TRAFICOM

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)

Traficomin julkaisuja 13/2020
PiTuKri – versio 1.1 – maaliskuu 2020

Sisältö

Johdanto 3
Käyttö 4
- Käyttötapaukset 4
- Arviointimenetelmät 5
- Riskienarviointi 6
- Rakenne 7
- Tietotyypit 7

Pilvipalvelujen ominaispiirteitä 10
- Pilvipalvelujen palvelumallit 10
- Pilvipalvelujen toteutusmallit 11
- Palvelun tuottaminen 12
- Tiedon ja palveluiden sijainti 13

Osa-alue 1: Esiehdot 14
Osa-alue 2: Turvallisuusjohtaminen 17
Osa-alue 3: Henkilöstöturvallisuus 24
Osa-alue 4: Fyysinen turvallisuus 27
Osa-alue 5: Tietoliikenneturvallisuus 33
Osa-alue 6: Identiteetin ja pääsyn hallinta 35
Osa-alue 7: Tietojärjestelmäturvallisuus 38
Osa-alue 8: Salaus 43
Osa-alue 9: Käyttöturvallisuus 45
Osa-alue 10: Siirrettävyys ja yhteensopivuus 48
Osa-alue 11: Muutostenhallinta ja järjestelmäkehitys 50

Liite 1: Esimerkkejä vaatimuskohtien kohdentamisesta 52
Palvelumallina IaaS 53
Palvelumallina PaaS 55
Palvelumallina SaaS 57

Liite 2: Esimerkkejä kriteeristön soveltamisesta vaatimustenmukaisuuden arviointiin 59
- Esimerkki 1: Salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arviointi 59
- Esimerkki 2: Turvallisuusluokitellun tiedon suojausten vaatimustenmukaisuuden arviointi 60

Liite 3: Viranomaisarviointi ja -hyväksyntä 61
- Tausta 61
- Arviointiprosessi 61
- Hyväksyntäprosessi 62
- Viranomaishyväksyntä 63

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-481-4

Johdanto

Pilvipalveluiden turvallisuuden arviointikriteeristön (PiTuKri) tavoitteena on edistää viranomaisten salassa pidettävän tiedon turvallisuutta tilanteissa, joissa tietoja käsitellään pilvipalveluissa. Kriteeristö on tarkoitettu työkaluksi pilvipalvelujen turvallisuuden arviointiin. Kriteeristö on laadittu Suomen kansallisten tarpeiden näkökulmasta. Laadinnassa on huomioitu kansallisen lainsäädännön uudistushankkeet siten, että kriteeristö tukee 2020 alussa uusiutunutta lainsäädäntöä [1,2]. Laadinnassa on hyödynnetty erityisesti BSI:n pilviturvallisuuskriteeristöä[3], CSA-pilviturvallisuusyhteisön suojausmatriisia[4], ISO27001[5]- ja ISO27017[6]-standardeja, sekä Katakri-kriteeristöä[7]. Kriteeristön tavoitteena on myös tukea ja konkretisoida Valtiovarainministeriön julkisen hallinnon pilvipalveluiden linjausten[8] käyttöönottoa.

Kriteeristö ottaa kantaa sekä viranomaisen kansallisiin salassa pidettäviin, että turvallisuusluokiteltuihin IV-luokan salassa pidettäviin tietoihin. Kriteeristö sivuaa[9] myös kansainvälisen RESTRICTED-tason turvallisuusluokiteltujen tietojen yleisiä suojausperiaatteita.

Kriteeristössä kuvattavat turvallisuusvaatimukset on mitoitettu siten, että tyypillisimmät salassa pidettäviin tietoihin kohdistuvat riskit saadaan pidettyä siedettävällä tasolla. Korkeampien turvallisuusluokkien tietojen turvallisuusjärjestelyihin otetaan kantaa vain pilvipalveluiden yleisen soveltuvuuden arvioinnin yhteydessä. Kriteeristöä voidaan hyödyntää myös viranomaisten julkisten tietojen suojaamiseen, sekä elinkeinoelämän tarpeisiin.

Kriteeristön päivitysversio 1.1 tarkentaa ensimmäisessä versiossa[10] kuvattuja käsitteitä ja käyttötapauksia, täydentää soveltamismahdollisuuksia sekä esittelee muita palautteissa toivottuja muokkauksia esimerkiksi vaatimusjaotteluun. Kyberturvallisuuskeskus jatkaa kriteeristön kehitystä. Kyberturvallisuuskeskus kerää kriteeristöön palautetta ja jatkokehitystoiveita[11], mitkä tullaan huomioimaan kriteeristön päivitetyissä versioissa. Kriteeristön käyttöön tullaan julkaisemaan myös tukityökaluja ja lisätietoaineistoja.

[1] Laki julkisen hallinnon tiedonhallinnasta (906/2019). URL: https://www.finlex.fi/fi/laki/alkup/2019/20190906.

[2] Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). URL: https://www.finlex.fi/fi/laki/alkup/2019/20191101.

[3] Bundesamt für Sicherheit in der Informationstechnik. 2017. Cloud Computing Compliance Controls Catalogue (C5) - Criteria to assess the information security of cloud services. URL: https://www.bsi.bund.de/EN/C5.

[4] Cloud Security Alliance. 2018. The Cloud Security Alliance Cloud Controls Matrix (CCM). URL: https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix.

[5] ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.

[6] ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

[7] Puolustusministeriö. 2015. Katakri 2015 - Tietoturvallisuuden auditointityökalu viranomaisille. URL: http://www.defmin.fi/Katakri.

[8] Valtiovarainministeriö. 2019. Julkisen hallinnon pilvipalvelulinjaukset. URL: http://urn.fi/URN:ISBN:978-952-251-982-5.

[9] Kansainväliseen turvallisuusluokiteltuun tietoon kohdistuu tiedon originaattori- ja omistajakohtaisesti vaihtelevia suojausvaatimuksia, jotka voivat erota paikoin merkittävästikin kansallisista vastineista. Lisätietoa: ncsa (at) traficom (piste) fi.

[10] Kyberturvallisuuskeskus. 2019. Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) - v1.0. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf.

[11] Palautteet ja kehitysehdotukset: ncsa (at) traficom (piste) fi.

Käyttö

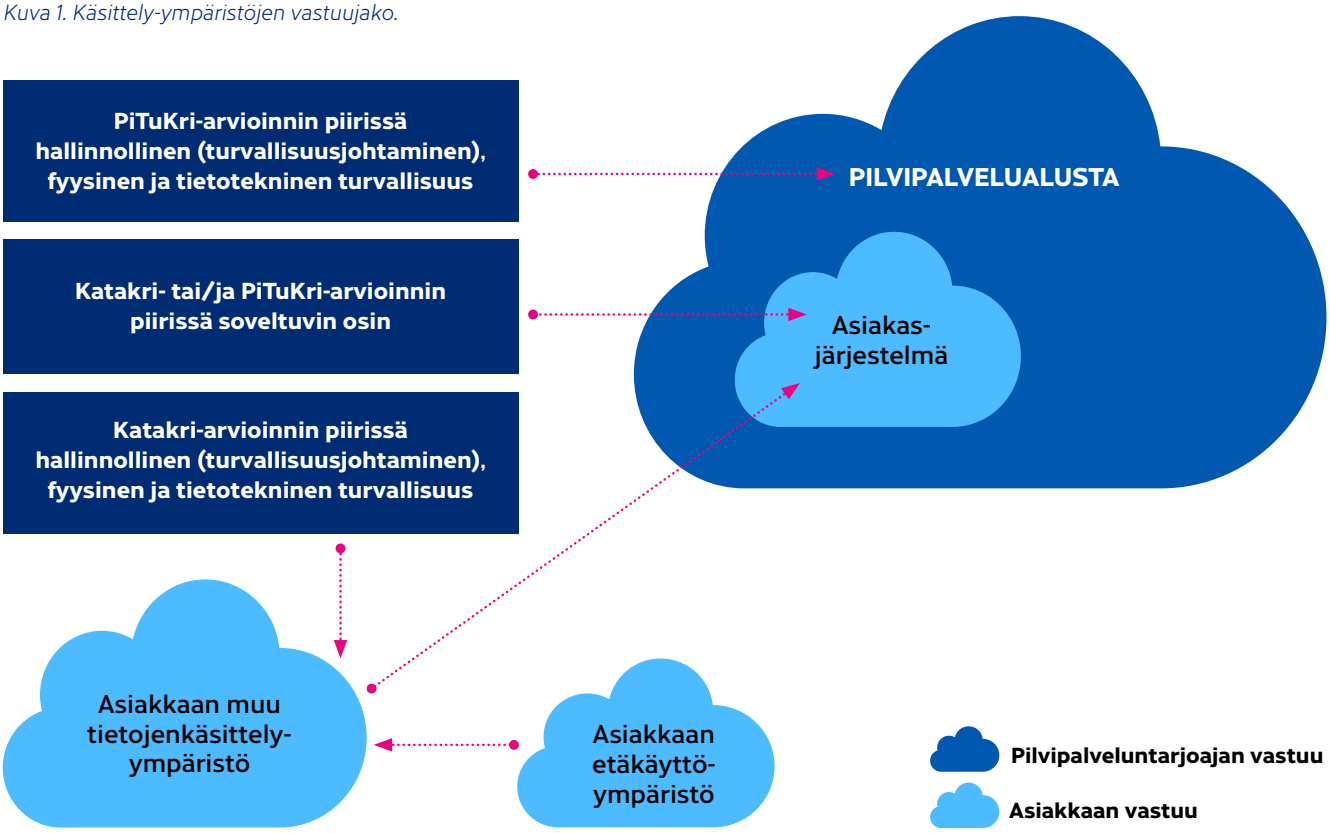
Käyttötapaukset

Kriteeristö on tarkoitettu käytettäväksi pilvipalveluiden turvallisuuden arvioinnissa. Sitä voidaan käyttää myös pilvipalveluntarjoajien omaehtoisen turvallisuustyön tukena. Kriteeristö on laadittu tukemaan erilaisia pilvipalveluita ja erilaisia käyttötapauksia. Kriteeristön tarkoituksenmukainen käyttö edellyttää käyttötapauskohtaista soveltamista.

Pilvipalveluissa käsiteltävien tietojen suojausten arviointi voidaan useimmissa käyttötapauksissa jakaa pilvipalveluntarjoajan ja asiakkaan vastuulle kuuluviin osuuksiin[12]. Asiakkaan vastuulle kuuluviin osuuksiin sisältyy tyypillisesti sekä pilvipalvelun asiakasjärjestelmän osuus, että asiakkaan muiden tiedonkäsittely-ympäristöjen osuus. Käsittely-ympäristöjen vastuujakoa on havainnollistettu kuvassa 1. Asiakkaan vastuulle kuuluvien osuuksien arviointiin voidaan käyttää myös esimerkiksi Katakri 2015 -viitekehystä.

Kriteeristössä kuvatut vaatimukset ovatkin useimmissa käyttötapauksissa perusteltuja kohdentaa pilvipalveluntarjoajan vastuulla olevaan osuuteen, joissain sekä pilvipalveluntarjoajan että pilvipalvelun asiakkaan osuuksiin, ja joissain vain asiakkaan vastuulla olevaan osuuteen. Joidenkin suojausten toteuttamisessa voi olla perusteltua hyödyntää sekä asiakkaan vastuulla olevan asiakasjärjestelmän, että pilvipalveluntarjoajan vastuulla olevan pilvipalvelualustan toiminnallisuuksia. Kriteeristön tarkoituksenmukainen käyttö edellyttää riittävää osaamista turvallisuuden arvioijalta, pilvipalveluntarjoajalta ja pilvipalvelun asiakkaalta. Esimerkkejä kriteeristön kohdentamisesta vastuittain on esitetty liitteessä 1.

Kuva 1. Käsittely-ympäristöjen vastuujako.



[12] Pilvipalveluntarjoajan tai asiakkaan osuuksiin liittyvien mahdollisten ulkoisten toimijoiden suojaukset on tyypillisesti perusteltua sisällyttää kyseisen osuuden arviointiin. Esimerkiksi tilanteessa, jossa pilvipalvelun asiakkaan vastuulle kuuluvan asiakasjärjestelmän ohjelmistokehitys on ulkoistettu kolmannelle osapuolelle, kuuluu kolmannen osapuolen turvallisuudesta varmistuminen pilvipalvelun asiakkaan vastuisiin.

Arviointimenetelmät

Pilvipalvelujen turvallisuuden arvioinnissa voidaan käyttää erilaisia menetelmiä. Joidenkin tietojen suojaamisen arvioinnissa saattaa olla riittävää nojautua esimerkiksi pilvipalveluntarjoajan tuottamaan itsearviointiin, mahdollisiin muihin sertifiointeihin sekä sopimusteknisiin sitoumuksiin. Joidenkin tietojen suojaamisen arvioinnissa on perusteltua edellyttää lisäksi ulkopuolisen riippumattoman tahon tekemää todennusta. Todennuksen tuottamien tulosten luotettavuus riippuu merkittävästi todennuksessa käytettyjen menetelmien luotettavuudesta. Esimerkiksi dokumentaation tutustuminen eroaa luotettavuudeltaan siitä, että pilvipalvelun suojaus todennettaisiin myös teknisen testaamisen keinoin. Todennuksessa voidaan usein hyödyntää myös esimerkiksi jatkuvan auditoinnin mahdollisuuksia lisänäytön lähteinä. Joidenkin tietojen suojaamisen arvioinnissa on perusteltua käyttää kansallisen tietoturvallisuusviranomaisen arviointipalvelua[13]. Lisätietoja pilvipalvelujen arviointiin liittyvistä haasteista sekä myös joitain ehdotettuja ratkaisumalleja on saatavissa esimerkiksi EU-SEC[14] -hankkeen tuotoksista.

PiTuKrissa kuvattujen vaatimusten täyttymisen osoittamiseen voi tietyin rajoituksin hyödyntää muita viitekehyksiä ja voimassa olevia sertifiointeja. Hyödyntämismahdollisuuksien arvioinnissa suositellaan huomioitavan erityisesti se, että eri viitekehykset ja sertifioinnit mittaavat toisistaan eroavia asioita. Jotkin viitekehykset mahdollistavat esimerkiksi tietoturvallisuuden hallintajärjestelmän sertifioinnin siten, että teknisten suojausten riittävyyden arvioinnissa nojataan sertifioinnin kohdeorganisaation riskienhallintapäätöksiin. Lähestymistapa eroaa esimerkiksi turvallisuusluokiteltujen tietojen suojaamiseen usein käytetystä mallista, jossa tiedon originaattori tai/ja omistaja asettaa tiedon suojaamiselle vähimmäisvaatimukset, jotka seuraavat tietoa koko sen elinkaaren ajan kaikissa tiedon käsittely-ympäristöissä ja -tilanteissa. Hyödyntämismahdollisuuksien arvioinnissa suositellaan huomioitavan myös se, että sertifioinnit voivat olla rajattuja kattamaan vain osajoukon salassa pidettävän tiedon käsittelyprosesseista tai -ympäristöistä, eri viitekehysten vaatimuksilla tavoitellaan eriävää luotettavuutta tiedon suojaamiselle, ja että myös vaatimusten täyttymisen todentamisen luotettavuus vaihtelee. Muita viitekehyksiä vasten tehtyjä sertifiointeja voidaankin arvioinneissa hyödyntää, mutta sellaisenaan ne eivät kuitenkaan mahdollista esimerkiksi Kyberturvallisuuskeskuksen hyväksynnän[15] myöntämistä.

[13] Kyberturvallisuuskeskus. 2019.
URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

[14] The European Security Certification Framework (EU-SEC). 2019. URL: https://www.sec-cert.eu/.

[15] Kyberturvallisuuskeskuksen NCSA-toiminnon hyväksyntäprosessia on kuvattu yksityiskohtaisemmin liitteessä 3.

Riskienarviointi

Kukin viranomainen vastaa tietojenkäsittelynsä riittävästä turvallisuudesta. Kukin viranomainen on viime kädessä itse vastuussa kyseiseen käyttötapaukseen riittävän kattavan ja luotettavan arvioinnin järjestämisestä, sekä arviointihavaintojen riskiperustaisesta käsittelystä. Käyttötapauksissa, joissa palvelua tarjotaan useammalle valtionhallinnon viranomaiselle keskitetyn palvelutuottajan kautta, suositellaan arviointien ja arviointihavaintojen hyödyntämistä siten, että päällekkäisiltä arvioinneilta vältytään. Tällaisissa käyttötapauksissa on erityisesti huomioitava, että jäännösriskien tulee olla kaikkien palvelua käyttävien viranomaisten hyväksymiä.

PiTuKrin tarkoituksenmukainen käyttö edellyttää kyseiseen käyttötapaukseen kohdennettua vaatimusten tulkintaa. Vaatimukset voivat olla korvattavissa myös muilla vastaavan tasoisilla suojauksilla. Vaatimuksissa tai toteutusesimerkeissä ei kuvata kaikkiin ympäristöihin tai erikoistapauksiin riittäviä suojauksia.

Pilvipalvelualustaan on mahdollista toteuttaa esimerkiksi palveluja, joiden suojaamisvastuut kuuluvat merkittävin osin palvelun asiakkaalle. Toisaalta erityisesti palvelun saatavuuteen vaikuttaa useampi tekijä, joista yhdenkin häiriintyminen voi estää palvelun käytön. Esimerkiksi alustakerroksen saatavuuspuutteet voivat estää sovelluskerrosta tarjoamasta palvelua asiakkaalle. Vastaavasti vaikka alustakerros olisi toteutettu korkeaa saatavuutta tukevaksi, sovelluskerroksen puutteet voivat estää palvelun käytön.

Käyttö voi estyä myös asiakkaan päätelaitteessa, tai päätelaitteen ja pilvipalvelun välisessä tietoliikenneyhteydessä olevasta häiriöstä johtuen. Kaikki kriteeristössä kuvatut vaatimukset eivät toisaalta sellaisinaan sovellu kaikkiin käyttötapauksiin, vaan edellyttävät tapauskohtaista arviointia. Joidenkin suojausten järjestäminen saattaa olla perusteltua pilvipalvelualustassa, joidenkin puolestaan vain asiakasjärjestelmässä. Joidenkin suojausten järjestäminen on perusteltua toteuttaa pilvipalvelualustan ja asiakasjärjestelmän toiminnallisuuksia yhdistellen.

Kriteeristöä voidaan hyödyntää myös viranomaisten salassa pidettävän tiedon suojaamisen vaatimustenmukaisuuden arvioinnissa. Liitteessä 2 kuvataan esimerkkejä siitä, kuinka kriteeristöä voidaan soveltaa salassa pidettävän ja turvallisuusluokitellun salassa pidettävän tiedon suojausten arviointiin.

Käyttötapauksissa, joissa tavoitteena on saada pilvipalvelualustalle tai siihen sijoitetulle asiakasjärjestelmälle toimivaltaisen viranomaisen myöntämä hyväksyntä[15], tulee toteutettujen suojausten olla riittäviä sekä kohdeorganisaation että toimivaltaisen viranomaisen riskienarvioinnin havaintoihin nähden. Erityisesti tilanteissa, joissa suojauksille käytetään korvaavaa menettelyä, tulee kohdeorganisaation pystyä osoittamaan, että näillä menettelyillä saavutetaan riittävä suojausvaikutus.

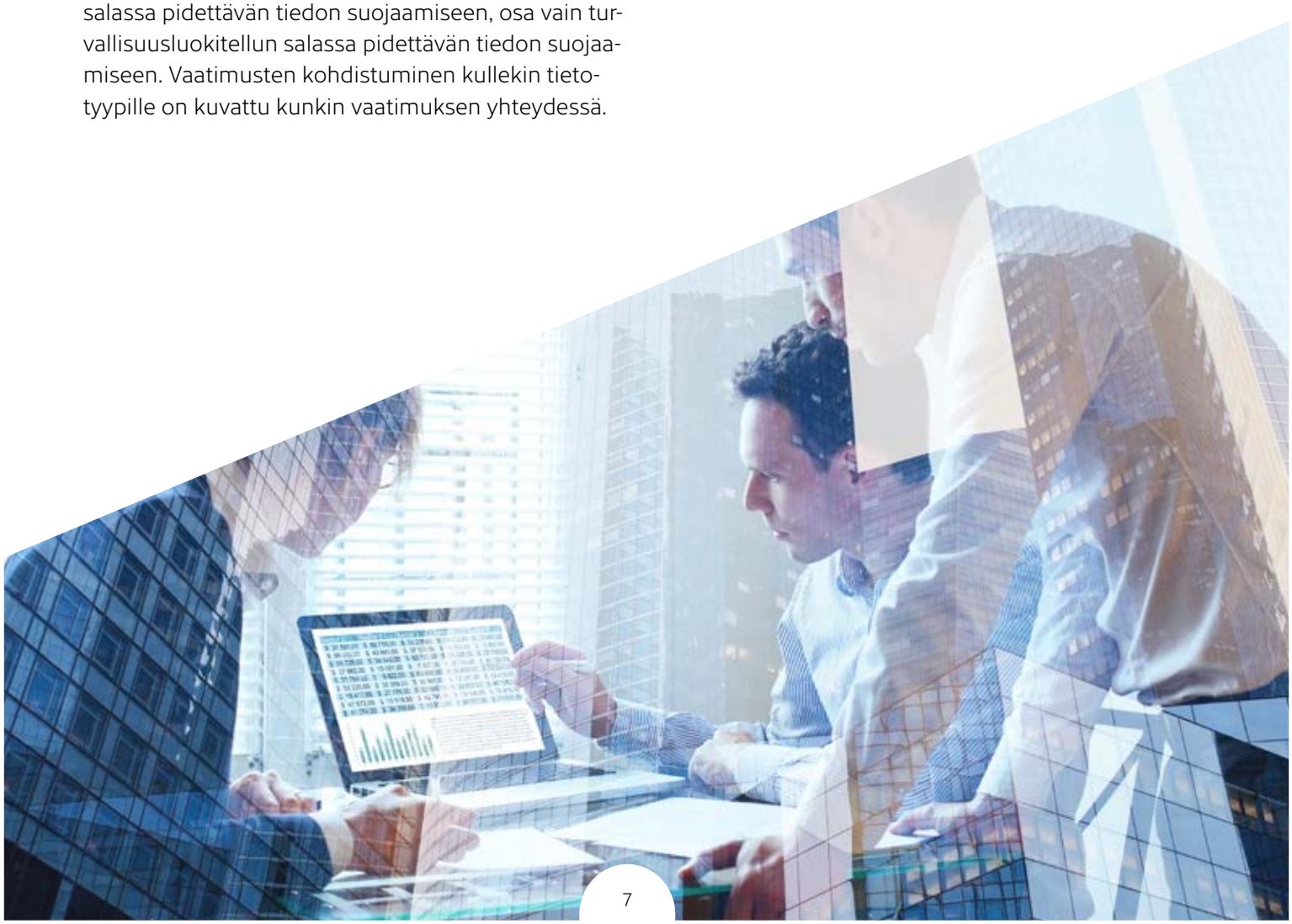
Rakenne

PiTuKri on jaettu 11 osa-alueeseen. Osa-alue 1, esiehdot, on erityisasemassa muihin osa-alueisiin nähden. Esiehdot määrittävät jatkoarvioinnin mahdollisuuksia ja tukevat salassa pidettävän tiedon suojaamisesta vastuussa olevien viranomaisten riskienhallintatyötä. Joillekin salassa pidettäville tiedoille esimerkiksi julkisen, monikansallisen pilvipalvelun jatkoarviointi on perusteltua. Joillekin tiedoille riskiperusteiset jatkoarviointimahdollisuudet voivat rajautua esimerkiksi vain kansallisesti tuotettuihin yksityisiin pilvipalveluihin. Jatkoarvioinnissa tulee huomioida, että esiehdot ottavat kantaa vain osaan yleisistä riskeistä. Esiehtojen täyttyminen ei siten vielä takaa tiedon riittävää suojaamista, vaan lisäksi tulee huomioida myös muissa osa-alueissa kuvatut suojaukset.

Osa-alueet koostuvat vaatimuskorteista. Vaatimuskortteihin on kuvattu vaatimuksen teema, konkreettinen vaatimus, vaatimuksen soveltamiskohteet, suojaustavoite, sekä vaatimuksen toteuttamisen ja tulkinnan tueksi tarkoitettuja lisätietoja. Vaatimukset on pyritty kuvaamaan siten, että ne mahdollistavat erilaisia toteutustapoja. Osa vaatimuksista kohdistuu salassa pidettävän tiedon suojaamiseen, osa vain turvallisuusluokitellun salassa pidettävän tiedon suojaamiseen. Vaatimusten kohdistuminen kullekin tietotyypille on kuvattu kunkin vaatimuksen yhteydessä.

Tietotyypit

Erilaisiin tietotyyppeihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eriävien tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Tietotyypit on jaoteltu suojaustarpeen mukaisiin, taulukossa 1 esiteltyihin luokkiin.



Taulukko 1. Tietotyypit.

Tietotyyppi	Kuvaus
Julkinen	Julkinen tieto. Suojaamistarpeet tyypillisesti eheyden ja saatavuuden näkökulmista.
Salassa pidettävä	Viranomaisen kansallinen salassa pidettävä tieto, jota ei ole turvallisuusluokiteltu. Useimmat viranomaisten salassa pidettävät tiedot sisältävät henkilötietoja, ja ovat siten myös henkilötietoihin liittyvän erityislainsäädännön piirissä, vrt. tietotyyppi "Henkilötieto".
Henkilötieto	Henkilötietojen suojaamiseen liittyvän erityislainsäädännön (ml. tietosuojalaki[16], laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä[17], sekä EU:n yleinen tietosuoja-asetus[18]) alaiset tiedot.
Varautumisen näkökulmasta suojattavat tiedot	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Poikkeavilla olosuhteilla tarkoitetaan tässä tilannetta, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.
TL IV	Viranomaisen kansalliset turvallisuusluokitellut IV-luokan salassa pidettävät tiedot. Suojaamistarve yleensä valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava myös lainsäädäntöjohdannaiset riskit[19].
Kansainvälinen RESTRICTED (KV-R)	RESTRICTED ja muut vastaavan tason kansainväliset turvallisuusluokitellut erityissuojattavat tieto-aineistot. Esimerkiksi vieraiden valtioiden ja kansainvälisten järjestöjen kanssa tehtyjen kahden- ja monenvälisten sopimusten[20] piiriin kuuluvat RESTRICTED-tason tiedot. Suojaamistarve yleensä yhden tai useamman valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava lainsäädäntöjohdannaiset riskit sekä kyseiseen tietoon kohdistuvat tiedon originaattorin tai/ja omistajan asettamat erityisvaatimukset[21].
Suuri määrä salassa pidettävää tai/ja henkilötietoa (TL IV tai TL III -kasauma)	Tilanteet, joissa kasautumisvaikutuksen arvioidaan[22] muodostavan turvallisuusluokitellun IV- tai III-tason tietovarannon. Esimerkiksi osa Suomen kriittisen infrastuktuurin ylläpitoon osallistuvien yritysten liikesalaisuuksista voi olla yksittäisinä tietoina salassa pidettäviä[23], mutta usean yrityksen muodostaman huoltovarmuuskriittisen kokonaisuuden kattavana kasaumana myös turvallisuusluokiteltuja[24] III-luokan salassa pidettäviä tietoja.
Suuri määrä TL IV -tietoa (TL III -kasauma)	Tilanteet, joissa kasautumisvaikutuksen arvioidaan muodostavan turvallisuusluokan III tietovarannon. Esimerkiksi valtionhallinnolle suunnattu yhteisöpilvi, johon kasautuu merkittävä määrä useiden viranomaisten turvallisuusluokan IV tietoa myös siten, että tietoja yhdistelemällä on muodostettavissa turvallisuusluokan III tietovaranto.
TL III ja II	Viranomaisen kansalliset turvallisuusluokan III tai/ja II tiedot. Suojaamistarve yleensä valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava myös lainsäädäntöjohdannaiset riskit.

Taulukossa 1 esitetty jaottelu ei kata kaikkia eri viranomaisten käyttötapauksia. Esimerkiksi varautumiseen liittyy eri viranomaisilla toisistaan eroavia tarpeita, joihin esitetty jaottelu ottaa kantaa vain osin. Arvioinnissa tulee myös huomioida, että suurikaan määrä salassa pidettävää tietoa ei aina johda kasautumisvaikutukseen ja turvallisuusluokittelun perusteiden[25] täyttymiseen. PiTuKrin tarkoituksenmukainen käyttö edellyttää käsiteltävien tietotyyppien tunnistamista ja kuhunkin käyttötapaukseen liittyvien riskien arviointia[26]. Tietotyyppien keskinäistä suhdetta on havainnollistettu kuvassa 2.

[16] Tietosuojalaki (1050/2018). URL: https://www.finlex.fi/fi/laki/alkup/2018/20181050.

[17] Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). URL: https://www.finlex.fi/fi/laki/alkup/2018/20181054.

[18] Euroopan parlamentin ja neuvoston asetus 2016/679. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[19] Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa pilvipalveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy pilvipalvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia.

[20] Lisätietoa kansainvälisistä sopimuksista Ulkoministeriön verkkosivuilla: https://um.fi/kahdenvaliset-ja-monenvaliset-sopimukset.

[21] Tyypillisenä erityisvaatimuksena turvallisuusluokitellun tiedon kaikkien käsittely-ympäristöjen hyväksyttämisvelvoite kansallisella turvallisuusjärjestelyjen hyväksyntäviranomaisella (SAA, Security Accreditation Authority, Suomessa Liikenne- ja viestintäviraston NCSA-toiminto).

[22] Arviointi edellyttää kyseessä olevan tietokasauman nykyisen sekä oletetun tulevan tietosisällön selvittämistä, ja arviota siitä, tuleeko tietovaranto julkisuuslain (1999/621) 24 §:n 1 momentin 2, 5 tai 7–11 kohdan mukaan turvallisuusluokiteltavaksi esimerkiksi III-luokan mukaisesti.

[23] Salassapidon perusteena tyypillisesti julkisuuslain (1999/621) 24 §:n 1 momentin 20 kohta.

[24] Salassapidon ja turvallisuusluokittelun perusteena voi joissain tapauksissa olla esimerkiksi julkisuuslain (1999/621) 24 §:n 1 momentin 7, 8, 10 kohdat.

[25] Julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) mukaan turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain (1999/621) 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.

[26] Kyberturvallisuuskeskus tukee viranomaisten riskienhallintatyötä muun muassa NCSA-toiminnon arviointi- ja hyväksyntäpalvelujen, sekä tietoturvallisuuden neuvontapalvelun kautta. Lisätietoa: https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/arviointi-hyvaksynta-ja-neuvonta.

Kuva 2. Tietotyypit.

Pilvipalvelujen ominaispiirteitä

Tässä luvussa esiteltävät pilvipalveluihin liittyvät kuvaukset pohjautuvat NIST:in[27] määritelmissä ja Valtiovarainministeriön julkisen hallinnon pilvilinjauksissa käytettyihin käsitteisiin. PiTuKrissa käsitteitä tarkennetaan turvallisuuden näkökulmasta suhteuttaen ne riskilähtöiseen pilvipalveluiden arviointitapaan.

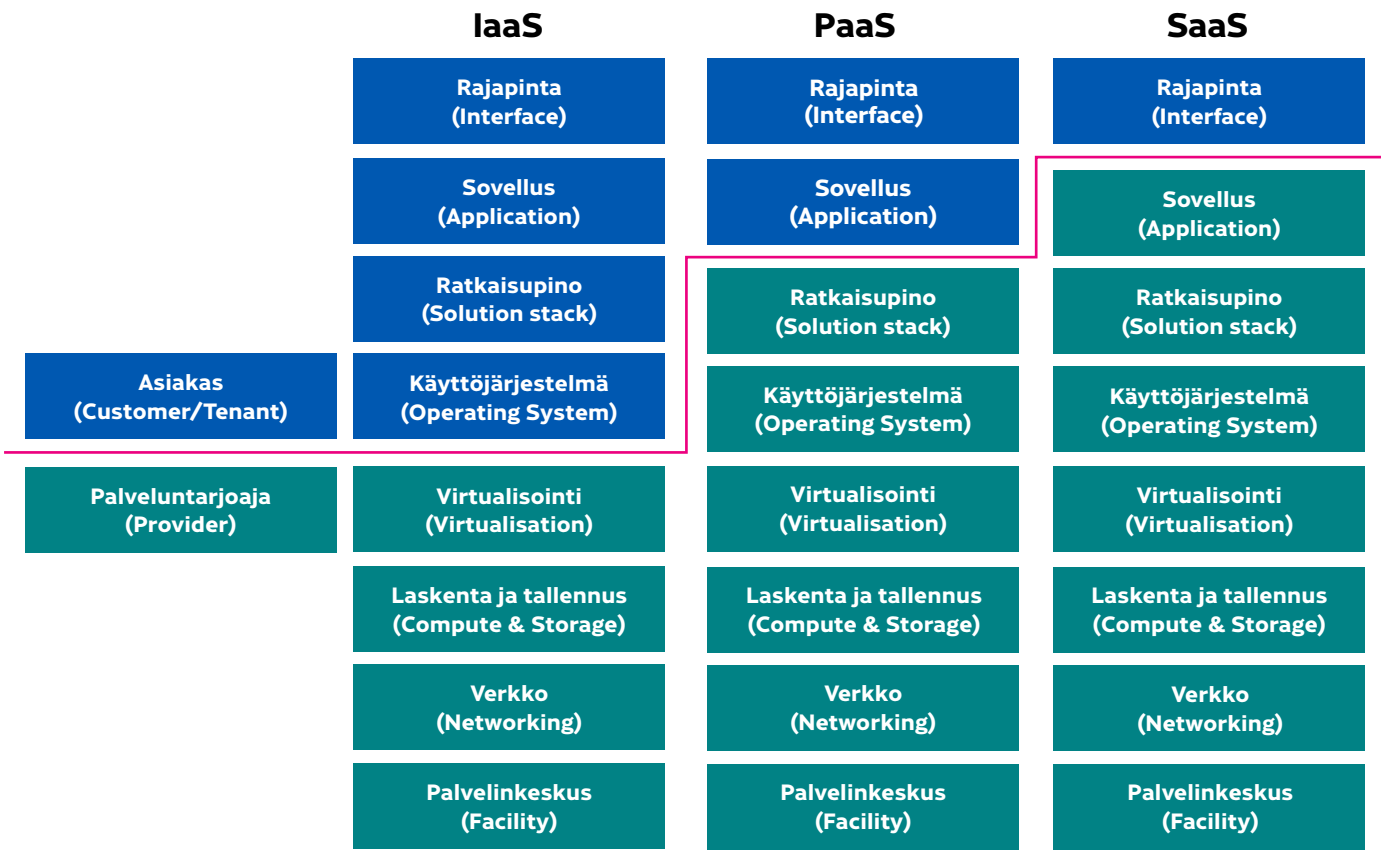
Pilvipalveluilla tarkoitetaan verkon yli saavutettavaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään jaettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi.

Pilvipalvelujen palvelumallit

Pilvipalveluiden yleisimmät palvelumallit voidaan jakaa infrastruktuuriin palveluna (Infrastructure as a Service, IaaS), ohjelmistoalustaan palveluna (Platform as a Service, PaaS) ja ohjelmistoon palveluna (Software as a Service, SaaS). IaaS-mallissa kaikki palveluiden tuottamiseen liittyvä infrastruktuuri hankitaan palveluntarjoajalta. PaaS-mallissa palvelut tuotetaan valmiin ohjelmistoalustan avulla. SaaS-mallissa palveluntarjoaja tuottaa palvelut kokonaisuudessaan.

Turvallisuuteen liittyvät vastuut jakautuvat kaikissa palvelumalleissa palveluntarjoajan ja asiakkaan välillä. Vastuiden jakautuminen riippuu palvelumallista sekä kyseisen palvelutoteutuksen yksityiskohdista. Esimerkiksi PaaS-palveluun liittyvä vastuujako voi erota paikoin merkittävästikin eri pilvipalveluntarjoajien välillä. Tyypillistä vastuujakoa on havainnollistettu kuvassa 3. Esimerkkejä kriteeristön kohdentamisesta vastuittain on kuvattu myös liitteessä 1.

Kuva 3. Tyypillinen vastuujakomalli.



[27] National Institute of Standards and Technology (NIST). 2011. Special Publication 800-145: The NIST Definition of Cloud Computing. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Pilvipalvelujen toteutusmallit

Pilvipalveluiden yleisimmät toteutusmallit voidaan jakaa yksityiseen pilveen (private cloud), yhdistelmäpilveen (hybrid cloud), ja julkiseen pilveen (public cloud). Muut toteutusmallit, esimerkiksi jonkin eri toimijoista koostuvan yhteisön yhteisöpilvet (community/government cloud), ovat yleensä arvioitavissa yleisimpien toteutusmallien pohjustamana.

Yksityisellä pilvellä tarkoitetaan palvelua, joka tuotetaan vain palvelua käyttävälle organisaatiolle. Palvelua voidaan tuottaa joko palveluntarjoajan tai/ja käyttäjäorganisaation konesaleista. Yksityisen pilven tyypillisenä vahvuutena on pilvipalveluinfrastruktuurin sekä siinä käsiteltävien tietojen fyysisen ja loogisen tason luotettava erottelu[28] muista tietojenkäsittely-ympäristöistä, käyttäjäorganisaatioista ja ulkoisista toimijoista. Yksityisellä pilvellä pystytään toteuttamaan tyypillisesti korkeamman turvatason palveluja, kuin muilla toteutusmalleilla.

Julkisella pilvellä tarkoitetaan palvelua, joka on julkisesti tarjolla ja hankittavissa kenen tahansa toimesta. Palvelua tuotetaan lähes poikkeuksetta palveluntarjoajan konesaleista. Julkisessa pilvessä pilvipalveluinfrastruktuuriin sekä siinä käsiteltäviin tietoihin kohdistuu yksityistä pilveä laajempi hyökkäyspinta-ala muun muassa palvelun muiden käyttäjien tai ulkoisten toimijoiden kautta.

Yhdistelmäpilvellä tarkoitetaan palvelua, jossa yhdistetään yksityinen pilvi sekä julkinen pilvi yhdeksi palvelukokonaisuudeksi. Esimerkiksi organisaation omassa konesalissa ajettavaa yksityistä pilveä voidaan täydentää julkisesta pilvestä hankittavilla palveluilla. Toteutuva turvataso riippuu tyypillisesti siitä, mitä tietoja on mahdollista siirtyä julkisen pilven puolelle, ja miten turvallisuus on järjestetty pilvitoteutusten rajapinnoissa.

[28] Yksityisen pilvipalvelun tarjoamiseen käytettävän pilvipalveluinfrastruktuurin (ml. hallinta- ja valvontaratkaisut) haavoittuvuusavaruus pystytään yleensä rajaamaan siten, että esimerkiksi ohjelmistohaavoittuvuuksiin ja virhekonfiguraatioihin liittyvät jäännösriskit ovat merkittävästi pienempiä kuin pilvipalveluinfrastruktuurissa, jota käytetään myös julkisten pilvipalvelujen tarjoamiseen. Pilvipalveluinfrastuktuurin sisäistä erottelua käsitellään yksityiskohtaisemmin vaatimuskortissa JT-03.

Palvelun tuottaminen

Pilvipalveluntarjoajalla on tyypillisesti pääsy kaikkeen palvelussa selväkielisessä muodossa käsiteltävään tietoon. Erilaisiin palveluntarjoajiin kohdistuu erilaisia riskejä. Palveluntarjoajat voidaan jakaa seuraaviin luokkiin:

- Organisaatio itse
- Kansallinen viranomainen/julkinen toimija
- Kansallinen yksityinen toimija
- Monikansallinen viranomainen/julkinen toimija (esimerkiksi EU-maista koostuva viranomaisyhteisö)
- Ei-kansallinen yksityinen toimija (EU- tai ETA-alue)
- Ei-kansallinen yksityinen toimija (muut maat)

Turvallisuuden näkökulmasta on keskeistä se, millainen varmuus palveluntarjoajan kyvykkyydestä ja luotettavuudesta voidaan saada. Esimerkiksi kotimaisten palveluntarjoajien luotettavuutta voidaan selvittää kansallisen yritysturvallisuusselvityksen[29] osana. Tilanteissa, joissa palvelun tuottamiseen osallistuu useita organisaatioita[30], riskit tulee arvioida ja huomioida kunkin palvelutuotantoon osallistuvan organisaation osalta.

Kansallisiksi palveluntarjoajiksi voidaan tulkita esimerkiksi seuraavat:

a) Yritys, jolle on myönnetty kansallinen yritysturvallisuustodistus (L 726/2014) seuraavasti:
    - Yrityksen oikeushenkilöt ovat Suomen kansalaisia, jotka pystyvät luotettavasti hallinnoimaan ja vastaamaan turvallisuusluokitellun tiedon suojaamisesta sekä hallinnollisen, fyysisen että tietotekninen suojauksen osalta.
    - Yrityksen toimintaan ei arvioida kohdistuvan luotettavuuteen oleellisesti vaikuttavia riskejä, esimerkiksi yrityksen omistusrakenteen kautta. (L 726/2014:n 37 §)
    - Turvallisuusluokiteltuun tietoon tai sen suojauksiin oleellisesti vaikuttaviin järjestelmäkomponentteihin ei ole pääsyä muilla kuin Suomen kansalaisilla. Esimerkiksi saman yrityksen ulkomaisesta emo-/tytäryhtiöstä ei ole pääsyä turvallisuusluokiteltuun tietoon tai sen suojaukseen oleellisesti vaikuttaviin järjestelmäkomponentteihin. Rajatapaukset, esimerkiksi tilanne, jossa ulkomaiselle emo-/tytäryhtiölle tarjotaan vain rajattu valvontanäkymä tiettyihin järjestelmäkomponentteihin, arvioidaan tapauskohtaisesti.
    - Turvallisuusluokitellut tiedot sijaitsevat elinkaarensa ajan fyysisesti Suomen maantieteellisten rajojen sisällä. Poikkeuksena tilanne, jossa hyväksytysti salatussa muodossa olevaa tietoa tietoa siirretään esimerkiksi Internetin yli.

b) Suomalainen viranomainen. (Soveltaen edellistä vastaavat ehdot.)

[29] Lisätietoa yritysturvallisuusselvityksestä: https://www.supo.fi/turvallisuusselvitykset/yritysturvallisuusselvitys.

[30] Esimerkiksi tilanteet, joissa pilvipalveluntarjoajan A tuottaman pilvipalvelualustan päälle on toteutettu asiakkaan B asiointijärjestelmä, jonka sovellustoiminnallisuutta ylläpitää ja kehittää yritys C.

Tiedon ja palveluiden sijainti

Pilvipalveluissa käsiteltävien tietojen käsittely tai säilytys, sekä pilvipalvelun tuottamiseen liittyvät ylläpito- ja muut hallinnointitoimet voivat sijaita maantieteellisesti eri sijainneissa. Eri sijainteihin voi liittyä erilaisia riskejä, esimerkiksi sovellettavaan lainsäädäntöön liittyen. Turvallisuuden näkökulmasta eri sijainteja voidaan jaotella seuraavasti:

- Suomi
- Tietosuojasääntelyn mahdollistamat alueet, usein esimerkiksi EU- tai ETA-alue
- Muut maat

Myös erilaiset maiden tai organisaatioiden väliset sopimukset voivat vaikuttaa sijaintiin liittyviin riskeihin. Turvallisuuden näkökulmasta myös palveluun kohdistuvat muut vaatimukset, esimerkiksi tietosuojaan tai varautumiseen liittyen, voivat asettaa maantieteellisiä rajoitteita pilvipalvelun valintaan. Sijaintiin liittyviä riskien arvioinnissa suositellaan huomioitavaksi myös se, että yleiset pilvipalveluihin soveltuvat salaustekniset suojaukset[31] eivät tuo merkittävää lisäsuojaa lainsäädäntöjohdannaisia riskejä vastaan. Sijaintia koskevien mahdollisuuksien, riskien ja vaatimusten arvioinnissa suositellaan myös huomioitavaksi EU:n asetus tietojen vapaasta liikkuvuudesta (2018/1807[32]), jota ei kuitenkaan sovelleta[33] esimerkiksi kansallisen turvallisuuden ja varautumisen perusteella asetettaviin sijaintivaatimuksiin.

[31] Esimerkiksi yleiset omien avainten käyttöön (BYOK, Bring Your Own Keys) tai pilvipalveluntarjoajan fyysiseen konesaliin sijoitettaviin laitteistopohjaisiin turvamoduuleihin (HSM, Hardware Security Module) pohjautuvat ratkaisumallit rajaavat, mutta eivät tyypillisesti estä pilvipalveluntarjoajan pääsymahdollisuuksia palvelussa käsiteltävään tietoon. Vrt. vaatimuskortti SA-03.

[32] Euroopan parlamentin ja neuvoston asetus 2018/1807. 2018. URL: https://eur-lex.europa.eu/eli/reg/2018/1807/oj.

[33] Liikenne- ja viestintäministeriön selvitys muiden kuin henkilötietojen vapaan liikkuvuuden esteistä Suomessa. 2019. URL: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161774/LVM_11_19_Muiden%20kuin%20henkil%C3%B6tietojen%20vapaan%20liikkuvuuden%20esteist%C3%A4.pdf.

Osa-alue 1: Esiehdot

EE-01	Järjestelmäkuvaus
Vaatimus	1) Pilvipalvelusta on järjestelmäkuvaus. Pilvipalveluntarjoajan kuvauksen perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Järjestelmäkuvauksesta tulee käydä ilmi vähintään: a) Pilvipalvelun palvelu- ja toteutusmallit, sekä näihin liittyvät palvelutasosopimukset (Service Level Agreements, SLAs). b) Pilvipalvelun tarjoamisen elinkaaren (kehittäminen, käyttö, käytöstä poisto) periaatteet, menettelyt ja turvatoimet, valvontatoimet mukaan lukien. c) Pilvipalvelun kehittämisessä, ylläpidossa/hallinnassa ja käytössä käytettävän infrastruktuurin, verkon ja järjestelmäkomponenttien kuvaus. d) Muutostenhallinnan periaatteet ja käytännöt, erityisesti turvallisuuteen vaikuttavien muutosten käsittelyprosessit. e) Käsittelyprosessit merkittäville normaalikäytöstä poikkeaville tapahtumille, esimerkiksi toimintatavat merkittävissä järjestelmävikaantumisissa. f) Pilvipalvelun tarjoamiseen ja käyttöön liittyvät roolit ja vastuunjako asiakkaan ja pilvipalveluntarjoajan välillä. Kuvauksesta on käytävä selvästi esille ne toimet, jotka kuuluvat asiakkaan vastuulle pilvipalvelun turvallisuuden varmistamisessa. Pilvipalveluntarjoajan vastuisiin tulee sisältyä yhteistyövelvollisuus erityisesti poikkeamatilanteiden selvittelyssä. g) Alihankkijoille siirretyt tai ulkoistetut toiminnot.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Kuvauksen tavoitteena on mahdollistaa palvelun yleisen soveltuvuuden ja riskien arviointi suhteessa asiakkaan käyttötapaukseen.
Lisätietoja	Infrastruktuurin, verkon ja järjestelmäkomponenttien kuvauksen tulee olla riittävän yksityiskohtainen, jotta kuvauksen pohjalta pystytään arvioimaan palvelun yleistä soveltuvuutta ja riskejä suhteessa asiakkaan käyttötapaukseen. Vrt. KT-01 (Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi). Infrastruktuurin kuvauksessa voidaan tietyin rajauksin hyödyntää myös ohjelmistokoodia, jonka pohjalta kyseinen infrastruktuuri rakennetaan. Palvelumalleja ovat esimerkiksi infrastruktuuri palveluna (Infrastructure as a Service, IaaS), ohjelmistoalusta palveluna (Platform as a Service, PaaS) ja ohjelmisto palveluna (Software as a Service, SaaS). Toteutusmalleja ovat esimerkiksi yksityinen pilvi (private cloud), yhdistelmäpilvi (hybrid cloud) ja julkinen pilvi (public cloud). Osa pilvipalveluntarjoajista tarjoaa asiakkailleen mahdollisuuden ottaa käyttöönsä uusia toiminnallisuuksia, jotka ovat esikatselu- tai testausvaiheessa. Mikäli tällaisia toiminnallisuuksia halutaan ottaa käyttöön salassa pidettävän tiedon käsittelyyn, suositellaan riskienarvioinnissa huomioitavaksi muun muassa käyttöönottoon liittyvät vastuut. Uusien toiminnallisuuksien toteutuksessa voi vielä olla turvallisuuspuutteita, joista mahdollisesti aiheutuvien vahinkojen korvaaminen on sopimuksissa usein osoitettu asiakkaalle.

