämisen.

<sup>12</sup> Laki tietoturvaluusuden arviointilaitoksista (1405/2011), <http://www.finlex.fi/fi/laki/alkup/2011/20111405>.

<sup>13</sup> [www.ncsa.fi](http://www.ncsa.fi) > Asiakirjat > Kuvaus järjestelmän vaatimustenmukaisuuden nykytilasta

Tilaaajaorganisaatiota edellytetään sitoutumaan suunnitelmassa kuvattavaan aikataulutukseen. Tilaaajaorganisaatiota edellytetään myös järjestävän tarkastuksen mahdollistavat menettelyt tarkastuksen kohteessa. Tällaisiin menettelyihin sisältyvät tyypillisesti soveltuvat henkilöstö- ja tilavaraukset, sekä tarvittavien loogisten ja fyysisten pääsyoikeuksien järjestämiset.

## 5. Tarkastus

Tarkastukseen sisältyy kohteen tietoturvallisuuden tutkiminen sen selvittämiseksi, vastaako kohteen tietoturvallisuuden tila siihen kohdistuvia vaatimuksia. Tarkastus koostuu yleensä hallinnollisesta ja teknisestä osuudesta. Tarkastukseen sisältyy yleensä myös fyysisen turvallisuuden osuus. Tarkastuksessa käytettyjä todennusmenetelmiä on kuvattu yksityiskohtaisemmin Viestintäviraston ohjeessa tietoturvallisuuden arviointilaitoksille<sup>14</sup> (luvut 5.4.2 ja 5.4.3).

Tilaaajaorganisaatiolle luovutetaan tarkastuksen päätteeksi listaus tarkastuksessa havaituista poikkeamista. Tilaaajaorganisaatiolle toimitetaan pyydettäessä myös raportti järjestelmän tai sen osakokonaisuuden vaatimustenmukaisuuden nykytilasta. Raportti toimitetaan lähtökohtaisesti kuuden viikon kuluessa viimeisimmästä tarkastuskäynnistä.

## 6. Arvioinnin jatkamisen perusteet

Arviointiprosessissa tarkastus- ja raportointialiprosessia jatketaan lähtökohtaisesti tilaaajaorganisaation tarpeiden mukaisesti. Hyväksyntäprosessissa tarkastus- ja raportointialiprosessia jatketaan, kunnes järjestelmälle asetettujen vaatimusten on todennettu täyttyneen. Arviointi- tai hyväksyntäprosessi voidaan päättää myös tilanteessa, jossa tarkastusta ei pystytä aloittamaan tai tarkastuksissa havaittujen poikkeamien korjausten etenemisestä ei saada näyttöä 6 kuukauden aikana, tai mikäli tilaaajaorganisaatio pyytää prosessin päättämistä.

## 7. Järjestelmän käytölle ehdollinen hyväksyntä tai todistus

Vaatimukset täyttävälle kansainvälistä suojattavaa tietoa käsittelevälle järjestelmälle voidaan myöntää hyväksyntä. Vaatimukset täyttävälle kansallista suojattavaa tietoa käsittelevälle järjestelmälle voidaan myöntää todistus vaatimustenmukaisuudesta. Sekä hyväksynnän että todistuksen myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason säilyttämiseen.

## HYVÄKSYNNÄN JA TODISTUKSEN VOIMASSAOLO

Viestintäviraston myöntämä hyväksyntä on voimassa lähtökohtaisesti 3 vuotta myöntämispäivästä lukien. Myös todistus voidaan myöntää määräajaksi, jos siihen on erityinen syy. Hyväksyntä tai todistus raukeaa, mikäli tarkastetussa kohteessa tapahtuu merkittävä sen turvallisuuteen vaikuttava muutos. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten esimerkiksi ohjelmistojen turvapäivitysten asennukset, eivät aiheuta voimassaolevan hyväksynnän tai todistuksen raukeamista. Tapauskohtaiset ehdot hyväksynnän tai todistuksen raukeamiselle määritellään hyväksynnän tai todistuksen myöntämisen yhteydessä. Merkittävät muutokset tulee hyväksyttävä etukäteen Viestintävirastolla.

---

<sup>14</sup> Viestintäviraston ohje tietoturvallisuuden arviointilaitoksille,  
[https://www.viestintavirasto.fi/attachments/Ohje\\_tietoturvallisuuden\\_arviointilaitoksille.pdf](https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf).