1.8.2018

Viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit

Tilaajaorganisaation näkökulma

JOHDANTO

Kansainvälisistä tietoturvallisuusvelvoitteista, turvallisuusselvityksistä sekä viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annettujen lakien[1] mukaan Viestintäviraston tehtäviin kuuluvat erilaiset tietojärjestelmien turvallisuusarvioinnit ja -hyväksynnät. Viestintäviraston suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit sisältävät tilaajaorganisaatiolta vaadittavia suoritteita. Tässä ohjeessa kuvataan arviointi- ja hyväksyntäprosessit tilaajaorganisaation näkökulmasta. Kuvauksessa määritellään käytetyt termit, esitellään arvioinnin ja hyväksynnän edellytykset ja perittävien maksujen määräytyminen, esitellään tilaajaorganisaatiolta vaadittavia suoritteita osana arviointi- tai hyväksyntäprosessia sekä määritellään hyväksynnän voimassaolon ehdot.

MÄÄRITELMÄT

"Hyväksynnällä/hyväksyntäprosessilla" (accreditation) tarkoitetaan prosessia, jonka päätteeksi turvallisuusjärjestelyt hyväksyvä viranomainen[2] 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 määräajoin tapahtuvaa tutkimista sen selvittämiseksi, vastaako järjestelmä tai sen osa siihen kohdistuvia vaatimuksia.

---

[1] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Turvallisuusselvityslaki (726/2014). Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011).

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

ARVIOINNIN JA HYVÄKSYNNÄN EDELLYTYKSET SEKÄ PERITTÄVÄT MAKSUT

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

- viranomaisen määräämisvallassa olevat tai hankittavaksi suunnittelemat järjestelmät, joista viranomainen on tehnyt Viestintävirastolle arviointipyynnön (L 1406/2011[3], L 10/2015[4]), ja
- valtiovarainministeriön pyynnöstä tehtävät selvitykset valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta (L 1406/2011, L 10/2015).

Viestintäviraston hyväksyntämenettelyn piiriin kuuluvat

- valtionhallinnon toimijoiden järjestelmät siltä osin, kun ne liittyvät kansainvälisten tietoturvavelvoitteiden täyttämiseen (L 588/2004[5]), ja
- kansalliseen tai kansainväliseen yritysturvallisuusselvitysprosessiin hakeutuneiden yritysten järjestelmät siltä osin, kun ne edellyttävät kansallisen tietoturvallisuusviranomaisen (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 tietoturvallisuusarvioinnin tai -hyväksynnän, peritään käytettyyn aikaan perustuva maksu[6]. 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[7] vaatimukset.

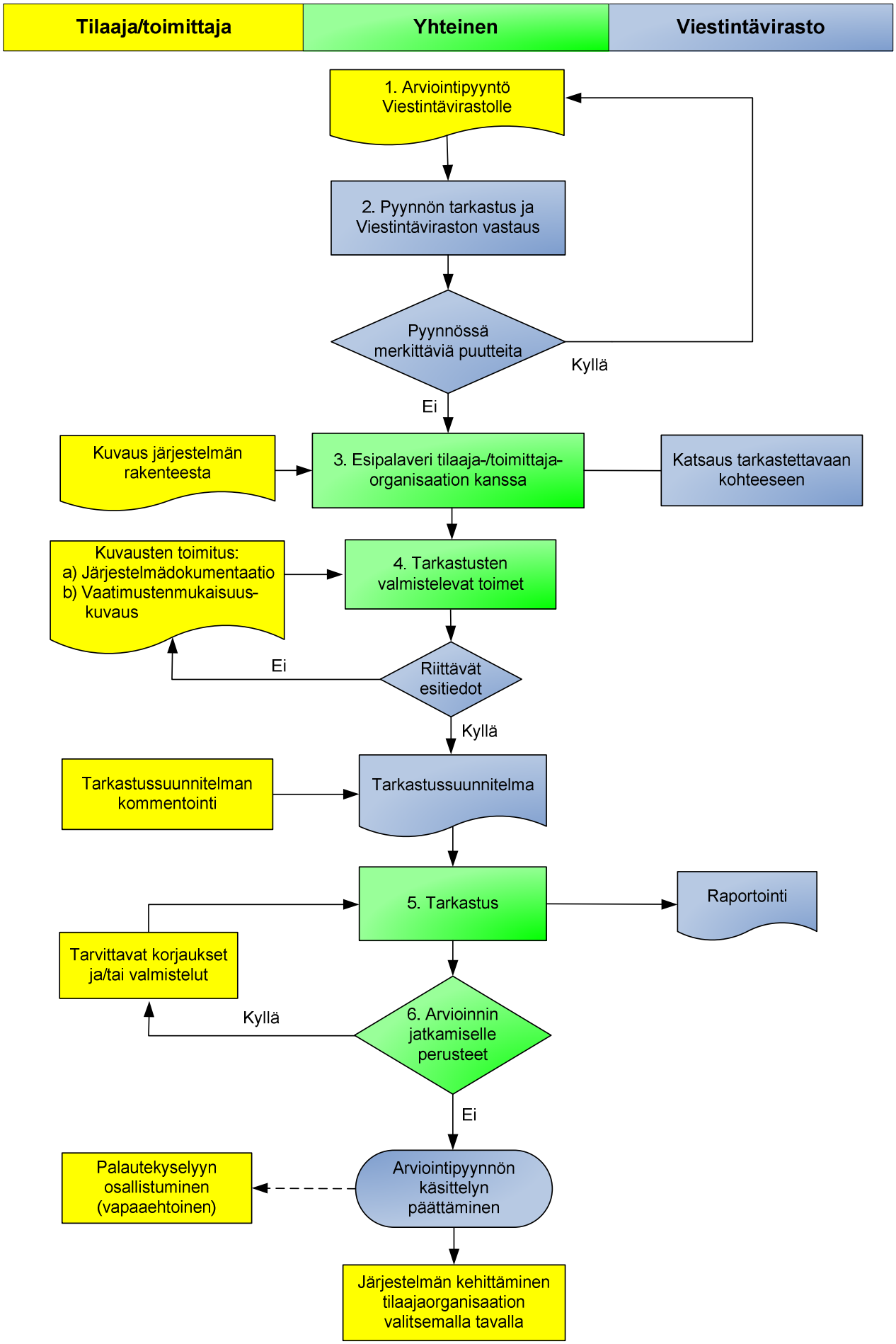
Arviointi-, todistus- tai hyväksyntäpyynnöstä on käytävä ilmi:

- Järjestelmän nimi
- Lyhyt luonnehdinta järjestelmästä ja sen laajuudesta
- Käsitteleekö 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

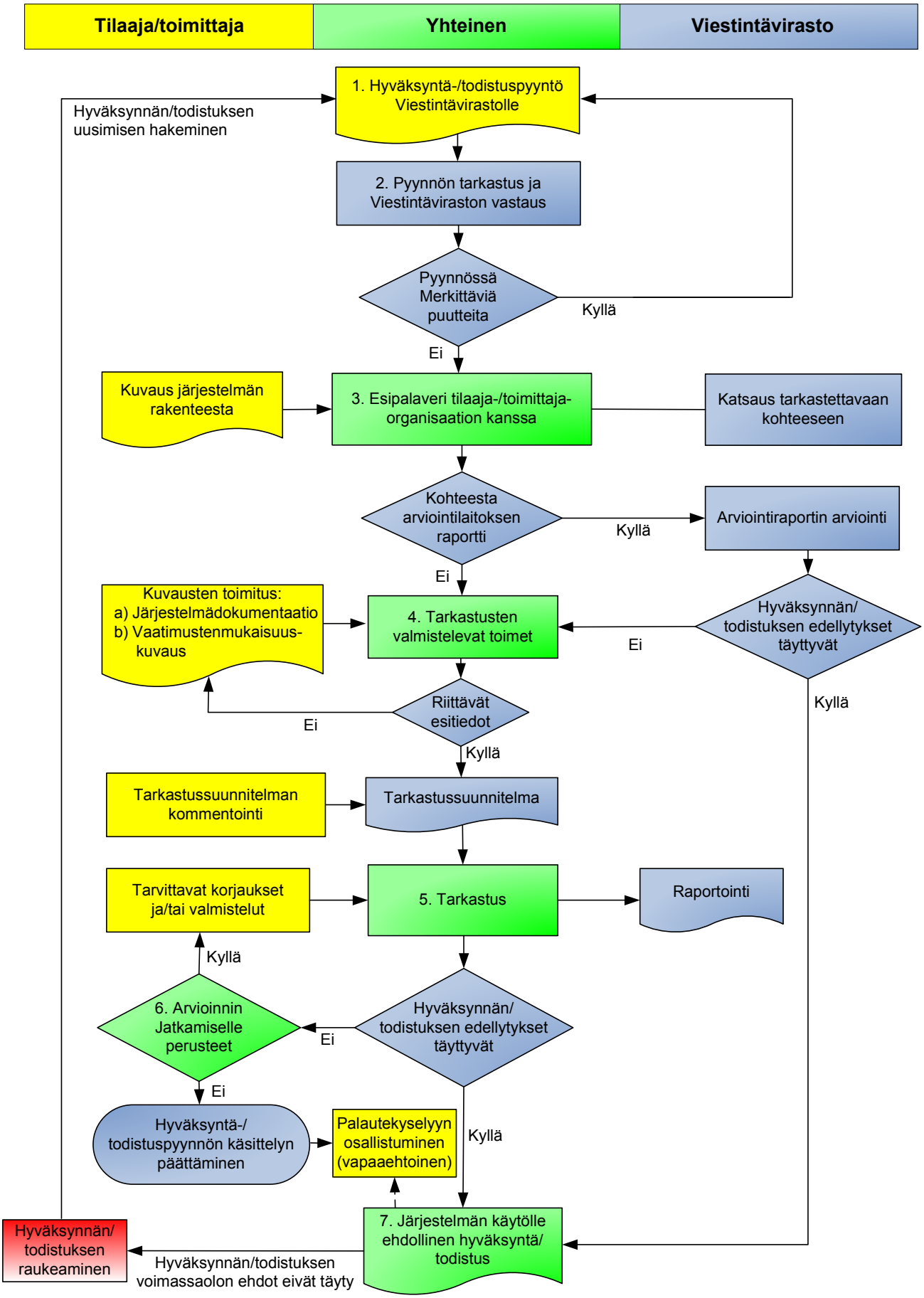
Pyyntöön on Viestintävirastolta saatavissa esitäytetty lomake[8]. Mikäli järjestelmään on tehty hyväksytyn arviointilaitoksen arviointi, pyydetään arviointilaitoksen raportti toimittamaan pyynnön liitteenä. Pyyntö on toimitettava kirjallisesti Viestintäviraston kirjaamoon osoitteeseen: Viestintävirasto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

---

[3] Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), http://www.finlex.fi/fi/laki/alkup/2011/20111406
[4] Laki julkisen hallinnon turvallisuusverkkotoiminnasta, http://www.finlex.fi/fi/laki/alkup/2015/20150010
[5] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), http://www.finlex.fi/fi/laki/alkup/2004/20040588
[6] Valtion maksuperustelaki (150/1992), http://www.finlex.fi/fi/laki/ajantasa/1992/19920150.
[7] www.defmin.fi/katakri; www.ncsa.fi > Asiakirjat > Työkalu tietoturvallisuuden arviointiin
[8] www.ncsa.fi > Asiakirjat > Pyyntö tietojärjestelmän tietoturvallisuushyväksynnälle/-arvioinnille



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 täyttyessä 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[9] mahdollisuuksien mukaan seuraavat dokumentit:

- Kuvaus järjestelmän rakenteesta[10]
- Tiedot mahdollisista aikaisemmista tarkastuksista, arvioinneista ja/tai hyväksynnöistä raportteineen
- Järjestelmäkohtaiset erityisvaatimukset[11]

Viestintävirastolla on mahdollisuus myöntää järjestelmälle todistus tai hyväksyntä pohjautuen hyväksytyn arviointilaitoksen suorittamaan arviointiin (L 1405/2011[12]). 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 tietoturvallisuusvaatimukset.

4. Tarkastusten valmistelevat toimet

Viestintävirasto laatii osana tarkastusten valmistelevia toimiaan tarkastussuunnitelmaluonnoksen, jossa kuvataan yleistasolla kyseisen järjestelmän tarkastamiseen liittyvät asiakokonaisuudet ja tarkastusten aikataulutus. 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 selvitä järjestelmän rakenne, toimintaperiaatteet ja suojaamiskäytännöt. Kuvausten 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[13]. Arviointi- tai hyväksyntäprosessi päätetään, mikäli edellytettyjä kuvauksia ei toimiteta 6 kuukauden kuluessa esipalaverista lukien.

---

[9] 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 tietoturvallisuuden arvioinnista annetun lain (1406/2011) 6 §:ssä ja kansainvälisistä tietoturvallisuusvelvoitteista 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 tietoja koskevasta vaitiolovelvollisuudesta ja hyväksikäyttökiellosta (julkisuuslaki 22 § ja 23 §), joiden rikkomisesta säädetään rikoslaissa (julkisuuslaki 35 §). Viestintäviraston tulee lisäksi noudattaa julkisuuslain 18 §:n mukaista hyvää tiedonhallintatapaa ja asetusta tietoturvallisuudesta valtionhallinnossa, jossa säädetään asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

[10] Esimerkiksi verkkokuvat ja listaukset järjestelmäkomponenteista käyttöjärjestelmineen.

[11] Turvaluokiteltujen tietojen omistajat asettavat usein järjestelmän käyttöluvan ehdoksi järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn (SSRS, System-Specific Security Requirements Statement) täyttämisen.

[12] Laki tietoturvallisuuden arviointilaitoksista (1405/2011), http://www.finlex.fi/fi/laki/alkup/2011/20111405.

[13] www.ncsa.fi > Asiakirjat > Kuvaus järjestelmän vaatimustenmukaisuuden nykytilasta

Tilaajaorganisaatiota edellytetään sitoutumaan suunnitelmassa kuvattavaan aikataulutukseen. Tilaajaorganisaatiota 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[14] (luvut 5.4.2 ja 5.4.3).

Tarkastuskokonaisuuden päätteeksi käydään keskeiset havainnot läpi yhdessä kohdeorganisaation kanssa. Tilaajaorganisaatiolle toimitetaan pyydettäessä myös raportti järjestelmän tai sen osakokonaisuuden vaatimustenmukaisuuden nykytilasta. Raportti pyritään toimittamaan kuuden viikon kuluessa viimeisimmästä tarkastuskäynnistä.

6. Arvioinnin jatkamisen perusteet

Arviointiprosessissa tarkastus- ja raportointialiprosessia jatketaan lähtökohtaisesti tilaajaorganisaation 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 tilaajaorganisaatio 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 hyväksyttää etukäteen Viestintävirastolla.

TARJOTTAVAT TUKIPALVELUT JA LISÄTIETOKYSELYT

Viestintävirasto pystyy tukemaan arviointi- ja hyväksyntäprosesseihin osallistuvia organisaatioita tietoturvallisuuden neuvontapalvelulla. Neuvontapalvelun tarkoituksena on varmistaa, että asiakkailla on riittävä ymmärrys sovellettavasta tulkintakäytännöstä sekä soveltuvista ratkaisukäytännöistä. Neuvontapalvelun käyttö ei takaa, että arviointi- tai hyväksyntäpalvelun kohde täyttäisi kaikki siihen kohdistuvat suojausvaatimukset. Lopullinen arvio kohteen vaatimustenmukaisuuden nykytilasta tehdään aina osana arviointi- tai hyväksyntäpalvelua. Kohteen arviointiin välittömästi osallistuva asiantuntija ei voi jääviyssyistä neuvoa kohdeorganisaatiota arvioinnissa havaittujen puutteiden korjaamisessa kuin yleisellä, vaatimusten tulkintaa avaavalla tasolla. Lisätietoja on saatavilla osoitteesta accreditation (at) ficora (piste) fi.

[14] Viestintäviraston ohje tietoturvallisuuden arviointilaitoksille, https://www.viestintavirasto.fi/attachments/Ohje_tietoturvallisuuden_arviointilaitoksille.pdf.