EE-02	Lainsäädäntöjohdannaiset riskit
Vaatimus	1) Pilvipalveluun liittyvät lainsäädäntöjohdannaiset riskit ja velvoitteet on kuvattuna. Palveluntarjoajan tuottamien kuvausten perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Kuvausten tulee kattaa palvelun käytön ja palvelussa käsiteltävien tietojen koko elinkaaren. Kuvauksista on käytävä ilmi vähintään: a) Palvelussa käsiteltävän tiedon fyysinen sijainti koko tiedon elinkaaren ajalta, kattaen myös mahdolliset alihankinta-/ulkoistusketjut. b) Palvelun eri toimintojen (esimerkiksi ylläpito-/hallintaratkaisut, varmistukset) ja komponenttien fyysinen sijainti koko tiedon elinkaaren ajalta. c) Mahdolliset muut palvelun tuottamiseen osallistuvat tahot, esimerkiksi mahdolliset alihankinta-/ulkoistusketjut. d) Palvelun käyttöön ja palvelussa käsiteltäviin tietoihin sovellettava lainsäädäntö ja oikeuspaikka. e) Toimijat, joilla voi sovellettavasta lainsäädännöstä johtuen olla pääsy palvelussa käsiteltäviin tietoihin. 2) Lainsäädäntöjohdannaiset riskit eivät rajoita kyseisen pilvipalvelun soveltuvuutta kyseiseen käyttötapaukseen. 3) Pilvipalvelun asiakkaan tiedot sijaitsevat koko elinkaarensa ajan vain sopimuksessa kuvatuissa fyysisissä sijainneissa. Poikkeuksena tilanne, jossa pilvipalvelun asiakas on kirjallisesti etukäteen hyväksynyt tietojen siirron tai käsittelyn muissa fyysisissä sijainneissa. 4) Pilvipalveluntarjoajan sopimusehdot eivät rajoita kyseisen pilvipalvelun soveltuvuutta kyseiseen käyttötapaukseen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Kuvauksen tavoitteena on mahdollistaa palvelun yleisen soveltuvuuden ja riskien arviointi suhteessa loppuasiakkaan käyttötapaukseen.
Lisätietoja	Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa pilvipalveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy pilvipalvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia. 1a) ja 3) Tilanteissa, joissa palvelu on toteutettu siten, että tiedon fyysinen sijainti voi vaihdella, tulee kuvata kaikki mahdolliset fyysiset sijainnit, minne tiedot voivat elinkaarensa aikana palvelussa kulkeutua. 4) Viranomaisen voi olla haastavaa pystyä täyttämään esimerkiksi tiedonhallintalain (906/2019) 13 § velvoitetta varmistua tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta koko niiden elinkaaren ajan, mikäli sopimusehtojen muuttaminen on mahdollista yksipuolisesti. Henkilötietojen käsittely voi toisaalta tietosuojasääntelyn näkökulmasta estyä, mikäli pilvipalveluntarjoaja ei pysty tarjoamaan tietosuojasääntelyn mukaista sopimusta, jonka muuttaminen ei ole mahdollista yksipuolisesti, toisin sanoen ilman pilvipalvelun asiakkaan suostumusta. Vrt. TJ-07 (Vaatimustenmukaisuus ja tietosuoja). Arvioinnissa tulee huomioida EU:n yleisen tietosuoja-asetuksen 28 artiklan 4. kohdan sekä rikosasioiden tietosuojalain 17 §:n 2 momentin vaatimukset niin sanottuja alikäsittelijöitä käytettäessä. Palveluntarjoajan (rekisterinpitäjän) tulee tehdä henkilötietojen käsittelijän kanssa kirjallinen sopimus. Pilvipalveluiden sopimuksiin ja käyttöehtoihin saattaa liittyä myös erilaisia pilvipalvelutoimittajakohtaisia tapoja määritellä palvelun (tai sen osan) fyysisiä sijaintimaita. Henkilötietojen siirtäminen EU-/ETA-alueen ulkopuolelle tulee aina tehdä EU:n yleisessä tietosuoja-asetuksessa (V luku) tai rikosasioiden tietosuojalaissa (7 luku) säädettyjen edellytysten mukaisesti. Arvioinnissa suositellaan noudatettavan taulukossa 2 kuvattuja jatkoarvioinnin yleisperiaatteita.

Taulukko 2. Jatkoarvioinnin mahdollisuudet.

Tietotyyppi	Pilvipalvelu-tyyppi	Fyysinen sijainti	Palvelun-tarjoaja	Lisätietoja
Julkinen	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Soveltuvien suojausten arvioinnissa painotus riittävän eheyden ja saatavuuden varmistamisessa.
Salassa pidettävä	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Mikäli ei sisällä henkilötietoja. Mikäli sisältää, vertaa riviin "Henkilötieto" alla. Tulee myös huomioida, että tiedonhallintalain (906/2019) 13 § edellyttää riskien tunnistamista ja suojausten mitoittamista riskienarvioinnin mukaisesti. Viranomaisen riskienarvioinnin tulokset voivatkin edellyttää kattavampia suojauksia tai rajoituksia, kuin mihin PiTuKrissa otetaan kantaa.
Henkilötieto	Ei rajoitteita	Tietosuoja-sääntelyn mahdollistamat alueet, usein esim. EU/ETA	Ei rajoitteita, ellei kyseisiin henkilötietoihin liittyvän riskienarvioinnin perusteella rajauksia	Palvelukokonaisuuden tulee täyttää henkilötietojen suojaamiseen liittyvä erityislainsäädäntö. Henkilötietojen käsittely edellyttää tietojen luonteen perusteella tehtävää riskiarviointia, mistä voi seurata rajoitteita myös tietojen fyysisen sijainnin, tietojen hallinnoinnin ja palveluntarjoajan valintaan.
Varautumisen näkökulmasta suojattavat tiedot	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Tiedon hallinnoinnin oltava mahdollista tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
TL IV	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
Suuri määrä salassa pidettävää tai/ja henkilötietoa (TL IV -kasauma)	Ei rajoitteita	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
Kansainvälinen RESTRICTED (KV-R)	Yksityinen/ yhteisö	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana). Suojaamisessa huomioitava ko. tietoon kohdistuvat tiedon originaattorin tai/ja omistajan asettamat erityisvaatimukset. Vrt. Katakri 2015.
Suuri määrä salassa pidettävää tietoa tai/ja TL IV -tietoa tai/ja henkilötietoa (TL III -kasauma)	Yksityinen/ yhteisö[34]	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana). Kasautumisvaikutuksessa huomioitava menetelmät, joilla rajataan pääsy vain tehtävässä tarvittavaan yksittäiseen tai suppeaan osaan tietosisällöstä, ja joilla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä havaitaan. Kun arviointityökaluna käytetään PiTuKria, tulisi kasautumisvaikutus tulkita siten, että TL IV -vaatimusten lisäksi suojauksilta edellytetään tietovarannon fyysiselle suojaukselle turva-aluetta (FT-01), erityistä luotettavuutta erottelutoteutukselle (JT-03) sekä sovelluskerroksen turvallisuudelle (MH-02 / kohta 1), tehostettua jäljitettävyyttä ja havainnointikykyä (JT-01 / Kohdat 1f-g ja 4e) sekä tehtävien luotettavaa erottelua (HT-05 / kohta 5). Vrt. Katakri 2015 (I 01 / Lisätietoja / Kasautumisvaikutus).
TL III ja TL II	Yksityinen/ yhteisö	Suomi	Kansallinen viranomainen/ julkinen toimija/ yritys	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan luotettavuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana). Huomioitava turvallisuusluokan III tai/ja II lisäsuojausvaatimukset[35], vrt. Katakri 2015.

[34] Yhteistöpilvi (community/government cloud) tietyin rajauksin, esimerkiksi valtionhallinnon tai muun viranomaisyhteisön käyttöön rajattu palvelu.

[35] Käytännön toteutusmallina yleensä pilviteknologian käyttö fyysisesti suojattujen turva-alueiden sisällä siten, että kyseinen turvallisuusluokan III/II käsittely-ympäristö on kokonaisuudessaan fyysisesti ja loogisesti luotettavasti eriytettynä muista ympäristöistä.

Osa-alue 2: Turvallisuusjohtaminen

TJ-01	Turvallisuusperiaatteet
Vaatimus	1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. 3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan johdolle ja niiden toteutumista seurataan säännöllisesti.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuusperiaatteilla tavoitellaan sitä, että johto sitoutuu organisaation turvallisuustyöhön ja että turvallisuustyö tukee organisaation toimintaa.
Lisätietoja	Turvallisuusperiaatteet viestitään henkilöstölle ja tarvittaville sidosryhmille. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi yksittäisenä dokumenttina tai osana organisaation ohjeistokokonaisuutta. Vaatimuksen täyttymisen osoittamisessa voidaan hyödyntää voimassa olevaa ISO27001-sertifiointia, edellyttäen, että sertifiointi (ml. soveltamissuunnitelma) kattaa pilvipalvelun kehittämisessä ja tuottamisessa käytettävät prosessit.

TJ-02	Turvallisuuden vastuut
Vaatimus	1) Pilvipalvelun turvallisuuden hoitamisen tehtävät ja vastuut on määritelty ja dokumentoitu. 2) Pilvipalvelun tarjoamiseen ja käyttöön liittyvä vastuunjako asiakkaan ja palveluntarjoajan välillä on kuvattu. Vrt. EE-01. 3) Pilvipalvelun tietoturvallisuudesta vastaava henkilö on nimetty.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa.
Lisätietoja	Turvallisuusvastuiden määrittely on oleellista, jotta vastuuhenkilöt voivat toteuttaa heidän vastuullaan olevat turvallisuustehtävät. Mikäli muuta ei ole kuvattu, ovat kaikki turvallisuus-vastuut organisaation johdolla. Pilvipalvelupolitiikan tai vastaavan kuvauksen määrittelyn tavoitteena on tuoda selkeästi esille, mitkä turvallisuusasioista ovat asiakkaan vastuulla ja mitkä palveluntarjoajan.

TJ-03	Turvallisuusriskien hallinta
Vaatimus	1) Organisaatiolla on käytössä riskienhallintaprosessi. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi. Riskienhallintapäätökset vastuutahoineen dokumentoidaan. 2) Riskien analysoinnissa on käytettävä järjestelmällistä ja ymmärrettävää menetelmää. 3) Riskienhallinnan on katettava vähintään turvallisuusjohtamisen, tila- ja tietoturvallisuuden osa-alueet. 4) Tunnistetut riskit otetaan huomioon tarvittavien sidosryhmien osalta. Pilvipalveluntarjoajan tulee varmistaa, että asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Vrt. TJ-08. 5) Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvallisuus-tavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. 6) Turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon luokitteluperuste, määrä, muoto ja sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. 7) Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Riskienhallinnan tavoitteena on tunnistaa ja hallita toimintaedellytyksiä mahdollisesti vaarantavia tekijöitä ja pitää toimintaan kohdistuvat riskit sellaisissa rajoissa, etteivät toiminta ja tavoitteet ole uhattuna.
Lisätietoja	**Lainsäädännön tai viranomaisvaatimusten huomioiminen turvallisuustason suunnittelussa** Organisaation tulee tunnistaa, mitä lainsäädännön tai viranomaisen vaatimuksia omaan toimintaan liittyy. Näiden vaatimusten täyttäminen, esimerkiksi viranomaisen hyväksynnän saamiseksi, voi edellyttää organisaation sisäisiä turvallisuusvaatimuksia tiukempien suojausten toteuttamista. Vrt. TJ-07 (Vaatimustenmukaisuus ja tietosuoja). **Riskienhallinnan kohdentaminen salassa pidettävien tietojen näkökulmasta** Riskienhallintatoimet tulee kohdentaa siihen ympäristöön, jossa salassa pidettäviä tietoja on tarkoitus käsitellä. Riskienhallintatoimenpiteet voivat olla hallinnollisia (esim. henkilöstön koulutus, ohjeet) tai teknisiä (esim. ympäristön tekniset suojaukset). **Monitasoisen suojaamisen huomiointi riskienhallinnassa** Riskienhallinnan toimenpiteiden suunnittelun tavoitteena on vähentää toimintaan kohdis-tuvia riskejä. Näiden suunnittelussa hyvä periaate on turvallisuusjärjestelyjen monitasoisuus (defence in depth). Tämä tarkoittaa sitä, että mikäli yksittäinen turvallisuusjärjestely pettää, on jäljellä silti muita suojaustoimenpiteitä. Yksittäisiin riskeihin nähden riittävän suojauksen voi toteuttaa yksittäisillä luotettavilla turvatoimilla tai useampia turvatoimia yhdistelemällä. **Riskien hallinnan ja analysoinnin menetelmiä** Riskienhallintaan ja analysointiin on olemassa useita eri menetelmiä, joilla kullakin on omat vahvuutensa ja heikkoutensa. Useissa järjestelmällisissä menetelmissä toiminta perustuu uhkien ja haavoittuvuuksien tunnistamiseen, todennäköisyyksien ja vaikuttavuuden arviointiin, tarvittavien riskejä pienentävien toimenpiteiden määritykseen, jäännösriskien arviointiin sekä korjaavien toimien seurantaan.

TJ-04	Turvallisuushäiriöiden hallinta
Vaatimus	1) Organisaatiolla on menettelytavat turvallisuushäiriöiden asianmukaiseen käsittelyyn. 2) Organisaatiolla on käytössään selkeät prosessit turvallisuushäiriöiden ilmoittamisesta. Organisaatiolla on määritettynä henkilöt/tahot, joille turvallisuushäiriöistä tai niiden epäilyistä tulee ilmoittaa. 3) Turvallisuushäiriöiden määrää ja tyyppejä seurataan. Toteutuneiden häiriöiden uusiutuminen on pyrittävä estämään korjaussuunnitelmissa. 4) Asiakastiedon käsittelyyn liittyvät turvallisuushäiriöt tai niiden epäilyt ilmoitetaan kyseiselle asiakkaalle.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuushäiriöiden hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaaliksi. Ilmoitusvelvollisuus asiakkaalle tukee asiakkaan riskienarviointia ja muun muassa vahinkojen minimointia.
Lisätietoja	Vaatimuksen täyttämisessä voi hyödyntää esimerkiksi seuraavaa toimintamallia: Turvallisuushäiriöiden hallinta on 1) suunniteltu, 2) ohjeistettu ja koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, 4) harjoiteltu, ja erityisesti 5) viestintäkäytännöt ja vastuut on sovittu. Erityisesti turvallisuusluokiteltujen tietojen käsittelyyn liittyvistä häiriöistä, tietomurroista tai sellaisten yrityksistä suositellaan ilmoittamaan Kyberturvallisuuskeskukselle. Tunnistetusta rikollisesta toiminnasta suositellaan ilmoittamaan myös poliisille. Lisäksi tulee ottaa huomioon EU:n yleisen tietosuoja-asetuksen 33 artiklassa säädetty lyhyt määräaika, sekä rikosasioiden tietosuojalain 33 §:ssä säädetty palveluntarjoajan ilmoittamisvelvollisuus.

TJ-05	Jatkuvuudenhallinta
Vaatimus	1) Jatkuvuudenhallinnan prosessit ja menettelyt on suunniteltu, toteutettu, testattu ja kuvattu siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Järjestelyissä huomioidaan erityisesti, että a) toipuminen ja jatkuvuuden varmistaminen toimintavaatimuksiin nähden riittävässä ajassa on huomioitu suunnittelussa, b) toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset tietojen käsittelyyn ja säilyttämiseen, c) poikkeamista tehdyt havainnot tuodaan osaksi riskienarviointia, ja toipumis- ja jatkuvuussuunnitelmia päivitetään tehtyjen havaintojen ja saatujen tulosten perusteella, ja d) jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai saatavuuden menettäminen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Jatkuvuudenhallinnan tavoitteena on varmistaa palvelun jatkuvuus siten, että pystytään vastaamaan siihen kohdistuneisiin saatavuus-, eheys- ja luottamuksellisuusvaatimuksiin.
Lisätietoja	Vaatimuksen täyttämisessä voi hyödyntää esimerkiksi seuraavaa toimintamallia: Liiketoimintaan kohdistuvien vaikutusten analyysi sekä liiketoiminnan jatkuvuutta ja varautumista koskevat suunnitelmat todennetaan, päivitetään ja testataan säännöllisin väliajoin (vähintään kerran vuodessa) tai aina organisaatiota tai ympäristöä koskevien olennaisten muutosten jälkeen. Testit koskevat myös asiakkaita ja oleellisia kolmansia osapuolia (kuten keskeisiä toimittajia), joihin näillä asioilla on vaikutusta. Testit dokumentoidaan ja tulokset otetaan huomioon tulevissa liiketoiminnan jatkuvuutta koskevissa turvatoimissa. Konesalipalvelut (kuten vesihuolto, sähkö, lämpötilan ja kosteuden säätö, tietoliikenne ja Internet-yhteys) varmistetaan ja niitä seurataan ja ylläpidetään sekä testataan säännöllisin väliajoin niiden jatkuvan tehokkuuden varmistamiseksi. Palvelut on suunniteltu sisältämään automaattisia vikasietoisia mekanismeja ja esimerkiksi kahdennuksia. Huoltotyöt tehdään toimittajien suosittelemien huoltovälien ja -tavoitteiden mukaisesti, ja niitä tekee vain valtuutettu henkilöstö. Huoltopöytäkirjoja ja niissä mahdollisesti olevia merkintöjä epäillyistä tai havaituista puutteista säilytetään ennalta sovitun ajan. Vrt. FT-05 (Varautuminen ja jatkuvuudenhallinta) ja KT-03 (Varmistus- ja palautusprosessit). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi se, että pilvipalvelualustan päälle toteutetun asiakasjärjestelmän saatavuus on usein suoraan riippuvainen pilvipalvelualustan toimivuudesta.

TJ-06	Tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä
Vaatimus	1) Pilvipalvelun tuottamisen ja asiakastiedon käsittelyn kannalta olennaisten suojattavien kohteiden (tiedot, laitteistot, ohjelmistot, toimitilat) luokitteluun ja merkitsemiseen on käytössä yhdenmukainen menetelmä. 2) Tietosisällöltään salassa pidettävät suojattavat kohteet (tietoaineistot, laitteistot ja järjestelmät) on luokiteltu lakisääteisten vaatimusten perusteella. 3) Pilvipalvelun tuottamiseen ja asiakastiedon käsittelyyn liittyvät laitteistot ja ohjelmistot on tunnistettu. 4) Laitteistot ja ohjelmistot on luokiteltu niiden kriittisyyden mukaisesti. 5) Kullekin laitteistolle ja ohjelmistolle on nimetty omistaja/vastuutaho. 6) Laitteistoista ja ohjelmistoista pidetään ajantasaista kirjanpitoa siten, että muutokset hyväksyttyyn kokoonpanoon pystytään havaitsemaan vertaamalla toteutusta kirjanpitoon. (Vrt. MH-01: Muutostenhallinta.)
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Luokittelun tavoitteena on tunnistaa ja mitoittaa turvatoimet suojattavien kohteiden suojaustarpeen perusteella. Merkitsemisen tavoitteena on mahdollistaa luokittelun mukaisten turvatoimien käytännön toteutus.
Lisätietoja	Luokituksen voi ilmaista eri tavoin riippuen tietoaineistosta, käsittely-ympäristöstä ja käyttäjistä. Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään selkeämmin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet. Vaatimuskohdan 5 täyttämiseen voidaan hyödyntää myös menettelyä, jossa pilvipalveluntarjoaja luokittelee kaiken asiakkaan palveluun tuottaman tietoaineiston sisäisen luokittelunsa mukaiseksi siten, että kyseisen luokittelun omaavien suojattavien kohteiden (tietoaineistot, laitteistot ja järjestelmät) käsittelyn suojaukset täyttävät salassa pidettävän tai/ja turvallisuusluokitellun salassa pidettävän tiedon suojausvaatimukset koko tiedon elinkaaren ajalta. Laitteisto- ja ohjelmistokirjanpidon ylläpitämiseen suositellaan automatisoituja menettelyjä. Kirjanpidon ajantasaisuus voidaan vaihtoehtoisesti varmistaa esimerkiksi kuukausittain tehtävillä manuaalisilla tarkastuksilla. Kirjanpidon muutoshistoria (tehdyt muutokset) tulee olla jälkikäteen selvitettävissä. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että a) asiakas on tunnistanut pilvipalveluun sijoitettavat suojattavat kohteet (asiakkaan tietoaineistot, järjestelmät ja mahdollisesti myös laitteistot), ja luokitellut ne lakisääteisten vaatimusten perusteella, b) asiakas on varmistanut, että kyseisten suojattavien kohteiden sijoittamiselle kyseiseen pilvipalveluun ei ole esteitä (vrt. EE-02), c) asiakas on varmistanut, että pilvipalveluntarjoaja on tietoinen kyseisten suojattavien kohteiden luokittelusta, ja että myös d) asiakkaalla on asiakkaan vastuulle kuuluvasta kokonaisuudesta ajantasainen kirjanpito siten, että muutokset hyväksyttyyn kokoonpanoon pystytään havaitsemaan vertaamalla toteutusta kirjanpitoon. (Vrt. MH-01: Muutostenhallinta.)

TJ-07	Vaatimustenmukaisuus ja tietosuoja
Vaatimus	1) Pilvipalveluun sovellettavien lakien ja säädösten määräykset sekä menettelyt näiden noudattamiseksi on tunnistettu ja dokumentoitu, sekä säännöllisesti päivitetty. 2) Riippumattomat kolmannet osapuolet arvioivat vähintään vuosittain pilvipalveluun liittyvän toiminnan, prosessit ja tietotekniikkajärjestelmät soveltuvin osin, erillisessä arviointisuunnitelmassa määritellyn kuvauksen mukaisesti. Arvioinnin tulee pyrkiä tunnistamaan mahdolliset tapaukset, joissa lakeja tai säädöksiä ei noudateta. Arviointisuunnitelma kattaa palvelun turvallisuuden siten, että kaikki keskeiset turvallisuuteen vaikuttavat kokonaisuudet arvioidaan korkeintaan kolmen vuoden välein. Havaitut poikkeamat dokumentoidaan, priorisoidaan ja korjataan niiden kriittisyyden mukaisesti. 3) Pilvipalvelun toimintaan kohdistetaan vähintään vuosittain sisäinen tarkastus, jonka tavoitteena on selvittää kuinka palvelu kokonaisuutena vastaa turvakäytäntöjensä ja sopimus- sekä lainsäädännöllisten vastuiden täyttämiseen. 4) Ylin johto vastaa siitä, että havaitut poikkeamat priorisoidaan ja korvaavat suojaukset tai korjaukset toteutetaan riittävän nopeasti.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Lainsäädännöllisten ja sopimusvelvoitteiden täyttäminen.
Lisätietoja	Pilvipalveluntarjoajan tulee huolehtia esimerkiksi henkilötietojen käsittelyn turvallisuudesta asiaa koskevan sääntelyn mukaisesti, ks. esim. tietosuojalaki (1050/2018), laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018, rikosasioiden tietosuojalaki), sekä yleisen tietosuoja-asetuksen (GDPR, (EU) 2016/679) 32 artikla. Henkilötietojen luokittelu ja luokittelun mukainen käsittely voi olla tarpeen, mikäli erilaisten henkilötietojen suojaustarpeet (oikeudelliset vaatimukset, arvo, arkaluonteisuus) eroavat tai/ja mikäli niitä käsitellään eroavasti suojattuna pilvipalveluntarjoajan eri toiminnoissa tai järjestelmissä. Vrt. vaatimuskortti EE-02. Henkilötietojen käsittelyä valvovana viranomaisena Suomessa toimii Tietosuojavaltuutettu (TSV). Henkilötietojen tietoturvaloukkauksista tulee ilmoittaa sekä TSV:lle, että tarvittaessa myös käyttäjille GDPR 33 ja 34 artiklojen mukaan. Henkilötietoloukkausten ilmoittamisessa tulee huomioida myös muu lainsäädäntö. Esimerkiksi asetuksessa (EU) 611/2013 säädetään teleyritysten velvollisuudesta ilmoittaa henkilötietojen tietoturvaloukkauksista Liikenne- ja viestintävirastolle ja tarvittaessa myös käyttäjille. Vrt. TJ-04 (Turvallisuushäiriöiden hallinta). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että asiakas ei voi ulkoistaa omaa vastuutaan vaatimustenmukaisuuden toteuttamisesta, mukaan lukien sen varmistamista, että ulkoistuskumppani (tässä erityisesti pilvipalvelun-tarjoaja) täyttää käsitellyille tiedoille asetetut vaatimukset.

TJ-08	Palveluntarjoajien ja toimittajien turvallisuus
Vaatimus	1) Asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Varmistettava erityisesti, että a) ennen palveluntarjoajan/toimittajan henkilöstön pääsyä suojattaviin kohteisiin, henkilöstö on läpikäynyt vastaavat suojaustoimenpiteet (sopimukset, salassapito-sitoumukset, turvaselvitykset, koulutukset), kuin pilvipalveluntarjoajankin henkilöstö, b) palveluntarjoajat/toimittajat on kirjallisesti ohjeistettu ja sopimuksin velvoitettu noudattamaan vähintään vastaavantasoisia suojauksia, kuin organisaatiokin, c) sopimusvelvoitteiden noudattamisen varmistamiseen ja valvontaan on käytössä luotettavat menettelyt, d) turvallisuusluokitellun tiedon käsittelyyn suoraan tai epäsuoraan osallistuvat palveluntarjoajat ja toimittajat ovat voimassa olevan viranomaishyväksynnän, tai vastaavan menettelyn piirissä. Menettely kattaa soveltuvin osin sekä hallinnollisen (turvallisuusjohtamisen), fyysisen että teknisen tietoturvallisuuden kokonaisuudet.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan siltä osin, kun siihen liittyy ulkoisia palveluntarjoajia tai/ja toimittajia.
Tietotyypit	1a-1c: Salassa pidettävä, henkilötiedot 1d: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojattavien kohteiden turvallisuus varmistetaan myös tilanteissa, joissa niihin on suora tai epäsuora pääsy pilvipalveluntarjoajan omilla palveluntarjoajilla tai/ja toimittajilla. Vrt. MH-02 (Järjestelmäkehitys).
Lisätietoja	Ulkoistus- ja toimitusketjujen turvallisuus vaikuttaa usein suoraan myös pilvipalvelussa käsiteltävien tietojen suojauksiin. Mikäli pilvipalveluntarjoajan palvelun turvallisuus nojaa joiltain osin ulkoistuksiin tai toimitusketjuihin, myös näiden turvallisuus on huomioitava pilvipalvelun kokonaisturvallisuuden suunnittelussa ja ylläpidossa. Tulee myös huomioida EU:n yleisen tietosuoja-asetuksen 28 artiklan 4. kohdan sekä rikosasioiden tietosuojalain 17 §:n 2 momentin vaatimukset henkilötietojen käsittelystä niin sanottuja alikäsittelijöitä käytettäessä. Palveluntarjoajan (rekisterinpitäjän) tulee tehdä henkilötietojen käsittelijän kanssa kirjallinen sopimus. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä palveluntarjoajia.

Osa-alue 3: Henkilöstöturvallisuus

HT-01	Työsuhteen elinkaaren huomioiminen
Vaatimus	1) Organisaatiolla on käytössä turvallisuuden huomioon ottava menettely työsuhteen elinkaaren eri vaiheissa. Erityisesti huomioidaan toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Henkilöstöön liittyvien riskien pienentäminen työsuhteen elinkaaren aikana.
Lisätietoja	Turvallisuustekijät huomioon ottava menettely edellyttää tyypillisesti menettelyohjeita, jotka on koulutettu ja saatavilla tarvittavilla henkilöstöryhmillä. Menettelyohjeet voidaan jakaa esimerkiksi työsuhteen elinkaaren mukaisiin kokonaisuuksiin. Ohjekokonaisuuksia voivat olla esimerkiksi rekrytointiohjeet, perehdyttämisohjeet, työsuhteen aikaisten muutosten ohjeet, työsuhteen päättymisen ohjeet ja ohjeet yksityiskohtaisempiin toimiin kuten esimerkiksi ohjeet käyttö- ja pääsyoikeuksien muutoksiin. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

HT-02	Henkilöstön luotettavuuden arviointi
Vaatimus	1) Pilvipalvelun asiakkaiden tietoja tai yhteistä IT-infrastruktuuria käyttämään pääsevien sisäisten ja ulkoisten työntekijöiden taustat tarkistetaan paikallisen lainsäädännön mahdollistamien menettelyjen mukaisesti ennen työsuhteen alkua. Lainsäädännön sallimissa rajoissa tarkistukseen sisällyttävä vähintään: a) Henkilöllisyyden todentaminen. b) Työhistorian todentaminen. c) Koulutustaustan todentaminen. 2) Turvallisuusluokiteltujen aineistojen käsittelyyn liittyvien henkilöiden luotettavuus selvitetään ja sitä seurataan asianmukaisen tason turvallisuusselvitysmenettelyin.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 2: TL IV & KV-R, TL III (kasauma) (keskeiset turvallisuusvastaavat, tekniset ylläpitäjät tai vastaavat henkilöt, joilla on pääsy suureen määrään TL IV -tietoa tai mahdollisuus vaikuttaa näiden tietojen suojaamiseen.)
Suojaustavoite	Henkilöstön luotettavuuteen liittyvien riskien pienentäminen.
Lisätietoja	2) Mikäli on olemassa suora tai epäsuora pääsy asiakkaiden suojattaviin tietoihin. Esimerkiksi virtualisointialustan (hypervisor) ylläpidolla on usein käytännössä pääsy myös virtuaalikoneissa käsiteltäviin asiakkaiden tietoihin. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

HT-03	Salassapito- ja vaitiolositoumukset
Vaatimus	1) Salassapito- tai vaitiolositoumusmenettely on käytössä. Salassapitosopimukset on allekirjoitettava ennen sopimussuhteen alkamista tai ennen kuin pilvipalvelun asiakkaiden tietoja koskeva käyttöoikeus myönnetään.
Soveltuvuus	Pilvipalvelun tarjoajan sisäisten työntekijöiden, ulkoisten palveluntarjoajien ja toimittajien henkilöstö.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Henkilöstön luotettavuuteen liittyvien riskien pienentäminen erityisesti tietoisuuden lisäämisellä.
Lisätietoja	Salassapitosopimuksessa (tai vast.) tulee kuvata vähintään seuraavat asiat: • Mitä tietoja on käsiteltävä salassa pidettävinä • Salassapitosopimuksen ehdot • Mihin toimiin on ryhdyttävä, kun sopimus päättyy (eli esimerkiksi tietovälineet on tuhottava tai palautettava) • Kuka omistaa tiedot • Mitkä säännöt ja säädökset koskevat salassa pidettävien tietojen käyttöä ja luovuttamista muille osapuolille, jos tarpeen • Seuraamukset salassapitosopimuksen ehtojen rikkomisesta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

HT-04	Turvallisuustietoisuus
Vaatimus	1) Keskeiset turvallisuuteen liittyvät periaatteet ja toimintatavat on kuvattuna. 2) Turvalliset toimintatavat on henkilöstölle jalkautettuna siten, että henkilöstön riittävästä turvatietoisuudesta pystytään varmistumaan. 3) Turvallisuuteen liittyvien kuvausten/ohjeistusten ajantasaisuus sekä jalkautuminen käytäntöön varmistetaan säännöllisesti, vähintään vuosittain. 4) Turvallisuuteen liittyvät ohjeet kattavat henkilötietoihin ja salassa pidettävään tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta. 5) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti.
Soveltuvuus	Pilvipalvelun tarjoajan sisäisten työntekijöiden, ulkoisten palveluntarjoajien ja toimittajien henkilöstö.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Turvallisuuteen liittyvillä periaatteilla (vrt. TJ-01) ja kuvauksilla/ohjeistuksilla sekä niiden jalkauttamisella tavoitellaan sitä, että turvalliset toimintatavat on suunniteltu ja että henkilöstö pystyy käytännössäkin toimimaan turvallisesti, huomioiden myös erikoistilanteet. Vrt. KT-01 (Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi).
Lisätietoja	Turvallisuusvastuiden määrittely on oleellista, jotta vastuuhenkilöt voivat toteuttaa heidän vastuullaan olevat turvallisuustehtävät. Mikäli muuta ei ole kuvattu, ovat turvallisuusvastuut organisaation johdolla. Vrt. TJ-02 (Turvallisuuden vastuut). Vaatimuksen täyttämisessä voidaan hyödyntää esimerkiksi seuraavaa menettelyä: 1) Henkilöstölle annetaan ohjeet ja koulutusta salassa pidettävien tietojen asianmukaisesta käsittelystä. 2) Salassa pidettävien tietojen käsittelyä koskeva koulutus on säännöllistä ja koulutuksiin osallistuneet henkilöt dokumentoidaan. 3) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti. 4) Tietoturvaa koskevat kohderyhmittäin räätälöidyt turvallisuuskoulutukset ja turvallisuustietoisuuden kehittämisohjelmat ovat tarjolla ja pakollisia kaikille pilvipalvelun tarjoajan sisäisille ja ulkoisille työntekijöille. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

HT-05	Tiedonsaantitarpeet ja tehtävien erottelu
Vaatimus	1) Salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ylläpidetään luetteloa. Tällaisiksi työtehtäviksi tulkitaan kuuluvaksi myös sellaiset kehitys- ja ylläpitotehtävät, joissa on suora tai epäsuora mahdollisuus päästä salassa pidettävään tietoon, tai muuten oleellisesti vaikuttaa salassa pidettävän tiedon suojauksiin. 2) Pääsy salassa pidettävään tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty. 3) Luetteloa turvallisuusluokiteltujen tietojen käsittelyoikeuksista ylläpidetään luokittain. 4) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi. 5) Turvallisuusluokan III kasaumalle lisäksi: Kriittiset tehtävät ja vastuualueet on eriytetty eri henkilöille, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Erityishuomiota kiinnitettävä siihen, että yksittäinen henkilö ei pysty poistamaan toimiensa jälkiä tai merkittävästi estämään poikkeavien toimien havaitsemista.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3-4: TL IV & KV-R, TL III (kasauma) 5: TL III (kasauma)
Suojaustavoite	Suojaustavoitteena on mahdollistaa salassa pidettävän tiedon päätyminen vain valtuutetuille henkilöille tiedonsaantitarpeen (need-to-know) mukaisesti, ja siten pienentää salassa pidettävään tietoon kohdistuvia riskejä.
Lisätietoja	Tiedonsaantitarpeen määrittämistä helpottaa se, että organisaatio on kuvannut periaatteet, jolla organisaation henkilöt pääsevät salassa pidettäviin tietoihin, sekä prosessin tai menettelytapaohjeet, joilla työtehtäväperusteisesti pääsy myönnetään ja hallinnoidaan muutostilanteissa. Käsittelyoikeusmäärittelyissä sekä työtehtävä- ja roolimäärittelyissä tulisi ottaa huomioon, ettei synny vaarallisia työ- tai rooliyhdistelmiä. Useimmissa järjestelmissä riittävä tehtävien erottelu on toteutettavissa järjestelmän ylläpitoroolien (ja henkilöiden) ja lokien valvontaan osallistuvien roolien (ja henkilöiden) erottelulla toisistaan. Usein käytettynä valvontamekanismina on myös se, että kriittiset ylläpito- ja vastaavat toimet vaativat kahden tai useamman henkilön hyväksynnän (”two man rule”). Vaatimuksen arvioinnissa tulee huomioida myös vastuujako pilvipalveluntarjoajan ja asiakkaan välillä. Pilvipalveluntarjoaja ei tyypillisesti pysty vaikuttamaan esimerkiksi asiakkaan vastuulla olevan järjestelmäosuuden kehittäjien tai ylläpitäjien tiedonsaantitarpeen varmistamiseen. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaankin huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Osa-alue 4: Fyysinen turvallisuus

FT-01	Monitasoinen suojaaminen ja riskienhallinta
Vaatimus	1) Fyysiset turvatoimet on toteutettu monitasoisen suojaamisen periaatetta noudattaen. 2) Suojattavat tilat rakennuksessa on luokiteltu turvallisuusalueiksi (hallinnollinen alue, turva-alue) ja niillä on selkeästi määritellyt ja näkyvät rajat. 3) Korkeintaan turvallisuusluokan IV salassa pidettävää tietoa sisältävät tietovarannot ja tietojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle. 4) Turvallisuusluokan III kasauman muodostaneet tietovarannot ja tietojen pääsynrajauksiin ja -valvontaan käytettävät tietojärjestelmät on sijoitettava turva-alueelle. 5) Hallinnollisilla alueilla on selkeästi määritetyt näkyvät rajat ja joihin vain organisaation valtuuttamilla henkilöillä on pääsy ilman saattajaa. 6) Turva-alueilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle. 7) Turvatoimet on mitoitettu riittävälle tasolle siten, että ne vastaavat riskienarvioinnissa todettuja riskejä.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojaustavoitteena on luvattoman pääsyn estäminen pilvipalveluntarjoajan konesaliin, salassa pidettäviin tietoihin sekä varkauksien, vahinkojen, menetysten, taloudellisten tappioiden ja häiriöiden ennalta estäminen sekä vaikutusten minimointi.
Lisätietoja	Monitasoisella suojaamisella tarkoitetaan sitä, että toteutetaan joukko toisiaan täydentäviä turvatoimia. Mikäli mahdollista, tilat muodostavat keskenään sisäkkäisiä vyöhykkeitä, joissa korkeamman suojaustarpeen tilat ovat sisimpänä. Turvatoimet suunnitellaan kokonaisuutena, jossa otetaan huomioon salassa pidettävän tiedon suojaustaso, määrä, rakennusten ympäristö ja rakenne. Pilvipalveluntarjoajalla tulee olla käytössään riskienhallintaprosessi (vrt. TJ-03). Arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältävien tilojen tai rakennusten riskejä arvioidaan säännöllisesti (väh. 1 krt / vuosi) pilvipalveluntarjoajan toimesta. Riskeillä on nimetyt omistajat, arvioinnista vastaavat vastuuhenkilöt ja määritellyistä hallintatoimista vastaavat henkilöt. Riskienarviointi dokumentoidaan. Vaatimusten täyttämisessä voidaan hyödyntää seuraavaa menettelyä: Rakennus suunnitellaan niin, että sen ulkoseinät ja kuori muodostavat ensimmäisen turvallisuustason. Kulku rakennuksen sisään valvotaan ja hallitaan esimerkiksi kulunvalvontajärjestelmällä ja lukituksilla. Korkeamman suojaustarpeen tietoa käsitellään rakennuksen sisemmissä osissa siten, että tunkeutuminen tiloihin on vaikeaa ja hidasta. Turvallisuustekniset ratkaisut täydentävät rakenteellisia ratkaisuja. Suunnittelussa otetaan huomioon ikkunat, ovet ja muut aukot.

FT-02	Rakenteet ja turvallisuusjärjestelmät
Vaatimus	1) Arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältävien tilojen tai rakennusten ulkorajat suojataan fyysisesti kestävällä tavalla sekä nykyaikaisilla ja asianmukaisilla turvatoimilla.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojaustavoitteena on luvattoman pääsyn estäminen pilvipalveluntarjoajan konesaliin, salassa pidettäviin tietoihin sekä varkauksien, vahinkojen, menetysten, taloudellisten tappioiden ja häiriöiden ennalta estäminen sekä vaikutusten minimointi.
Lisätietoja	Aluetta rajaavan aidan tai ulkokuoren seinä-, katto-, lattia-, ikkuna-, ovi- tai talotekniikan aukkojen rakenteilta ei vaadita erityisiä ominaisuuksia. Käyttötarkoitusten mukaiset rakenteet soveltuvat. Turvallisuustekniikan tulee tukea tilan ja rakennuksen kokonaisturvallisuutta. Mahdollisia turvatoimia voisivat olla esimerkiksi sijoittuminen riittävälle etäisyydelle ulkopuolisista toimijoista, aidat, vartiointi tai tekniset valvontajärjestelmät (mm. kulunvalvonta-, rikosilmoitin-, kameravalvontajärjestelmät). Järjestelmät tulee huoltaa säännöllisesti valmistajan suositusten mukaan ja varmistua niiden käyttökunnosta. Turvallisuusjärjestelmiä ja -laitteita tulee testata (väh. 1 krt / kk) ja pitää käyttökuntoisina säännöllisesti. Testaukset tulee dokumentoida. **Vaatimusten täyttämisessä (TL IV) voidaan hyödyntää seuraavaa tai vastaavaa menettelyä:** • Rakennuksen seinät ovat rakenteeltaan: teräsbetoni (50mm), lämmöneriste mineraalivilla (80mm), teräsbetoni (60mm). Tietoja säilyttävän konesalin seinärakenteet ovat rakenteeltaan: palolevy (12mm), kipsilevy + villa + kipsilevy (70mm). • Rakennus on kokonaisuudessaan kulunvalvonta- ja rikosilmoitinjärjestelmällä suojattu. Konesaliin johtavilla reiteillä on myös kameravalvonta. Järjestelmiä hallitaan ja valvotaan ulkoisen vartiointiliikkeen toimesta, jonka kanssa organisaatiolla on turvallisuussopimus. Järjestelmien huoltaminen, ylläpito, testaaminen ja dokumentointi ovat vastuutettu organisaation turvallisuudesta vastaavalle henkilölle. Järjestelmien toimivuus testataan kerran kuukaudessa. **Vaatimusten täyttämisessä (TL III kasautumisvaikutus) voidaan hyödyntää seuraavaa tai vastaavaa menettelyä:** **Konesalin tai rakennuksen seinät, lattia ja katto:** • Rakenteiden on oltava lujuudeltaan ja rakennustavaltaan sellaisia, että tilaan tunkeutuminen ei ole mahdollista ilman työkaluilla tapahtuvaa rakenteiden rikkomista. • Rakenteet tai niiden osat eivät saa olla ulkopuolelta rikkomatta irrotettavissa. Luokan 3 murronsuojaseinä täyttää edellä olevat vaatimukset. Väliseinärakenteen tulee ulottua lattiasta kattoon. • Kevyet rakenteet on vahvistettava. • Seinärakenteet voivat olla esimerkiksi: - 1x12mm kipsilevy + 1,5mm teräslevy + 12mm vaneri + runko + 12mm vaneri + 1,5mm teräslevy + 1x12mm kipsilevy. - Teräsbetoni; ≥ 80 mm. - Poltettu tiili; ≥ 85 mm+2x1,5mm teräslevy sisäpuolella tai 1,5mm teräslevy ulkopuolella ja 1,5mm teräslevy sisäpuolella. - Harkko; ≥ 70 mm+2x1,5 mm teräslevy sisäpuolella, vaihtoehtoisesti 1,5mm teräslevy ulkopuolella ja 1,5mm teräslevy sisäpuolella. Teräslevyjen päällä kipsilevy. • Lattiarakenteet voivat olla esimerkiksi: - Ontelolaatta, yli 320 mm. - Betoni ≥ 80 mm. - Muut lattiarakenteet; teräslevyvahvistus ≥3 mm. • Kattorakenteet voivat olla esimerkiksi: - Ontelolaatta. - Betoni ≥80 mm. - Muut kattorakenteet; teräslevyvahvistus ≥3 mm. Lasirakenteissa, kuten lasi- ja siirtolasiseinissä on oltava standardin SFS-EN 356 P6B mukainen suojalasitus tai ne on suojattava riittävän vahvuisella rullakalterilla tai teräsristikolla.

FT-02	Rakenteet ja turvallisuusjärjestelmät
Lisätietoja	**Ikkunat ja aukot** Ikkunoiden lasiruudut on kiinnitettävä ja ikkunat suljettava siten, ettei niitä voi ulkopuolelta rikkomatta irrottaa tai avata. Ikkunoiden ja kattoikkunoiden oltava standardin SFS-EN 356 P6B mukaista suojalasitusta tai ne on suojattava kiinteällä/lukitulla rullakalterilla, teräsristikolla tai -verkolla tai aukkojen suojauslevyllä. Muut aukot, kuten savunpoisto- ja ilmanottoaukot, on suojattava kiinteällä tai lukitulla teräsristikolla. Suojausvaatimus ei koske ikkunaa tai aukkoa, joka on vähintään 4 m:n korkeudella maan pinnasta tai muusta seisomatasosta. Suojattaessa ikkunoita ja lasisiirtoseiniä muulla kuin murronsuojalasilla on käytettävän suojarakenteen aukkokoko valittava suojattavien laitteiden koon mukaan siten, ettei esineiden kuljettaminen suojarakenteen läpi ole mahdollista sitä rikkomatta. **Ovet, saranat ja karmit:** Oven rakenteen on oltava lujuudeltaan seinärakennetta vastaava. Ovirakenteen on oltava seuraavanlainen: • Karmi on kiilattava rakenteisiin lukkojen ja saranoiden kohdalta. • Karmiin saranapuolelle on kiinnitettävä saranoiden kohdalle murtosuojatapit. • Käyntiväli lukkosivulla ei saa olla suurempi kuin 5 mm. • Huultamattoman oven käyttölukko on suojattava rakoraudalla. • Oven lasi on kiinnitettävä siten, ettei sitä voi ulkopuolelta rikkomatta irrottaa. Ovien lasit on oltava P6B murronsuojalasia tai ne on suojattava rullakalterilla, teräsristikolla tai -verkolla. Ovi, joka on testattu standardin SFS-EN 1627 mukaan luokkaan 3 täyttää edellä olevat vaatimukset. **Lukitus:** • Kiinteästi oveen asennettavalla käyttölukolla vastalevyineen, joka on standardin SFS 7020 mukaan luokiteltu joko luokkaan 1 tai 2. • Kiinteästi oveen asennettavalla varmuuslukolla vastalevyineen, joka on standardin SFS 7020 mukaan luokiteltu luokkaan 3 tai 4. **Turvallisuusjärjestelmät:** Turvallisuusjärjestelmien laitetila tulee sijoittaa turvallisuusaluetta vastaavalle alueelle. Laitetilan kulkuoikeudet määritellään työperusteisen tarpeen mukaisesti. Turvallisuusjärjestelmät tulee olla säännöllisen huollon, päivitysten ja testauksen piirissä, jolla varmistetaan järjestelmien toimintakunto ja tietoturvallisuus. Turvallisuusjärjestelmien etäyhteydet ja kenttälaitteiden asennus tulee toteuttaa riskienarvioinnin pohjalta riittävän tietoturvallisesti siten, että turvallisuusjärjestelmiin on vain valtuutetuista päätelaitteista/verkoista mahdollista päästä käsiksi ja että liikenneyhteys ja turvallisuusjärjestelmän rajapinnat on suojattu siten, että ulkopuolisilla ei ole pääsyä välitettyihin tietoihin. Korotettua rakenteellista murtoturvallisuutta ei kuitenkaan edellytetä, mikäli tilat ovat jatkuvasti miehitetty turvallisuushenkilöstön toimesta. Lisäksi turvallisuushenkilöstöllä on oltava riittävä valvontakyky, jotta poliisi tai turvallisuushenkilöstö saa indikaation tunkeutumisesta siinä määrin ajoissa, ettei tunkeutuja ehdi saada haltuunsa suojattavaa tietoa. Valvontakyky voidaan toteuttaa tarkastuskierrosten sekä turvajärjestelmien reaaliaikaisen valvonnan tai niiden yhdistelmien avulla. **Rikosilmoitinjärjestelmä ja hälytyksensiirto:** Suojattavan tilan ovet, aukot, ikkunat ovat valvottava rikosilmoitinjärjestelmän avulla. Rikosilmoitinjärjestelmän keskuslaitteet ja ilmaisimet tulee olla hyväksytty vähintään Finanssialan (FA):n luokkaan 3. Ilmoituksensiirto tulee toteuttaa valvottuna tai kahdennettuna yhteytenä. Ilmoituksensiirtolaitteen avulla tulee siirtää vartioimisliikkeelle tai muuhun turvallisuusvalvomoon vähintään seuraavat tiedot: murto, päälle/pois, sabotaasi, vika. Järjestelmää tulee operoida henkilökohtaisen koodin avulla (vähintään 4-merkkinen). Radioteitse toimivina ilmaisimina hyväksytään vain henkilökohtaiset hätäpainikkeet. Tilat tulee olla valvottuina, kun tiloissa ei oleskella. **Kulunvalvontajärjestelmä:** Turva-alueen rajalla on käytettävä sähköistä kulunvalvontaa sisään ja ulos mentäessä. Sisään mentäessä käytettävä kaksoistunnistusta (esimerkiksi pääsykoodi ja sähköinen tunniste). Kulunvalvontatunnisteiden tulee käyttää nykyaikaista ja salattua lukutekniikkaa tai organisaation tulee järjestää tunnisteidenhallinta organisaation turvallisuusohjeiden mukaisesti (TL III + TL IV). **Kameravalvontajärjestelmä:** Turvallisuusalueita, kulkureittejä ja sitä ympäröivää aluetta valvotaan tallentavalla kameravalvonnalla. Kameravalvonta ja tallenteiden säilytysaika toteutettava organisaation riskienarvioinnin perusteella.

FT-03	Luvattoman pääsyn estäminen
Vaatimus	1) Kulkua arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältäviin tiloihin tai rakennuksiin suojataan ja valvotaan sähköisen kulunvalvonta-järjestelmän avulla ja/tai mekaanisilla/sähkömekaanisilla avaimilla luvattoman pääsyn estämiseksi. 2) Kulkuoikeuksien hallinta on järjestetty siten, että luvaton pääsy salassa pidettävään tietoon on estetty. Pääsy salassa pidettäviä tietoja sisältäviin tiloihin sallitaan ainoastaan työtehtävistä johtuvan tiedonsaantitarpeen perusteella.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa käsiteltävään salassa pidettävään tietoon, sitä käsitteleviin laitteistoihin, tai edellä mainittujen turvallisuudesta huolehtiviin järjestelmiin on pääsy vain valtuutetuilla henkilöillä.
Lisätietoja	Vaatimusten täyttämisessä voidaan hyödyntää seuraavaa menettelyä: a) Organisaatiossa on käytössä kuvalliset henkilökortit tai vastaavat näkyvät tunnisteet, ja ne ovat esillä tiloissa kuljettaessa. b) Myönnetyistä kulkuoikeuksista ja käytetyistä mekaanisista avaimista on laadittu dokumentti tai loki, joita ylläpitää organisaation nimetty vastuuhenkilö. Kulkuoikeuksien ja mekaanisten avainten myöntämis-, katoamis- ja poistamisprosessi on kuvattu kirjallisesti. Kulkuoikeuksia ja avaimia tarkastellaan säännöllisesti ja tarpeen mukaan (väh. 6kk välein tai työntekijän työsuhteen alkaessa, loppuessa tai henkilön vaihtaessa työtehtävää). c) Avainten hallintaan nimetyllä vastuuhenkilöllä on hallussaan lukostokaavio ja avainkortti. d) Kulunvalvontajärjestelmässä on käytössä kahteen tekijään perustuva tunnistautuminen (esimerkiksi tunniste + PIN-koodi). Kulkuoikeudet ja mekaaniset avaimet on yksilöity käyttäjäkohtaisesti. Mikäli käytössä on yhteiskäyttötunnuksia, on toteutettu korvaava menettely henkilön luotettavaan yksilöintiin. e) Mekaaniset avaimet ovat kopiosuojattua sarjaa. Konesalin mekaaniset avaimet ovat eri sarjassa kuin rakennuksen muut avaimet. Vara-avaimien tai kulkutunnisteen säilytys (esim. hätätilanteita varten) on järjestetty sinetöitynä lukitussa paikassa. Kuittaus avaimen tai kulkutunnisteen noudosta pystytään todentamaan jälkikäteen. f) Avaimia on säilytettävä turvallisesti, eikä niitä saa merkitä siten, että ne voi yhdistää kohteeseen. Ulkoseinään upotetuissa avainsäilöissä voidaan säilyttää vain erillisiä huoltotilojen avaimia tai reittiavainta kiinteistöön.

FT-04	Palveluntuottajat ja vierailijat
Vaatimus	1) Vierailijat tunnistetaan, varustetaan vierailijakortilla ja kirjataan. Organisaatiolla on dokumentoitu vierailijapolitiikka. Vierailijoiden suhteen sovelletaan aina isäntäperiaatetta. 2) Siivous-, huolto- ja muu palveluntuottajien henkilöstö tunnistetaan, varustetaan vierailija-korteilla ja kirjataan. Säännölliset palveluntuottajat varustetaan kuvallisella henkilökortilla. 3) Alueella itsenäisesti liikkuvat tai suojattaviin kohteisiin käsiksi pääsevät palveluntuottajat on turvallisuusselvitetty. Henkilöt, joita ei pystytä tai ei ole vielä turvallisuusselvitetty liikkuvat saatettuna. Vrt. HT-02. 4) Huoltoihin, päivityksiin ja ylläpitoon liittyvät käytännöt on kirjallisesti kuvattu ja dokumentoitu.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa olevaan salassa pidettävään tietoon, sitä käsitteleviin laitteistoihin, tai edellä mainittujen turvallisuudesta huolehtiviin järjestelmiin on pääsy vain valtuutetuilla, luotettavaksi arvioiduilla henkilöillä.
Lisätietoja	Käytäntöjen ja ohjeiden tulisi ottaa huomioon vähintään seuraavat: a) Tietojen eheyden turvaaminen koko elinkaaren ajan, b) salassa pidettävien tietojen turvallinen poistaminen ennen ulkopuolisten tekemää korjausta tai huoltoa, c) salassa pidettävän tiedon säilytystilan tai sitä rajaavan tilan murtohälytysjärjestelmän, kulunvalvontajärjestelmään ja muihin valvontajärjestelmiin liittyvien laitetilojen ja niiden laitteistojen huolto-, asennus- ja siivoustoimet tapahtuvat vain niiden henkilöiden toimesta, joilla on erityinen lupa ja turvallisuusselvitys alueelle, tai organisaatioon kuuluvan henkilökunnan valvonnassa, d) vastaavien palveluntuottajien kanssa on tehty sopimukset (esim. polttoaine varavoimakoneita varten), e) organisaatiolla on voimassaolevat turvallisuussopimukset vartiointiliikkeen (turvallisuuspalvelut) ja kiinteistöpalveluita (ilma, vesi, sähkö, polttoaine, siivous) tuottavan yrityksen kanssa, f) hälytysten vasteaika on sellainen, että kiinnijäämisriski on merkittävä, g) organisaatiolla on henkilöstölle kirjallisesti kuvattu huoltotoimenpiteiden aikaiset ja muiden katkosten ennakoivat toimenpiteet, h) turvallisuusjärjestelmien asennus- ja huoltotoimenpiteet suoritetaan nimetyn yrityksen toimesta, minkä henkilöt ovat turvallisuusselvitetty, i) siivous suoritetaan kerran kuukaudessa tai tarvittaessa. Siivoojat ovat turvallisuusselvitetty. Siivoojat on varustettu kuvallisella henkilökortilla.

FT-05	Varautuminen ja jatkuvuudenhallinta
Vaatimus	1) Salassa pidettäviä tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältäviä tiloja tai rakennuksia suojataan tulipalolta, vesivahingolta, räjähdyksiltä, levottomuuksilta ja muilta luonnon ja ihmisten aiheuttamilta uhilta rakenteellisilla, teknisillä ja organisatorisilla turvatoimilla. 2) Keskeisen infrastuktuurin suojauksessa toteutetaan ainakin seuraavat turvatoimet: a) Rakenteelliset turvatoimet: Rakenteellinen palosuojaus (seinä-, lattia-, katto- ja ovi/ikkuna-rakenteiden palonkestävyys sekä läpivientien tiivistäminen paloluokkaa vastaavilla tuotteilla). b) Tekniset turvatoimet: i. Tila tai rakennus on kytketty automaattiseen paloilmoitinjärjestelmään, jonka hälytys välittyy hätäkeskukseen. ii. Suojattava tila on varustettu muusta kiinteistöstä erillisellä ilmanvaihtojärjestelmällä ja automaattisilla palonrajoittimilla (esim. automaattiset savupellit). iii. Tilaan on asennettu suojattavasta tiedosta riippuen riittävät olosuhde-, lämpötila- ja kosteusanturit (verkkovirran- tai paineenvaihtelut, kuumuus/kylmyys, vesivuodot). iv. Käytössä on automaattiset sammutusjärjestelmät, jotka havaitsevat esim. tulipalon aikaisessa vaiheessa ja aloittavat alkusammutuksen. v. Sähkön häiriötön saanti on varmistettu sähkönsyötön turvaavilla laitteilla (UPS, varavoima). vi. Tietoliikenteen varmistukset, ja jäähdytysjärjestelmän kahdennus. c) Organisatoriset turvatoimet: i. Pelastussuunnitelman laatiminen. ii. Nimetty vastuuhenkilö tai taho, kenelle tieto hälytyksistä välittyy. iii. Säännölliset pelastusharjoitukset ja paloturvallisuustarkastukset paloturvallisuus-määräysten noudattamisen toteamiseksi. iv. Jatkuvuussuunnittelu.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelun konesalien (ja vastaavien) toiminnan jatkuvuus on suojattu yleisiä riskejä vastaan. Soveltuviin jatkuvuutta tukeviin turvatoimiin sisältyy tyypillisesti seuraavat:
Lisätietoja	**Soveltuviin jatkuvuutta tukeviin turvatoimiin sisältyy tyypillisesti seuraavat:** **Rakenteellinen suojaus:** - Palo-osastointi, palon tai vuodon mahdolliseksi rajaamiseksi - Palonkestävien materiaalien käyttö, esim. 60 tai 90 min - Palokatkotuotteet, joilla estetään savu- ja palokaasujen kulkeutuminen muihin tiloihin **Tekninen suojaus:** - Laitteiden säännöllisen toimivuuden testaaminen ja dokumentointi - Prosessien toimivuus ja tiedon välittyminen oikeille tahoille tai henkilöille - Varakaapeloinnit ja yhteydet, järjestelmien kahdennukset, varmuuskopioiden sykli ja laajuus - Jatkuvuussuunnittelun häiriöt a) toimitilojen b) järjestelmien c) henkilöstön täysimääräisessä saatavuudessa **Organisatorinen suojaus:** - Pelastussuunnitelmalla ja jatkuvuudenhallinnalla on tarkoitus kuvata toimenpiteet, joilla ennalta ehkäistään, minimoidaan, rajoitetaan ja palaudutaan toimintahäiriöistä, onnettomuuksista, vahingoista ja poikkeuksellisista tapahtumista. - Suunnitelmien päivittäminen tulisi olla vähintään vuosittaista Kriittiset palvelimet ja laitteet tulee tunnistaa ja varmentaa toimintavaatimusten mukaisesti. Vrt. TJ-05 (Jatkuvuudenhallinta) ja KT-03 (Varmistus- ja palautusprosessit). Mikäli järjestelmän toimintavaatimukset ovat korkeat, on järjestelmien saatavuus varmennettava murtoa, ilkivaltaa, paloa, lämpöä, kaasuja, pölyä, tärinää, vettä ja sähkönkäytön katkoksia vastaan. Kriittisiä palvelin- ja laitetiloja ohjaavan LVI-automaationhallinnan etäkäyttö on estetty. Kriittisten palvelin- ja laitetilojen olosuhdesensoreja suojataan ja valvotaan. Pilvipalvelutoteutuksen keskeinen infrastruktuuri tulisi olla vähintään kahdessa erillisessä paikassa.

Osa-alue 5: Tietoliikenneturvallisuus

TT-01	Tietoliikenneverkon rakenne
Vaatimus	1) Pilvipalveluympäristö on erotettu muista ympäristöistä. 2) Pilvipalveluympäristö on ulkoreunan sisäpuolella jaettu erillisiin alueisiin (vyöhykkeet, segmentit, mikrosegmentit tai vastaavat). 3) Liikennöintiä rajoitetaan ja valvotaan siten, että vain erikseen hyväksytty, toiminnalle välttämätön liikennöinti sallitaan (default-deny) pilvipalveluympäristön ulkoreunalla ja sisäisten alueiden välillä.
Soveltuvuus	Verkkopalomuurit (tai vastaavat verkkolaitteet, esimerkiksi reitittimet), työasemien ja palvelinten ohjelmistopalomuurit, muut pilvipalveluympäristöön (ml. hallinta) kuuluvat järjestelmät.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Palvelun tuottamiseen liittyvän ympäristön liikenteen rajoittamisella vain välttämättömiin yhteyksiin tavoitellaan turvattomista verkoista tulevien hyökkäysten riskien pienentämistä sekä suojattavan ympäristön rajaamista hallittavaan kokonaisuuteen. Sisäisten alueiden välisellä suodatuksella tavoitellaan mahdollisten tietoturvapoikkeamien (ml. tietomurrot) tai niiden yritysten vahinkojen rajaamista sekä poikkeamien havainnointikykyä.
Lisätietoja	Tietojenkäsittely-ympäristöjen erottelu on eräs vaikuttavimmista tekijöistä salassa pidettävän tiedon suojaamisessa. Erottelun tavoitteena on rajata salassa pidettävän tiedon käsittely-ympäristö hallittavaksi kokonaisuudeksi, ja erityisesti pystyä rajaamaan salassa pidettävän tiedon käsittely vain riittävän turvallisiin ympäristöihin. Tietojenkäsittely-ympäristön ulkoreunan erotteluun tulee käyttää oikein konfiguroitua palomuuria tai vastaavaa verkkolaitetta. Myös erotteluun käytettävä palomuuri (tai vastaava verkkolaite) tulee suojata luvattomalta pääsyltä. Suojauksia voidaan täydentää ja tukea myös niin sanotulla Zero Trust -lähestymistavalla, jossa eri toimijoiden toimintamahdollisuuksia voidaan rajoittaa ja valvoa erityisesti toimijoiden ja toiminteiden tunnistamiseen ja todentamiseen pohjautuen. Kytkentöjen ja konfiguraatioiden turvallisesta toiminnasta tulee varmistua säännöllisesti, vrt. MH-01 (Muutostenhallinta). Saatavuuden ja riittävän dokumentoinnin varmistamisen kannalta tarkoituksenmukainen ratkaisu on usein palomuurisääntöjen sekä palomuurien konfiguraatioiden varmuuskopiointi, ja varmuuskopioiden säilytys riittävän suojatusti. Vaatimuksen tulkinnassa tulee huomioida vastuunjako pilvipalvelutarjoajan ja asiakkaan välillä. Mikäli arvioinnin tavoitteena on saada kattava kuva salassa pidettävän tiedon suojaamisen riittävyydestä, arvioinnin tulisi lähtökohtaisesti kattaa sekä pilvipalveluntarjoajan että asiakkaan vastuulla olevat osiot koko tiedon elinkaaren ajalta. Arvioinnissa tulee huomioida esimerkiksi se, että IaaS-mallissa pilvipalveluntarjoaja ei tyypillisesti pysty ottamaan kantaa asiakkaan vastuulla olevien ohjelmistopalomuurien konfiguraation turvallisuuteen. Toisaalta, asiakas ei tyypillisesti pysty vaikuttamaan pilvipalveluntarjoajan tuottaman IaaS-infrastruktuurialustan suojauksiin. Mikäli asiakas on toteuttanut ohjelmistopalomuurauksen käyttäen pilvipalveluntarjoajan tarjoamaa ohjelmistokomponenttia, asiakas pystyy tyypillisesti vaikuttamaan palomuuraukseen vain tekemänsä konfigurointinsa turvallisuuden osalta. Tässä käyttötapauksessa suositellaankin varmistamaan, että pilvipalveluntarjoaja vastaa tuottamiensa ohjelmistokomponenttien turvallisuudesta myös tilanteissa, joissa kyseisissä ohjelmistokomponenteissa ilmenee asiakkaan salassa pidettävien tietojen suojaamiseen vaikuttavia turvallisuuspuutteita. Tällaisissa tilanteissa suositellaan huomioitavan vastuut myös turvallisuuspuutteiden korjaamisen ja vahingonkorvausten osalta. Tilanteissa, joissa infrastruktuurin tai esimerkiksi liikennesuodatuksen turvallisuus nojaa ohjelmistokoodiin, tulee erityisesti ohjelmistokoodin pääsyn- ja versionhallintaan kiinnittää erityistä huomiota. Vrt. MH-01 (Muutostenhallinta), MH-02 (Järjestelmäkehitys) ja IP-03 (Hallintayhteydet). Toisaalta ohjelmistokoodiin nojautuva toteutus voi tietyin rajauksin mahdollistaa ympäristön kuvauksen ja sen turvallisuuden arvioinnin versionhallinnan tukemana. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakkaan osuutta. Vaatimukset soveltuvat yleensä suoraan esimerkiksi tilanteisiin, joissa IaaS-palvelumallilla tarjottuun pilvipalvelualustaan on toteutettu asiakkaan vastuulla oleva asiakasjärjestelmä.

TT-02	Yleisiä verkkohyökkäyksiä vastaan suojautuminen
Vaatimus	1) Organisaatio ylläpitää riskienarviointia, joka kattaa yleisiltä verkkohyökkäyksiltä suojautumisen. 2) Suojaukset on mitoitettu siten, että yleiset verkkohyökkäykset eivät vaaranna palvelun tai siinä käsiteltävien tietojen luottamuksellisuutta, eheyttä tai saatavuutta.
Soveltuvuus	Palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa käsiteltävien tietojen käyttö ei esty, tai niiden luottamuksellisuus tai eheys ei vaarannu yleisten verkkohyökkäysten seurauksena.
Lisätietoja	Kaikkia liitettyjä tietotekniikkajärjestelmiä tulisi lähtökohtaisesti käsitellä epäluotettavina ja varautua yleisiin verkkohyökkäyksiin. Yleisiin verkkohyökkäyksiin varautumiseen sisältyy esimerkiksi vain tarpeellisten toiminnallisuuksien pitäminen päällä. Toisin sanoen jokaiselle päällä olevalle toiminnallisuudelle tulisi olla perusteltu toiminnallinen tarve. Toiminnallisuus tulisi rajata suppeimpaan toiminnalliset vaatimukset täyttävään osajoukkoon (esimerkiksi toiminnallisuuksien näkyvyyden rajaus). Lisäksi tulisi ottaa huomioon esimerkiksi osoitteiden väärentämisen (spoofing) estäminen ja verkkojen näkyvyyden rajaaminen. Erityisesti Internet-rajapinnoissa myös (hajautettujen) palvelunestohyökkäysten riskiä vastaan tulee suojautua. Toisaalta joissain sisäisissä rajapinnoissa palvelunestohyökkäysten riski voi olla hyväksyttävissä ilman erillissuojauksiakin. Vaatimuksen tulkinnassa tulee huomioida vastuunjako pilvipalvelutarjoajan ja asiakkaan välillä. Esimerkiksi IaaS-mallissa pilvipalveluntarjoaja ei tyypillisesti pysty ottamaan kantaa muun muassa asiakasjärjestelmän ohjelmistokerroksen vikasietoisuuteen tai esimerkiksi asiakkaan vastuulla olevien ohjelmistopalomuurien konfiguraation turvallisuuteen. Toisaalta taas esimerkiksi SaaS-mallissa pilvipalveluntarjoajalla on usein merkittävät vastuut muun muassa palvelunestohyökkäysriskin hallinnoinnissa.

Osa-alue 6: Identiteetin ja pääsyn hallinta

IP-01	Käyttöoikeushallinta
Vaatimus	1) Käyttöoikeuksien hallinnointi toteuttaa vähimpien oikeuksien periaatetta: a) Käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon on ennalta määritelty prosessi. b) Tietojenkäsittely-ympäristön käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä. c) Järjestelmän käyttäjistä ylläpidetään listaa. Jokaisesta myönnetystä käyttöoikeudesta jää merkintä. d) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. e) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. f) Käyttö- ja pääsyoikeudet pidetään ajan tasalla. Tarpeettomat käyttäjätilit ja oikeudet poistetaan, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan). g) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. h) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti, vähintään puolivuosittain.
Soveltuvuus	Verkkolaitteet, palvelimet, tietojärjestelmät sekä työasemat ja muut päätelaitteet.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Käyttöoikeuksien hallinnointi toteuttaa vähimpien oikeuksien periaatetta: Käyttäjätunnukset on myönnetty ja luovutettu vain niille, joilla on niihin oikeus ja tehtävään/rooliin liittyvä tarve. Käyttöoikeudet on rajattu vain välttämättömiin toiminnallisuuksiin, sovelluksiin, laitteisiin ja verkkoihin.
Lisätietoja	Käyttöoikeuksien hallinnan keskeinen tavoite on pystyä varmistumaan siitä, että vain oikeutetuilla käyttäjillä on pääsy tietojenkäsittely-ympäristöön ja sen sisältämään suojattavaan tietoon. Käyttöoikeuksien taustalla on suositeltavaa olla jokin sopimus tai muu dokumentoitu peruste, joka voidaan todentaa (esim. työsuhde, sopimus toteutettavasta työstä ympäristössä). Kaikkien käyttäjätunnusten osalta on huolehdittava tunnusten elinkaaresta siten, että vain tarpeelliset tunnukset ovat voimassa ja aktiivisia ja tarpeettomat käyttäjätunnukset poistetaan välittömästi. Käyttöoikeudet tulee rajata vain toiminnallisen tarpeen edellyttämään osajoukkoon. Tarpeettoman laajat oikeudet mahdollistavat ko. käyttäjälle, prosessille tai edellä mainitut haltuun saavalle hyökkääjälle tarpeettoman laajat toimintamahdolliset. Käyttöoikeuksien rajaamisella vähimpien oikeuksien periaatteen mukaiseksi voidaan pienentää sekä tahallisten että tahattomien tekojen, kuin myös esimerkiksi haittaohjelmista aiheutuvia riskejä. Erityisesti tulee huomioida, että ylläpito-oikeuksia käytetään vain ylläpitotoimiin. Ylläpitotunnuksella varustettua käyttäjätiliä ei tule käyttää esimerkiksi web-selailuun tai sähköpostin käyttöön. Pääsyoikeuksien ajantasaisuudesta varmistuminen edellyttää yleensä sitä, että kaikkien työntekijöiden, toimittajien ja ulkopuolisten käyttäjien pääsy- ja käyttöoikeudet katselmoidaan säännöllisin väliajoin, esimerkiksi kuuden kuukauden välein. Tehtävänkuvan muutoksissa ja erityisesti työsuhteen päättymisen yhteydessä oikeuksien muuttamiseen ja poistamiseen on oltava selkeä, sovittu menettely. Tämä voi tapahtua esimerkiksi siten, että esimies ilmoittaa muutoksista etukäteen vastuuhenkilöille, jolloin kaikki oikeudet saadaan pidettyä ajantasaisina. Tämä voi edelleen tarkoittaa sitä, että käyttö- ja pääsyoikeudet poistetaan/muutetaan keskitetystä hallintajärjestelmästä tai yksittäisistä järjestelmistä erikseen. Vaatimuksen soveltamisessa tulee huomioida vastuujako pilvipalveluntarjoajan ja asiakkaan välillä. Tyypillisesti pilvipalveluntarjoaja on vastuussa pilvipalvelun tuottamiseen liittyvän järjestelmäkokonaisuuden käyttöoikeushallinnasta, asiakkaan vastuun koskiessa palveluntarjoajan palvelukokonaisuuden (IaaS, PaaS tai SaaS) päälle rakentuvan osuuden käyttöoikeushallintaa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaankin huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

IP-02	Käyttäjätunnistus
Vaatimus	1) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjät sekä palvelun käyttäjät tunnistetaan ja todennetaan luotettavasti ennen pääsyä suojattavaan tietoon: a) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet. b) Kaikki käyttäjät tunnistetaan ja todennetaan. c) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti. d) Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin. e) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille. f) Käyttäjien todennus tehdään vahvasti, vähintään kahteen tekijään nojautuen (esimerkiksi salasana + token). Yhteys on salattu käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. i. Poikkeuksena tilanne, jossa todennus tehdään fyysisesti suojatun turvallisuusalueen (Vrt. FT-01) sisällä vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, 1. käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, 2. käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 2) Tilanteissa, joissa yhteys kulkee fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan konesalin ja ylläpidon/asiakkaan päätelaitteen välillä), tieto/tietoliikenne on suojattu viranomaisen hyväksymällä salausratkaisulla. 3) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjien päätelaitteet ja järjestelmät tunnistetaan riittävän luotettavasti ennen pääsyä suojattavaan tietoon.
Soveltuvuus	Verkkolaitteet, palvelimet, tietojärjestelmät sekä työasemat ja muut päätelaitteet.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 2-3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Tietoihin ja palveluihin pääsyn rajaaminen vain valtuutettuihin käyttäjiin.
Lisätietoja	Tunnistamisen ja todentamisen luotettavaan järjestämiseen kuuluu huolehtiminen siitä, että 1) todennusmenetelmä on suojattu välimieshyökkäyksiltä (man-in-the-middle), 2) sisäänkirjautuessa, ennen todennusta, ei paljasteta mitään tarpeetonta tietoa, 3) todennuksessa käytettävät tunnistamistiedot (todennuskredentiaalit) ovat aina salatussa muodossa, jos ne lähetetään verkon yli, 4) todennusmenetelmä on suojattu uudelleenlähetyshyökkäyksiä vastaan, ja 5) todennusmenetelmä on suojattu brute force -hyökkäyksiä vastaan. Tilanteissa, joissa pilvipalveluun tunnistautumisessa hyödynnetään federoitua identiteetinhallintaa, tai/ja identiteetin- ja pääsynhallintajärjestelmiä (organisaation omia tai esimerkiksi pilvipalveluntarjoajan tuottamia), tulee arvioinnissa kiinnittää erityistä huomiota tunnistuspalvelun (Identity Provider, IdP) sekä attribuuttien välitysketjun luotettavuuteen. Salassa pidettävän tiedon käsittelyyn soveltuvat vain sellaiset tunnistuspalvelut, jotka tarjoavat vahvaan ensitunnistamiseen perustuvaa identiteettiä ja joiden attribuuttien välitysketju pystytään toteuttamaan riittävän turvallisesti tunnistukseen nojaavaan palveluun (Relying Party, RP tai Service Provider, SP) asti. Koska salassa pidettävän tiedon suojaus on yleensä suoraan riippuvainen tunnistuspalvelun luotettavuudesta, tunnistuspalvelun turvallisuudesta varmistuminen kuuluu lähes poikkeuksetta osaksi pilvipalvelun turvallisuuden arviointia. Esimerkiksi attribuuttien välityksen salausteknistä suojausta on tyypillisesti perusteltua arvioida samansuuntaisesti kuin kyseessä olevan tietotyypin suojaamiseen sovellettavan salausratkaisun avainten välitystä (vrt. SA-01, SA-02 ja SA-03). Identiteetinhallintamalleista organisaatiokeskeinen (organization-centric identity management) soveltuu yleensä esimerkiksi käyttäjäkeskeistä (user-centric) paremmin salassa pidettävän tiedon suojaamistarpeisiin, joissa on huomioitava myös käyttäjän sidonta tiettyyn organisaatioon sekä turvallisuustoteutuksen luotettavuudesta varmistuminen. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

IP-03	Hallintayhteydet
Vaatimus	1) Hallintapääsy tapahtuu pilvipalveluympäristössä rajattujen, hallittujen ja valvottujen pisteiden (esimerkiksi hyppykoneet, hallintaportaalit ja vast.) kautta. Hallintapääsyn mahdollistavat pisteet eriytetään toisistaan vähintään siten, että pilvipalveluntarjoajan ja eri asiakkaiden hallintapisteet, sekä niiden kautta saavutettavat palvelut, ovat toisistaan luotettavasti eroteltuna (vrt. JT-03). 2) Hallintapääsy edellyttää vahvaa, vähintään kahteen todennustekijään (esimerkiksi salasana + token) pohjautuvaa käyttäjätunnistusta. 3) Hallintaliikenne on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. 4) Hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (vrt. FT-01) ulkopuolelle viedyt asiakastietoa sisältävät päätelaitteet ja muut tietovälineet (kiintolevyt, USB-muistit ja vastaavat) säilytetään salattuina käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja, tai tietovälineitä ei jätetä valvomatta. Vrt. SA-01 ja FT-01. 5) Viranomaisen turvallisuusluokitellun tiedon hallinta on mahdollista vain kyseisen turvallisuusluokan mukaisilta päätelaitteilta ja ympäristöistä sekä fyysisiltä alueilta (vrt. FT-01). 6) Viranomaisen turvallisuusluokitellun tiedon hallintaan on pääsy vain viranomaisen hyväksymällä menettelyllä salatulla hallintayhteydellä. 7) Turvallisuusluokiteltua tietoa sisältävien päätelaitteiden ja muiden tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) salaus on viranomaisen hyväksymä.
Soveltuvuus	Pilvipalveluympäristön etähallintaan käytettävät järjestelmät, ml. esimerkiksi verkkolaitteet, palvelimet, sekä työasemat ja muut päätelaitteet. Kattaa sekä pilvipalvelualustan, että sen päälle tuotetun asiakasjärjestelmän.
Tietotyypit	1-4: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 5-7: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Hallintayhteydet on suojattu riittävällä tasolla, jotta niitä hyödyntämällä ei ole asiakastietoon tai pilvipalveluun valtuuttamatonta pääsyä.
Lisätietoja	Pilvipalveluympäristöissä etähallinta on yleensä tyypillisin hallintamenettely sekä itse pilvipalvelualustan, että asiakkaan järjestelmien osalta. Etähallinnaksi tulkitaan esimerkiksi pilvipalveluntarjoajan ylläpitotoimet, jotka tapahtuvat fyysisesti suojatun konesaliympäristön ulkopuolelta käsin. Etähallinnaksi tulkitaan myös pilvipalvelun asiakkaan, omalle vastuulleen kuuluvaan järjestelmäosaan kohdistuvat ylläpitotoimet. Hallintayhteyksien suojausten arvioinnissa tulisi huomioida erityisesti se, miltä osin ko. hallintayhteyden kautta pystytään vaarantamaan pilvipalvelussa käsiteltävät tiedot. Useimmat hallintayhteystavat mahdollistavat pääsyn tietoon joko suoraan (esimerkiksi tietokantaylläpito pääsee yleensä tarvittaessa tietokannan sisältöön) tai epäsuoraan (esimerkiksi verkkolaiteylläpito pystyy yleensä muuttamaan tietojärjestelmää suojaavia palomuurisääntöjä). Hallintayhteyksiin tulkitaan kuuluvaksi lähtökohtaisesti kaikki yhteystavat, joilla on mahdollista vaikuttaa salassa pidettävien tietojen suojauksiin. Hallintayhteyksiin kuuluvat tyypillisesti myös pilvipalvelun asiakkaalle tarjottavat web-konsolit/-portaalit ja vastaavat etähallintayhteydet. Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn salassa pidettävään tietoon, tulee hallintayhteys ja siihen käytettävät päätelaitteet rajata lähtökohtaisesti samalle suojaus-/turvatasolle, kuin mitä ko. tietojenkäsittely-ympäristökin. Turvallisuusluokitellun tiedon käsittelyyn käytetyn ympäristön hallinta ei lähtökohtaisesti ole hallintaliikenteen turvallisuuskriittisestä luonteesta johtuen mahdollista heikommin suojatuista ympäristöistä tai päätelaitteista käsin. Turvallisuusluokiteltua tietoa sisältävän pilvipalvelualustan hallinnointi tuleekin rajata kyseisen turvallisuusluokan vaatimukset täyttäviin päätelaitteisiin. Huomioitava, että myös päätelaitteiden hallinnointiratkaisujen ja muiden niihin kytkeytyvien taustajärjestelmien tulee täyttää kyseisen turvallisuusluokan vaatimukset, kuten myös fyysiset tilat/alueet, joista hallintaa suoritaan. Päätelaitteiden ja niihin kytkeytyvien taustajärjestelmien (esimerkiksi hakemisto- ja hallintapalvelut) suojaamisessa tulee huomioida erityisesti TT-01 (Tietoliikenneverkon rakenne), IP-01 (Käyttöoikeushallinta), IP-02 (Käyttäjätunnistus), IP-03 (Hallintayhteydet), JT-01 (Jäljitettävyys ja havainnointikyky), JT-02 (Järjestelmäkovennus), JT-04 (Haittaohjelmasuojaus), JT-05 (Suojattavien kohteiden siirtäminen ja poistaminen), SA-01 (Salauskäytännöt ja avainhallinta), SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella), KT-04 (Haavoittuvuuksien hallinta) ja MH-01 (Muutostenhallinta) ja SI-02 (Tietoaineistojen tuhoaminen). Päätelaitteiden ja niihin kytkeytyvien taustajärjestelmien suojaamisessa ja suojaamisen arvioinnissa voidaan hyödyntää myös Katakri 2015 -viitekehystä. Kasautumisvaikutuksen seurauksena turvallisuusluokan III tietovarantojen hallintaratkaisuissa tulee lisäksi erityisesti huomioida, että hallintaan käytettävät päätelaitteet ovat luotettavasti eroteltuja Internet-kytkentäisistä verkoista. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää esimerkiksi niin sanottua hyppykonekäytäntöä, jossa kaikki hallintatoimet toteutetaan ja kirjataan (lokitetaan) hyppykoneen kautta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Osa-alue 7: Tietojärjestelmäturvallisuus

JT-01	Jäljitettävyys ja havainnointikyky
Vaatimus	1) Luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen on toteutettu. Erityisesti: a) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. b) Keskeiset tallenteet säilytetään vähintään 6 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. c) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta) vähimpien oikeuksien periaatteen mukaisesti. d) Lokitietojen välitys lokilähteiden ja lokikeräimen välillä on toteutettu suojatusti. Välityksen osapuolet tunnistetaan. Lokitiedot välitetään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. Vaihtoehtoisesti lokitiedot voidaan siirtää erillisen hallintaverkon kautta. e) Kellot on synkronoitu sovitun ajanlähteen kanssa. f) Turvallisuusluokan III kasaumalle lisäksi: Keskeiset tallenteet säilytetään vähintään 24 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. g) Turvallisuusluokan III kasaumalle lisäksi: Keskeiset lokitiedot ohjataan lokilähteistä erilliselle lokikeräimelle (tai erillisille lokikeräimille). 2) Pilvipalveluntarjoaja toimittaa asiakkaan pyynnöstä, pilvipalveluntarjoajan vastuualueeseen kuuluvien järjestelmäkomponenttien osalta, asiakkaaseen vaikuttavat lokitiedot muodossa, josta asiakas voi tutkia häneen vaikuttavia tapauksia. 3) Pilvipalveluntarjoaja tarjoaa mahdollisuuden (teknisen rajapinnan) reaaliaikaiseen tiedonvaihtoon asiakkaan kanssa asiakkaan tietojen turvallisuuteen liittyvien tapahtumien välittämiseen (lokitiedot, tapahtumatiedot, tietoturvahavainnot). 4) Luotettavat menetelmät turvallisuuspoikkeamien havaitsemiseksi on toteutettu. Erityisesti: a) On olemassa menettely, jolla kerätyistä tallenteista (vrt. KT-04) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan). b) Verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa. c) On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan. d) On olemassa menettely, jolla pilvipalveluun kuuluvista palvelimista ja muista kohteista (hosts) voidaan havainnoida poikkeamia. e) Turvallisuusluokan III kasaumalle lisäksi: On olemassa menettely, jolla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä pyritään havaitsemaan. 5) On olemassa menettely havaituista poikkeamista toipumiseen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1a-e, 2-3, 4a-d, 5: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 1f-g, 4e: TL III (kasauma)
Suojaustavoite	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitseminen ja selvittäminen, ml. tietomurtojen tutkinta ja korjaavien toimien suunnittelun tukena toimiminen.

JT-01	Jäljitettävyys ja havainnointikyky
Lisätietoja	Jäljitettävyydellä tarkoitetaan järjestelmäympäristön tapahtumien kirjaamista siten, että poikkeamatilanteessa voidaan selvittää mitä toimia ympäristössä on tehty, kenen toimesta ja mitä vaikutuksia toimilla on ollut. Keskeisiä tallenteita ovat tyypillisesti keskeisten verkkolaitteiden ja palvelinten lokitiedot. Myös esimerkiksi työasemien ja vastaavien lokitiedot kuuluvat tähän erittäin usein. Kattavuusvaatimuksen voi useimmin toteuttaa siten, että varmistaa, että ainakin työasemien, palvelinten, verkkolaitteiden (erityisesti palomuurien, myös työasemien sovellusmuurien) ja vastaavien lokitus on päällä. Verkkolaitteiden lokeista tulisi myös pystyä jälkikäteen selvittämään mitä hallintatoimenpiteitä verkkolaitteille on tehty, milloin ja kenen toimesta. Tapahtumalokeja olisi syytä kerätä järjestelmän toiminnasta, käyttäjäaktiviteeteista, turvaan liittyvistä tapahtumista ja poikkeuksista. Suositeltu tapa lokien turvaamiseksi on ohjata keskeiset lokitiedot vahvasti suojatulle lokipalvelimelle/-palvelimille, jonka/joiden tiedot varmuuskopioidaan säännöllisesti. Sekä ylläpitäjien oikeusturvan, kuin myös tietomurtoepäilyjen tutkinnan tukemiseksi, suositellaan tehtävien erottelua toteutettavaksi siten, että lokitietojen ylläpito on eriytetty muusta ylläpitohenkilöstöstä. Lokitietojen tallennus- ja seurantaohjelmiston toimivuutta tulee myös seurata. Lokitietojen säilytysajoissa tulee huomioida kyseessä olevan käyttötapauksen tarpeet. Esimerkiksi viranomaistoiminnassa rikosoikeudelliset vanhentumisajat voivat johtaa tyypillisesti vähintään viiden vuoden säilytysaikatarpeisiin. Väärinkäyttöyrityksen havaitseminen edellyttää useimmissa ympäristöissä käytännössä automatisoitujen havainnointi- ja hälytystyökalujen käyttöä. Lokitietojen manuaalinen tarkastelu on yleensä riittävä vain ympäristöissä, joissa lokimassat ovat hyvin pieniä ja lokien tarkasteluun on osoittaa riittävät henkilöresurssit. Tietojenkäsittely-ympäristön palauttaminen takaisin suojattuun tilaan kohtuullisessa ajassa edellyttää yleensä suunniteltuja, kuvattuja, koulutettuja sekä harjoiteltuja prosesseja sekä teknisiä menetelmiä. Verkkoliikennöinnin osalta tarkkailuun ja havaitun hyökkäyksen vaikutusten rajoittamiseen on useita soveltuvia toteutusmahdollisuuksia keskeisten verkkosolmujen tasolla tapahtuvasta tarkastelusta aina työasema- ja palvelinkohtaisiin sensoreihin sekä näiden yhdistelmiin. Riippumatta käytetyistä verkkolaitteista ja toimittajista, verkkotason havainnointikyvyn käytännön toteutus edellyttää tyypillisesti verkkoliikenteen normaalin tilan tuntemista. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

JT-02	Järjestelmäkovennus
Vaatimus	1) Käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. 2) Kovennettu asennus sisältää vain sellaiset komponentit ja palvelut, sekä käyttäjien ja prosessien oikeudet, jotka ovat välttämättömiä toimintavaatimusten täyttämiseksi ja turvallisuuden varmistamiseksi.
Soveltuvuus	Pilvipalvelun tuottamiseen liittyvät laitteistot ja ohjelmistot. Käsiteltäessä viranomaisen turvallisuusluokiteltua tietoa, kattaa myös hallintaan käytettävät päätelaitteet taustajärjestelmineen (esim. hakemistopalvelut).
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pienentää ohjelmistovirheiden ja virhekonfiguraatioiden riskiä poistamalla tarpeettomat toiminallisuudet käytöstä.
Lisätietoja	Turvallisen ohjelmistokoodin tekeminen on osoittautunut haastavaksi. Mitä enemmän ympäristössä on ohjelmistokoodia, sitä enemmän on mahdollisuuksia ohjelmistovirheille, toisin sanoen haavoittuvuuksille. Mitä enemmän ohjelmistokoodin turvallisuuteen nojaavia palveluja on tarjolla, sitä todennäköisempää on, että palveluissa on myös haavoittuvuuksia. Riskejä voidaan pienentää haavoittuvuuspinta-alaa pienentämällä, toisin sanoen tarjoamalla vain välttämättömiä palveluja alttiiksi hyökkäyksille. Järjestelmät ovat yleensä tulvillaan ominaisuuksia. Ominaisuudet ovat yleensä oletusarvoisesti päällä ja helppo ottaa käyttöön. Ominaisuudet ovat toisaalta usein myös tarpeettoman turvattomilla asetuksilla. Jos tarpeettomia ominaisuuksia ei poisteta käytöstä, nämä ovat myös pahantahtoisen toimijan käytettävissä. Jos välttämättömien palvelujen tarpeettoman turvattomia asetuksia ei muuteta, ovat nämä myös pahantahtoisen toimijan käytettävissä. Järjestelmissä on oletusarvoisesti usein käytössä esimerkiksi ennalta määriteltyjä ylläpitosalasanoja, valmiiksi asennettuja tarpeettomia ohjelmistoja ja tarpeettomia käyttäjätilejä. Koventamisella tarkoitetaan yleisesti järjestelmän asetusten muuttamista siten, että järjestelmän haavoittuvuuspinta-alaa saadaan pienennettyä. Järjestelmissä on yleisesti otettava käyttöön vain käyttövaatimusten kannalta olennaiset toiminnot, laitteet ja palvelut. Vastaavasti esimerkiksi automaattisille prosesseille on annettava vain ne tiedot, oikeudet tai valtuutukset, jotka ovat niiden tehtävien suorittamiseksi välttämättömiä, jotta rajoitetaan onnettomuuksista, virheistä tai järjestelmän resurssien luvattomasta käytöstä mahdollisesti aiheutuvia vahinkoja. Koventamiseen ja kovennetun asennuksen ylläpitämiseen voidaan usein hyödyntää myös konfiguraationhallintatyökaluja. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

JT-03	Tiedon erottelu
Vaatimus	1) Asiakkaiden salassa pidettävät tiedot säilytetään luotettavasti toisistaan eroteltuna yhteiskäyttöisissä virtuaalisissa ja fyysisissä järjestelmissä.
Soveltuvuus	Salassa pidettävän asiakastiedon käsittelyyn liittyvät verkkolaitteet, virtualisointialustat, tallennusjärjestelmät, muistit, siirtomediat ja vastaavat.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakkaiden salassa pidettävään tietoon on pääsy vain kyseisellä asiakkaalla.
Lisätietoja	Erottelu on toteutettava riittävän luotettavasti, joko loogisen tai/ja fyysisen erottelun menetelmillä. Eräs yleinen käytössä oleva erottelumenetelmä esimerkiksi yhteiskäyttöisten verkkolaitteiden ja tallennusjärjestelmien osalta on salaus. Asiakaskohtaisilla avaimistoilla toteutettavaa tietoliikenteen salausta (data-in-transit) ja salausta tallennettaessa (data-at-rest) voidaan hyödyntää myös muiden turvatavoitteiden, esimerkiksi laitteistojen turvallisen hävittämisen, tukevana suojauksena. Vrt. SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella) ja KT-03 (Varmistus- ja palautusprosessit). Jos samaa laitteistoa käytetään useiden asiakkaiden tiedon käsittelyyn samanaikaisesti, tulee varmistua siitä, että tietojen fyysinen ja looginen erottelu on riittävän turvallinen. Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Esimerkiksi turvallisuusluokitellut tiedot voidaan säilyttää fyysisesti erillisellä virtualisointialustalla, jossa esimerkiksi mahdollisiin prosessorihaavoittuvuuksiin liittyvät rajapinnat on rajattu vain turvallisuusluokiteltujen tietojen valtuutettujen käyttäjien saavutettaviksi. Jos samaa laitteistoa käytetään useiden eri asiakkaiden tietojen käsittelyyn, mutta ei samanaikaisesti, tulee varmistua myös siitä, että edellisen asiakkaan tiedot on poistettu riittävän turvallisesti laitteistosta (ml. kaikki osat, BIOS, erilaisten muiden laitteiden välimuistit). Mikäli asiasta ei saada riittävää varmuutta, tulee tietojen käsittelyyn käyttää erillisiä fyysisiä laitteita. Vrt. SI-02 (Tietoaineistojen tuhoaminen). Turvallisuusluokitellun salassa pidettävän tiedon omistajat voivat varata itselleen tarkastusoikeuden kaikkiin verkkoihin/järjestelmiin, joissa heidän omistamaansa tietoa käsitellään. Tarkastuksissa edellytetään usein fyysistä ja loogista pääsyä tarkastettavaan kohteeseen, ja siten tarkastajilla on usein teknisesti mahdollisuus päästä myös kohteessa käsiteltävään tietoon. Erityisesti ympäristöissä, joissa on tarve käsitellä useamman eri omistajan tietoa, tulee varmistua siitä, että verkon/järjestelmän toteutustapa mahdollistaa tarkastukset siten, että tiedon omistajat eivät pääse käsiksi toistensa tietoihin tarkastuksen yhteydessä. Erityisesti palvelumalleilla IaaS ja PaaS, turvallisuusluokitellun tiedon erottaminen tulee varmistaa fyysisesti erillisillä verkoilla tai salatuilla virtuaalisilla tai ohjelmistopohjaisilla paikallisverkoilla. Vrt. SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella).

JT-04	Haittaohjelmasuojaus
Vaatimus	1) Pilvipalvelussa, mukaan lukien sen hallinnointiin käytettävissä järjestelmäympäristöissä, toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.
Soveltuvuus	Pilvipalveluun tuottamiseen liittyvät järjestelmät, mukaan lukien sen hallinnointiin käytettävät järjestelmäympäristöt.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakastiedon eheys, luottamuksellisuus tai saatavuus on riittävällä tasolla suojattu yleisiä haittaohjelmariskejä vastaan.
Lisätietoja	Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä (vrt. JT-02), käyttöoikeuksien rajauksilla (vrt. IP-01), järjestelmien pitämisellä turvallisuuspäivitysten tasolla (vrt. KT-04), poikkeamien havainnointikyvyllä (vrt. JT-01), henkilöstön turvatietoisuudesta varmistumalla (vrt. HT-04) ja myös haittaohjelmantorjuntaohjelmistojen käytöllä. Riskejä voidaan pienentää myös riskialttiiden ympäristöjen eriyttämisellä tuotantoympäristöistä sekä muun muassa siirreltävien medioiden (esimerkiksi USB-muistien) käytön rajauksilla. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. Esimerkiksi mikäli asiakkaan vastuulle kuuluva asiakasjärjestelmä mahdollistaa tiedostojen lataamisen asiakasjärjestelmään, haittaohjelmasuojaukselle yleensä riskienhallinnalliset perusteet.

JT-05	Suojattavien kohteiden siirtäminen ja poistaminen
Vaatimus	1) Laitteita, ohjelmistoja, siirtomedioita tai vastaavia saa siirtää fyysisesti suojattujen toimitilojen ulkopuolelle vain erilliseen valtuutukseen pohjautuen. 2) Fyysisesti suojatun toimitilan ulkopuolella tapahtuva siirto ja käsittely tapahtuu siirrettävän suojattavan kohteen (luokituksen) mukaisesti. 3) Siirrettäessä asiakkaan salassa pidettävää tietoa fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolella, tieto on salatussa muodossa (vrt. SA-02) tai suojattava kohde on pilvipalveluntarjoajan henkilöstön jatkuvan valvonnan alaisuudessa. 4) Viranomaisen turvallisuusluokitellun tiedon suojaamisessa käytetään viranomaisen hyväksymiä salauskäytäntöjä, -vahvuuksia ja -tuotteita (vrt. SA-01).
Soveltuvuus	Asiakastietoa sisältävät laitteistot.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 4: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Suojattavaa asiakastietoa ei vaarannu tilanteissa, joissa sitä siirretään fyysisesti suojattujen turvallisuusalueiden (esimerkiksi konesalit) ulkopuolella.
Lisätietoja	Erityisesti huomioitavaa: • Tietojen turvallinen poistaminen sekä tietovälineen tuhoaminen, vrt. SI-02 (Tietoaineistojen tuhoaminen) • Siirrettävien tietovälineiden salaus • Tietojen siirtäminen uudelle tietovälineelle, kun tietoväline korvataan Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että mikäli asiakkaan vastuulle kuuluva osuus siirtää salassa pidettävää tai/ja turvallisuusluokiteltua tietoa esimerkiksi asiakkaan päätelaitteille/päätelaitteilta, tulee tiedon/tietoliikenteen olla riittävän luotettavasti salatussa muodossa.

Osa-alue 8: Salaus

SA-01	Salauskäytännöt ja avainhallinta
Vaatimus	1) Salauskäytäntöjen ja salausavainten hallinnan prosessit on suunniteltu, toteutettu ja kuvattu. 2) Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Prosessit edellyttävät vähintään a) kryptografisesti vahvoja avaimia, b) turvallista avaintenjakelua, c) turvallista avainten säilytystä, d) säännöllisiä avaintenvaihtoja, e) vanhojen tai paljastuneiden avainten vaihdon, ja f) valtuuttamattomien avaintenvaihtojen estämisen. 3) Viranomaisen turvallisuusluokitellun tiedon suojaamisessa käytetään viranomaisen hyväksymiä salauskäytäntöjä, -vahvuuksia ja -tuotteita.
Soveltuvuus	Asiakastiedon suojaaminen suoraan tai epäsuoraan tilanteissa, joissa salaus on suojauksen toteuttava menetelmä.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Salausmenetelmien käyttö tuottaa riittävän luotettavan suojauksen.
Lisätietoja	Erityisesti liikennöitäessä julkisen tai muun heikommin suojatun verkon kautta, salausratkaisut ovat usein ainoita suojauksia salassa pidettävän tiedon luottamuksellisuuden, ja tyypillisesti myös eheyden suojaamisessa. Koska salausratkaisujen mahdollisia puutteita on usein äärimmäisen haastavaa korvata muilla suojauksilla, salausratkaisun valintaan ja turvalliseen käyttötapaan tulee kiinnittää erityistä huomiota. Tulee myös huomioida, että erityisesti pilvipalveluissa salauksen roolina on usein myös eri asiakkaiden tietojen erottelu (vrt. JT-03) yhteiskäyttöisessä infrastruktuurissa sekä esimerkiksi tiedon tuhoamisen (vrt. SI-02) luotettavuuden tukeminen. Erityisesti turvallisuusluokitellun tiedon suojaamisessa korostuu tarve käyttää salausratkaisuja, joiden riittävästä turvallisuudesta on luotettavaa näyttöä. Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salausratkaisun oikeellisesta toiminnasta varmistumisen lisäksi tulee huomioida muun muassa salausratkaisun käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun ja suojatun fyysisen alueen sisällä (esimerkiksi kahden turva-alueen välinen liikennöinti hallinnollisen alueen kautta). Muihin salausratkaisun arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja eheydelle. Erilaisiin tietoaineistoihin kohdistuu erilaisia riskejä. Esimerkiksi viranomaisten turvallisuusluokitellut tiedot ovat yleensä miellettävissä valtion turvallisuuden (yleisen edun) näkökulmasta suojattaviksi. Turvallisuusluokiteltuihin tietoihin voidaan toisaalta usein olettaa kohdistuvan eriävien tahojen kiinnostus, kuin esimerkiksi turvallisuusluokittelemattomiin henkilötietoihin. Riskien eroavaisuus tulee huomioida myös salausratkaisujen valinnassa. Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään. Salausratkaisun salausavainten hallinnointiprosessien tuleekin olla suunniteltuja, toteutettuja ja kuvattuja/ohjeistettuja. Erityisesti salausratkaisujen osalta tulee riskienarvioinnissa huomioida myös toimitusketjujen turvallisuus. Vaikka salausratkaisu olisi riittävän turvallinen esimerkiksi salausratkaisun valmistajalta lähtiessään, toimitusketjun suojaamispuutteet voivat mahdollistaa salausratkaisun peukaloinnin, ja siten johtaa turvattoman salausratkaisun käyttöönottoon tietojärjestelmän tai palvelun osana. Vrt. SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella) ja SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella). Lisätietoja on saatavissa Kyberturvallisuuskeskuksesta. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

SA-02	Salaus fyysisesti suojatun alueen ulkopuolella
Vaatimus	1) Siirrettäessä asiakkaan salassa pidettävää tietoa hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (esimerkiksi palveluntarjoajan konesali, vrt. FT-01) ulkopuolella, tai matalamman turvallisuustason verkon kautta, salassa pidettävä tieto siirretään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. 2) Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. 3) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. SA-01).
Soveltuvuus	Salausratkaisut konesalien välillä, salausratkaisut muiden matalammin suojattujen verkkojen kautta liikennöitäessä.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakastiedon luottamuksellisuus tai eheys ei vaarannu tilanteissa, joissa sitä siirretään epäluotettavien verkkojen kautta.
Lisätietoja	Internet, sekä operaattorin tarjoamat MPLS-verkot ja esimerkiksi niin sanotut mustat kuidut (dark fiber) tulkitaan julkisiksi verkoiksi. Radiorajapinnan käyttö langattomissa verkkoyhteyksissä (esim. WLAN, 4G) tulkitaan poistumiseksi fyysisesti suojatun turvallisuusalueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan julkisen verkon kautta liikennöinniksi, mikä tulee huomioida erityisesti liikenteen salauksessa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

SA-03	Salaus fyysisesti suojatun alueen sisäpuolella
Vaatimus	1) Kun asiakkaan salassa pidettävää tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (vrt. FT-01) ja kyseisen turvallisuustason verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää, mikäli tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin. Vrt. JT-03. 2) Asiakkaiden salassa pidettävät tiedot tallennetaan pilvipalveluun salatussa muodossa, mikäli käytetään yhteiskäyttöistä laitteistoa. Vrt. JT-03. 3) Salausavaimistot ovat asiakaskohtaisesti eroteltuja. 4) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. SA-01).
Soveltuvuus	Asiakastiedon käsittely-ympäristöt pilvipalvelukokonaisuudessa, mukaan lukien esimerkiksi levyjärjestelmä- ja varmistusratkaisut.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 4: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Eri asiakkaiden tietojen erottelusuojauksen tukeminen salausteknisin menetelmin tilanteissa, joissa eri asiakkaiden tietoja käsitellään yhteiskäyttöisillä laitteistoilla. Monitasoisen suojauksen toteuttaminen, tukien koko elinkaaren mittaista suojaamista.
Lisätietoja	2: Ei koske laskutukseen tai muuhun asiakassuhteen hallinnointiin liittyvää metatietoa. Yleisesti huomioitava, että lähtökohtaisesti pilvipalveluntarjoajalla on aina pääsy palvelussa käsiteltävään tietoon, mikäli tieto on elinkaarensa aikana palvelussa selväkielisessä muodossaan (esimerkiksi asiakkaalle näytettävä kuvana). Esimerkiksi yleiset omien avainten käyttöön (BYOK, Bring Your Own Keys) tai pilvipalveluntarjoajan fyysiseen konesaliin sijoitettaviin laitteistopohjaisiin turvamoduuleihin (HSM, Hardware Security Module) pohjautuvat ratkaisumallit rajaavat, mutta eivät tyypillisesti estä pilvipalveluntarjoajan pääsymahdollisuuksia palvelussa käsiteltävään tietoon. Salausta voidaan käyttää kuitenkin täydentävänä suojauksena tukemaan esimerkiksi eri asiakkaiden tietojen erottelua, suojattavien kohteiden tuhoamisprosessia tai tehtävien erottelua. Vrt. JT-03 (Tiedon erottelu). Erityisesti pilvipalvelujen skaalautuvuuden ja asiakaskohtaisen erottelun yhdistämiseen salaus on usein suositeltava toteutustapa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että useissa pilvipalveluratkaisuissa asiakastiedon salaamiskäytännöt ovat osin asiakkaan vastuulla ja konfiguroitavissa.

