Liikenne- ja viestintäviraston ohje tietojärjestelmien tietoturvallisuuden arviointi- ja hyväksyntäprosesseista

Sisältö

1 JOHDANTO

Tämä ohje on tarkoitettu viranomaisille ja yrityksille (*asiakasorganisaatiot*), joilla on tarve käsitellä kansallista tai kansainvälistä turvallisuusluokiteltua tietoa sähköisessä muodossa. Ohjeessa kuvataan Liikenne- ja viestintävirasto Traficomin tietojärjestelmien arviointi- ja hyväksyntäprosessit asiakasorganisaation näkökulmasta. Ohjeessa kuvataan arvioinnin ja hyväksynnän edellytykset sekä esitellään arviointi- ja hyväksyntäprosessit asiakasorganisaatiolta edellytettävien toimenpiteiden näkökulmasta.

Tietojärjestelmien arviointeihin ja hyväksyntöihin liittyvät Traficomin tehtävät säädetään laissa kansainvälisistä tietoturvallisuusvelvoitteista (588/2004, kv-titulaki), turvallisuusselvityslaissa (706/2014) ja laissa viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista (1406/2011, arviointilaki). Kansainvälisissä tietoturvallisuusvelvoitteissa hyväksyntäviranomaisen rooleista käytetään yleensä nimeä NCSA (*National Communications Security Authority* tai *National CIS Security Authority*) sekä SAA (*Security Accreditation Authority*).

Kansainvälisten tietoturvallisuusvelvoitteiden mukaisesti esimerkiksi EU:n ja Naton turvallisuusluokiteltua tietoa käsittelevien tietojärjestelmien tulee läpikäydä hyväksyntäprosessi (akkreditointi). Vastaava velvoite koskee tyypillisesti myös kahden- tai monenvälisten tietoturvallisuussopimusten piiriin kuuluvia toisen valtion turvallisuusluokiteltuja tietoja valtioiden rajat ylittävän tietojärjestelmäosuuden osalta (ks. luku 4.6.2). Edellä mainituissa tilanteissa haetaan Traficomin hyväksyntää tietojärjestelmissä käsiteltävien kansainvälisten turvallisuusluokiteltujen tietojen suojaamiseen.

Kansallista turvallisuusluokiteltua tietoa käsitteleviin viranomaisten tietojärjestelmiin ei kohdistu lainsäädännöstä yleistä velvoitetta tietojärjestelmän hyväksynnälle (akkreditoinnille)[1]. Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019, tiedonhallintalaki) mukaisesti tiedonhallintayksikön[2] on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Viranomaisen tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti (13 §). Traficomin arviointia on mahdollista hakea tietojärjestelmissä käsiteltävien kansallisten turvallisuusluokiteltujen tietojen suojaamiseen[3].

Ohje on voimassa toistaiseksi. Ohje korvaa aikaisemman 15.5.2023 annetun ohjeen.

2 ARVIOINNIN JA HYVÄKSYNNÄN EDELLYTYKSET

2.1 Arviointi- ja hyväksyntäpyynnöt

Traficomin tietoturvallisuusarvioinnit ja -hyväksynnät edellyttävät asiakasorganisaatiolta perusteltua tosiasiallista tarvetta käsitellä kansallista tai kansainvälistä turvallisuusluokiteltua tietoa sähköisesti.

Arviointimenettelyn piiriin kuuluvat

- viranomaisen määräämisvallassa olevat tai hankittavaksi suunnittelemat järjestelmät, joista viranomainen on tehnyt Traficomille arviointipyynnön (arviointilaki ja laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015 tuve-laki)), ja
- valtiovarainministeriön pyynnöstä tehtävät selvitykset valtionhallinnon viranomaisen määräämisvallassa olevien tietojärjestelmien tai tietoliikennejärjestelyjen yleisestä tietoturvallisuuden tasosta (arviointilaki ja tuvelaki).

[1] Esimerkiksi lain julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) mukaisiin tietojärjestelmiin ei kohdistu lainsäädännöstä yleistä velvoitetta tietojärjestelmän hyväksynnälle (akkreditoinnille). Valtioneuvoston asetuksen julkisen hallinnon turvallisuusverkkotoiminnasta (1109/2015) 10§:n mukaan turvallisuusverkon palvelujen tietoturvallisuus- ja varautumisvaatimusten täyttyminen on kuitenkin arvioitava ja todettava noudattaen arviointilakia (1406/2011) ja kansainvälisistä tietoturvallisuusvelvoitteista annettua lakia (588/2004). Valtiovarainministeriö on myös antanut julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain (10/2015) 14.4 §:n mukaisella toimivallalla määräyksen koskien turvallisuusverkkolain mukaisten palvelujen ja niihin liitettävien viranomaisten tietojärjestelmien arviointia.

[2] Tiedonhallintayksiköllä tarkoitetaan viranomaista, jonka tehtävänä on järjestää tiedonhallinta julkisen hallinnon tiedonhallinnasta annetun lain vaatimusten mukaisesti (906/2019, 2 §).

[3] Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista (1406/2011) 4.3 §:n ja lain perustelujen mukaisesti tässä ohjeessa kuvattu tietojärjestelmien arviointitoiminta liittyy ensisijaisesti turvallisuusluokitellun tiedon suojaamisen arviointiin.

Traficomin hyväksyntämenettelyn piiriin kuuluvat

- valtionhallinnon toimijoiden järjestelmät siltä osin, kun ne liittyvät kansainvälisten tietoturvavelvoitteiden täyttämiseen (kv-titulaki),
- kansalliseen tai kansainväliseen yritysturvallisuusselvitysprosessiin hakeutuneiden yritysten järjestelmät siltä osin, kun ne edellyttävät kansallisen tietoturvallisuusviranomaisen (NCSA) hyväksyntää (kv-titulaki) tai Traficomin selvitystä vaatimustenmukaisuudesta (turvallisuusselvityslaki, kv-titulain 12 §),
- kansainvälisen tietoturvavelvoitteen täyttämiseen (kv-titulaki) liittyvät yritysten järjestelmät niiltä osin, kuin niihin ei sovelleta yritysturvallisuusselvitysprosessin menettelyjä, ja
- viranomaisten tietojärjestelmät, joista viranomainen hakee Traficomin todistusta vaatimustenmukaisuudesta (arviointilaki).

2.2 Priorisointi

Traficom suorittaa arviointi- ja hyväksyntätehtävät käytettävissään olevien voimavarojen mukaisesti ottaen huomioon kansainvälisten tietoturvallisuusvelvoitteiden noudattamisen sekä pyydettyjen toimenpiteiden merkityksen viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden yleiseen parantamiseen (arviointilaki, 4 § 3 mom.). Traficomin priorisointikäytännössä huomioidaan myös käsiteltävän tiedon turvallisuusluokka sekä se, että kansallisten turvallisuusluokkien IV ja III arviointi on mahdollista hankkia arviointilaitoksilta.

2.3 Tiedonsaantioikeus

Traficom tekee arvioinnit ja hyväksynnät viranomaisena, ja näihin osallistuvat asiantuntijat ovat virkavastuulla toimivia virkamiehiä. Arvioinneissa ja hyväksynnöissä noudatetaan hallintolakia (434/2003). Virastolla, sen virkamiehillä ja sen lukuun mahdollisesti toimivilla muilla asiantuntijoilla on oikeus saada nähtäville tai käyttöönsä ne tiedot, jotka ovat tarpeen arviointia varten ja päästä arvioinnin kohteen toimitiloihin.

Tiedonsaantioikeudesta ja pääsystä toimitiloihin säädetään arviointilain 6 §:ssä, kv-titulain 16 §:ssä ja turvallisuusselvityslain 39 §:ssä. Viranomainen, virkamiehet ja viranomaisen toimeksiannosta toimivat noudattavat asiakirjoja ja tietoja käsitellessään lakia viranomaisten toiminnan julkisuudesta (621/1999, julkisuuslaki). Julkisuuslaissa säädetään muun muassa salassa pidettävien tietoja koskevasta vaitiolovelvollisuudesta ja hyväksikäyttökiellosta (julkisuuslaki 22 § ja 23 §), joiden rikkomisesta säädetään rikoslaissa (julkisuuslaki 35 §). Traficomin tulee lisäksi noudattaa julkisuuslain 18 §:n mukaista hyvää tiedonhallintatapaa sekä tiedonhallintalakia (906/2019) ja turvallisuusluokitteluasetusta (1101/2019), joissa säädetään asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

On hyvä huomata, että virkamiehillä tai viranomaisen toimeksiannosta toimivilla ei ole oikeutta sitoutua salassapitosopimuksiin, vaan heitä sitovat edellä kuvatut velvoitteet suoraan lain nojalla.

2.4 Maksut

Organisaatiolta, joka on pyytänyt Traficomilta tietojärjestelmän tietoturvallisuusarvioinnin tai -hyväksynnän, peritään käytettyyn aikaan perustuva maksu[4]. Asiakasorganisaatiolla on oikeus saada Traficomilta arvio maksun suuruudesta.

[4] Valtion maksuperustelaki (150/1992), http://www.finlex.fi/fi/laki/ajantasa/1992/19920150. Liikenne- ja viestintäministeriön asetus Liikenne- ja viestintäviraston sähköiseen viestintään liittyvistä suoritteista perittävistä maksuista (1256/2021) sekä sen muutos (497/2022), https://www.finlex.fi/fi/laki/alkup/2022/20220497.

3 ARVIOINTIPROSESSI

Arviointiprosessin tavoitteena on tukea kansallisen turvallisuusluokitellun tiedon suojaamisesta vastuussa olevien viranomaisten riskienhallintatyötä. Arviointiprosessi tuottaa asiakasorganisaatiolle Traficomin lausunnon siitä, miltä osin järjestelmä täyttää siihen kohdistuvat vaatimukset ja miltä osin järjestelmässä on poikkeamia. Tässä luvussa kuvataan arviointiprosessin vaiheet sillä tarkkuudella, että asiakasorganisaatio saa selkeän yleiskuvan siltä edellytettävistä toimista. Arviointiprosessia on havainnollistettu kuvassa 1.

3.1 Arviointipyynnön sisältö ja toimittaminen Traficomille

Arviointipyyntö suositellaan lähetettäväksi, kun asiakasorganisaatiossa uskotaan, että arvioinnin kohde täyttää valitun arviointikriteeristön[5] vaatimukset. Arviointipyynnöstä on käytävä ilmi:

- Arvioinnin pyytävä viranomainen (yritykset eivät voi itsenäisesti pyytää arviointia)
- Järjestelmän nimi
- Lyhyt luonnehdinta järjestelmästä ja sen laajuudesta
- Käsiteltävien tietojen tyyppi ja omistaja (esimerkiksi kansallinen tai/ja toisen valtion Suomelle luovuttama tieto)
- Korkein käsiteltävän tiedon turvallisuusluokka
- 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 Traficomilta saatavissa lomakepohja[6]. Pyyntö on toimitettava kirjallisesti Traficomin kirjaamoon[7]. Traficom pyrkii antamaan vastauksensa arvioinnin aloittamisen mahdollisuuksista neljän viikon kuluessa pyynnön saapumisesta. Mikäli pyynnöstä ilmenee, että edellytyksiä arviointiprosessin aloittamiseen ei ole, pyyntö palautetaan täydennettäväksi. Jos Traficom katsoo, että arvioinnin aloittamiselle ei ole edellytyksiä ja asiakasorganisaatio on eri mieltä, Traficom voi tarvittaessa antaa asiasta valituskelpoisen perustellun päätöksen. Arviointiprosessin aloittamisen edellytysten täyttyessä Traficomin vastauksesta selviää:

- Ehdotus esipalaverin ajaksi
- Esipalaveriin asiakasorganisaatiolta edellytettävät kuvaukset (ks. tarkemmin arvioinnin osalta luku 3.2)

3.2 Esipalaveri asiakasorganisaation kanssa

Esipalaverin tavoitteena on saada yleiskuva arvioinnin kohteena olevasta tietojärjestelmästä, sekä saavuttaa yhtenevä ymmärrys arviointiprosessin käytännön toimista. Esipalaveri pidetään lähtökohtaisesti seuraavien toimijoiden kesken:

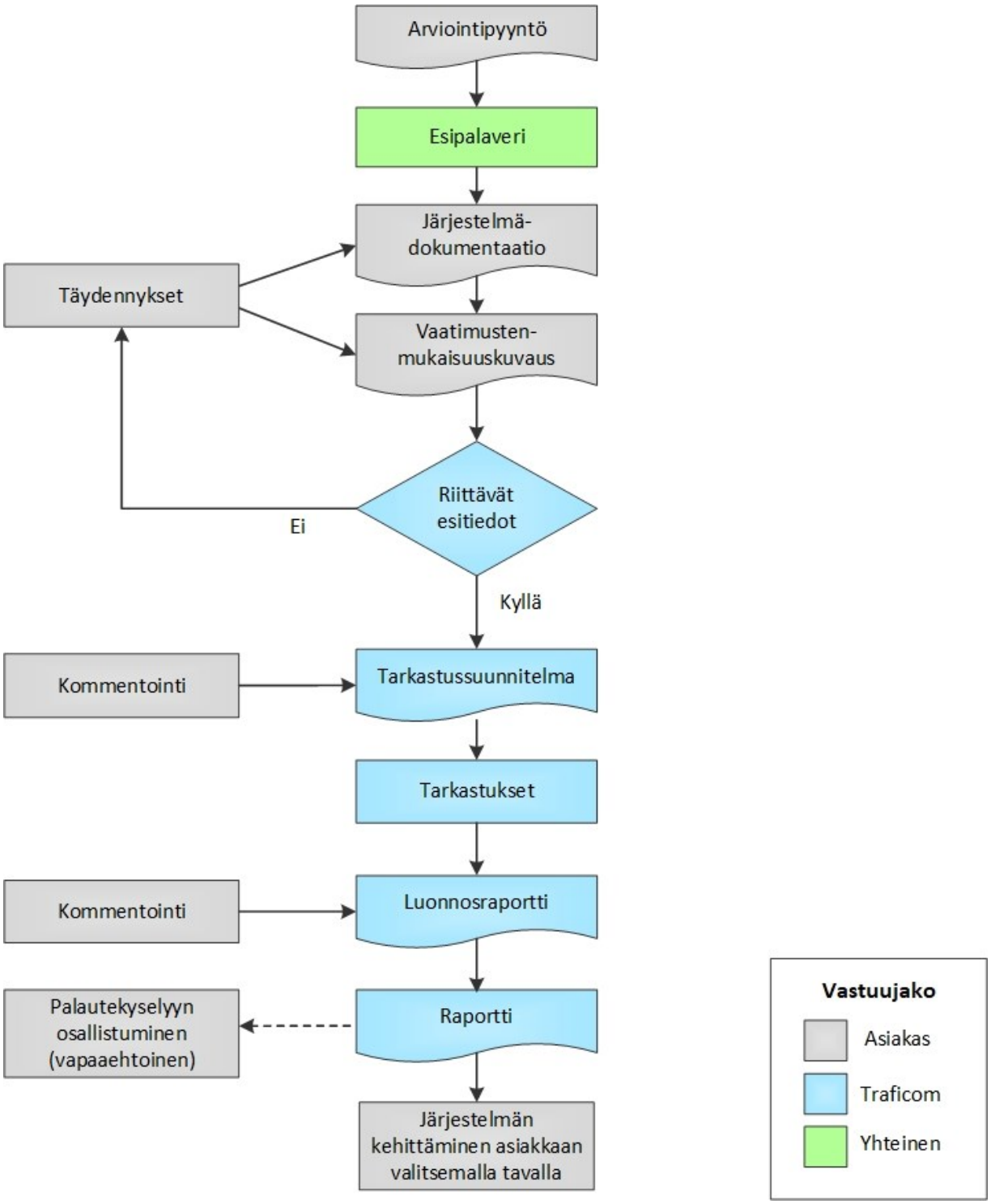
- Arvioijat (Traficom)
- Järjestelmän omistaja (vastuuviranomainen) mahdollisine alihankkijoineen (esimerkiksi järjestelmän rakentaja tai/ja ylläpitäjä)

Esipalaverissa Traficomille luovutetaan mahdollisuuksien mukaan seuraavat dokumentit:

- Kuvaus järjestelmän rakenteesta[8]
- Tiedot mahdollisista aikaisemmista tarkastuksista, arvioinneista ja/tai hyväksynnöistä raportteineen
- Tiedot mahdollisista järjestelmäkohtaisista erityisvaatimuksista

Esipalaverissa sovitaan myös aikataulu kattavamman järjestelmädokumentaation sekä vaatimustenmukaisuuskuvauksen toimittamiselle.

[5] Tyypillisesti Katakri (https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille).
[6] www.ncsa.fi > Lomakkeita > Pyyntö tietojärjestelmän tietoturvallisuushyväksynnälle tai -arvioinnille.
[7] Liikenne- ja viestintävirasto Traficom / Kirjaamo, Kyberturvallisuuskeskus / Tietojärjestelmäturvallisuus-yksikkö, Erik Palménin aukio 1, Helsinki, PL 313, 00059 TRAFICOM. Lisätietoa: https://www.traficom.fi/fi/kirjaamo.
[8] Esimerkiksi verkkokuvat ja listaukset järjestelmäkomponenteista käyttöjärjestelmineen.



Kuva 1. Arviointiprosessi.

3.3 Esitiedot ja tarkastussuunnitelma

Traficom laatii osana arvioinnin valmistelua tarkastussuunnitelmaluonnoksen, jossa kuvataan yleistasolla kyseisen järjestelmän tarkastamiseen liittyvät asiakokonaisuudet ja tarkastusten aikataulutus. Asiakasorganisaatiota edellytetään toimittamaan tarkastussuunnitteluun seuraavat esitiedot:

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

Asiakasorganisaation toimittamista kuvauksista tulee selvitä järjestelmän rakenne, toimintaperiaatteet ja suojaamiskäytännöt. Kuvausten tulee olla sellaisella tarkkuudella, että niiden avulla pystytään suunnittelemaan järjestelmän tarkastuskokonaisuudet[9] ja räätälöimään tarkastuksessa käytetyt työkalut tarkastuskohteen mukaisesti. Vaatimustenmukaisuuskuvaukseen on Traficomilta saatavissa lomake[10]. Arviointiprosessi lopetetaan, mikäli edellytettyjä kuvauksia ei toimiteta kolmen kuukauden kuluessa esipalaverista lukien.

Asiakasorganisaatiolle annetaan mahdollisuus kommentoida tarkastussuunnitelmaa. Suunnitelma viimeistellään yhteistyössä asiakasorganisaation kanssa. Asiakasorganisaatiota edellytetään järjestävän tarkastuksen mahdollistavat menettelyt tarkastuksen kohteessa. Tällaisiin menettelyihin sisältyvät tyypillisesti soveltuvat henkilöstö- ja tilavaraukset, sekä tarvittavat pääsyoikeudet fyysiseen tilaan ja tietojärjestelmiin.

3.4 Tarkastukset ja raportointi

Tarkastukseen sisältyy kohteen tietoturvallisuuden tutkiminen sen selvittämiseksi, vastaako kohteen tietoturvallisuus siihen kohdistuvia vaatimuksia. Tarkastukseen voi sisältyä tietojärjestelmän teknisen tietoturvallisuuden lisäksi myös tietojärjestelmän suojaamiseen liittyvä hallinnollisen tai/ja fyysisen turvallisuuden osuus. Tarkastuksessa käytettyjä todennusmenetelmiä on kuvattu yksityiskohtaisemmin liitteessä 1.

Tarkastuskokonaisuuden päätteeksi käydään keskeiset havainnot läpi yhdessä asiakasorganisaation kanssa. Asiakasorganisaatiolle toimitetaan myös raporttiluonnos järjestelmän tai sen osakokonaisuuden vaatimustenmukaisuudesta arvioinnin ajankohtana. Raporttiluonnos pyritään toimittamaan kuuden viikon kuluessa viimeisimmästä tarkastuskäynnistä. Asiakasorganisaatiolle annetaan mahdollisuus kommentoida raporttiluonnosta, minkä jälkeen raportti viimeistellään ja toimitetaan asiakasorganisaatiolle. Arviointiprosessi päättyy lähtökohtaisesti[11] vaatimustenmukaisuutta kuvaavan raportin toimitukseen. Jos Traficom katsoo, että arvioinnin jatkamiselle ei ole edellytyksiä ja asiakasorganisaatio on eri mieltä, Traficom voi tarvittaessa antaa asiasta valituskelpoisen perustellun päätöksen. Traficom kehittää arviointiprosessia siitä saatujen havaintojen perusteella ja toivoo, että asiakasorganisaatio osallistuu arviointiprosessiin liittyvään palautekyselyyn.

[9] Tarkastuskokonaisuus voi koostua esimerkiksi tietojärjestelmän yhden käyttöpisteen teknisen tietoturvallisuuden tarkastelusta useamman tarkastuspäivän aikana.
[10] www.ncsa.fi > Lomakkeita > Kuvaus järjestelmän vaatimustenmukaisuuden nykytilasta
[11] Arviointiprosessia voidaan tapauskohtaisesti ja kertaluonteisesti jatkaa havaittujen poikkeamien korjausten tarkastamisella ja raportoinnilla, mikä asiakasorganisaatio kykenee toteuttamaan korjaukset viipymättä raportin toimittamisen jälkeen. Traficom tekee päätöksen arviointiprosessin jatkamisen edellytyksistä kuultuaan asiasta asiakasorganisaatiota.

4 HYVÄKSYNTÄPROSESSI

Hyväksyntäprosessin päätavoitteena on varmistua siitä, että tietojärjestelmässä saavutetaan turvallisuusluokitelluille tiedoille riittävä suojaamisen taso ja että sitä ylläpidetään tietojärjestelmän elinkaaren ajan. Tässä luvussa kuvataan hyväksyntäprosessin vaiheet sillä tarkkuudella, että asiakasorganisaatio saa selkeän yleiskuvan siltä edellytettävistä toimista.

Hyväksyntäprosessi voidaan jakaa seitsemään päävaiheeseen:
1. Hyväksyntäsuunnittelu
2. Riskienarviointi ja turvallisuussuunnittelu
3. Toteutus ja testaus
4. Arviointi
5. Hyväksyntä ja käyttöönotto
6. Hyväksynnän ylläpito
7. Hyväksyntätarpeen päättyminen

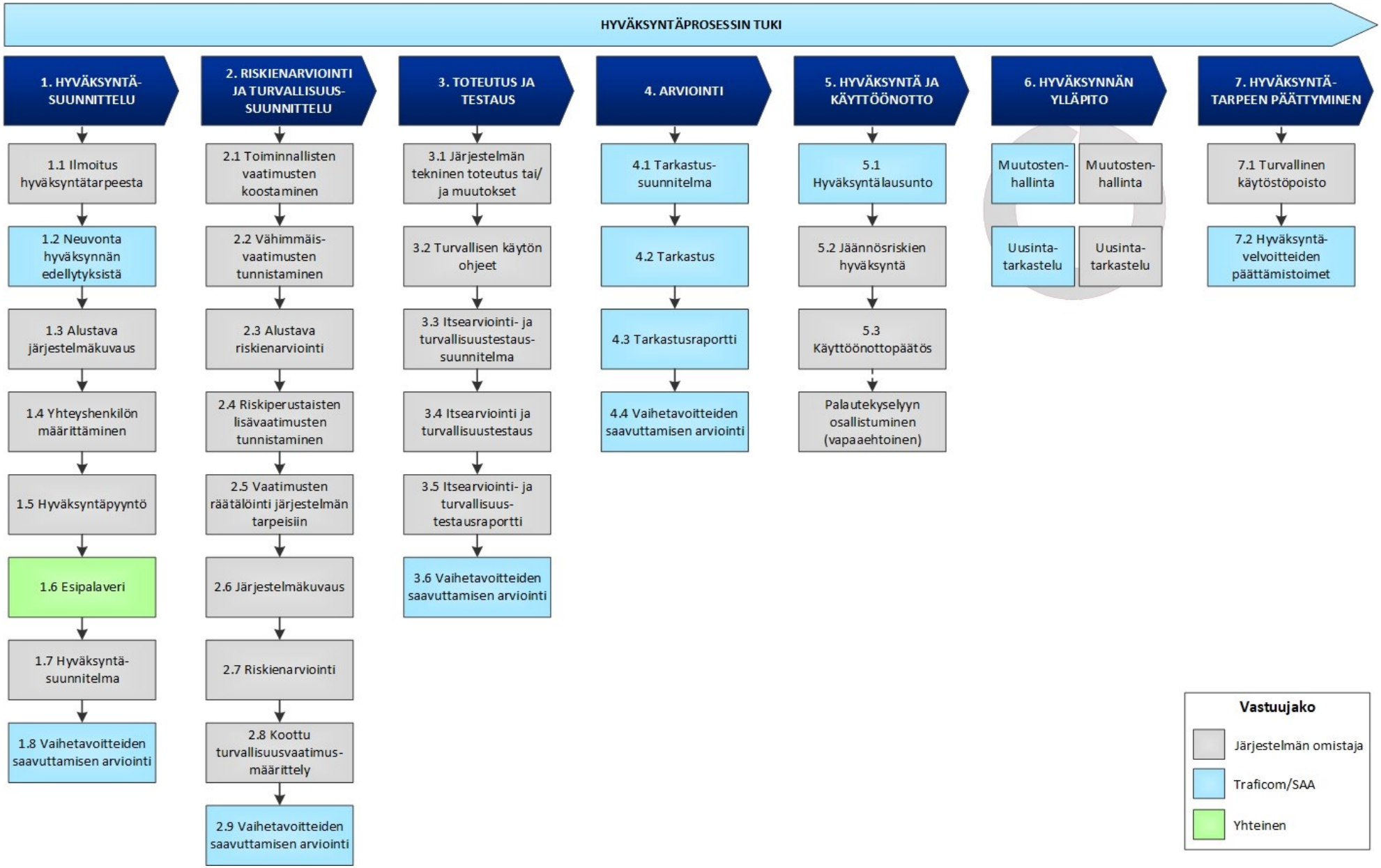
Hyväksyntäprosessin päävaiheita on havainnollistettu kuvassa 2. Hyväksyntäprosessia on havainnollistettu yksityiskohtaisemmin kuvassa 3. Hyväksyntäprosessin vaiheita voidaan räätälöidä kunkin tietojärjestelmän elinkaaren vaiheen sekä erityispiirteet huomioon ottaen.

Kuva 2. Hyväksyntäprosessin päävaiheet.

Hyväksyntäprosessin soveltaminen olemassa oleviin tietojärjestelmiin
Hyväksyntäprosessin vaiheita on tyypillisesti tarpeen räätälöidä erityisesti silloin, kun jo olemassa olevalle tietojärjestelmälle havaitaan tarve hyväksyntäprosessin läpikäynnille. Tällainen tarve voi ilmaantua esimerkiksi tilanteessa, jossa aikaisemmin kansallisen turvallisuusluokitellun tiedon käsittelyyn käytetyn tietojärjestelmän käyttötarve laajenee koskemaan myös EU:n tai Naton turvallisuusluokitellun tiedon käsittelyä.

Olemassa olevien tietojärjestelmien hyväksyntäprosessissa voidaan tyypillisesti hyödyntää aikaisemmin järjestelmän suojaamiseksi jo tehtyä työtä. Esimerkiksi järjestelmäkuvaukset (vaiheet 1.3 ja 2.6) riskienarviointi (vaiheet 2.3 ja 2.7) turvallisen käytön ohjeet (vaihe 3.2) voivat olla lähes sellaisinaan tai pienillä päivityksillä suoraan hyödynnettävissä. Vastaavasti mikäli järjestelmään on jo aikaisemmin laadittu kattavaan riskienarviointiin pohjautuva järjestelmäkohtainen turvallisuusvaatimusmäärittely (vaihe 2.8), voidaan hyväksyntäprosessissa keskittyä varmistumaan siitä, että vaatimusmäärittelyä täydennetään kattamaan myös uusien käsittelytarpeiden (esimerkiksi EU:n tai Naton turvallisuusluokitellun tiedon käsittely) mukanaan tuomat lisäriskit ja niitä pienentävät suojaukset. Järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn ajantasaisuus ja kattavuus on keskeisessä roolissa hyväksyntäprosessin myöhemmissä vaiheissa, esimerkiksi järjestelmän testauksessa (vaiheet 3.3 - 3.5) ja tarkastuksessa (vaihe 4.2).

Hyväksyntäprosessin tuki
Traficom tarjoaa asiakkailleen tukea koko hyväksyntäprosessin ajan. Tukeen sisältyy muun muassa yksityiskohtainen neuvonta prosessin vaiheista sekä eri vaiheiden tueksi laaditut mallipohjat. Traficomin Kyberturvallisuuskeskuksen kattavaa uhkatietoa hyödynnetään erityisesti tietojärjestelmäkohtaisen riskienarvioinnin sekä valittavien suojausten riittävyyden arvioinnin tukena.



Kuva 3. Hyväksyntäprosessi.

Vaihe 1: Hyväksyntäsuunnittelu

Hyväksyntäsuunnittelun tavoitteena on varmistaa hyväksyntäprosessin sujuvan etenemisen perusta: Tieto hyväksyntätarpeesta riittävän varhaisessa vaiheessa, tieto hyväksyntäprosessin edellytyksistä, yhteyshenkilöt ja vastuutahot, pyyntö hyväksyntäprosessin aloittamiseksi ja yhdessä sovittava hyväksyntäsuunnitelma.

Kuva 4. Hyväksyntäsuunnittelu osana hyväksyntäprosessia.

Vaihe 1.1: Ilmoitus hyväksyntätarpeesta

Ilmoitus hyväksyntätarpeesta suositellaan lähetettäväksi mahdollisimman varhaisessa vaiheessa, jotta mahdollisen hyväksyntätarpeen edellytykset pystytään huomioimaan tietojärjestelmän elinkaaren vaiheissa alusta lukien. Vapaamuotoinen ilmoitus hyväksyntätarpeesta pyydetään lähettämään osoitteeseen ncsa (at) traficom (piste) fi tai neuvontapalvelu (at) traficom (piste) fi.

Vaihe 1.2: Neuvonta hyväksynnän edellytyksistä

Hyväksyntäprosessin sujuvuuden varmistamiseksi Traficom suosittelee, että hyväksyntäprosessi aloitetaan palaverilla, jossa käydään läpi tietojärjestelmän hyväksyntäprosessin vaiheet sekä keskeiset tietojärjestelmän omistajalta edellytettävät toimet osana prosessia.

Vaihe 1.3: Alustava järjestelmäkuvaus

Toiminnallisten vaatimusten pohjalta laaditun alustavan järjestelmäkuvauksen tavoite on hahmottaa tietojärjestelmän arkkitehtuuria ylätasolla. Sen avulla myöhemmässä vaiheessa valittavat suojaukset pystytään sitomaan järjestelmän toiminnallisiin tarpeisiin ja arkkitehtuuriin. Alustavan järjestelmäkuvauksen perusteella pystytään yleensä myös arvioimaan sitä, onko suunniteltu arkkitehtuuri toteuttamiskelpoinen tavoiteltuihin toiminnallisiin tarpeisiin ja toisaalta yleisimpiin turvallisuusriskeihin vastaamisessa.

Vaihe 1.4: Yhteyshenkilön määrittäminen

Tietojärjestelmän omistajan (vastuuviranomaisen) tulee määrittää yhteyshenkilö, joka toimii hyväksyntäprosessin yhteyspisteenä koko hyväksyntäprosessin ajan, ja vastaa hyväksyntäprosessiin liittyvien toimien koordinoinnista ja etenemisestä järjestelmän omistajalla ja sen mahdollisissa alihankkijoissa.

Vaihe 1.5: Hyväksyntäpyyntö

Hyväksyntäpyyntövaiheen sisältö ja toimittaminen mukailee luvussa 3.1 kuvattua arviointipyyntöä. Pyyntöön on Traficomilta saatavissa lomakepohja[12]. Pyyntö on toimitettava kirjallisesti Traficomin kirjaamoon[13].

Vaihe 1.6: Esipalaveri

Esipalaverin tavoitteena on saada alustava yleiskuva hyväksynnän kohteena olevasta tietojärjestelmästä, sekä saavuttaa yhtenevä ymmärrys hyväksyntäprosessin käytännön toimista. Esipalaverissa keskitytään tyypillisesti hyväksyntäprosessin vaiheisiin, edellytyksiin, vastuisiin ja aikataulutukseen. Esipalaveri pidetään lähtökohtaisesti seuraavien toimijoiden kesken:

- Arvioijat (Traficom)
- Järjestelmän omistaja (vastuuviranomainen) mahdollisine alihankkijoineen (esimerkiksi järjestelmän rakentaja tai/ja ylläpitäjä)

Kuva 5. Hyväksyntä-suunnittelu.

Mikäli kyseessä on jo olemassa oleva tietojärjestelmä tai mikäli järjestelmäsuunnittelu on jo aloitettu esipalaveriin mennessä, Traficomille luovutetaan mahdollisuuksien mukaan seuraavat dokumentit:

- Kuvaus järjestelmän suunnitellusta tai jo olemassa olevasta rakenteesta[14]
- Tiedot mahdollisista aikaisemmista tarkastuksista, arvioinneista ja/tai hyväksynnöistä raportteineen
- Tiedot mahdollisista järjestelmäkohtaisista erityisvaatimuksista

[12] www.ncsa.fi > Lomakkeita > Pyyntö tietojärjestelmän tietoturvallisuushyväksynnälle tai -arvioinnille.
[13] Liikenne- ja viestintävirasto Traficom / Kirjaamo, Kyberturvallisuuskeskus / Tietojärjestelmäturvallisuus-yksikkö, Erik Palménin aukio 1, Helsinki, PL 313, 00059 TRAFICOM. Lisätietoa: https://www.traficom.fi/fi/kirjaamo.
[14] Esimerkiksi verkkokuvat ja listaukset järjestelmäkomponenteista käyttöjärjestelmineen.

Vaihe 1.7: Hyväksyntäsuunnitelma
Hyväksyntäsuunnitelmaan kootaan hyväksyntäprosessin aikataulutus, vastuutahot sekä tunnistetut riippuvuudet. Hyväksyntäsuunnitelma voidaan laatia Traficomin mallipohjaan, tai vastaavat tiedot voidaan kuvata myös esimerkiksi järjestelmän omistajan ja Traficomin välisen esipalaverin muistioon. Kuten muutkin hyväksyntäprosessin vaiheiden asiakirjat, hyväksyntäsuunnitelma valmistellaan järjestelmän omistajan ja Traficomin yhteistyössä.

Vaihe 1.8: Vaihetavoitteiden saavuttamisen arviointi
Arvioidaan, onko hyväksyntäsuunnitelman perusteella edellytykset jatkaa hyväksyntäprosessin seuraavaan vaiheeseen vai tarvitaanko vielä täydennyksiä. Keskeisten edellytysten täyttyessä hyväksytään jatko hyväksyntäprosessin seuraavaan vaiheeseen.

Vaihe 2: Riskienarviointi ja turvallisuussuunnittelu

Riskienarvioinnin ja turvallisuussuunnittelun päätavoitteena on se, että järjestelmään ja siinä käsiteltäviin tietoihin kohdistuvat turvallisuustavoitteet tulevat huomioiduksi jo järjestelmän suunnitteluvaiheessa ja järjestelmän elinkaaren myöhemmissä vaiheissa. Valmistelutyössä pystytään yleensä huomioimaan ja tarvittaessa myös korjaamaan mahdolliset turvallisuuspuutteet jo varhaisessa vaiheessa. Tämä tukee koko hyväksyntäprosessin nopeutta ja kustannustehokkuutta.

Kuva 6. Riskienarviointi ja turvallisuussuunnittelu osana hyväksyntäprosessia.

Vastuu valmistelutyöhön sisältyvien kuvausten laatimisesta on asiakasorganisaatiolla[15]. Kuvausten hyväksyntävastuu on Traficomilla. Valmistelutyöhön kuuluvia tehtäviä on mahdollista yhdistellä tarkoituksenmukaisesti. Esimerkiksi riskienarviointi ja tietojärjestelmäkuvaus voi olla perusteltua sisällyttää osaksi järjestelmäkohtaista turvallisuusvaatimusmäärittelyä.

Asiakasorganisaation valmistelutyössä on hyvä huomioida erityisesti turvallisuusvaatimusmäärittelyn järjestelmäkohtaisuus. Tällä tarkoitetaan sitä, että vähimmäisvaatimukset ja riskiperusteiset lisävaatimukset kootaan järjestelmäkohtaiseen turvallisuusvaatimusmäärittelyyn. Järjestelmäkohtaisessa turvallisuusvaatimusmäärittelyssä huomioidaan tiedon luottamuksellisuuden ja eheyden lisäksi myös tiedon saatavuuteen liittyvät näkökulmat. Järjestelmäkohtaisessa turvallisuusvaatimusmäärittelyssä tulee huomioida myös mahdolliset yhteenliitännät muihin tietojärjestelmiin sekä mahdolliset riippuvuudet muista tietojärjestelmistä. Vaatimusten täyttämisessä on rajallinen mahdollisuus hyödyntää myös korvaavia suojauksia tilanteissa, joissa ne ovat riskienhallinnallisesti perusteltuja[16]. Turvallisuusluokitellun tiedon suojaamiseen liittyvien vaatimusten koostumista on havainnollistettu kuvassa 7.

Kuva 7. Vaatimusten koostuminen.

Kuvausten laadinta on yleensä iteratiivinen prosessi, jossa asiakasorganisaatio alihankkijoineen käy aktiivista vuoropuhelua Traficomin kanssa. Traficomilta on saatavissa mallipohjat, joissa kuvataan yksityiskohtaisemmin kuvausten valmistelussa tarvittavien tietojen kattavuutta ja tarkkuutta. **Traficom suosittelee, että asiakasorganisaatio hyödyntää Traficomin tukea erityisesti tietojärjestelmäkohtaisessa riskienarvioinnissa sekä suojausten valinnassa.**

[15] Asiakasorganisaationa on usein tietojärjestelmän omistaja. Tilanteissa, joissa esimerkiksi tietojärjestelmään liittyvää suunnittelu-, rakennus- tai testaustyöhön osallistuu alihankkijoita tai toimittajia, asiakasorganisaatio on vastuussa kokonaisuuden hallinnasta.
[16] Esimerkiksi tietojärjestelmään kohdistuva vaatimus vahvasta, useaan todennustekijään pohjautuvasta tunnistautumisesta voi joissain ympäristöissä olla toteutettavissa myös fyysisen turvallisuuden menettelyin.

Vaihe 2.1: Toiminnallisten vaatimusten koostaminen
Järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn laadinta suositellaan yleensä aloitettavaksi toiminnallisten vaatimusten koostamisesta. Toiminnalliset vaatimukset ohjaavat tietojärjestelmän jatkosuunnittelua ja sovellettavien suojausten valintaa.

Vaihe 2.2: Vähimmäisvaatimusten tunnistaminen
Vähimmäisvaatimuksiin sisältyvät tyypillisesti lakisääteiset vaatimukset, kuten esimerkiksi velvoite turvallisuusluokitellun tiedon salaamiseen siirrettäessä sitä julkisen verkon yli. Jos samassa järjestelmässä on tarkoitus käsitellä suojausvaatimuksiltaan eroavia tietoja, esimerkiksi kansallista, EU:n tai/ja Naton turvallisuusluokiteltua tietoa, tulee näihin kaikkiin kohdistuvat vähimmäisvaatimukset tunnistaa ja koota osaksi järjestelmäkohtaista turvallisuusvaatimusmäärittelyä.

Vaihe 2.3: Alustava riskienarviointi
Alustavan riskienarvioinnin tavoite on tunnistaa keskeisimmät tietojärjestelmään ja siinä käsiteltäviin tietoihin kohdistuvat riskit, ja arvioida riskejä vähimmäisvaatimuksista seuraavien vähimmäissuojausten valossa. Alustavassa riskienarvioinnissa pystytään yleensä tunnistamaan myös toiminnallisiin tarpeisiin (esimerkiksi saatavuuteen) liittyvät riskit, joita ei ainoastaan vähimmäisvaatimukset täyttämällä pystytä useinkaan pienentämään riittävästi. Alustava riskienarviointi tuottaakin usein tietoa riskiperustaisten lisävaatimusten tunnistamiseen.

Vaihe 2.4: Riskiperustaisten lisävaatimusten tunnistaminen
Useissa tietojärjestelmissä on perusteltua täydentää vähimmäisvaatimuksia riskiperustaisilla lisävaatimuksilla. Tyypillisesti lisävaatimukset liittyvät esimerkiksi tietojärjestelmän toiminnallisiin tarpeisiin tai esimerkiksi tavanomaisesta korkeampiin saatavuus- tai jatkuvuustarpeisiin. Lisävaatimukset perustuvat tyypillisesti tietojärjestelmäkohtaiseen riskienarviointiin tai tietojärjestelmän omistajan (vastuuviranomaisen) toimintaa ohjaaviin muihin vaatimuksiin.

Vaihe 2.5: Vaatimusten räätälöinti järjestelmän tarpeisiin
Suojausvaatimukset suositellaan räätälöitäväksi riskienarvioinnin perusteella siten, että löydetään sopiva tasapaino toiminnallisten tarpeiden, kustannusten ja turvallisuuteen kohdistuvan jäännösriskin välillä. Räätälöinnissä myös konkretisoidaan, miten juuri kyseisessä tietojärjestelmässä mikäkin vaatimus toteutetaan (esimerkiksi käyttäjätunnistuksen toteutus vain tietotekniikalla vs. osin fyysiseen turvallisuuteen nojautuen). Räätälöinti tukee myös sitä, että tietojärjestelmittäin merkittävästikin eroavat saatavuustarpeet ja niiden varmistamiseen tähtäävät suojaukset saadaan mitoitettua ja kuvattua juuri kyseisen tietojärjestelmän tarpeisiin sopiviksi. Kuten muissakin hyväksyntäprosessin vaiheissa, vaatimusten räätälöinti pohjautuu yhteistyöhön ja keskusteluihin tietojärjestelmän omistajan (vastuuviranomaisen) ja Traficomin kanssa.

Kuva 8. Turvallisuus-suunnittelu.

Vaihe 2.6: Järjestelmäkuvaus
Toiminnallisten ja turvallisuusvaatimusten pohjalta laadittavan täydennetyn järjestelmäkuvauksen tavoite on tukea myöhemmissä vaiheessa järjestelmän toteuttamista, järjestelmäomistajan itsearviointia ja testaamista sekä tietojärjestelmän arviointia. Järjestelmänkuvauksen tavoitteena on tukea myös järjestelmän omistajan muutostenhallintaa sekä riskienarviointia järjestelmän koko elinkaaren ajan.

Vaihe 2.7: Riskienarviointi
Täydennetyn riskienarvioinnin tavoite on tarjota perusteet valituille suojauksille ja tukea järjestelmän turvallisuudesta huolehtimista ja muutostenhallintaa koko järjestelmän elinkaaren ajan.

Vaihe 2.8: Koottu turvallisuusvaatimusmäärittely
Tietojärjestelmäkohtaiseen turvallisuusvaatimusmäärittelyyn kootaan tyypillisesti vaiheissa 2.1 - 2.7 laaditut kuvaukset, jotta nämä ovat helposti hyödynnettävissä tietojärjestelmän elinkaaren muissa vaiheissa. Koottua turvallisuusvaatimusmäärittelyä hyödynnetään muun muassa tietojärjestelmän teknisessä suunnittelussa ja toteuttamisessa, turvallisuuden testaamisessa ja arvioinnissa sekä myöhemmin myös hyväksytyn järjestelmän muutostenhallinnassa.

Vaihe 2.9: Vaihetavoitteiden saavuttamisen arviointi
Arvioidaan, onko riskien arvioinnin ja turvallisuusvaatimusten määrittelyn perusteella edellytykset jatkaa hyväksyntäprosessin seuraavaan vaiheeseen vai tarvitaanko täydennyksiä. Keskeisten edellytysten täyttyessä hyväksytään jatko hyväksyntäprosessin seuraavaan vaiheeseen.

Vaihe 3: Toteutus ja testaus

Toteutus ja testaus -vaiheen päätavoite on tukea järjestelmän omistajaa (vastuuviranomaista) turvallisuussuunnittelun pohjalta syntyneen järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn mukaisen tietojärjestelmän ja sen suojausten käyttöönotossa. Vaiheen tavoite on tuottaa tietojärjestelmän omistajalle tieto siitä, miten turvallisuusvaatimusmäärittely on tietojärjestelmässä toteutettu ja tukea järjestelmän omistajan vastuulle kuuluvaa tietojärjestelmän suojaamista koko sen elinkaaren ajan.

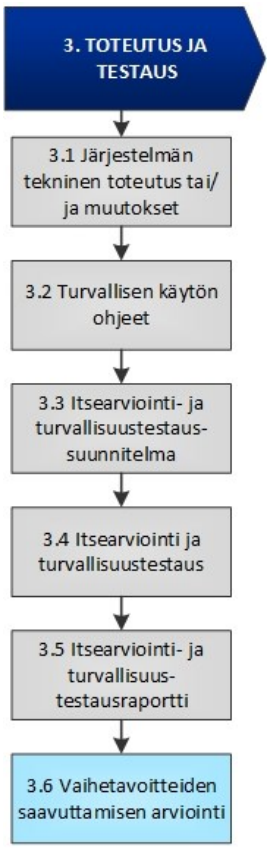
Kuva 9. Toteutus ja testaus osana hyväksyntäprosessia.

Vaihe 3.1: Järjestelmän tekninen toteutus tai/ja muutokset
Järjestelmän toteutus tai/ja muutokset järjestelmäkuvauksen (vaihe 2.6) ja turvallisuusvaatimusmäärittelyn (vaihe 2.8) pohjalta.

Vaihe 3.2: Turvallisen käytön ohjeet
Turvallisen käytön ohjeiden tarkoitus on varmistaa, että tietojärjestelmän loppukäyttäjät ja ylläpitäjät tuntevat tietojärjestelmän turvalliseen käyttöön liittyvät menettelyt eikä loppukäyttäjien tai ylläpitäjien toiminta vaaranna järjestelmän turvallisuutta. Turvallisen käytön ohjeet suositellaan laadittavaksi rooleittain esimerkiksi eri loppukäyttäjärooleille ja eri ylläpitoroolien henkilöstölle. Ylläpitäjien ohjeisiin sisältyy tyypillisesti esimerkiksi haavoittuvuuksienhallintaan sekä muutosten- ja käyttäjähallintaan liittyvät säännölliset toimenpiteet.

Vaihe 3.3: Itsearviointi- ja turvallisuustestaussuunnitelma
Itsearviointi- ja testaussuunnitelman tavoitteena on, että tietojärjestelmän omistaja (vastuuviranomainen) pystyy varmistumaan vastuullaan olevan tietojärjestelmän suojaamisesta järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn mukaisilla suojauksilla. Itsearviointi- ja testaussuunnitelman tulee kattaa jokaisen turvallisuusvaatimusmäärittelyyn kootun vaatimuksen toteuttaminen tietojärjestelmässä. Kuten muissakin hyväksyntäprosessin vaiheissa, itsearviointi- ja testaussuunnitelma pohjautuu tietojärjestelmän omistajan (vastuuviranomaisen) ja Traficomin yhteistyöhön ja keskusteluihin. Mitä syvällisemmin ja kattavammin itsearviointi ja testaus saadaan toteutettua, ja mitä nopeammin siinä mahdollisesti havaittavat puutteet korjattua, sitä todennäköisemmin myös hyväksyntäprosessin seuraavat vaiheet etenevät nopeasti.

Vaihe 3.4: Itsearviointi ja turvallisuustestaus
Järjestelmän omistajan vastuulla olevaan itsearviointiin ja turvallisuustestaukseen voidaan hyödyntää myös järjestelmän omistajan alihankkijoita, edellyttäen että alihankkijoiden käyttö on huomioitu edellisessä vaiheessa laaditussa suunnitelmassa.



Kuva 10. Toteutus ja testaus.

Vaihe 3.5: Itsearviointi- ja turvallisuustestausraportti
Itsearviointi- ja turvallisuustestausraportissa selostetaan kunkin turvallisuusvaatimusmäärittelyssä kuvatun vaatimuksen täyttymisen tila ja vaatimuksen todentamiseen käytetyt menetelmät. Järjestelmän omistaja vastaa havaittujen puutteiden korjaamisesta.

Vaihe 3.6: Vaihetavoitteiden saavuttamisen arviointi
Arvioidaan, onko tietojärjestelmällä itsearvioinnin ja turvallisuustestauksen perusteella edellytykset jatkaa hyväksyntäprosessin seuraavaan vaiheeseen vai tarvitaanko muutoksia tai täydennyksiä. Keskeisten edellytysten täyttyessä hyväksytään jatko hyväksyntäprosessin seuraavaan vaiheeseen.

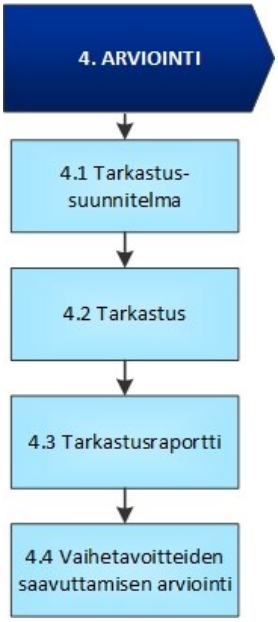
Vaihe 4: Arviointi

Arviointivaiheen keskeisenä tavoitteena on täydentää tietojärjestelmän omistajan (vastuuviranomaisen) itsearviointia ja testausta todentamisella, jonka tekee riippumaton ulkoinen arvioija. Riippumattomassa arvioinnissa otetaan huomioon asiakkaan itsearvioinnin ja testauksen toteutus ja havainnot.

Kuva 11. Arviointi osana hyväksyntäprosessia.

Vaihe 4.1: Tarkastussuunnitelma

Traficom laatii tarkastussuunnitelmaluonnoksen, jossa kuvataan yleistasolla kyseisen järjestelmän tarkastamiseen liittyvät asiakokonaisuudet ja tarkastusten aikataulu. Asiakasorganisaatio voi halutessaan kommentoida tarkastussuunnitelmaa ja Traficom viimeistelee sen yhteistyössä asiakasorganisaation kanssa. Asiakasorganisaation täytyy järjestää tarkastamisessa tarvittavat menettelyt kuten henkilöstö- ja tilavaraukset, sekä tarvittavat pääsyoikeudet fyysiseen tilaan ja tietojärjestelmiin.



Kuva 12. Arviointi.

Vaihe 4.2: Tarkastus

Tarkastuksessa tutkitaan kohteen tietoturvallisuutta sen selvittämiseksi, vastaako kohteen tietoturvallisuuden tila siihen kohdistuvia vaatimuksia. Tarkastukseen sisältyy tietojärjestelmän teknisen tietoturvallisuuden lisäksi tyypillisesti myös tietojärjestelmän suojaamiseen liittyvä hallinnollinen ja fyysinen turvallisuus. Hallinnollisen ja fyysisen turvallisuuden osuuksissa nojaudutaan tyypillisesti suojelupoliisin tai Pääesikunnan arvioihin turvallisuusjärjestelyjen riittävyydestä, ellei toimivaltaisten turvallisuusviranomaisten kesken ole muuta sovittu tehtävien hoitamiseksi tarkoituksenmukaisesti (588/2004). Myös kaupallisten tietoturvallisuuden arviointilaitosten palveluja voi olla mahdollista hyödyntää suojelupoliisin tai Pääesikunnan arviointeihin valmistautumisessa. Tarkastuskokonaisuuden päätteeksi käydään keskeiset havainnot läpi asiakasorganisaation kanssa. Tarkastuksessa käytettyjä todennusmenetelmiä on kuvattu yksityiskohtaisemmin liitteessä 1.

Vaihe 4.3: Tarkastusraportti

Asiakasorganisaatiolle toimitetaan pyydettäessä myös raportti järjestelmän tai sen osakokonaisuuden tietoturvallisuuden nykytilasta.

Vaihe 4.4: Vaihetavoitteiden saavuttamisen arviointi

Arvioidaan, onko tietojärjestelmälle määriteltyjen vaatimusten täyttyminen pystytty todentamaan arvioinnissa ja onko tietojärjestelmällä edellytykset jatkaa hyväksyntäprosessin seuraavaan vaiheeseen. Keskeisten edellytysten täyttyessä hyväksytään jatko hyväksyntäprosessin seuraavaan vaiheeseen.

Vaihe 5: Hyväksyntä ja käyttöönotto

Hyväksyntä ja käyttöönotto -vaiheessa kootaan järjestelmän hyväksyntään ja sen ylläpitämiseen sekä järjestelmän käyttöönottoon liittyvät ehdot ja rajoitukset, jotta järjestelmä saadaan käyttöön ja jotta sitä ylläpidetään hyväksyttävillä jäännösriskitasoilla.

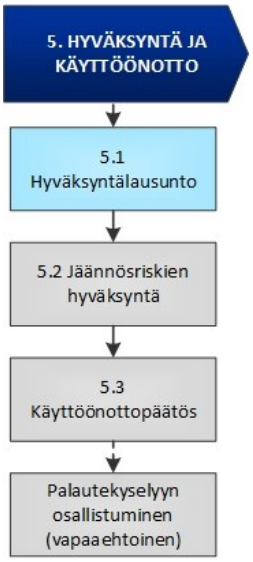
Kuva 13. Hyväksyntä ja käyttöönotto osana hyväksyntäprosessia.

Vaihe 5.1: Hyväksyntälausunto

Järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn täyttävälle järjestelmälle voidaan laatia hyväksyntälausunto[17]. Hyväksyntälausunnossa kuvataan tyypillisesti hyväksynnän kattavuus sekä ehdot sen ylläpitämiselle ja uusimiselle. Hyväksyntälausunnon ehtona on, että tarkastuksen kohde säilyttää turvallisuuden tason vähintään tarkastetun mukaisena.

Hyväksyntälausunto on voimassa pääsääntöisesti kolme vuotta myöntämispäivästä lukien[18]. Hyväksyntälausunnon voimassaolo lakkaa, mikäli kohteessa tapahtuu merkittävä sen turvallisuuteen vaikuttava muutos. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten ohjelmistojen turvapäivitysten asennukset, eivät aiheuta hyväksyntälausunnon voimassaolon lakkaamista. Tapauskohtaiset ehdot määritellään hyväksyntälausunnossa. Merkittävät muutokset tulee hyväksyttää etukäteen Traficomilla.

Jos järjestelmän on todettu täyttävän järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn vähimmäisvaatimukset, mutta ei riskiperustaisia lisävaatimuksia (vrt. kuva 7), järjestelmälle voidaan laatia tilapäinen hyväksyntälausunto[19]. Tilapäinen hyväksyntälausunto on voimassa tyypillisesti vain lyhytaikaisesti ja edellyttää asiakasorganisaatiolta uskottavaa suunnitelmaa, jonka mukaisesti järjestelmä saatetaan täyttämään myös riskiperustaiset lisävaatimukset.



Kuva 14. Hyväksyntä ja käyttöönotto.

Vaihe 5.2: Jäännösriskien hyväksyntä

Turvallisuusvaatimusmäärittelyn osin tai kokonaan täyttävään, hyväksyntälausunnon tai tilapäisen sellaisen saaneeseen tietojärjestelmään jää jäännösriskejä, joiden hyväksyntä kuuluu tietojärjestelmän omistajan (vastuuviranomainen) vastuulle. Tietojärjestelmän omistajaa suositellaan punnitsemaan riskienarvioinnissaan sitä, ovatko jäännösriskit hyväksyttävissä sellaisenaan, vai edellyttääkö järjestelmän omistaja tietojärjestelmään lisäsuojauksia jäännösriskien pienentämiseksi ennen käyttöönottopäätöstä.

Vaihe 5.3: Käyttöönottopäätös

Päätös järjestelmän käyttöönottamisesta on tietojärjestelmän omistajan vastuulla. Omistaja voi asettaa käyttöönotolle hyväksyntälausunnon tai tilapäisen sellaisen ehtojen lisäksi myös muita ehtoja tai rajoitteita, esimerkiksi hyväksyntälausuntoa lyhyemmän voimassaoloajan.

Palautekyselyyn osallistuminen (vapaaehtoinen)

Traficom kehittää hyväksyntäprosessia siitä saatujen havaintojen perusteella ja toivoo, että asiakasorganisaatio osallistuu hyväksyntäprosessiin liittyvään palautekyselyyn.

[17] Engl. SAS, Security Accreditation Statement.
[18] Hyväksyntälausunnon enimmäispituuteen otetaan kantaa useissa kansainvälisissä tietoturvallisuusvelvoitteissa. Enimmäispituuden määritys perustuu tyypillisesti riskienhallinnalliseen tasapainoon jäännösriskien, toiminnallisten tarpeiden ja käytettävissä olevien resurssien välillä.
[19] Engl. ISAS, Interim Security Accreditation Statement.

Vaihe 6: Hyväksynnän ylläpito

Tietojärjestelmää ja sen turvallisuuden tasoa tulee ylläpitää tietojärjestelmän elinkaaren ajan hyväksyntälausunnon ehtojen mukaisesti. Kuten edellä kuvattu, tapauskohtaiset ehdot määritellään hyväksyntälausunnossa. Tavanomaisesta ylläpidosta aiheutuvat muutokset, kuten ohjelmistojen turvapäivitysten asennukset, eivät aiheuta hyväksyntälausunnon voimassaolon lakkaamista. Sen sijaan merkittäviin muutoksiin liittyvät riskit ja muutosten toteuttamismahdollisuudet tulee arvioida yhteistyössä Traficomin kanssa. Tällaisia voivat olla esimerkiksi merkittävät verkkorakenteen, henkilöstön, turvakäytäntöjen tai toimitilojen muutokset.

Kuva 15. Hyväksynnän ylläpito osana hyväksyntäprosessia.

Hyväksyntälausunnon ylläpito nojaa tyypillisesti merkittävin osin tietojärjestelmän omistajan (vastuuviranomaisen) muutoshallintakäytäntöihin. Hyväksyntälausunnon jatkamiseksi arvioidaankin tapauskohtaisesti miltä osin voidaan nojautua muutoshallintakäytäntöjen tuottamiin tietoihin, muihin tietojärjestelmän omistajan tuottamiin tietoihin ja miltä osin on tarvetta myös riippumattoman osapuolen arvioinnille.

Erityisesti tietojärjestelmille, joita kehitetään ketterän kehitysmallin mukaisesti, ensimmäinen hyväksytty (akkreditoitu) ja käyttöönotettu versio muuttuu tyypillisesti merkittävästi hyväksynnän ylläpitovaiheen aikana. Ensimmäinen hyväksytty versio kattaakin tällaisissa tapauksissa tyypillisesti tietojärjestelmäalustan ja kehitystyön suojaamisen sekä muutostenhallinnan käytännöt. On myös tyypillistä, että saman tietojärjestelmäalustan päälle kehitetään useita eri palveluja.

Kuva 16. Hyväksynnän ylläpito.

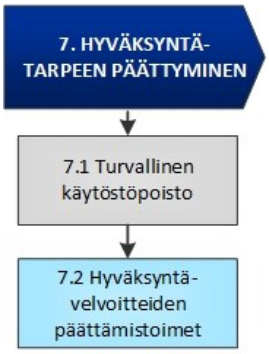
Vaihe 7: Hyväksyntätarpeen päättyminen

Hyväksyntätarve voi päättyä tietojärjestelmän elinkaaren päättyessä tai esimerkiksi korvaavan järjestelmän käyttöönoton myötä. Tämän vaiheen tavoitteena on varmistua siitä, että tietojärjestelmässä sen elinkaaren aikana käsitellyt tiedot eivät vaarannu käsittelyn päättyessä.

Kuva 17. Hyväksyntätarpeen päättyminen osana hyväksyntäprosessia.

Vaihe 7.1: Turvallinen käytöstäpoisto
Tietojärjestelmän omistajan vastuulle kuuluvassa turvallisessa käytöstäpoistossa täytyy tyypillisesti olla menettelyt tietojärjestelmän luotettavaan tuhoamiseen ja täytyy huomioida esimerkiksi tiettyjen salausteknisten aineistojen tai laitteistojen (COMSEC) käsittelyn vaatimukset.

Vaihe 7.2: Hyväksyntävelvoitteiden päättämistoimet
Hyväksyntävelvoitteiden päättämistoimiin voi sisältyä kirjanpidollisten toimien lisäksi esimerkiksi salausteknisten laitteistojen kansainvälisiin velvoitteisiin liittyvät palautukset.



Kuva 18. Hyväksyntätarpeen päättyminen.

4.1 Prosessien erityispiirteitä

4.1.1 Kansainvälisten järjestöjen toimittamien tietojärjestelmien hyväksyntäprosessi

Tässä luvussa kuvatut menettelyt soveltuvat muun muassa EU:n ja Naton turvallisuusluokitellun tiedon sähköisen käsittelyn arviointiin. Joidenkin kansainvälisten järjestöjen omistamiin ja jäsenmaihin toimittamiin tietojärjestelmiin on käytössä moniportainen hyväksyntäprosessi. Esimerkiksi joihinkin EU:n turvallisuusluokiteltua tietoa käsitteleviin tietojärjestelmiin käytetään mallia, jossa Traficomin vastuulla on tarkastusten perusteella antaa tietojärjestelmän vaatimustenmukaisuutta kuvaava lausunto[20] jäsenmaista koostuvalle turvallisuushyväksyntälautakunnalle[21], joka on vastuussa kyseisen tietojärjestelmän hyväksyntälausunnon myöntämisestä. Joidenkin kansainvälisten järjestöjen toimittamien tietojärjestelmien hyväksyntäprosesseissa on myös tietojärjestelmäkohtaisia, kyseisen tietojärjestelmän turvallisuushyväksyntälautakunnassa sovittuja eroavaisuuksia. Eroavaisuudet voivat koskea esimerkiksi vaatimustenmukaisuutta kuvaavien lausuntojen kattavuuden rajauksia tai lausuntojen jakamista vaiheittain toimitettaviin osa-alueisiin. Vaatimustenmukaisuuslausunnot painottuvat tyypillisesti toimitettua tietojärjestelmää ympäröiviin suojauksiin kuten fyysiseen turvallisuuteen, henkilöstöturvallisuuteen sekä käyttöpisteen hajasäteilysuojaukseen.

4.1.2 Kahdenvälisten tietoturvallisuussopimusten piiriin kuuluvien tietojärjestelmien hyväksyntä

Kahdenvälisissä tietoturvallisuussopimuksissa[22] on pääsääntöisesti sovittu vastavuoroisen suojaamisen periaatteesta. Tämä tarkoittaa sitä, että sopijakumppaneiden kyseessä olevan luokan tietoa suojataan kussakin maassa kuten kyseessä olevan maan kansallinen lainsäädäntö vastaavan luokan tiedon suojauksilta edellyttää. Yksityiskohdat tulee varmistaa tapauskohtaisesti kunkin käsiteltävän tiedon sopimuksesta. Lisäksi tulee varmistaa, liittyykö kyseiseen käsiteltävään tietoon muita erityisvaatimuksia, esimerkiksi hankekohtaisia lisämäärityksiä.

Kahden- tai monenvälisiin sopimuksiin liittyy usein erityisvaatimus rajat ylittävän osuuden hyväksyttämisestä toimivaltaisilla turvallisuusviranomaisilla. Tällöin hyväksyntäprosessia sovelletaan valtioiden rajat ylittävään tietojärjestelmäosuuteen, joka koostuu tyypillisesti sähköisestä tiedonsiirtoratkaisusta ja siihen liittyvästä yhdyskäytäväratkaisusta. Edellä mainittuihin sisältyy tyypillisesti myös salausratkaisu, sen Suomessa sijaitseva käyttöpiste sekä tiedon vastaanotto-/lähetysjärjestelmä. Yhdyskäytäväratkaisuun liitettyyn tai muuhun kansalliseen tietojärjestelmään, jossa käsitellään toisen sopijapuolen turvallisuusluokiteltua tietoa, sovelletaan yleensä sopimusten perusteella vastavuoroisuusperiaatetta, eikä se siten tyypillisesti sisälly Liikenne- ja viestintäviraston hyväksyntäprosessiin. Vastaavaa periaatetta sovelletaan myös sellaisiin kansainvälisiin harjoituksiin, joissa on tarve käsitellä kahden- tai monenvälisten sopimusten piiriin kuuluvaa turvallisuusluokiteltua tietoa ja joissa tietojärjestelmien hyväksyntävastuut jakautuvat kyseiseen harjoitukseen osallistuvien kesken.

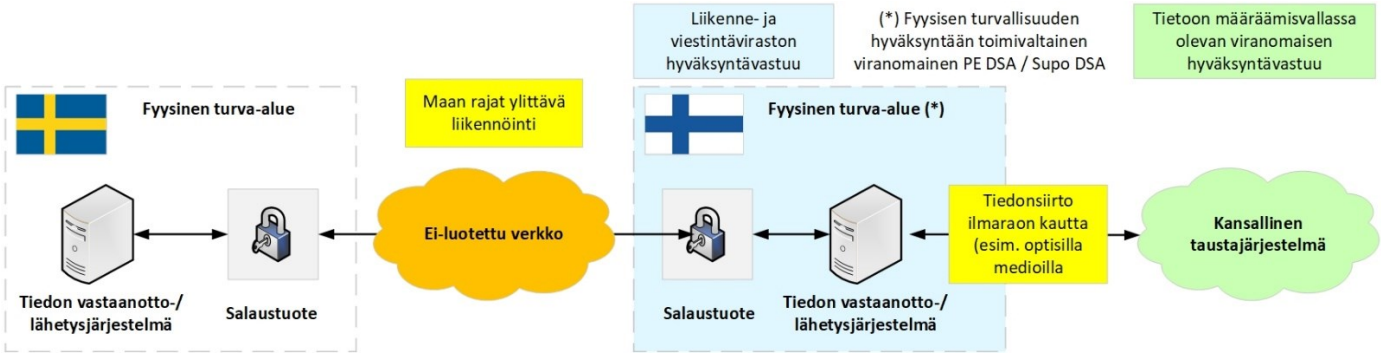
Taulukossa 1 on kuvattuna kansallisten ja kansainvälisten turvallisuusluokiteltujen tietojen sähköisen käsittelyn (tietojärjestelmien) hyväksyntävastuut viranomaisittain. Kuvaus ei ota kantaa tietojenkäsittelyyn liittyvän turvallisuusjohtamisen ja fyysisen turvallisuuden hyväksyntävastuisiin. Kuvaus ottaa kantaa kansallisten turvallisuusluokiteltujen tietojen lisäksi yleisimpiin kahden- tai monenvälisten sopimusten piiriin kuuluviin tietoihin, sekä vertailun vuoksi myös EU:n ja Naton turvallisuusluokiteltuihin tietoihin. Kuvaus ei kata kaikkia erityistapauksia, eikä esimerkiksi yksittäisen sopimuksen alaisissa hankekohtaisissa määrityksissä sovittuja eroavia käytäntöjä.

Kuvassa 19 on havainnollistettu hyväksyntävastuita tilanteessa, jossa on kyseessä kansainvälinen, kahden- tai monenvälinen sopimus, johon sisältyy rajat ylittävää tiedonsiirtoa. Kuvassa 20 on havainnollistettu hyväksyntävastuita tilanteessa, jossa on kyseessä kansainvälinen, kahden- tai monenvälinen sopimus, johon sisältyy rajat ylittävää tiedonsiirtoa ja jossa tiedon lähetys-/vastaanottojärjestelmä on yhdistetty yhdyskäytäväratkaisulla kansalliseen taustajärjestelmään.

[20] Engl. SoC, Statement of Compliance.
[21] Engl. SAB, Security Accreditation Board.
[22] Voimassa olevat tietoturvallisuussopimukset: https://um.fi/voimassa-olevat-tietoturvallisuussopimukset.

Käsiteltävä tieto	Hyväksyntäviranomainen
Kansallinen	Tietoon määräämisvallassa oleva viranomainen (tiedonhallintayksikkö)
Kansainvälinen, kahden tai monenvälisiin sopimuksiin liittyvä (ei rajat ylittävää tiedonsiirtoa)	Kuten kansalliselle tiedolle. Poikkeuksena tilanne, jossa sopimusosapuolen erillisvaatimuksena kansallisen SAA-viranomaisen (Liikenne- ja viestintävirasto) lausunto vaatimustenmukaisuudesta.
Kansainvälinen, kahden tai monenvälisiin sopimuksiin liittyvä (sisältäen rajat ylittävän tiedonsiirron) Ks. kuvat 19 ja 20.	Rajat ylittävän osuuden[23] osalta Liikenne- ja viestintävirasto. Kansallisen taustajärjestelmän osalta kuten kansalliselle tiedolle. Poikkeuksena tilanne, jossa sopimusosapuolen erillisvaatimuksena kansallisen SAA-viranomaisen (Liikenne- ja viestintävirasto) lausunto vaatimustenmukaisuudesta taustajärjestelmälle.
EU:n tai Naton turvallisuusluokiteltu tieto	Liikenne- ja viestintävirasto koko sähköiselle tietojenkäsittely-ympäristölle.

Taulukko 1. Tietojenkäsittely-ympäristön hyväksyntävastuuviranomaiset.



Kuva 19. Hyväksyntävastuut rajat ylittävän liikennöinnin tapauksessa.

Kuva 20. Hyväksyntävastuut rajat ylittävän liikennöinnin tapauksessa yhdyskäytäväratkaisun kanssa.

[23] Rajat ylittävä osuus kattaa tyypillisesti salausratkaisun, sen Suomessa sijaitsevan käyttöpisteen sekä tiedon vastaanotto-/lähetysjärjestelmän. Jos vastaanotto-/lähetysjärjestelmä on ilmaraolla eroteltu kansallisesta järjestelmästä, kansallisen järjestelmän hyväksyntävastuussa on ko. järjestelmää hallinnoiva kansallinen viranomainen. Jos vastaanotto-/lähetysjärjestelmä on kytketty yhdyskäytäväratkaisulla kansalliseen taustajärjestelmään, sisältyy ko. yhdyskäytäväratkaisun hyväksyntävastuu Liikenne- ja viestintävirastolle. Vastaavaa periaatetta sovelletaan myös sellaisiin kansainvälisiin harjoituksiin, joissa on tarve käsitellä kahden- tai monenvälisten sopimusten piiriin kuuluvaa turvallisuusluokiteltua tietoa ja joissa tietojärjestelmien hyväksyntävastuut jakautuvat kyseiseen harjoitukseen osallistuvien kesken.

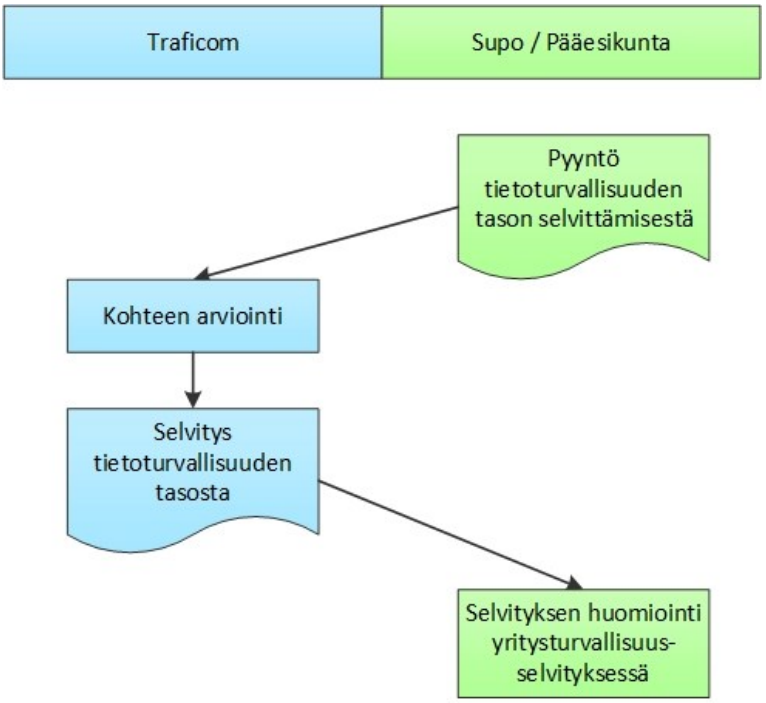
4.1.3 Tietojärjestelmien tietoturvallisuuden tason selvitys osana yritysturvallisuusselvitystä

Turvallisuusselvityslain mukaisissa yritysturvallisuusselvityksissä suojelupoliisi tai Pääesikunta arvioi yrityksen turvallisuusjärjestelyjen hallinnollisen turvallisuuden, henkilöstöturvallisuuden sekä fyysisen turvallisuuden riittävyyden ja Traficom tietoteknisen turvallisuuden riittävyyden. Yritysturvallisuusselvityksen käynnistämisestä ja yritysturvallisuusselvitystodistuksen antamisesta vastaa lain mukaan suojelupoliisi tai Pääesikunta, tai kansainvälisten tietoturvallisuusvelvoitteiden tapauksessa kansallinen turvallisuusviranomainen. Pyynnön Traficomille voivat tehdä vain nämä viranomaiset eli yritys ei voi itsenäisesti saada arviointia vireille Traficomissa.

Traficom noudattaa arvioinnissa soveltuvin osin edellä kuvattua hyväksyntäprosessia. Esimerkiksi järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn laadinnassa sovelletaan suoraan Katakri-arviointityökalua.

Traficom antaa arviointinsa perusteella suojelupoliisille tai Pääesikunnalle tietojärjestelmien tietoturvallisuuden tasoa koskevan selvityksen. Selvityslausuntoon liitetään arviointiraportti. Lausunto ja raportti toimitetaan myös asianosaiselle yritykselle. On huomattava, että lausunto tai raportti eivät ole Traficomin hyväksyntä järjestelmälle, vaan ainoastaan osaselvitys suojelupoliisin tai Pääesikunnan päätökseen, jota tehtäessä myös näiden viranomaisten vastuulla olevat osa-alueet huomioidaan.

Yritysturvallisuusselvitysten vastuujakoa on havainnollistettu kuvassa 4.



Kuva 21. Yritysturvallisuusselvitysten vastuujako.

4.1.4 Kansainvälisen hyväksyntävelvoitteen alaisen RESTRICTED-luokan tietoa käsittelevän yrityksen tietojärjestelmän hyväksyntä

On tilanteita, joissa kansainvälinen tietoturvallisuusvelvoite edellyttää yrityksen tietojärjestelmän hyväksyntää (akkreditointia) RESTRICTED-luokan tietojen käsittelyyn, mutta ei edellytä turvallisuusselvityslain mukaista yritysturvallisuusselvitystä (ks. luku 4.6.3). Tällainen tilanne voi ilmetä lähinnä silloin, kun yritys osallistuu EU:n tai Naton RESTRICTED-luokan tiedon sähköistä käsittelyä edellyttävään hankkeeseen, jossa ei ole tarvetta korkeampien turvallisuusluokkien tietojen käsittelylle. Näissä tilanteissa Traficom noudattaa edellä kuvattua hyväksyntäprosessia soveltuvin osin. Esimerkiksi järjestelmäkohtaisen turvallisuusvaatimusmäärittelyn laatimisessa sovelletaan suoraan Katakri-arviointityökalua, josta poimitaan kyseessä olevan kansainvälisen tietoturvallisuusvelvoitteen edellyttämät osakokonaisuudet. Tällaisiin hankkeisiin osallistuvia yrityksiä suositellaan olemaan yhteydessä Traficomiin jo varhaisessa vaiheessa, jotta RESTRICTED-luokan tietojen sähköiseen käsittelyyn mahdollisesti liittyvät erityisvaatimukset pystytään huomioimaan jo tietojärjestelmien suunnittelussa. Traficom sopii tarvittaessa muiden kv-titulaissa määriteltyjen viranomaisten kanssa fyysisen ja hallinnollisen turvallisuuden arvioinnin tarkoituksenmukaisesta työnjaosta.

4.1.5 Todistus viranomaiselle tietojärjestelmän vaatimustenmukaisuudesta

Kun viranomainen hakee Traficomilta arviointilain mukaista todistusta tietojärjestelmän vaatimustenmukaisuudesta, Traficom noudattaa arvioinnissa soveltuvin osin edellä kuvattua hyväksyntäprosessia.

Viranomaisen tietojärjestelmän arviointeja voivat tehdä myös hyväksytyt tietoturvallisuuden arviointilaitokset, jotka Traficom on hyväksynyt tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011, arviointilaitoslaki) nojalla ja joille on myönnetty pätevyys turvallisuusluokitellun tiedon suojaamisen arviointiin. Tämän ohjeen antamishetkellä arviointilaitoksille on myönnetty rajattuja pätevyyksiä turvallisuusluokkien IV ja III tietoja käsittelevien tietojärjestelmien arviointiin Katakri-viitekehystä vasten. Arviointilaitos voi arviointilaitoslain mukaan antaa todistuksen järjestelmän vaatimustenmukaisuudesta ja todistuksen tiedot voidaan kohteen suostumuksella merkitä turvallisuusselvitysrekisteriin (lain 9 § ja 13 a §). Arviointilaitoslain antama todistus on lainsäädännön näkökulmasta yhtä pätevä kuin Traficomin antama, eikä arviointilaitoksen todistuksen lisäksi yleensä pitäisi olla tarvetta hakea Traficomin todistusta.

4.1.6 Arviointilaitoksen työn hyödyntäminen osana Traficomin hyväksyntäprosessia

Traficomilla on mahdollisuus hyödyntää omassa hyväksyntälausuntoon tai yritysturvallisuusselvitykseen tähtäävässä arvioinnissaan arviointilaitoksen tekemää arviointia. Tällöin Traficom tarkastelee tarkastusten rajauksia ja arviointilaitoksen arviointiraporttien tietoja ja tekee tarvittaessa itse täydentäviä arviointeja tai pyytää asiakasorganisaatiolta lisäselvitystä sen varmistamiseksi, että kohde täyttää soveltuvat tietoturvallisuusvaatimukset. Asiakasorganisaatioita suositellaan hyödyntämään arviointilaitoksia erityisesti tietojärjestelmien turvallisuustestaukseen, jotta yleisimmät tekniset turvallisuuspuutteet pystyttäisiin havaitsemaan ja myös korjaamaan jo arviointilaitosten tarkastusten pohjalta.

5 LISÄTIETOKYSELYT

Lisätietoja on saatavilla osoitteesta neuvontapalvelu (at) traficom (piste) fi.

Liite 1: Traficomin käyttämät todennusmenetelmät

Tässä liitteessä kuvataan yleisimmät tarkastuksissa käytettävät todennusmenetelmät. Yleisimmät hallinnolliset (H) todennusmenetelmät on esitetty taulukossa 1. Taulukossa 2 esitetään puolestaan yleisimmät tekniset (T) todennusmenetelmät.

Taulukko 2. Hallinnolliset todennusmenetelmät.

ID	Todennusmenetelmä	Luokat[24]	Huomioitavaa
H1	Haastattelut	TL IV - TL I	Kohteena soveltuvat henkilöt, tyypillisesti sisältäen johdon, ylläpidon/kehityksen ja loppukäyttäjien edustajat.
H2	Dokumentaatioon tutustuminen	TL IV - TL I	Kattaen verkkokuvat, järjestelmäkuvaukset, prosessikuvaukset ja vastaavat.

Taulukko 3. Tekniset todennusmenetelmät.

ID	Todennusmenetelmä	Luokat[24]	Huomioitavaa
T1	Passiivinen rajapinta-analyysi	TL IV - TL I	Menetelmään sisältyy verkko-/järjestelmäkuvien rakentamiset sekä liikenneanalyysit.
T2	Järjestelmä-konfiguraatioiden turvallisuuden tarkastelu	TL IV - TL I	Menetelmä kattaa kaikki kohteen turvallisuuteen vaikuttavat osakokonaisuudet. Osakokonaisuuksia ovat tyypillisesti esimerkiksi palvelinten ja työasemien käyttöjärjestelmät sekä muut alustaan asennetut ohjelmistot, verkkolaitteiden konfiguraatiot, tietokantojen konfiguraatiot sekä muut järjestelmän turvallisuuteen vaikuttavat ohjelmistot.
T3	Aktiivinen rajapinta-analyysi	TL IV - TL I	Menetelmään sisältyy porttiskannaukset, haavoittuvuusskannaukset (tunnetut haavoittuvuudet) sekä toimintavarmuustestaukset (tuntemattomat haavoittuvuudet). Toimintavarmuustestauksella tarkoitetaan tässä ohjeessa erityisesti virheellisen syötteen lähettämiseen (engl. fuzz testing) perustuvaa koestusta. Toimintavarmuustestausta edellytetään vain turvallisuuden kannalta kriittisiin järjestelmäosiin. Tällaisia ovat esimerkiksi turvallisuusluokan III yhdyskäytäväratkaisut, eri verkkoteknologioiden väliset liityntärajapinnat sekä suurten tietomassojen pääsynhallintamekanismit (kasautumisvaikutus).
T4	Sovellusturvallisuuden tarkastelut järjestelmätyypeittäin	TL IV - TL I	Menetelmä kattaa kohteen turvallisuuteen vaikuttavien sovelluskomponenttien tarkastelut, esimerkiksi web-sovellukset, Java-palvelin-/asiakasohjelmistot ja ERP-järjestelmien sisäiset pääsynhallinta-mekanismit.
T5	Salausratkaisujen turvallisuuden todentaminen	TL IV - TL I	Kohteissa, joissa käytetään Traficomin NCSA-toiminnon vaatimustenmukaiseksi arvioimaa salausratkaisua[25], todennetaan salausasetusten ja hallintakäytäntöjen turvallisuuden riittävyys suhteessa arvioinnin yhteydessä määritettyyn käyttöpolitiikkaan. Vastaavasti toimitaan myös tilanteissa, joissa käytetään esimerkiksi EU:n hyväksymää salausratkaisua EU:n turvallisuusluokiteltujen tietojen suojaamiseen. Tilanteissa, joissa kohteessa ei ole käytössä ennestään arvioitua tai hyväksyttyä salausratkaisua, Traficomin NCSA-toiminto voi tiettyjen ehtojen täyttyessä arvioida ratkaisun turvallisuuden tapauskohtaisesti.

[24] Kattaen myös kansainväliset vastineet, tyypillisesti RESTRICTED, CONFIDENTIAL, SECRET ja TOP SECRET.
[25] Liikenne- ja viestintävirasto Traficom. 2025. Liikenne- ja viestintävirasto Traficomin NCSA-toiminnon hyväksymät salausratkaisut. URL: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/ncsa/liikenne-ja-viestintavirasto-traficomin-ncsa-toiminnon-hyvaksymat-salausratkaisut.

T6	Käytettävyystestaukset (ml. kuormitustestaukset)	TL IV - TL I	Käytetään vain järjestelmiin, joilla on korkeat käytettävyysvaatimukset (esim. ihmishenkiä suojaavat turvajärjestelmät, joille järjestelmän omistaja on määritellyt korkeat saatavuusvaatimukset). Kattaa tyypillisesti sovellusten stressitestit, palvelunestohyökkäyksen kestokykytestaukset sekä kohteen jatkuvuuden hallinnan / toimintavarmuuden menettelyjen arvioinnin.
T7	Fyysisen turvallisuuden suojausten todentamismenetelmät	TL IV - TL I	Toteutus kansainvälisten turvallisuusluokiteltujen tietoaineistojen osalta suojelupoliisilla tai Pääesikunnalla.
T8	Yhdyskäytäväratkaisujen turvallisuuden testaukset	TL III - TL I	Kohteissa, joissa käytetään Traficomin Yhdyskäytäväratkaisuohjeen[26] luvussa 4 kuvattua luotettavana pidettävää yhdyskäytäväratkaisua, todennetaan toteutetun ratkaisun turvallisuuden riittävyys suhteessa Yhdyskäytäväratkaisuohjeessa kuvattuihin vaatimuksiin. Tilanteissa, joissa kohteessa ei ole käytössä em. ohjeen ko. luvun mukaista yhdyskäytäväratkaisua, Traficomin NCSA-toiminto voi tiettyjen ehtojen täyttyessä arvioida ratkaisun turvallisuuden tapauskohtaisesti.
T9	Poikkeamahavainnointi-kyvyn testaukset	TL IV - TL I	Kattaa erityisesti suojattavan ympäristön sisällä tehtävien valtuuttamattomien toimien ja niiden yritysten havainnointikyvyn testauksen, sekä tapauskohtaisesti hyökkäystoimien jäljittelyyn[27] perustuvat menetelmät.
T10	Hajasäteilysuojausten (TEMPEST) todentaminen	TL III - TL I	Kattaa tyypillisesti tilan, laitteiston, koteloinnin tai/ja esimerkiksi laitteiston asennustavan hajasäteilysuojauksen riittävyyden arvioinnin. Edellytettävän hajasäteilysuojauksen taso riippuu käsiteltävän tiedon alkuperäisestä luovuttajasta (originator) ja tiedon turvallisuusluokasta.
T11	Luvattomien teknisten laitteiden olemassaolon todentaminen[28]	TL III - TL I	Tapauskohtainen soveltaminen, tyypillisesti tilan käyttötarpeen mukaisesti.
T12	Uhkatietojohdannaiset menetelmät	TL III - TL I	Tapauskohtainen soveltaminen, tyypillisesti painottuen turvallisuusluokkien II ja I ympäristöihin.

[26] Liikenne- ja viestintävirasto Traficom. 2021. Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf.
[27] Engl. Adversary Emulation.
[28] Engl. Technical Surveillance Counter-Measures (TSCM).