Osa-alue 9: Käyttöturvallisuus

KT-01	Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi
Vaatimus	1) Pilvipalvelusta on kattavat järjestelmäkuvaukset sekä ohjeet palvelun turvalliseen ylläpitoon ja hallinnointiin. Kuvaukset ja ohjeistukset ovat sellaisella tasolla, että niiden avulla pystytään uskottavasti välttämään käytön aikaiset virheet sekä varmistumaan sopimusvelvoitteiden mukainen palautuminen häiriötilanteista. 2) Järjestelmäkuvaukset ja ohjeet pidetään ajan tasalla. 3) Järjestelmäkuvaukset ja ohjeet ovat henkilöstölle jalkautettuna ja saatavilla roolien mukaisesti.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Tavoitteena pystyä välttämään käytön aikaiset virheet sekä varmistumaan sopimusvelvoitteiden mukainen palautuminen häiriötilanteista.
Lisätietoja	Erityisesti tilanteissa, joissa pilvipalvelun merkittävä järjestelmäkomponentti vikaantuu, tulee palvelun korjaamisen tueksi olla riittävän kattavat kuvaukset järjestelmästä. Kuvausten tulee olla sellaisten henkilöiden saatavilla, jotka tarvitsevat niitä tilanteen palauttamisessa. Kuvaukset tukevat myös tilanteissa, joissa avainhenkilöt ovat estyneitä poikkeavan tilanteen korjaamisesta. Huomioitava riittävät kuvaukset ja ohjeistukset myös tilanteissa, joissa asiakas tai asiakkaan valtuuttama kolmas osapuoli ylläpitää tai kehittää pilvipalvelualustan päälle tuotettua asiakasjärjestelmää. Jatkuvuutta voidaan tukea myös esimerkiksi automatisoituja häiriönkorjaustoimintoja (esimerkiksi konttien uudelleenkäynnistys) hyödyntämällä. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

KT-02	Suorituskyvyn hallinta
Vaatimus	1) Pilvipalvelun suorituskyky (kapasiteetti) mitoitetaan siten, että palvelutasosopimusten mukainen palvelutaso pystytään luotettavasti tarjoamaan. Mitoitukseen on sisällyttävä toteutuneen suorituskykytarpeen seuranta sekä tulevien suorituskykytarpeiden ennusteet. 2) Pilvipalveluntarjoajan on mahdollistettava asiakkaalle annettujen järjestelmäresurssien (esim. tietojenkäsittely- tai tallennuskapasiteetin) käytön seuranta.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Tavoitteena se, että palvelutasosopimusten mukainen palvelutaso pystytään luotettavasti tarjoamaan.
Lisätietoja	Suorituskykytarpeen seuranta tukee mahdollisuuksia resurssien käyttöasteen optimointiin, tulevien tarpeiden arviointiin, sekä myös palvelutasosopimusten mukaisten velvoitteiden täyttämiseen.

KT-03	Varmistus- ja palautusprosessit
Vaatimus	1) Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu osana jatkuvuussuunnitelmaa siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Erityisesti huomioitava: a) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO). b) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO). c) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti. d) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä). 2) Varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto. Suuri määrä tietoa voi edellyttää tiukempia suojauksia (kasautumisvaikutus). Erityisesti huomioitava: a) Pääsy varmuuskopioihin on rajattu vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyille henkilöille tai rooleille. b) Varmistus- ja palautusprosessit ovat jäljitettävissä (lokitus) ja valvottuja siten, että luvattomat toimet (esimerkiksi valtuuttamattomat palautukset) pyritään havaitsemaan. c) Tilanteissa, joissa varmuuskopioita säilytetään toisessa fyysisessä sijainnissa, myös tämän sijainti on fyysisen ja loogisen pääsynhallinnan osalta vähintään vastaavalla tasolla. d) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan toiseen konesaliin) verkon välityksellä, tieto/tietoliikenne on salattuna käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-02 ja SA-03. e) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle siirtomedialla (esimerkiksi varmistusnauhat tai -levyt), siirtomedia siirretään jatkuvan valvonnan alaisuudessa. Siirtomedialle tai sen sisältämälle tiedolle suositellaan salausta. f) Varmistusmediat hävitetään luotettavasti (vrt. SI-02). 3) Viranomaisen turvallisuusluokiteltua tietoa sisältävien varmuuskopioiden osalta lisäksi huomioitava: a) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan toiseen konesaliin) verkon välityksellä, tieto/tietoliikenne on suojattu viranomaisen hyväksymällä salausratkaisulla. b) Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, erottelumenettelyt (esimerkiksi salaus tai/ja fyysisesti erilliset tallennejärjestelmät ja -mediat) on toteutettu varmistusjärjestelmän liittymien ja tallennemedioiden osalta. Vrt. JT-03 ja SA-03.
Soveltuvuus	Pilvipalvelun varmistus- ja palautusprosessit. Huomioitava myös tilanteet, joissa osa prosesseista riippuvaisia asiakasjärjestelmän toteutuksesta.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 3: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakastiedon saatavuuden, eheyden ja luottamuksellisuuden suojaaminen varmistus- ja palautusprosesseissa.
Lisätietoja	Palautustestaus voidaan myös automatisoida tapahtuvaksi esimerkiksi viikoittain. Myöskin palautus tulee suojata vähintään vastaavan tasoisesti kuin alkuperäinen tieto (ml. myös tuhoaminen, vrt. SI-02). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia. Joissain käyttötapauksissa saattaa olla esimerkiksi varautumistarpeista perusteltua, että asiakasjärjestelmän käsittelemä tieto tai/ja infrastruktuuri on varmistettu/kahdennettu myös täysin asiakkaan hallinnoimaan ympäristöön.

KT-04	Haavoittuvuuksien hallinta
Vaatimus	1) Pilvipalvelun koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi. Erityisesti huomioitava: a) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja riskiperusteisesti tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti (vrt. MH-01). b) Järjestelmät tarkistetaan tunnettujen haavoittuvuuksien varalta automaattisesti vähintään kuukausittain. Jos suunnitelluista asetuksista tai turvapäivitystasosta on poikettu, syyt analysoidaan, ja poikkeamat korjataan tai dokumentoidaan poikkeamahallintaprosessin mukaisesti (ks. TJ-04). c) Pilvipalvelun turvallisen toiminnan kannalta keskeiset komponentit tarkistetaan riippumattoman tahon tunkeutumistestauksella säännöllisesti, vähintään vuosittain. Merkittävät poikkeamat korjataan välittömästi. d) Pilvipalvelun asiakkaalle tiedotetaan merkittävistä haavoittuvuuksista ja niiden vaikutuksista asiakkaan tietojen suojaamiseen. Tiedotus on erityisen tärkeää tilanteissa, joissa haavoittuvuuden hallinta edellyttää toimia sekä pilvipalveluntarjoajalta että asiakkaalta.
Soveltuvuus	Pilvipalvelukokonaisuuteen kuuluvat ohjelmistot ja laitteistot.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Ohjelmistohaavoittuvuuksiin liittyvien riskien pitäminen siedettävällä tasolla.
Lisätietoja	Turvallisen ohjelmistokoodin tekeminen on osoittautunut haastavaksi. Ohjelmistovirheiden, toisin sanoen haavoittuvuuksien, hyödyntäminen on useissa hyökkäystyypeissä jossain vaiheessa mukana. Vastuulliset toimittajat korjaavat ohjelmistoistaan löytyneitä haavoittuvuuksia. Riskejä voidaan pienentää korjausten asennuksilla. Haavoittuvuuksien hallintaan liittyy ohjelmisto- ja järjestelmäympäristön jatkuva seuranta ja kehittäminen siten, että ohjelmistotoimittajien haavoittuvuuskorjaukset voidaan asentaa mahdollisimman nopeasti. Lisäksi on syytä seurata käytettävien ohjelmistoversioiden tukea niiden toimittajalta. Vanhentuneisiin ohjelmistoversioihin ei julkaista aktiivisesti päivityksiä, jolloin myös tietoturvahaavoittuvuuksien korjaaminen voi olla mahdotonta. Haavoittuvuuksien korjaamisessa on huomioitava korjausten vaikutukset palveluihin. Jos korjausten tekeminen aiheuttaa katkon asiakkaan palveluun, on se suositeltavaa ajoittaa palvelun asiakkaille vähiten haitalliseen aikaan tai etukäteen sovitun palvelukatkon aikana. Korjausten testaaminen esimerkiksi testiympäristössä voi olla perusteltua, mikäli halutaan varmistua siitä, että korjaavat päivitykset eivät aiheuta odottamattomia muutoksia palvelussa. Haavoittuvuuksien hallintaa voidaan tehdä aktiivisesti: • varmistamalla vastuut ja tehtävänjaon haavoittuvuuksien korjaamisen osalta, • seuraamalla järjestelmäkehitystä ja palveluntuotannossa käytettävien ohjelmistojen tietoturvan tilannetta, ja • sopimalla jatkuvan seurannan menettelyistä, esim. skannaamalla omaa ympäristöä tunnettujen haavoittuvuuksien osalta. B: Tarkastus kattaa kaikki järjestelmät, jotka liittyvät kokonaisuuteen rajapintojen kautta. Tarkastukseen voidaan hyödyntää esimerkiksi ajastettuja haavoittuvuusskannauksia tai konfiguraatiohallintatietokantoja (CMDB, configuration management database). Turvapäivitysten asennuksessa voidaan hyödyntää myös menettelyä, jossa esimerkiksi virtuaalikoneista ylläpidetään luotettua, turvapäivitysten tasolla olevaa levykuvaa (golden image), ja käytössä olevat virtuaalikoneet korvataan tällä ajantasaisella levykuvalla säännöllisesti. Tässä ratkaisumallissa erityisesti huolellisuutta tulee kohdistaa menettelyihin, joilla pyritään varmistamaan levykuvan eheys. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Osa-alue 10: Siirrettävyys ja yhteensopivuus

SI-01	Siirrettävyys ja yhteensopivuus
Vaatimus	1) Pilvipalvelun ohjelmointirajapinnat (API, Application Programming Interface) on julkaistu siten, että ne mahdollistavat yhteentoimivuuden eri ohjelmistokomponenttien ja ohjelmistojen kanssa. 2) Pilvipalvelu tukee yleisesti käytettyjä muotoja ohjelmistojen siirrettävyyteen (esimerkiksi Open Virtualization Format, Docker, Kubernetes tai vastaavat). 3) Pilvipalveluntarjoaja tarjoaa teknisen rajapinnan tai muun menetelmän asiakkaan tietojen toimitukseen asiakkaalle soveltuvassa, käyttökelpoisessa ja yleisesti yhteensopivassa muodossa. Muodot on kuvattu riittävällä tasolla asiakkaan kanssa solmittavissa sopimuksissa. 4) Tietojen tuontiin ja vientiin sekä palvelun hallinnointiin käytetään turvallisia, vakiintuneita verkkoprotokollia siten, että siirrettävien tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta voidaan varmistua. 5) Viranomaisen turvallisuusluokitellun tiedon siirrossa käytetään viranomaisen hyväksymiä salausratkaisuja.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	1-4: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 5: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakkaalla on mahdollisuus vaihtaa pilvipalveluntarjoajaa ja hyödyntää oman palvelunsa toteuttamiseen useita pilvipalveluntarjoajia. Asiakastietojen siirto ei vaaranna tietojen luottamuksellisuutta, eheyttä tai saatavuutta.
Lisätietoja	Tapauskohtaisesti arvioitava se, minkä verran on perusteltua edellyttää siirrettävyyttä tilanteissa, joissa pilvipalveluun toteutettu palvelu käyttää kyseisen pilvipalvelualustan ominaisuuksia palvelun toteuttamiseen. Lähtökohtaisesti aina on kuitenkin perusteltua edellyttää asiakastietojen (esimerkiksi tietokantaan tallennettujen asiakasrekisterien sisällön) siirrettävyyttä jossain helposti koneellisesti käsiteltävässä muodossa. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti tiedon/tietoliikenteen salaus tilanteissa, joissa salassa pidettävää tietoa tuodaan/viedään palveluun/palvelusta.

SI-02	Tietoaineistojen tuhoaminen
Vaatimus	1) Tietoaineistojen tuhoaminen on järjestetty riittävän luotettavasti. 2) Tuhoaminen kattaa koko salassa pidettävän tiedon elinkaaren siltä osin, kun tieto on ollut pilvipalvelussa. 3) Asiakkaan salassa pidettävät tiedot tuhotaan luotettavasti erityisesti seuraavissa tilanteissa: a) Asiakkaan pyytäessä tietojensa tuhoamista. b) Asiakkaan sopimuksen päättyessä. c) Laitteistohuollon, -ylläpidon ja -vaihdon tapauksissa (esimerkiksi asiakkaan salassa pidettävää tietoa sisältävän rikkoontuneen levyn vaihto). 4) Turvallisuusluokitellun tietoaineiston tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
Soveltuvuus	Asiakkaan suojattavaa tietoa sisältäneet tallennemediat ja vastaavat järjestelmät.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma) 4: TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Asiakkaan salassa pidettävän tiedon luottamuksellisuus ei vaarannu tilanteissa, joissa sen käsittelyyn käytetyt tallennemediat ja vastaavat järjestelmät poistetaan käytöstä, tai kyseinen asiakastieto tulee muista syistä poistaa pilvipalvelusta.
Lisätietoja	**Tuhoamisen luotettavuus** Tietoaineistojen tuhoamisen luotettavuuteen vaikuttaa merkittävästi se, miten eri tietoaineistot ovat elinkaarensa aikana olleet sijoitettuina pilvipalveluun. Esimerkiksi selväkielisessä muodossa tallennettujen turvallisuusluokiteltujen tietoaineistojen luotettava tuhoaminen voi edellyttää kyseisten tallennemedioiden fyysistä tuhoamista. Luotettava tuhoaminen voikin edellyttää myös sitä, että tietoaineistojen tallennuksen fyysinen ja looginen sijainti voidaan selvittää tietoaineiston elinkaaren ajalta. Toisaalta mikäli turvallisuusluokittelemattomat salassa pidettävät tiedot on tallennettu pilvipalveluun vain riittävän luotettavaksi arvioidussa salatussa muodossa (vrt. SA-03: Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella), jäännösriskit saattavat olla hyväksyttävissä, mikäli salaukseen käytetty avaimisto pystytään luotettavasti tuhoamaan. Menettely voi tukea myös henkilötietojen tuhoamista niiden lakisääteisen säilytysajan jälkeen. **Tuhoaminen silppuamalla** Aineistojen silppuaminen voidaan toteuttaa esimerkiksi siten, että - paperiaineistojen silppukoko on enintään 30 mm2 (DIN 66399 / P5 tai DIN 32757 / DIN 4), - magneettisten kiintolevyjen silppukoko on enintään 320 mm2 (DIN 66399 / H-5), - SSD-kiintolevyjen ja USB-muistien silppukoko on enintään 10 mm2 (DIN 66399 / E-5), ja - optisten medioiden silppukoko on enintään 10 mm2 (DIN 66399 / O-5). Käytettäessä edellä mainittuja silppukokoja, voidaan silppuamisesta syntyvä jäte hävittää normaalin toimistojätteen mukaisesti. **Tuhoaminen ylikirjoittamalla** Tuhoamiseen voidaan hyödyntää asiakkaan salassa pidettävää tietoa sisältäneiden muistialueiden ylikirjoittamista. Tällöin tulee huomioida erityisesti käytetyn ylikirjoitusmenetelmän soveltuvuus kyseiselle tallennemedialle sekä prosessi vastuutahoineen. Sähköisten aineistojen tuhoamista on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ylikirjoitusohjeessa (www.ncsa.fi > Ohjeita > "Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö"). **Tuhoaminen eri menetelmiä yhdistäen** Tuhoamiseen voidaan käyttää tukevina suojauksina myös muita menetelmiä, joilla tietojen kokoaminen estetään luotettavasti (esimerkiksi silpun polttaminen tai kiintolevyn sulattaminen). Tietojen kokoamismahdollisuuksiin vaikuttaa myös ulkopuolisille luovutettavan silpun määrä. Myös salauksella pystytään pienentämään huomattavasti salassa pidettävään tietoon kohdistuvia riskejä tiedon ja laitteistojen elinkaarten eri vaiheissa. **Sähköisten aineistojen tuhoamisessa huomioon otettavaa** Erityisesti sähköisten aineistojen luotettavan tuhoamisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän salassa pidettävän tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys (esimerkiksi viranomaisen hyväksymä ylikirjoitusmenettely) ei ole mahdollista, salassa pidettävää tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että salassa pidettävää tietoa ei viedä huoltotoimenpiteen yhteydessä. Vrt. salauksen mahdollisuudet jäännösriskien pienentämisessä (SA-03: Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että mikäli tuhoaminen nojaa joiltain osin salaukseen, salausavainten tuhoamisen tulee tapahtua riittävän luotettavasti.

Osa-alue 11: Muutostenhallinta ja järjestelmäkehitys

MH-01	Muutostenhallinta
Vaatimus	1) Pilvipalveluun tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutosten-hallintamenettely. Muutostenhallintamenettely huomioi myös vaatimustenmukaisuuden (vrt. TJ-07) sekä sopimusvelvoitteet. 2) Muutoksiin liittyvät riskit arvioidaan ja hyväksytetään soveltuvilla tahoilla. 3) Muutokset testataan ennen niiden käyttöönottoa tuotantoympäristössä. 4) Testausympäristöt ovat eroteltuja tuotantoympäristöistä. 5) Testaus suunnitellaan ja toteutetaan siten, että se tuottaa luotettavan kuvan muutoksen vaikutuksista ennen siirtoa tuotantoympäristöön.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus ei vaarannu palveluun tehtävien muutosten seurauksena.
Lisätietoja	Vaatimusten täyttämisessä voidaan hyödyntää seuraavaa menettelyä: 1) On määritelty prosessit, joilla peruutetaan muutokset virheiden tai turvallisuusongelmien takia sekä palautetaan aiempaan tilaansa ne järjestelmät tai palvelut, joihin tällä oli vaikutusta. 2) Ennen muutoksen siirtoa tuotantoympäristöön arvioidaan, onko suunnitellut testit suoritettu menestyksellisesti ja vaaditut hyväksynnät myönnetty. 3) Hätätilanteissa (esimerkiksi merkittävissä laiterikoissa tai tietomurtotapauksissa) voidaankäyttää kevennettyä muutostenhallintaprosessia edellyttäen, että muutosten turvavaikutukset selvitetään normaaliprosessia vastaavalla kattavuudella jälkikäteen (tyypillisesti pisimmillään viikon sisällä muutoksista). 4) Testaus- ja tuotantoympäristöjen erottelu on toteutettu luotettavasti joko fyysisen tai loogisen erottelun menettelyillä, jotta pyritään välttämään valtuuttamaton pääsy ja muutokset tuotantoympäristöön ja -dataan. Tuotantodataa ei siirretä kehitys- tai testausympäristöihin datan luottamuksellisuuden suojaamiseksi. 5) Muutostenhallinnan menettelyihin sisältyy rooleihin perustuvia oikeuksia, joilla varmistetaan tehtävien asianmukainen erottaminen muutosten kehittämisessä, käyttöönotossa ja siirtämisessä ympäristöstä toiseen. Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

MH-02	Järjestelmäkehitys
Vaatimus	1) Sovellukset ja ohjelmointirajapinnat (API:t) suunnitellaan, kehitetään, testataan ja otetaan käyttöön alan hyvien turvallisuuskäytäntöjen mukaisesti. Rajapintojen on kestettävä yleiset hyökkäysmenetelmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu. 2) Tuotantoympäristö on eriytetty muista ympäristöistä (esimerkiksi kehitys-, testaus- ja laadunvarmistusympäristöistä). 3) Versionhallinnan turvallisuus on huomioitu vähintään siten, että menettelyt luotettavasti estävät valtuuttamattomien versioiden siirron tuotantoympäristöön. 4) Turvallisen ohjelmistokehitysprosessin käytännöt on jalkautettu organisaatioon jokaiseen osaan, joka on tekemisissä kyseisen ohjelmiston kanssa. 5) Tilanteissa, joissa pilvipalvelun (tai sen osan) lähdekoodin suunnittelu, kehittäminen, testaus tai provisiointi ulkoistetaan, sopimuksissa huomioidaan erityisesti: a) turvallisen ohjelmistokehitysprosessin vaatimukset (erityisesti suunnittelun, kehitystyön ja testauksen osalta), b) näyttö riittävästä testauksesta, c) hyväksymistestaus sovittujen toiminnallisten ja ei-toiminnallisten vaatimusten mukaisesti, ja d) oikeus testata kehitysprosessia ja valvontatoimia, myös pistokokeina.
Soveltuvuus	Pilvipalvelukokonaisuuteen liittyvä järjestelmäkehitys.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV & KV-R, TL III (kasauma)
Suojaustavoite	Pilvipalvelussa käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus ei vaarannu palveluun tehtävän järjestelmäkehityksen seurauksena.
Lisätietoja	1: Turvallisuuskäytäntöjä ovat esimerkiksi OWASP web-sovelluksille, ja järjestelmäkehityksen elinkaarimallit (SDLC, Systems Development Life Cycle). 5: Vrt. TJ-08 (Palveluntarjoajien ja toimittajien turvallisuus). Asiakkaan vastuulla olevan osuuden arvioinnissa suositellaan huomioitavaksi erityisesti, että vastaavat vaatimukset koskevat myös asiakasta ja asiakkaan osuuteen liittyviä mahdollisia palveluntarjoajia.

Liite 1: Esimerkkejä vaatimuskohtien kohdentamisesta

Tässä liitteessä kuvataan esimerkkejä PiTuKrissa kuvattujen vaatimusten kohdentamisesta. Esimerkit on jaettu palvelumalleittain asiakkaan ja pilvipalveluntarjoajan vastuisiin. Esimerkeissä käytetty kuvitteellinen pilvipalvelu on toteutettu yleistä, kuvassa 3 esitettyä vastuumallia mukaillen.

Huom: Pilvipalveluiden käytännön ilmentymät eroavat toisistaan sekä teknisten toteutusten, että myös vastuujaon osalta. Esimerkiksi PaaS-palvelumallilla tuotetun pilvipalvelualustan ja sen päälle toteutetun asiakasjärjestelmän suojaamisen vastuut voivat erota merkittävästikin eri palveluntarjoajien välillä. Mielekäs arviointi edellyttääkin kyseisen pilvipalveluntarjoajan ja kyseisen asiakasjärjestelmän teknisten toteutusten sekä vastuujaon erityispiirteiden huomiointia.

Palvelumallina IaaS

Tässä esimerkissä kuvataan PiTuKrissa kuvattujen vaatimusten kohdentaminen vastuittain tilanteessa, jossa asiakasjärjestelmä on sijoitettu pilvipalveluntarjoajan IaaS-palvelumallilla tuotettuun alustaan.

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (soveltuvuuden arviointi)	x
	3	-	x
	4	x (soveltuvuuden arviointi)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (soveltuvin osin)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	x	x
JT-03	1	- (Ellei asiakasjärjestelmässä edelleen eri erottelutarpeisia asiakkaiden tietoja.)	x
JT-04	1	x	x

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d	x (mikäli asiakas toteuttaa siirron asiakasympäristön kautta/välityksellä)	x
	2 e-f	-	x
	3	x	x
KT-04	1 a-b	x	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (sopimuksen osalta)	x
	4-5	x (voi soveltua asiakkaan konfigurointimahdollisuuksien osalta)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x	x

Palvelumallina PaaS

Tässä esimerkissä kuvataan PiTuKrissa kuvattujen vaatimusten kohdentaminen vastuittain tilanteessa, jossa asiakasjärjestelmä on sijoitettu pilvipalveluntarjoajan PaaS-palvelumallilla tuotettuun alustaan.

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (soveltuvuuden arviointi)	x
	3	-	x
	4	x (soveltuvuuden arviointi)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (soveltuvin osin)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	- (Huom: Vaihtelua palveluntarjoajittain vastuurajoista, esimerkiksi sovellusten osalta.)	x
JT-03	1	- (Ellei asiakasjärjestelmässä edelleen eri erottelutarpeisia asiakkaiden tietoja.)	x

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
JT-04	1	- (Huom: Vaihtelua palveluntarjoajittain vastuurajoista.)	x
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d-f	-	x
	3	x	x
KT-04	1 a-b	x (Huom: Vaihtelua palveluntarjoajittain vastuurajoista, esimerkiksi mahdollisen asiakaskohtaisen osuuden palomuuri-ohjelmisto ja mahdolliset asiakkaan vastuulla olevat IAM-järjestelmät.)	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (sopimuksen osalta)	x
	4-5	x (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x (Huom: Vaihtelua palveluntarjoajittain.)	x

Palvelumallina SaaS

Tässä esimerkissä kuvataan PiTuKrissa kuvattujen vaatimusten kohdentaminen vastuittain tilanteessa, jossa asiakas hyödyntää pilvipalveluntarjoajan SaaS-palvelumallilla tuotettua sovellusta.

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (soveltuvuuden arviointi)	x
	3	-	x
	4	x (soveltuvuuden arviointi)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (Soveltuvin osin, esimerkiksi toiminta tilanteessa, jossa verkkoyhteys pilvipalveluun ei käytettävissä)	x
TJ-06	1	-	x
	2	x	x
	3-4	-	x
	5	x (käytettävien sovellusten asiakkaan vastuulla olevien osuuksien omistaja/ vastuutaho)	x
	6	x (käytettävien sovellusten ja niiden asiakkaan vastuulla olevien osuuksien kirjanpito ja muutoshallinta)	x
TJ-07	1-4	x (sovellusten käytön vaatimusten-mukaisuuden ja tietosuojan arviointi)	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	-	x
TT-02	1-2	-	x
IP-01	1 a-h	x	x

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
IP-02	1-3	x (yleensä keskittyen turvallisten asetusten konfigurointiin ko. palvelun asetuksista, sekä asiakkaan päätelaitteiden turvallisuuteen)	x
IP-03	1	-	x
	2-7	x (yleensä keskittyen turvallisten asetusten konfigurointiin ko. palvelun asetuksista, sekä asiakkaan päätelaitteiden turvallisuuteen)	x
JT-01	1-5	-	x
JT-02	1-2	-	x
JT-03	1	-	x
JT-04	1	-	x
JT-05	1-4	-	x
SA-01	1-3	x (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)	x
SA-02	1-3	x (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)	x
SA-03	1	-	x
	2-4	x (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)	x
KT-01	1-2	-	x
	3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1-3	-	x
KT-04	1 a-d	-	x
SI-01	1-2	-	x
	3	x (sopimuksen osalta)	x
	4-5	x (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)	x
SI-02	1-4	- (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)	x
MH-01	1-2	x (painotus yleensä hallinnollisissa menettelyissä)	x
	3-5	- (voi soveltua räätälöidyissä sovelluksissa, jossa testaukseen mahdollisesti myös asiakkaan osallistuminen tarpeen)	x
MH-02	1-5	-	x

Liite 2: Esimerkkejä kriteeristön soveltamisesta vaatimustenmukaisuuden arviointiin

Esimerkki 1: Salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arviointi

Tässä kuvataan esimerkki siitä, kuinka kriteeristöä voidaan soveltaa turvallisuusluokittelemattoman salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arviointiin suhteessa tiedonhallintalain (906/2019) vaatimuksiin. Esimerkissä asiakkaana on viranomainen A, joka haluaa arvioida uuden, vielä suunnitteluvaiheessa olevan pilvipalveluun sijoitettavan tietojärjestelmänsä suojausten riittävyyttä turvallisuusluokittelemattoman salassa pidettävän tiedon käsittelyyn.

Viranomainen A on tunnistanut tiedonhallintalain ja PiTuKrin vaatimusten välillä seuraavat A:n järjestelmäympäristöön kohdistuvat yhteydet:

- 12 §: Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen: HT-02 (Henkilöstön luotettavuuden arviointi); HT-03 (Salassapito- ja vaitiolositoumukset)
- 14 §: Tietojen siirtäminen tietoverkossa: SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella) / Kohdat 1-2; SA-01 / Kohdat 1-2.
- 16 §: Tietojärjestelmien käyttöoikeuksien hallinta: IP-01 (Käyttöoikeushallinta)
- 17 §: Lokitietojen kerääminen: JT-01 (Jäljitettävyys ja havainnointikyky) / kohdat 1-3
- 21 §: Tietoaineistojen säilytystarpeen määrittäminen (tuhoaminen säilytysajan päätyttyä): SI-02 (Tietoaineistojen tuhoaminen)

Tiedonhallinnan järjestämiseen (4 §) soveltuu keskeisesti järjestelmäympäristöön liittyvien vastuiden määrittely vaatimuskortissa TJ-02 (Turvallisuuden vastuut), ajantasaisten ohjeiden järjestäminen vaatimuskortissa HT-04 (Turvallisuustietoisuus) sekä valvonta vaatimuskortissa TJ-07 (Vaatimustenmukaisuus ja tietosuoja). Toisaalta tietojenkäsittelyyn liittyvien riskien tunnistamiseen ja tietoturvallisuustoimenpiteiden riskienarviointipohjaiseen mitoittamiseen soveltuu suoraan vaatimuskortti TJ-03 (Turvallisuusriskien hallinta).

Viranomainen A on lisäksi tunnistanut omassa riskienhallinnassaan (13 §), että esimerkiksi riittävän vikasietoisuuden ja toiminnallisen käytettävyyden saavuttamiseksi pystytään hyödyntämään vaatimuskortteja TJ-05 (Jatkuvuudenhallinta), KT-03 (Varmistus- ja palautusprosessit), MH-01 (Muutostenhallinta) ja MH-02 (Järjestelmäkehitys), kuten myös TT-02 (Yleisiä verkkohyökkäyksiä vastaan suojautuminen). Tietoturvallisuuden tilan seurantaa (13 §) tukee suoraan JT-01 (Jäljitettävyys ja havainnointikyky). Toisaalta esimerkiksi elinkaaren kestävään suojaukseen liittyy oleellisesti KT-04 (Haavoittuvuuksien hallinta) ja SI-02 (Tietoaineistojen tuhoaminen). Toisaalta A on tunnistanut, että käyttöoikeushallinto edellyttää luotettavasti toimiakseen myös käyttäjätunnistusta (IP-02), ja toisaalta esimerkiksi järjestelmän haavoittuvuusavaruuden pienentämiseksi verkkotekniset rajaukset (TT-01) ja järjestelmäkovennukset (JT-02) ovat riskiperusteisesti välttämättömiä. Koska järjestelmän turvallisuus nojaa suoraan hallintayhteyksien suojauksiin (IP-03), myös nämä A näkee kriittisiksi järjestelmältä edellytettäviksi suojauksiksi.

Viranomainen A on riskienarvioinnissaan (13 §) lisäksi tunnistanut, että tietoaineistojen turvallisuuden luotettava varmistaminen (15 §) edellyttää myös fyysisen turvallisuuden (FT-01 - FT-05) huomioimista soveltuvin osin. Jotta viranomainen A pystyy saamaan varmuutta turvallisuustyön jatkuvuudesta ja ylläpidosta, myös turvallisuusjohtamisen osa-alue on hyödynnettävissä soveltuvin osin.

Viranomainen A on riskienhallinnassaan tehnyt tietoisen valinnan siitä, että mikäli kehitettävä tietojärjestelmä olisi myöhemmin tarpeen siirtää toiseen pilvipalvelualustaan, tämä voisi aiheuttaa merkittäviä kustannuksia ja edellyttää järjestelmän uudelleenrakennusta merkittävässä määrin. A hyväksyykin siirrettävyyteen liittyvät riskit, ja ei sovella esimerkiksi vaatimuskorttia SI-01 (Siirrettävyys) tähän kyseiseen järjestelmään.

Esimerkki 2: Turvallisuusluokitellun tiedon suojausten vaatimustenmukaisuuden arviointi

Tässä kuvataan esimerkki siitä, kuinka kriteeristöä voidaan soveltaa turvallisuusluokitellun salassa pidettävän tiedon suojausten vaatimustenmukaisuuden arviointiin suhteessa tiedonhallintalain (906/2019) ja turvallisuusluokitteluasetuksen (1101/2019) vaatimuksiin. Esimerkissä asiakkaana on viranomainen B, joka haluaa arvioida uuden, vielä suunnitteluvaiheessa olevan pilvipalveluun sijoitettavan tietojärjestelmänsä suojausten riittävyyttä turvallisuusluokan IV (KÄYTTÖ RAJOITETTU) salassa pidettävän tiedon käsittelyyn.

Viranomainen B on tunnistanut tiedonhallintalain (906/2019) ja PiTuKriin koottujen vaatimusten välillä vastaavat yhteydet, kuin esimerkissä 1 kuvattu viranomainen A:kin. Viranomainen B on lisäksi tunnistanut turvallisuusluokitteluasetuksen (1101/2019) ja PiTuKriin koottujen vaatimusten välillä seuraavat suorat B:n järjestelmäympäristöön kohdistuvat yhteydet:

- 6 §: Turvallisuusluokitellun asiakirjan antamisen edellytykset: EE-01 (Järjestelmäkuvaus); EE-02 (Lainsäädäntöjohdannaiset riskit)
- 8 §: Käsittelyoikeudet ja niiden luettelointi: HT-05 (Tiedonsaantitarpeet ja tehtävien erottelu) / kohdat 1-3; HT-04 (Turvallisuustietoisuus); HT-03 (Salassapito- ja vaitiolositoumukset)
- 9 §: Turvallisuusalueet: FT-01 (Monitasoinen suojaaminen ja riskienhallinta) / kohta 2; FT-03 (Luvattoman pääsyn estäminen)
- 10 §: Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla: FT-01 (Monitasoinen suojaaminen ja riskienhallinta), FT-02 (Rakenteet ja turvallisuusjärjestelmät), FT-03 (Luvattoman pääsyn estäminen), FT-04 (Palveluntuottajat ja vierailijat), FT-05 (Varautuminen ja jatkuvuudenhallinta); IP-03 (Hallintayhteydet); JT-05 (Suojattavien kohteiden siirtäminen ja poistaminen)
- 11 §: Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset / kohta 1: TT-01 (Tietoliikenneverkon rakenne) / kohdat 1 ja 3
- 11 §: Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset / kohta 3: IP-01 (Käyttöoikeushallinta) / kohta b.
- 11 §: Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset / kohta 5: IP-02 (Käyttäjätunnistus)
- 11 §: Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset / kohta 6: JT-02 (Järjestelmäkovennus)
- 11 §: Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset / kohta 7: SA-01 (Salauskäytännöt ja avainhallinta)
- 12 §: Asiakirjan siirtäminen tietoverkon kautta: SA-02 (Salaus fyysisesti suojatun turvallisuusalueen ulkopuolella); SA-03 (Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella); SA-01 (Salauskäytännöt ja avainhallinta)
- 15 §: Asiakirjan tuhoaminen: SI-02 (Tietoaineistojen tuhoaminen)

Lisäksi sähköisiä viestejä, esimerkiksi sähköpostin liitteenä olevia haittaohjelmia ja myös suorempia pilvipalvelun sovellusturvallisuutta vastaan kohdistettuja hyökkäyksiä, vastaan suojautumisessa (1101/2019 / 11 § / kohta 2) keskeisiä suojauksia ovat TT-01 (Tietoliikenneverkon rakenne), TT-02 (Yleisiä verkkohyökkäyksiä vastaan suojautuminen), KT-04 (Haavoittuvuuksien hallinta), JT-04 (Haittaohjelmasuojaus), JT-02 (Järjestelmäkovennus), MH-02 (Järjestelmäkehitys), sekä luonnollisesti myös JT-01 (Jäljitettävyys ja havainnointikyky).

Toisaalta tietojärjestelmän eheyden suojaamisen (1101/2019 / 11 § / kohta 4) keskeisenä menetelmänä on fyysinen turvallisuus, johon soveltuvat suoraan kohdat FT-01 (Monitasoinen suojaaminen ja riskienhallinta), FT-02 (Rakenteet ja turvallisuusjärjestelmät), FT-03 (Luvattoman pääsyn estäminen), FT-04 (Palveluntuottajat ja vierailijat) ja FT-05 (Varautuminen ja jatkuvuudenhallinta). Fyysisen suojauksen ulkopuolella eheyssuojauksissa huomioitava salauksen (SA-02) lisäksi puolestaan muun muassa IP-03 (Hallintayhteydet) ja JT-05 (Suojattavien kohteiden siirtäminen ja poistaminen).

Viranomainen B on selkeästi myös havainnut, että monitasoisen suojauksen (1101/2019 / 7 §) toteuttaminen edellyttää toisiaan tukevia suojauksia sekä turvallisuusjohtamiseen, että fyysiseen ja tietoteknisen turvallisuuteen, esimerkiksi tietoliikenneverkon rakenteen moniportaista jakamista ja valvontaa (TT-01: Tietoliikenneverkon rakenne / kohdat 2-3).

Liite 3: Viranomaisarviointi ja -hyväksyntä

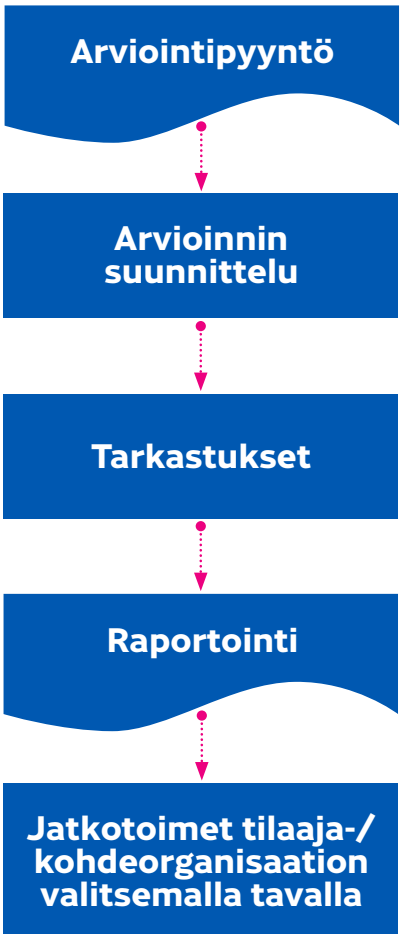
Tausta

Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista[36] mukaisesti viranomaiset saavat käyttää tietojärjestelmiensä tietoturvallisuuden arvioinnissa Liikenne- ja viestintävirasto Traficomia tai sen hyväksymää tietoturvallisuuden arviointilaitosta[37]. PiTuKria voidaan käyttää työkaluna selvitettäessä, miten viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman pilvipalvelupohjaisen tietojärjestelmän tietoturvallisuudesta on huolehdittu suhteessa kansallisen tai kansainvälisen tiedon suojaustarpeisiin[38].

Tässä liitteessä kuvataan PiTuKrin eri käyttötapauksia pilvipalvelupohjaisten tietojärjestelmien arvioinneissa. Kuvauksessa keskitytään yritysturvallisuusselvityksen ja viranomaisten tietojärjestelmien arvioinnin käyttötapauksiin, joissa toimivaltaisena viranomaisena on Traficom. Kuvaus on jaoteltu arviointi- ja hyväksyntäprosessien sekä viranomaishyväksynnän esittelyyn. Kuvauksessa ei käsitellä muita käyttötapauksia, esimerkiksi käyttöä osana organisaation sisäistä turvallisuustyötä.

Arviointiprosessi

Tietojärjestelmien turvallisuuden arviointiprosessi (L 1406/2011) alkaa, kun arvioinnin kohde toimittaa Traficomille arviointipyynnön. Arviointiprosessin keskeisiä muita vaiheita ovat arvioinnin suunnittelu, tarkastukset sekä raportointi. Arviointiprosessia on havainnollistettu yksinkertaistetussa muodossaan kuvassa 4. Arviointiprosessia voidaan hyödyntää esimerkiksi kohdeorganisaation sisäisen turvallisuustyön tukena, jättäen muun muassa jäännösriskien käsittelyn täysin kohdeorganisaation vastuulle. Arviointiprosessia kuvataan yksityiskohtaisemmin ohjeessa ”NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma”[39].



Kuva 4. Arviointiprosessi yksinkertaistettuna

[36] Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), https://www.finlex.fi/fi/laki/alkup/2011/20111406. Laki liikenne- ja viestintäministeriön hallinnonalan virastouudistuksen täytäntöönpanoa sekä virastojen tehtävien uudelleenorganisointia koskevan lainsäädännön voimaanpanosta (937/2018), https://www.finlex.fi/fi/laki/smur/2018/20180937.

[37] Laki tietoturvallisuuden arviointilaitoksista (L 1405/2011), https://www.finlex.fi/fi/laki/ajantasa/2011/20111405.

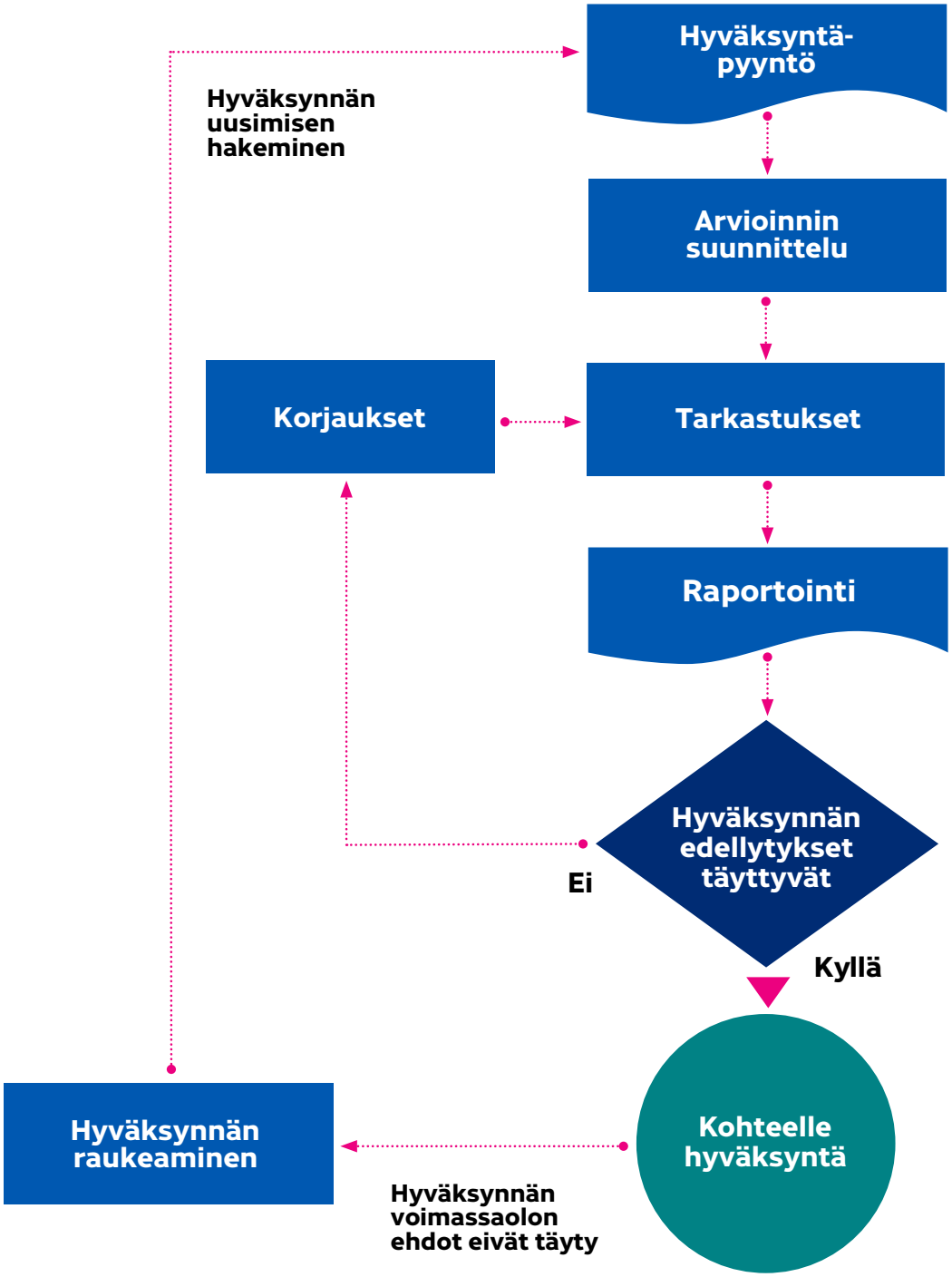
[38] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588. Turvallisuusselvityslaki (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

[39] Kyberturvallisuuskeskus. 2019. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

Hyväksyntäprosessi

Liikenne- ja viestintävirasto Traficomin hyväksyntään tähtäävä hyväksyntäprosessi (L 588/2004 tai 1406/2011) alkaa, kun arvioinnin kohde toimittaa Traficomille hyväksyntäpyynnön. Hyväksyntäprosessi mukailee arviointiprosessia sillä keskeisellä erolla, että tarkastuksissa mahdollisesti havaittujen poikkeamien tulee olla todennetusti korjattuja ennen, kuin hyväksyntä voidaan myöntää. Hyväksyntäprosessia on havainnollistettu yksinkertaistetussa muodossaan kuvassa 5. Hyväksyntäprosessia voidaan hyödyntää esimerkiksi silloin, kun arvioinnin kohde haluaa osoittaa tietojärjestelmänsä suojausten riittävyyden Traficomin hyväksynnällä. Hyväksyntäprosessissa riskienarviointi toteutetaan hyödyntäen sekä kohdeorganisaation, että Traficomin arvioita. Hyväksyntäprosessia kuvataan yksityiskohtaisemmin ohjeessa “NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma”.

Kuva 5. Hyväksyntäprosessi yksinkertaistettuna



Viranomaishyväksyntä

Liikenne- ja viestintävirasto Traficom voi myöntää vaatimukset täyttävälle kansallista tai kansainvälistä turvallisuusluokiteltua tietoa käsittelevälle järjestelmälle hyväksynnän (accreditation). Hyväksynnän myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason säilyttämiseen. Hyväksyntä edellyttää tyypillisesti[40] myös sitä, että järjestelmä on kokonaisuudessaan Suomen lainsäädännön alaisuudessa.

Hyväksynnän voimassaolo 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 raukeamista. Tapauskohtaiset ehdot hyväksynnän raukeamiselle määritellään hyväksynnän myöntämisen yhteydessä. Merkittävät muutokset tulee hyväksyttää etukäteen Traficomilla.

[40] Poikkeuksena esimerkiksi kansainväliseen viranomaisyhteistyöhön liittyvät järjestelmähankkeet, joissa järjestelmäkokonaisuuksien osien tarkastamisen ja hyväksyntien toimivallasta ja vastuusta on kyseiseen viranomaisyhteistyöhön osallistuvien jäsenmaiden turvallisuusviranomaisten kesken erikseen toisin sovittu.

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi

Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus