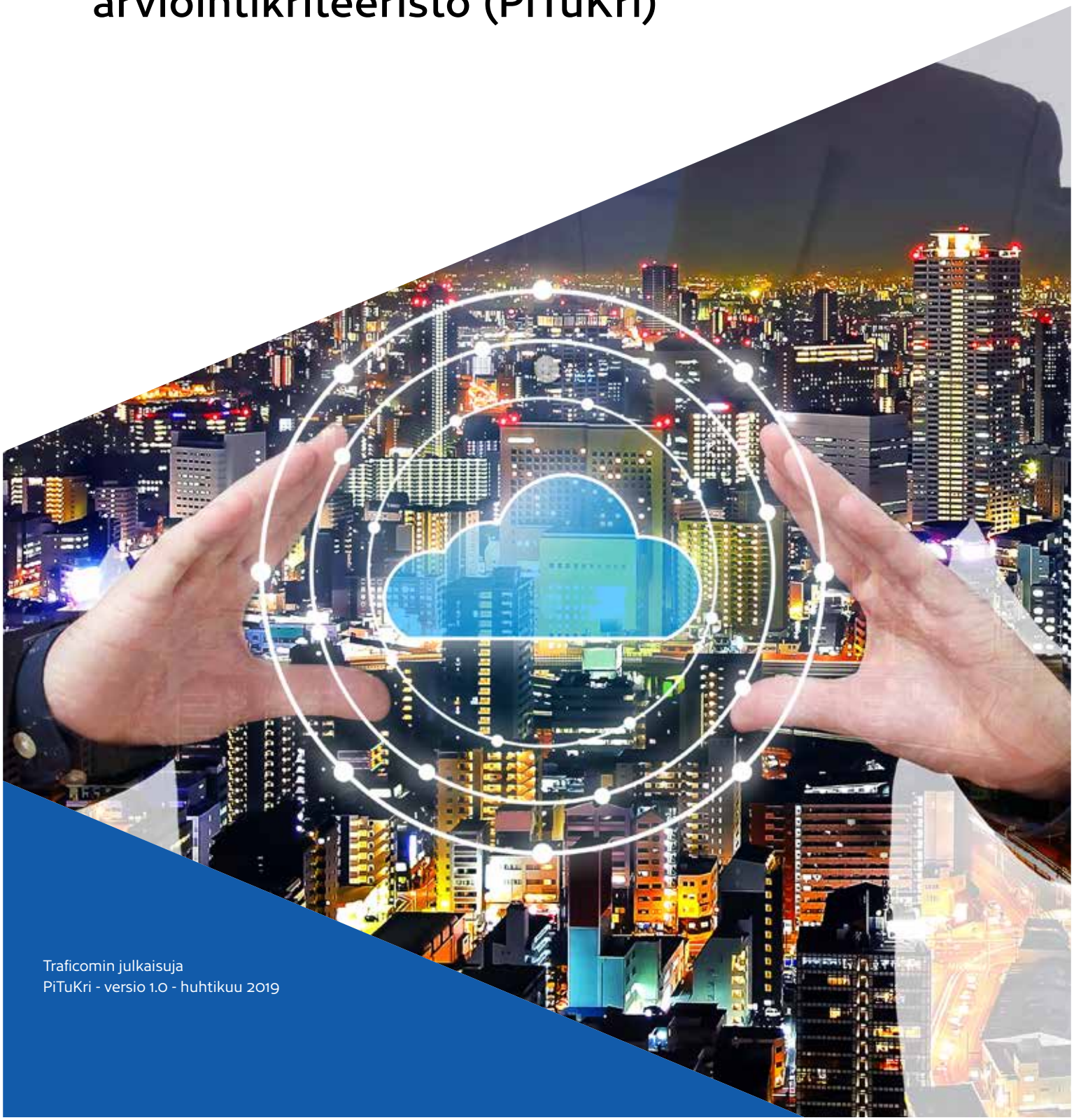
TRAFICOM
Kyberturvallisuuskeskus

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)



Traficomin julkaisuja
PiTuKri - versio 1.0 - huhtikuu 2019

Sisältö

Liikenne- ja viestintävirasto Traficom
Kyberturvallisuuskeskus
ISBN 978-952-311-328-2 (verkkojulkaisu)

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 myös uusiutuvaa lainsäädäntöä[1].

Laadinnassa on hyödynnetty erityisesti BSI:n pilviturvallisuuskriteeristöä[2], CSA-pilviturvallisuusyhteisön suojausmatriisia[3], ISO27001[4]- ja ISO27017[5]-standardeja, sekä Katakri-kriteeristöä[6]. Kriteeristön tavoitteena on myös tukea ja konkretisoida Valtiovarainministeriön julkisen hallinnon pilvipalveluiden linjausten käyttöönottoa[7].

Kriteeristö ottaa kantaa sekä viranomaisen turvallisuusluokiteltuihin IV-luokan salassa pidettäviin tietoihin, että muihin kuin turvallisuusluokiteltuihin salassa pidettäviin tietoihin. 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.

Kyberturvallisuuskeskus jatkaa kriteeristön kehitystä. Kyberturvallisuuskeskus kerää kriteeristöön palautetta ja jatkokehitystoiveita, mitkä tullaan huomioimaan kriteeristön päivitetyissä versioissa. Kriteeristön käyttöön tullaan julkaisemaan myös tukityökaluja ja lisätietoaineistoja.

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. Kriteeristössä kuvatut vaatimukset voivat joissain käyttötapauksissa olla perusteltua kohdentaa vain pilvipalveluntarjoajan vastuulla olevaan osuuteen, joissain sekä pilvipalveluntarjoajan että pilvipalvelun asiakkaan osuuksiin, ja joissain vain asiakkaan vastuulla olevaan osuuteen. Tarkoituksenmukainen käyttö edellyttää riittävää osaamista turvallisuuden arvioijalta, pilvipalveluntarjoajalta ja pilvipalvelun asiakkaalta.

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[8]. Lisätietoja pilvipalvelujen arviointiin liittyvistä haasteista sekä myös joitain ehdotettuja ratkaisumalleja on saatavissa esimerkiksi EU-SEC -hankkeen[9] 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 (tiedon omistava viranomainen) 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.

[1] Hallintovaliokunta. 2019. URL: https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_38+2018.pdf.

[2] 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.

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

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

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

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.

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 käytettävyyteen (saatavuuteen) vaikuttaa useampi tekijä, joista yhdenkin häiriintyminen voi estää palvelun käytön. Esimerkiksi alustakerroksen käytettävyyspuutteet voivat estää sovelluskerrosta tarjoamasta palvelua asiakkaalle. Vastaavasti vaikka alustakerros olisi toteutettu korkeaa käytettävyyttä 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. Esimerkkejä kriteeristön soveltamisesta on kuvattu liitteessä 1.

Käyttötapauksissa, joissa tavoitteena on saada pilvipalvelualustalle tai siihen sijoitetulle asiakasjärjestelmälle toimivaltaisen viranomaisen myöntämä hyväksyntä, 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. Kyberturvallisuuskeskuksen NCSA-toiminnon arviointi- ja hyväksyntäprosessia on kuvattu yksityiskohtaisemmin liitteessä 2.

Rakenne

PiTuKri on jaettu kymmeneen osa-alueeseen. Osa-alue 1, esiehdot, on erityisasemassa muihin osa-alueisiin nähden. Esiehdot määrittävät jatkoarvioinnin mahdollisuuksia ja tukevat kansallisen 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.

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 vain turvallisuusluokitellun tiedon suojaamiseen, osa myös muun salassa pidettävän tiedon suojaamiseen. Vaatimusten kohdistuminen kullekin tietotyypille on kuvattu yksityiskohtaisesti kunkin vaatimuksen yhteydessä.

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

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

[8] Kyberturvallisuuskeskus. 2018. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-NCSA-toiminnon-suorittamat-tietoturvallisuustarkastukset.pdf.

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

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.

Tietotyyppi	Kuvaus
Julkinen	Julkinen tieto. Suojaamistarpeet tyypillisesti eheyden ja käytettävyyden (saatavuuden) näkökulmista.
Salassa pidettävä	Viranomaisen salassa pidettävä tieto, jota ei ole turvallisuusluokiteltu ja joka ei sisällä henkilötietoja. Kattaa (kriteeristön julkaisuhetkellä huhtikuussa 2019) voimassa olevan lainsäädännön mukaiset turvallisuusluokittelemattomat suojaustason IV tiedot, sekä uusiutuvan lainsäädännön[10] mukaiset turvallisuusluokittelemattomat salassa pidettävät tiedot, mitkä eivät sisällä henkilötietoja.
Henkilötieto	Henkilötietojen suojaamiseen liittyvän erityislainsäädännön (ml. EU:n yleinen tietosuoja-asetus[11]) alaiset tiedot. Useimmat viranomaisten salassa pidettävät tiedot sisältävät henkilötietoja, ja ovat siten myös henkilötietoihin liittyvän erityislainsäädännön piirissä.
TL IV	Viranomaisen turvallisuusluokitellut IV-luokan salassa pidettävät tiedot. Suojaamistarve yleensä valtion turvallisuuden (yleisen edun) näkökulmasta. Suojaamisessa huomioitava myös lainsäädäntöjohdannaiset riskit[12].
Suuri määrä salassa pidettävää tietoa (TL III -kasauma)	Kasautumisvaikutuksen tulkitaan muodostavan turvallisuusluokitellun III-tason tietovarannon. Esimerkiksi valtionhallinnon turvallisuusviranomaisten kattavat henkilötiedot, tai/ja muut viranomaisen operaatioturvallisuuden vaarantavat henkilötiedot.
Suuri määrä TL IV tietoa (TL III -kasauma)	Kasautumisvaikutuksen tulkitaan muodostavan turvallisuusluokitellun III-luokan tietovarannon.
Varautuminen	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Poikkeavilla olosuhteilla tarkoitetaan tässä tilannetta, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle.
TL III ja II	Viranomaisen turvallisuusluokitellut III- tai/ja II-luokan 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. PiTukrin tarkoituksenmukainen käyttö edellyttää käsiteltävien tietotyyppien tunnistamista ja kuhunkin käyttötapaukseen liittyvien riskien arviointia.

[10] Hallintovaliokunta. 2019. URL: https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/HaVM_38+2018.pdf.

[11] Euroopan parlamentin ja neuvoston asetus 2016/679. 2016. URL: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI.

[12] 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 sekä muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia.


880120
574854
212165
64165

Pilvipalvelujen ominaispiirteitä

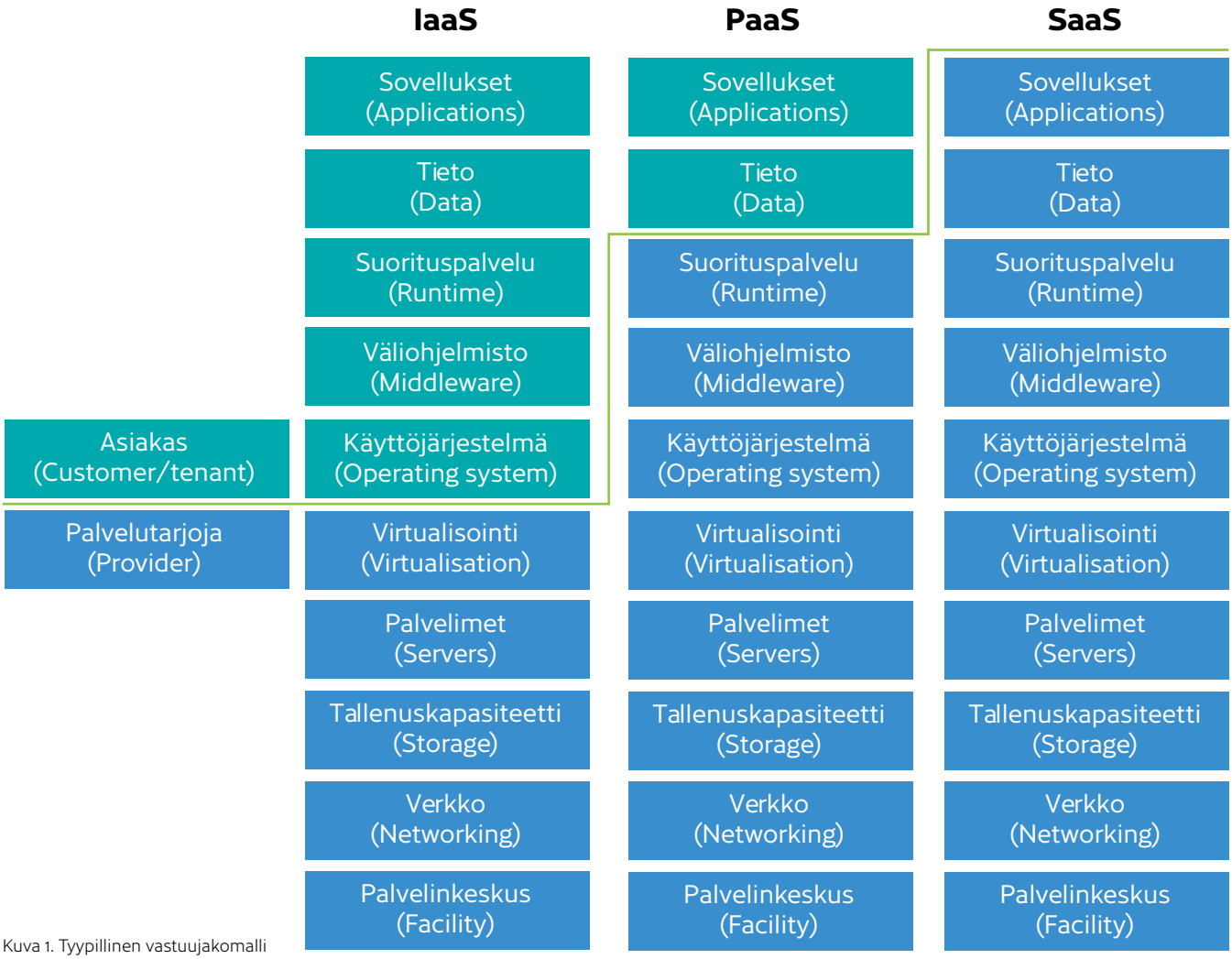
Tässä luvussa esiteltävät pilvipalveluihin liittyvät kuvaukset pohjautuvat NIST:in[13] määritelmissä ja Valtiovarainministeriön julkisen hallinnon pilvilinjauksissa käytettyihin käsitteisiin. PiTuKrissa käsitteitä tarkennetaan turvallisuuden näkökulmasta suhteuttaen ne riskilähtöiseen pilvipalveluiden 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. Tyypillistä vastuujakoa on havainnollistettu kuvassa 1.



Kuva 1. Tyypillinen vastuujakomalli

[13] 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 tietojen luotettava erottelu 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 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.

Palvelun tuottaminen

Pilvipalvelutuottajalla on tyypillisesti pääsy kaikkeen palvelussa selväkielisessä muodossa käsiteltävään tietoon. Erilaisiin palvelutuottajiin kohdistuu erilaisia riskejä. Palvelutuottajat 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 osana. Tilanteissa, joissa palvelun tuottamiseen osallistuu useita organisaatioita[14], riskit tulee arvioida ja huomioida kunkin palvelutuotantoon osallistuvan organisaation osalta.

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.

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

Osa-alue 1: Esiehdot

EE 01	Järjestelmäkuvaus
Vaatimus	Pilvipalvelusta tulee olla järjestelmäkuvaus. Kuvauksen perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen 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 palveluntarjoajan välillä. Sisältäen myös yhteistyövelvollisuuden sekä pilvipalvelun asiakkaan vastaavat valvontatoimet. g) Alihankkijoille siirretyt tai ulkoistetut toiminnot.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
Suojaustavoite	Kuvauksen tavoitteena on mahdollistaa palvelun yleisen soveltuvuuden ja riskien arviointi suhteessa loppuasiakkaan 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 tulee olla 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. b) Palvelun eri toimintojen (esimerkiksi ylläpito-/hallintaratkaisut, varmistukset) ja komponenttien fyysinen sijainti koko tiedon elinkaaren ajalta. c) Mahdolliset muut palvelun tuottamiseen osallistuvat tahot, esimerkiksi ulkoistukset. 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 tietojen tulee sijaita koko elinkaarensa ajan vain sopimuksessa kuvatuissa fyysisissä sijainneissa. Poikkeuksena tilanne, jossa pilvipalvelun asiakas on kirjallisesti etukäteen hyväksynyt tietojen siirron tai käsittelyn muissa fyysisissä sijainneissa.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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 sekä 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. Arvioinnissa suositellaan noudatettavan taulukossa 2 kuvattuja jatkoarvioinnin yleisperiaatteita.

Taulukko 2. Jatkoarvioinnin mahdollisuudet.

Tietotyyppi	Pilvipalvelu-tyyppi	Fyysinen sijainti	Pilvipalvelu-tarjoaja	Lisätietoja
Julkinen	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Soveltuvien suojausten arvioinnissa painotus riittävän eheyden ja käytettävyyden (saatavuuden) varmistamisessa.
Salassa pidettävä	Ei rajoitteita	Ei rajoitteita	Ei rajoitteita	Mikäli ei sisällä henkilötietoja. Mikäli sisältää, katso seuraava rivi.
Henkilötieto	Ei rajoitteita	Tietosuoja-sääntelyn mahdollistamat alueet, usein esim. EU/ETA	Ei rajoitteita	Palvelukokonaisuuden tulee täyttää henkilötietojen suojaamiseen liittyvä erityislainsäädäntö (ml. EU:n yleinen tietosuoja-asetus). Tietojen sijainti ja hallinnointi kansallisen tai/ja EU:n tietosuojasääntelyn mahdollistamalla alueella.
TL IV	Ei rajoitteita	Suomi	Kansallinen	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 tietoa (TL III -kasauma[15])	Yksityinen / yhteisö[16]	Suomi	Kansallinen	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. Vrt. Katakri 2015 (I 01 / Lisätietoja / Kasautumisvaikutus).
Suuri määrä TL IV tietoa (TL III -kasauma)	Yksityinen / yhteisö	Suomi	Kansallinen	Tietoon ei saa olla suoraa tai epäsuoraa pääsyä muiden valtioiden viranomaisilla. Fyysinen sijaintirajaus kattaa myös hallinnointi-, varmistus- ja muut ylläpitoratkaisut. Palveluntarjoajan turvallisuus 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. Vrt. Katakri 2015 (I 01 / Lisätietoja / Kasautumisvaikutus).
Varautuminen	Ei rajoitteita	Suomi	Kansallinen	Tietoon kohdistuu tarve olla käytettävissä myös poikkeavissa olosuhteissa (varautuminen). Tiedon hallinnoinnin oltava mahdollista tilanteessa, jossa yhteiskunnan verkkoyhteydet on rajoitettu Suomen maantieteellisten rajojen sisäpuolelle. Palveluntarjoajan turvallisuus voidaan selvittää (esimerkiksi kansallisen yritysturvallisuusselvityksen osana).
TL III ja II	Yksityinen / yhteisö	Suomi	Kansallinen	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, vrt. Katakri 2015.

[15] Kasautumisvaikutuksen tulkitaan muodostavan turvallisuusluokitellun III-luokan tietovarannon. Esimerkiksi valtionhallinnon turvallisuusviranomaisten kattavat henkilötiedot, tai/ja muut viranomaisen operaatioturvallisuuden vaarantavat henkilötiedot.

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

Osa-alue 2: Turvallisuusjohtaminen

TJ 01	Turvallisuusperiaatteet
Vaatimus	1) Pilvipalveluntarjoajalla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat pilvipalveluntarjoajan 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
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 tulee olla nimetty.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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 turvallisuusvastuut 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) Pilvipalveluntarjoajalla 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 on otettava huomioon tarvittavien sidosryhmien osalta. Pilvipalveluntarjoajan tulee varmistaa, että asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään pilvipalveluntarjoajan toimeksiannosta. Vrt. TJ 08 (Palveluntarjoajien ja toimittajien turvallisuus). 5) Riskienhallintaprosessia ja sen tuloksia hyödynnetään pilvipalveluntarjoajan turvallisuus tavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. 6) Turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon suojaustaso, määrä, muoto, luokitteluperuste ja sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. 7) Pilvipalveluntarjoaja dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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** Pilvipalveluntarjoajan tulee tunnistaa, mitä lainsäädännön tai viranomaisen vaatimuksia omaan toimintaan liittyy. Näiden vaatimusten täyttäminen, esimerkiksi viranomaisen hyväksynnän saamiseksi, voi edellyttää pilvipalveluntarjoajan 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 kohdistuvia 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	Turvallisuuspoikkeamien hallinta
Vaatimus	1) Pilvipalveluntarjoajalla tulee olla menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn. 2) Pilvipalveluntarjoajalla tulee olla käytössään selkeät prosessit turvallisuuspoikkeamien ilmoittamisesta. Organisaatiossa tulee olla määritettynä henkilöt/tahot, joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa. 3) Turvallisuuspoikkeamien määrää ja tyyppejä tulee seurata. Toteutuneiden poikkeamien uusiutuminen on pyrittävä estämään korjaussuunnitelmissa. 4) Asiakastiedon käsittelyyn liittyvät poikkeamat tai niiden epäilyt tulee ilmoittaa kyseiselle asiakkaalle.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
Suojaustavoite	Turvallisuuspoikkeamien 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: Turvallisuuspoikkeamien 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 poikkeamista, tietomurroista tai sellaisten yrityksistä suositellaan ilmoittamaan Kyberturvallisuuskeskukselle. Tunnistetusta rikollisesta toiminnasta suositellaan ilmoittamaan myös poliisille.

TJ 05	Jatkuvuudenhallinta
Vaatimus	Jatkuvuudenhallinnan prosessit ja menettelyt on suunniteltu, toteutettu, testattu ja kuvattu siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Järjestelyissä tulee huomioida 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 käytettävyyden (saatavuuden) menettäminen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
Suojaustavoite	Jatkuvuudenhallinnan tavoitteena on varmistaa palvelun jatkuvuus siten, että pystytään vastaamaan siihen kohdistuneisiin käytettävyys-, 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 (Varmuuskopiointi).

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
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 2 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 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.

TJ 07	Vaatimustenmukaisuus ja tietosuoja
Vaatimus	1) Pilvipalveluntarjoajan on tunnistettava, dokumentoitava ja päivitettävä säännöllisesti pilvipalveluun sovellettavien lakien ja säädösten määräykset sekä menettelyt näiden noudattamiseksi. 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. Arviointisuunnitelman tulee kattaa palvelun turvallisuus siten, että kaikki keskeiset turvallisuuteen vaikuttavat kokonaisuudet tulee arvioitua 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
Suojaustavoite	Lainsäädännöllisten ja sopimusvelvoitteiden täyttäminen.
Lisätietoja	Pilvipalveluntarjoajan tulee huolehtia esimerkiksi henkilötietojen käsittelyn turvallisuudesta yleisen tietosuoja-asetuksen (EU) 2016/679 32 artiklan mukaisesti. 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. Henkilötietojen suojaamista Suomessa valvova viranomainen on tietosuojavaltuutetun toimisto (TSV). Henkilötietojen merkittävistä loukkauksista tulee ilmoittaa sekä TSV:lle, että 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 viestintävirasto Traficomille ja käyttäjille. Vrt. TJ 04 (Turvallisuuspoikkeamien hallinta).

TJ 08	Palveluntarjoajien ja toimittajien turvallisuus
Vaatimus	Pilvipalveluntarjoajan tulee varmistaa, että asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään pilvipalveluntarjoajan toimeksiannosta. Varmistettava erityisesti, että a) ennen palveluntarjoajan/toimittajan henkilöstön pääsyä suojattaviin kohteisiin, tulee henkilöstön olla läpikäynyt vastaavat suojaustoimenpiteet (sopimukset, salassapitositoumukset, turvaselvitykset, koulutukset), kuin pilvipalveluntarjoajankin, b) palveluntarjoajat/toimittajat on kirjallisesti ohjeistettu ja sopimuksin velvoitettu noudattamaan vähintään vastaavantasoisia suojauksia, kuin pilvipalveluntarjoajakin, 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. Menettelyn tulee 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
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.

Osa-alue 3: Henkilöstöturvallisuus

HT 01	Työsuhteen elinkaaren huomioiminen
Vaatimus	Pilvipalveluntarjoajalla on käytössä turvallisuuden huomioon ottava menettely työsuhteen elinkaaren eri vaiheissa. Erityisesti tulee huomioida toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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.

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) Salassa pidettävien aineistojen käsittelyyn liittyvien henkilöiden luotettavuus selvitetään ja sitä seurataan asianmukaisen tason turvallisuusselvitysmenettelyin.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV 2: TL IV (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 suora tai epäsuora pääsy asiakkaiden suojattaviin tietoihin. Esimerkiksi virtualisointialustan (hypervisor) ylläpidolla usein käytännössä pääsy myös virtuaalikoneissa käsiteltäviin asiakkaiden tietoihin.

HT 03	Salassapito- ja vaitiolositoumukset
Vaatimus	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
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

HT 04	Turvallisuustietoisuus
Vaatimus	1) Keskeisten turvallisuuteen liittyvien periaatteiden ja toimintatapojen tulee olla kuvattuna. 2) Turvalliset toimintatavat tulee olla henkilöstölle jalkautettuna siten, että henkilöstön riittävästä turvatietoisuudesta pystytään varmistumaan. 3) Turvallisuuteen liittyvien kuvausten/ohjeistusten ajantasaisuus sekä jalkautuminen käytäntöön tulee varmistaa säännöllisesti, vähintään vuosittain. 4) Turvallisuuteen liittyvät ohjeet kattavat 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
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.

HT 05	Tiedonsaantitarpeet ja tehtävien erottelu
Vaatimus	1) Palveluntarjoaja ylläpitää luetteloa salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä. 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) Palveluntarjoaja ylläpitää luetteloa salassa pidettävien tietojen käsittelyoikeuksista suojaustasoittain. 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.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV 3-4: TL IV
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. 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.


TECHNOLOGY

Osa-alue 4: Fyysinen turvallisuus

FT 01	Monitasoinen suojaaminen ja riskienhallinta
Vaatimus	1) Fyysiset turvatoimet on toteutettu monitasoisen suojaamisen periaatetta noudattaen. 2) Tilat rakennuksessa on luokiteltu hallinnolliseksi alueeksi, turva-alueeksi tai tekniseksi turva-alueeksi ja niillä selkeästi määritellyt ja näkyvät rajat. 3) Turvatoimet on mitoitettu riittävälle tasolle siten, että ne vastaavat pilvipalveluntarjoajan riskienarvioinnissa todettuja riskejä.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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	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
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 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.

FT 03	Luvattoman pääsyn estäminen
Vaatimus	1) Kulkua arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältäviin tiloihin tai rakennuksiin suojataan ja valvotaan sähköisen kulunvalvontajärjestelmän 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
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.

FT 04	Palveluntuottajat ja vierailijat
Vaatimus	1) Vierailijat tunnistetaan, varustetaan vierailijakortilla ja kirjataan. Pilvipalveluntarjoajalla 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 tietoihin käsiksi pääsevät palveluntuottajat on turvallisuusselvitetty. Henkilöt, joita ei pystytä tai ehditä turvallisuusselvittää, 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
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 huomioida 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. Tilan tai rakennuksen kytkeminen 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. Automaattiset sammutusjärjestelmät, jotka havaitsevat esim. tulipalon aikaisessa vaiheessa ja aloittavat alkusammutuksen. v. Sähkön häiriötön saanti varmistettava sähkönsyötön turvaavilla laitteilla (UPS, varavoima). vi. Tietoliikenteen varmistukset, tietojärjestelmien kahdennukset, varmuuskopiointi 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
Suojaustavoite	Pilvipalvelun konesalien (ja vastaavien) toiminnan jatkuvuus on suojattu yleisiä riskejä vastaan.
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 käytettävyydessä 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 (Varmuuskopiointi). Mikäli järjestelmän toimintavaatimukset ovat korkeat, on järjestelmien käytettävyys 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
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	Suojattavaa tietoa käsittelevä tietojenkäsittely-ympäristö tulee erottaa muista ympäristöistä. Ulkoreunan erotteluun tulee käyttää oikein konfiguroitua palomuuria tai vastaavaa verkkolaitetta. Myös erotteluun käytettävä palomuuri (tai vastaava verkkolaite) tulee suojata luvattomalta pääsyltä. Käytettävyyden 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 KT 05 (Etäkäyttö ja -hallinta). Toisaalta ohjelmistokoodiin nojautuva toteutus voi tietyin rajauksin mahdollistaa ympäristön kuvauksen ja sen turvallisuuden arvioinnin versionhallinnan tukemana.

TT 02	Yleisiä verkkohyökkäyksiä vastaan suojautuminen
Vaatimus	1) Pilvipalveluntarjoajan tulee ylläpitää riskienarviointia, joka ottaa kantaa yleisiltä verkko hyökkäyksiltä suojautumiseen. 2) Suojaukset tulee mitoittaa siten, että yleiset verkkohyökkäykset eivät vaaranna palvelun tai siinä käsiteltävien tietojen luottamuksellisuutta, eheyttä tai käytettävyyttä (saatavuutta).
Soveltuvuus	Palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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.

TT 03	Hallintayhteydet
Vaatimus	1) Hallintapääsyn tulee tapahtua pilvipalveluympäristössä rajattujen, hallittujen ja valvottujen pisteiden kautta. 2) Hallintapääsyn tulee edellyttää vahvaa, useaan todennustekijään pohjautuvaa käyttäjätunnistusta. 3) Etäkäytössä hallintaliikenteen tulee olla salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. JT 08 (Salauskäytännöt ja avainhallinta). 4) Viranomaisen turvallisuusluokitellun tiedon hallinnan tulee olla mahdollista vain ko. turvallisuusluokan mukaisilta päätelaitteilta. 5) Viranomaisen turvallisuusluokitellun tiedon hallintaan tulee päästä etäkäytössä vain viranomaisen hyväksymällä menettelyllä salatulla hallintayhteydellä. KT 05 (Etäkäyttö ja -hallinta).
Soveltuvuus	Verkkolaitteet, palvelimet, sekä työasemat ja muut päätelaitteet. Kattaa sekä pilvipalvelualustan, että sen päälle tuotetun asiakasjärjestelmän.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV 4-5: TL IV
Suojaustavoite	Hallintayhteydet on suojattu riittävällä tasolla, jotta niitä hyödyntämällä ei ole asiakastietoon tai pilvipalveluun valtuuttamatonta pääsyä.
Lisätietoja	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 ja vastaavat etähallintayhteydet. Vrt. KT 05 (Etäkäyttö ja -hallinta). Erityisesti tilanteissa, joissa hallintayhteys mahdollistaa suoran tai epäsuoran pääsyn salassa pidettävään tietoon, tulisi 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 päätelaitteistä käsin. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää esimerkiksi niin sanottua hyppykone-käytäntöä, jossa kaikki hallintatoimet toteutetaan ja kirjataan (lokitetaan) hyppykoneen kautta. Etähallinnan edellytyksiä on kuvattu tarkemmin vaatimuskortissa KT 05 (Etäkäyttö ja -hallinta).

Osa-alue 6: Tietojärjestelmäturvallisuus

JT 01	Käyttöoikeushallinta
Vaatimus	Käyttöoikeuksien hallinnoinnin tulee toteuttaa vähimpien oikeuksien periaatetta: a) Käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon tulee olla ennalta määritelty prosessi. b) Tietojenkäsittely-ympäristön käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä. c) Järjestelmän käyttäjistä tulee ylläpitää listaa. Jokaisesta myönnetystä käyttöoikeudesta tulee jäädä merkintä (paperi tai sähköinen). d) Käyttöoikeuden myöntämisen yhteydessä tulee tarkistaa, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. e) Käyttöoikeuksien käsittelyn ja myöntämisen tulee olla ohjeistettu. f) Tarpeettomat käyttäjätilit ja oikeudet tulee poistaa, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan). g) Tulee olla olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. h) Käyttö- ja pääsyoikeudet tulee katselmoida säännöllisesti, vähintään puolivuosittain.
Soveltuvuus	Verkkolaitteet, palvelimet, sekä työasemat ja muut päätelaitteet.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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	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.

JT 02	Käyttäjätunnistus
Vaatimus	1) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan käyttäjät, sekä asiakkaan ylläpitokäyttäjät tulee tunnistaa ja todentaa luotettavasti ennen pääsyä suojattavaan tietoon: a) Käytössä tulee olla yksilölliset henkilökohtaiset käyttäjätunnisteet. b) Kaikki käyttäjät tulee tunnistaa ja todentaa. c) Tunnistamisessa ja todennuksessa tulee käyttää tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti. d) Käyttäjätunnusten tulee lukittua tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin. e) Järjestelmien ja sovellusten ylläpitotunnusten tulee olla henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat salasanojen hallintakäytännöt yhteiskäyttöisille tunnuksille. f) Todennus tehdään fyysisesti suojatun alueen sisällä vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, i. käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä. ii. käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. g) Hallintayhteyksien todennus tehdään etäkäytössä vahvasti, vähintään kahteen tekijään nojautuen (esimerkiksi salasana + token). Hallintayhteyden tulee olla salattu käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. JT 08 (Salauskäytännöt ja avainhallinta). 2) Viranomaisen salassa pidettävää tietoa käsittelevien palvelujen osalta lisäksi: Tilanteissa, joissa hallintayhteys kulkee fyysisesti suojatun alueen ulkopuolelle (esimerkiksi pilvipalveluntarjoajan konesalin ja ylläpidon/asiakkaan päätelaitteen välillä), tiedon/tietoliikenteen tulee olla suojattu viranomaisen hyväksymällä salausratkaisulla.
Soveltuvuus	Verkkolaitteet, palvelimet, sekä työasemat ja muut päätelaitteet.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV 2: TL IV
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.

JT 03	Jäljitettävyys ja havainnointikyky
Vaatimus	1) Luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen on toteutettu. Erityisesti: a) Tallenteiden tulee olla riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todetamiseen. b) Keskeiset tallenteet tulee säilyttää vähintään 6 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. c) Lokitiedot ja niiden kirjauspalvelut tulee suojata luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta) vähimpien oikeuksien periaatteen mukaisesti. d) Keskeiset lokitiedot tulee ohjata lokilähteistä erilliselle lokikeräimelle (tai erillisille lokikeräimille). e) Lokitietojen välitys lokilähteiden ja lokikeräimen välillä tulee toteuttaa suojatusti. Välityksen osapuolet tulee tunnistaa. Lokitiedot tulee välittää käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. JT 08 (Salauskäytännöt ja avainhallinta). Vaihtoehtoisesti lokitiedot voidaan siirtää erillisen hallintaverkon kautta. f) Kellot on synkronoitu sovitun ajanlähteen kanssa. 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 (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 havaituista poikkeamista toipumiseen.
Soveltuvuus	Tuotettavan palvelun turvallisuus kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
Suojaustavoite	Tietojen luvattoman muuttamisen ja muun luvattoman tai asiattoman tietojen käsittelyn havaitseminen ja selvittäminen, ml. tietomurtojen tutkinta ja korjaavien toimien suunnittelun tukena toimiminen.
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. 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.

JT 04	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
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.

JT 05	Tiedon erottelu
Vaatimus	Asiakkaiden salassa pidettävät tiedot säilytetään luotettavasti toisistaan eroteltuna yhteiskäyttöisissä virtuaalisissa ja fyysisissä järjestelmissä.
Soveltuvuus	Salassa pidettävän asiakastiedon käsittelyyn liittyvät verkkolaitteet, tallennusjärjestelmät, muistit, siirtomediat, ja vastaavat.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
Suojaustavoite	Asiakkaiden salassa pidettävään tietoon on pääsy vain kyseisellä asiakkaalla.
Lisätietoja	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 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 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. TA 03 (Tietoaineistojen hävittäminen). 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-in-rest) voidaan hyödyntää myös muiden turvatavoitteiden, esimerkiksi laitteistojen turvallisen hävittämisen, tukevana suojauksena. Vrt. TA 02 (Salaus fyysisesti suojatun alueen sisäpuolella) ja KT 03 (Varmuuskopiointi). 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, turvallinen erottaminen tulee varmistaa fyysisesti erillisillä verkoilla tai salatuilla virtuaalisilla tai ohjelmistopohjaisilla paikallisverkoilla. Vrt. TA 02 (Salaus fyysisesti suojatun alueen sisäpuolella).

JT 06	Haittaohjelmasuojaus
Vaatimus	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
Suojaustavoite	Asiakastiedon eheys, luottamuksellisuus tai käytettävyys on riittävällä tasolla suojattu yleisiä haittaohjelmariskejä vastaan.
Lisätietoja	Haittaohjelmariskejä vastaan voidaan suojautua esimerkiksi järjestelmien kovennusmenettelyillä (vrt. JT 04), käyttöoikeuksien rajauksilla (vrt. JT 01), järjestelmien pitämisellä turvallisuuspäivitysten tasolla (vrt. KT 04), poikkeamien havainnointikyvyllä (vrt. JT 03), 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.

JT 07	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 tapahtuvan siirron ja käsittelyn tulee tapahtua siirrettävän kohteen (luokituksen) mukaisesti. 3) Siirrettäessä asiakkaan salassa pidettävää tietoa, siirron tulee noudattaa turvallisen etäkäytön periaatteita (Vrt. KT 05: Etäkäyttö ja -hallinta).
Soveltuvuus	Asiakastietoa sisältävät laitteistot.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV 3: TL IV
Suojaustavoite	Suojattavaa asiakastietoa ei vaarannu tilanteissa, joissa sitä siirretään fyysisesti suojattujen alueiden (esimerkiksi konesalit) ulkopuolella.
Lisätietoja	Erityisesti huomioitavaa: • Tietojen turvallinen poistaminen sekä tietovälineen hävittäminen • Siirrettävien tietovälineiden salaus • Tietojen siirtäminen uudelle tietovälineelle, kun tietoväline korvataan

JT 08	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 suojauksen toteuttava menetelmä.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV 3: TL IV
Suojaustavoite	Salausmenetelmien käyttö tuottaa riittävän luotettavan suojauksen.
Lisätietoja	Salausratkaisujen arvioinnissa huomioidaan useita eri tekijöitä. Salausvahvuuden ja salausratkaisun oikeellisesta toiminnasta varmistumisen lisäksi huomioidaan muun muassa salausratkaisun käyttöympäristön uhkataso. Esimerkiksi Internetin yli liikennöitäessä uhkataso eroaa merkittävästi tilanteeseen, jossa salausta käytetään liikennöintiin hallitun ja suojatun fyysisen alueen sisällä. Muihin salausratkaisun arvioinnissa huomioitaviin tekijöihin kuuluvat esimerkiksi ko. käyttötapauksen vaatimukset tiedon salassapitoajalle ja eheydelle. Salauksen suojausvaikutus voidaan menettää osin tai täysin tilanteissa, joissa avainhallinnan heikkouksia pystytään valtuuttamattomasti hyödyntämään. Vrt. TA 01 (Salaus fyysisesti suojatun alueen ulkopuolella) ja TA 02 (Salaus fyysisesti suojatun alueen sisäpuolella). Lisätietoja on saatavissa Kyberturvallisuuskeskuksesta.

Osa-alue 7: Tietoaineistoturvallisuus

TA 01	Salaus fyysisesti suojatun alueen ulkopuolella
Vaatimus	1) Siirrettäessä asiakkaan salassa pidettävää tietoa hyväksyttyjen fyysisesti suojattujen alueiden (esimerkiksi palveluntarjoajan konesali) 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. JT 08 (Salauskäytännöt ja avainhallinta). 2) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. JT 08).
Soveltuvuus	Salausratkaisut konesalien välillä, salausratkaisut muiden matalammin suojattujen verkkojen kautta liikennöitäessä.
Tietotyypit	1: Salassa pidettävä, henkilötiedot, TL IV 2: TL IV
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, 3G) tulkitaan poistumiseksi fyysisesti suojatun alueen ulkopuolelle. Toisin sanoen radiorajapinnan käyttö rinnastetaan julkisen verkon kautta liikennöinniksi, mikä tulee huomioida erityisesti liikenteen salauksessa.

TA 02	Salaus fyysisesti suojatun alueen sisäpuolella
Vaatimus	1) Kun asiakkaan salassa pidettävää tietoa siirretään hyväksyttyjen fyysisesti suojattujen alueiden ja kyseisen turvallisuustason verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää, mikäli tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin. Vrt. JT 05 (Tiedon erottelu). 2) Asiakkaiden salassa pidettävät tiedot tulee tallentaa pilvipalveluun salatussa muodossa, mikäli käytetään yhteiskäyttöistä laitteistoa. Vrt. JT 05 (Tiedon erottelu). 3) Salausavaimistojen tulee olla asiakaskohtaisesti eroteltuja. 4) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. JT 08).
Soveltuvuus	Asiakastiedon käsittely-ympäristöt pilvipalvelukokonaisuudessa, mukaan lukien esimerkiksi levyjärjestelmä- ja varmistusratkaisut.
Tietotyypit	1-3: Salassa pidettävä, henkilötiedot, TL IV 4: TL IV
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 hävitysprosessia tai tehtävien erottelua. Vrt. JT 05 (Tiedon erottelu). Erityisesti pilvipalvelujen skaalautuvuuden ja asiakaskohtaisen erottelun yhdistämiseen salaus on usein suositeltava toteutustapa.

TA 03	Tietoaineistojen hävittäminen
Vaatimus	1) Tietoaineistojen hävittäminen on järjestetty luotettavasti. Hävittämisessä käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain. Hävittämisen tulee kattaa koko salassa pidettävän tiedon elinkaaren siltä osin, kun tieto on ollut pilvipalvelussa. 2) Asiakkaan salassa pidettävät tiedot tulee hävittää luotettavasti erityisesti seuraavissa tilanteissa: a) Asiakkaan pyytäessä tietojensa hävittämistä. b) Asiakkaan sopimuksen päättyessä. c) Laitteistohuollon, -ylläpidon ja -vaihdon tapauksissa (esimerkiksi asiakkaan salassa pidettävää tietoa sisältävän rikkoontuneen levyn vaihto).
Soveltuvuus	Asiakkaan suojattavaa tietoa sisältäneet tallennemediat ja vastaavat järjestelmät.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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 pilvipalvelun saavutettavista.
Lisätietoja	**Hävittäminen 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. **Hävittäminen ylikirjoittamalla** Hävittämiseen voidaan hyödyntää asiakkaan salassa pidettävää tietoa sisältäneiden muistialueiden ylikirjoittamista. Tällöin tulee huomioida erityisesti käytetyn ylikirjoitusmenetelmän soveltuvuus kyseiselle tallennemedialle sekä prosessi vastuutahoineen. Sähköisten aineistojen hävittämistä on kuvattu yksityiskohtaisemmin Kyberturvallisuuskeskuksen ylikirjoitusohjeessa (www.ncsa.fi > Ohjeita > ”Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö”). **Hävittäminen eri menetelmiä yhdistäen** Hävittämiseen 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. Mikäli salassa pidettävät tiedot tallennetaan pilvipalveluun vain riittävän luotettavaksi arvioidussa salatussa muodossa (vrt. TA 02: Salaus fyysisesti suojatun alueen sisäpuolella), jäännösriskit saattavat olla joillekin tietotyypeille hyväksyttävissä, mikäli salaukseen käytetty avaimisto pystytään luotettavasti hävittämään. **Sähköisten aineistojen hävittämisessä huomioon otettavaa** Erityisesti sähköisten aineistojen luotettavan hävittämisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän salassa pidettävän tiedon luotettavasta hävittämisestä 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 (TA 02: Salaus fyysisesti suojatun alueen sisäpuolella).

Osa-alue 8: Käyttöturvallisuus

KT 01	Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi
Vaatimus	1) Pilvipalvelusta tulee olla kattavat järjestelmäkuvaukset sekä ohjeet palvelun turvalliseen ylläpitoon ja hallinnointiin. Kuvausten ja ohjeistuksen tulee olla sellaisella tasolla, että niiden avulla pystytään uskottavasti välttämään käytön aikaiset virheet sekä varmistumaan sopimusvelvoitteiden mukainen palautuminen häiriötilanteista. 2) Järjestelmäkuvaukset ja ohjeet tulee pitää ajan tasalla. 3) Järjestelmäkuvausten ja ohjeiden tulee olla henkilöstölle jalkautettuna ja saatavilla roolien mukaisesti.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
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.

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) Pilvipalvelun asiakas kykenee valvomaan ja seuraamaan hallintaansa ja käyttöönsä annettujen järjestelmäresurssien (esim. tietojenkäsittely- tai tallennuskapasiteetin) jakelua estääkseen resurssien ruuhkautumisen.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	Salassa pidettävä, henkilötiedot, TL IV
Suojaustavoite	Tavoitteena se, että palvelutasosopimusten mukainen palvelutaso pystytään luotettavasti tarjoamaan.
Lisätietoja	Suorituskykytarpeen seuranta tukee mahdollisuuksia tulevien tarpeiden arvioinnissa, käyttöasteen optimointia, sekä myös palvelutasosopimusten mukaisten velvoitteiden täyttämistä.

KT 03	Varmuuskopiointi
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 sijainnin tulee olla fyysisen ja loogisen pääsynhallinnan osalta vähintään vastaavalla tasolla. d) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun alueen ulkopuolelle (esimerkiksi pilvipalveluntarjoajan toiseen konesaliin) verkon välityksellä, tiedon/tietoliikenteen tulee olla salattuna käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. JT 08 (Salauskäytännöt ja avainhallinta). e) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun alueen ulkopuolelle siirtomedialla (esimerkiksi varmistusnauhat tai -levyt), siirtomedia siirretään jatkuvan valvonnan alaisuudessa. Siirtomedialle tai sen sisältämälle tiedolle suositellaan salausta. f) Varmistusmediat hävitetään luotettavasti (vrt. TA 03: Tietoaineistojen hävittäminen). 3) Viranomaisen turvallisuusluokiteltua tietoa sisältävien varmuuskopioiden osalta lisäksi huomioitava: a) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun alueen ulkopuolelle (esimerkiksi pilvipalveluntarjoajan toiseen konesaliin) verkon välityksellä, tiedon/tieto liikenteen tulee olla suojattu viranomaisen hyväksymällä salausratkaisulla. b) Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, erottelumenettelyt (esimerkiksi salaus tai/ja fyysisesti erilliset tallennejärjestelmät ja -mediat) on toteutettava varmistusjärjestelmän liittymien ja tallennemedioiden osalta. Vrt. JT 05 (Tiedon erottelu) ja TA 02 (Salaus fyysisesti suojatun alueen sisäpuolella).
Soveltuvuus	Pilvipalvelun varmistus- ja palautusprosessit. Huomioitava myös tilanteet, joissa osa prosesseista riippuvaisia asiakasjärjestelmän toteutuksesta.
Tietotyypit	1-2: Salassa pidettävä, henkilötiedot, TL IV 3: TL IV
Suojaustavoite	Asiakastiedon käytettävyyden, 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.

KT 04	Haavoittuvuuksien hallinta
Vaatimus	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: Muutostenhallinta). b) Järjestelmät tarkistetaan tunnettujen haavoittuvuuksien varalta automaattisesti vähintään kuukausittain. Jos suunnitelluista asetuksista tai turvapäivitystasosta on poikettu, syyt analysoidaan, ja poikkeamat korjataan tai dokumentoidaan poikkeama hallintaprosessin mukaisesti (ks. TJ 04: Turvallisuuspoikkeamien hallinta). 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
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.

KT 05	Etäkäyttö ja -hallinta
Vaatimus	1) Järjestelmien etäkäyttö- ja etähallintaratkaisu edellyttää vahvaa, vähintään kahteen tekijään perustuvaa käyttäjätunnistusta. 2) Etäkäyttö- ja etähallintaliikenne on salattu käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. JT 08 (Salauskäytännöt ja avainhallinta). 3) Etähallinta on mahdollista vain keskitetysti hallitun ja valvotun pisteen, niin sanotun hyppykoneen kautta. 4) Elleivät hyväksyttyjen fyysisesti suojattujen alueiden ulkopuolelle viedyt asiakastietoa sisältävät tietovälineet (kiintolevyt, USB-muistit ja vastaavat) ole salattuja käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia, tietovälineet säilytetään vastaa vantasoisesti suojaten, kuin hallinnollisen turva-alueen lukittavissa toimistokalusteissa säilytettynä, tai tietovälineitä ei jätetä valvomatta. Vrt. JT 08 (Salauskäytännöt ja avainhallinta) ja FT 01 (Monitasoinen suojaaminen ja riskienhallinta). Viranomaisen turvallisuusluokitellun tiedon käsittelyssä lisäksi: 5) Vain käyttöympäristöön hyväksyttyjä, kyseisen turvallisuusluokan mukaisia laitteita ja etäyhteyksiä käytetään. 6) Etäkäyttö ja etähallintaratkaisu edellyttää viranomaisen ko. turvallisuusluokalle hyväksymää liikenteen salausta. 7) Tietovälineiden salauksen tulee olla viranomaisen hyväksymä.
Soveltuvuus	Pilvipalveluympäristön etäkäyttöön ja etähallintaan käytettävät järjestelmät, ml. päätelaitteet.
Tietotyypit	1-4: Salassa pidettävä, henkilötiedot, TL IV 5-7: TL IV
Suojaustavoite	Etäkäyttö- ja etähallintayhteydet on suojattu riittävällä tasolla, jotta niitä hyödyntämällä ei ole asiakastietoon tai pilvipalveluun valtuuttamatonta pääsyä.
Lisätietoja	Etäkäytöllä/-hallinnalla tarkoitetaan fyysisesti suojattujen alueiden tai epäluotetun verkon kautta tapahtuvaa tietojärjestelmien käyttöä/hallintaa. Normaalisti päätelaitteena toimii organisaation henkilön käyttöön antama kannettava tietokone. 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. Etäkäytöksi tulkitaan pilvipalvelun asiakkaan päätelaitteelta tapahtuva pilvipalveluun sijoitetun järjestelmän käyttö. Riittävän jäljitettävyyden toteuttamisessa voidaan hyödyntää esimerkiksi niin sanottua hyppykone-käytäntöä, jossa kaikki hallintatoimet toteutetaan ja kirjataan (lokitetaan) hyppykoneen kautta. Turvallisuusluokiteltua tietoa sisältävän pilvipalvelualustan hallinnointi tulee rajata kyseisen turvallisuusluokan vaatimukset täyttäviin päätelaitteisiin. Huomioitava, että myös päätelaitteiden hallinnointiratkaisujen tulee täyttää kyseisen turvallisuusluokan vaatimukset.

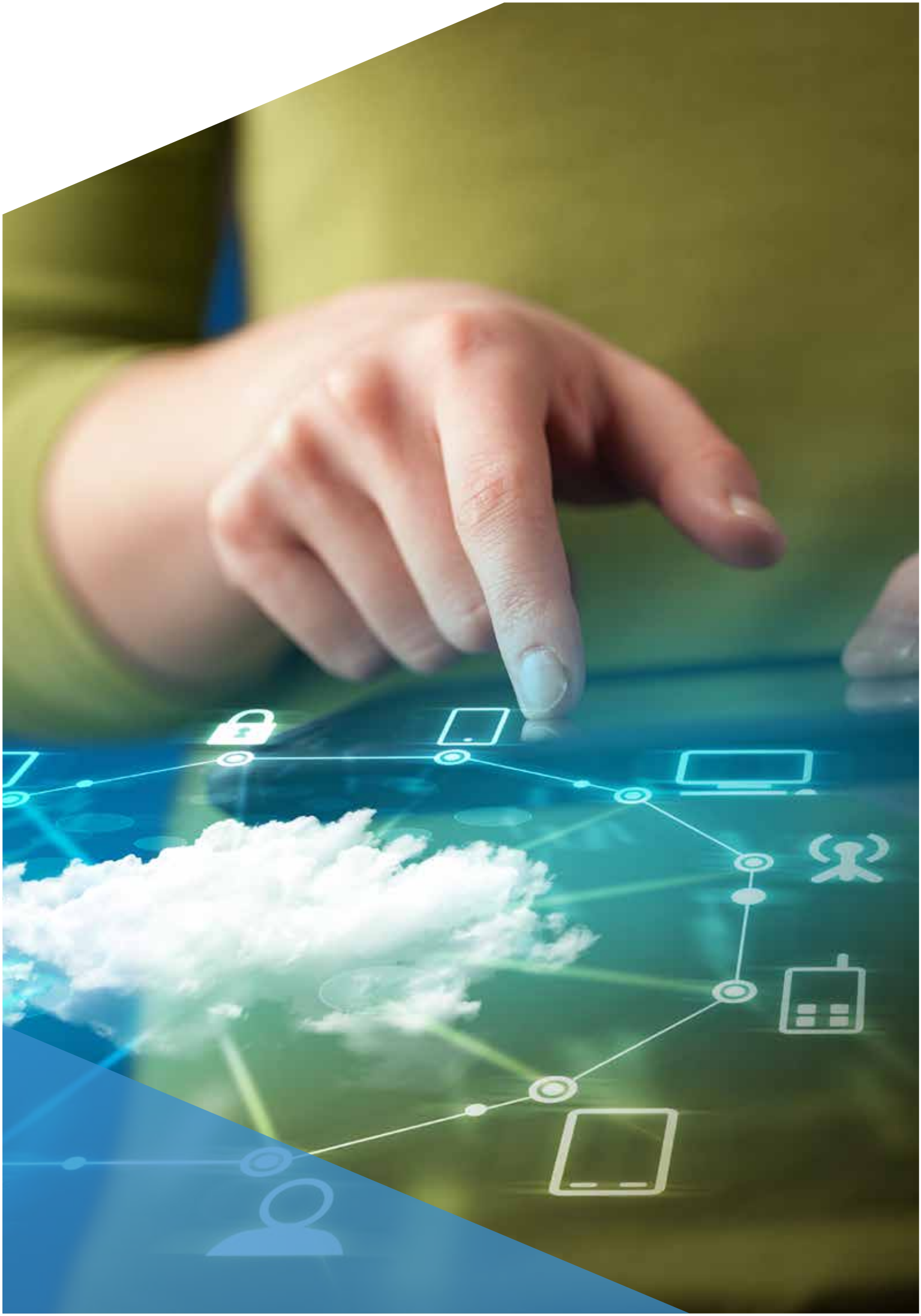
Osa-alue 9: Siirrettävyys ja yhteensopivuus

SI 01	Siirrettävyys ja yhteensopivuus
Vaatimus	1) Pilvipalvelun ohjelmointirajapintojen (API, Application Programming Interface) tulee olla julkaistuja siten, että ne mahdollistavat yhteentoimivuuden eri ohjelmistokomponenttien ja ohjelmistojen kanssa. 2) Pilvipalvelun tulee tukea yleisesti käytettyjä muotoja ohjelmistojen siirrettävyyteen (esimerkiksi Open Virtualization Format, Docker, Kubernetes tai vastaavat). 3) Asiakkaan pyynnöstä palveluntarjoajan on toimitettava asiakkaan tiedot soveltuvassa, käyttökelpoisessa ja yleisesti yhteensopivassa muodossa. Muodot on kuvattava riittävällä tasolla asiakkaan kanssa solmittavissa sopimuksissa. 4) Tietojen tuontiin ja vientiin sekä palvelun hallinnointiin tulee käyttää turvallisia, vakiintu neita verkkoprotokollia siten, että siirrettävien tietojen luottamuksellisuudesta, eheydestä ja käytettävyydestä voidaan varmistua. 5) Viranomaisen turvallisuusluokitellun tiedon siirrossa tulee käyttää viranomaisen hyväksymiä salausratkaisuja.
Soveltuvuus	Pilvipalvelu kokonaisuudessaan.
Tietotyypit	1-4: Salassa pidettävä, henkilötiedot, TL IV 5: TL IV
Suojaustavoite	Asiakkaalla on mahdollisuus vaihtaa pilvipalveluntarjoajaa ja hyödyntää oman palvelunsa toteuttamiseen useita pilvipalveluntarjoajia. Asiakastietojen siirto ei vaaranna tietojen luottamuksellisuutta, eheyttä tai käytettävyyttä.
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.

Osa-alue 10: Muutostenhallinta ja järjestelmäkehitys

MH 01	Muutostenhallinta
Vaatimus	1) Pilvipalveluun tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutostenhallintamenettely. Muutoshallintamenettely 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
Suojaustavoite	Pilvipalvelussa käsiteltävien tietojen luottamuksellisuus, eheys tai käytettävyys 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) voidaan käyttää 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 muu tokset tuotantoympäristöön ja -dataan. Tuotantodataa ei siirretä kehitys- tai testausympäristöihin datan luottamuksellisuuden suojaamiseksi. 5) Muutoshallinnan menettelyihin sisältyy rooleihin perustuvia oikeuksia, joilla varmistetaan tehtävien asianmukainen erottaminen muutosten kehittämisessä, käyttöönotossa ja siirtämisessä ympäristöstä toiseen.

MH 02	Järjestelmäkehitys
Vaatimus	1) Sovellukset ja ohjelmointirajapinnat (API:t) suunnitellaan, kehitetään, testataan ja otetaan käyttöön alan hyvien turvallisuuskäytäntöjen mukaisesti. 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, tulee sopimuksissa huomioida erityisesti: a) Turvallisen ohjelmistokehitysprosessin vaatimukset (erityisesti suunnittelun, kehitys työn 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
Suojaustavoite	Pilvipalvelussa käsiteltävien tietojen luottamuksellisuus, eheys tai käytettävyys 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).



Liite 1: Esimerkkejä kriteeristön soveltamisesta

Esimerkki 1: IaaS-palveluun toteutettu asiakasjärjestelmä

Tässä kuvataan tiiviisti esimerkki siitä, kuinka kriteeristöä voidaan soveltaa tilanteessa, jossa asiakasjärjestelmä on toteutettu IaaS-palvelumallilla tarjottavan pilvipalvelualustan päälle. Esimerkissä asiakkaana on viranomainen V, joka haluaa arvioida hiljattain valmistuneen uuden asiakasjärjestelmänsä kyvykkyyttä turvallisuusluokiteltujen IV-luokan tietojen suojaamiseen. Asiakasjärjestelmän suunnitellut käyttäjät ovat V:n henkilöstöä. Esimerkissä muita toimijoita ovat pilvipalveluntarjoaja P sekä V:n toimeksiannosta asiakasjärjestelmää kehittävä ja ylläpitävä yritys Y.

Kriteeristön käyttö voidaan tällaisessa tilanteessa jakaa kahteen käyttötapaukseen. Ensimmäinen käyttötapaus kohdistuu IaaS-mallilla tarjottavaan pilvipalvelualustaan. Toinen käyttötapaus kohdistuu alustan päälle toteutettavaan asiakasjärjestelmään.

Pilvipalvelualustan turvallisuus

IaaS-mallilla tarjottavan pilvipalvelualustan turvallisuus voidaan jakaa pilvipalveluntarjoajan P hallinnollisen ja henkilöstöturvallisuuden, sekä fyysisen ja teknisen tietoturvallisuuden kokonaisuuksiin. Mikäli viitearkkitehtuurina käytetään kuvan 1 (sivu 8) mukaista pinomallia, teknisen tietoturvallisuuden vastuut rajautuvat tyypillisesti virtualisointialustan sekä muun muassa provisiointipalvelujen rajapintoihin asti. Ylempien pinojen turvallisuusvastuut kohdistuvat puolestaan pilvipalvelun asiakkaalle. Tässä esimerkissä asiakkaan V vastuisiin sisältyy myös V:n toimeksiannosta asiakasjärjestelmää kehittävä ja ylläpitävä yritys Y.

Tällöin esimerkiksi pilvipalvelualustaan kuuluvien verkkolaitteiden sekä tallennus- ja varmistusjärjestelmien turvallisuuden ylläpito kuuluu pilvipalvelualustan arvioinnin osaksi. Myös esimerkiksi tietoliikenteen salaus konesalien välillä ja pilvipalvelualustan ylläpidon käyttöoikeushallinto kuuluu tyypillisesti osaksi pilvipalvelualustan arviointia. Pilvipalvelualustan arviointiin sisältyy tyypillisesti myös turvallisten etähallintayhteyksien järjestäminen pilvipalveluntarjoajan P ylläpitotoimia varten, sekä asiakkaan edustajien (V ja Y) provisiointitarpeiden täyttämiseksi.

Tässä esimerkissä Kyberturvallisuuskeskus on hiljattain arvioinut P:n tarjoaman IaaS-alustan turvallisuuden. Viranomainen V keskustelee arviointihavainnoista yhdessä Kyberturvallisuuskeskuksen ja pilvipalveluntarjoaja P:n kanssa. V päättää hyödyntää hiljattain tehdyn arvioinnin havaintoja omassa riskienarviointityössään suoraan, eikä teetä kyseiseen IaaS-alustaan erillisarviointia.

Asiakasjärjestelmän turvallisuus

Asiakkaana toimivan viranomaisen V vastuulle kuuluu edellä kuvatussa pinomallissa tyypillisesti pinot virtuaalikoneesta lähtien. Esimerkiksi virtuaalikoneen käyttöjärjestelmän asentaminen luotetusta lähteestä, käyttöjärjestelmän koventaminen sekä sen päivitysmenettelyt kuuluvat tyypillisesti pilvipalvelun asiakkaan vastuulle. Myös käyttöjärjestelmän päällä suoritettavan ohjelmiston, sekä sen ylläpitoon käytettävien hallintayhteyksien turvallisuusvastuut kohdistuvat asiakkaalle.

Tässä esimerkissä viranomainen V on vastuussa oman tietojenkäsittely-ympäristönsä sekä myös V:n toimeksiannosta toimivan Y:n suojauksista. Vastuut kattavat turvallisuusluokitellun tiedon käsittelyn hallinnollisen turvallisuuden, henkilöstöturvallisuuden, sekä fyysisen ja teknisen tietoturvallisuuden. Teknisen tietoturvallisuuden osalta vastuut sisältävät esimerkiksi asiakasjärjestelmän kehitykseen ja ylläpitoon käytettävät päätelaitteet hallintaratkaisuineen. Tässä esimerkissä viranomainen V on hiljattain arvioinut sekä omansa, että Y:n tietojenkäsittelyn turvallisuuden Katakri 2015 -viitekehystä vasten, ja keskittyy arvioinnissaan vain asiakasjärjestelmän teknisiin suojauksiin, ylläpitomenettelyt mukaan lukien.

Erikoistapauksia

Jotkin pilvipalveluntarjoajat tarjoavat asiakasjärjestelmän suojaamiseen pilvipalveluntarjoajan tuottamia ohjelmistoja. Esimerkiksi asiakasjärjestelmän palomuuraus, varmistus- tai lokijärjestelyt saattavat olla toteutettavissa pilvipalveluntarjoajan tuottamilla ohjelmistokomponenteilla. Tällaisissa tilanteissa vastuiden rajaus on huomioitava tapauskohtaisesti. Esi-

merkiksi mikäli pilvipalveluntarjoajan ohjelmistokomponentti ei syystä tai toisesta pystyisi toteuttamaan riittävää suojausta, esimerkiksi ohjelmistovirheestä johtuen, tulisi olla määritettynä kuuluuko tämä pilvipalveluntarjoajan vai asiakkaan vastuulle.

Asiakasjärjestelmien toiminnallisuus, käytettävyys (saatavuus) sekä turvallisuus voi rakentua useista tekijöistä. Erityisesti pilvipalveluja käytettäessä eri tekijöiden keskinäisillä riippuvuuksilla voi olla suuri merkitys. Esimerkiksi palvelun käytettävyyteen voi vaikuttaa asiakkaan vastuulla olevien ohjelmistokomponenttien sisäinen toimivuus, pilvipalveluntarjoajan palvelualustan ohjelmistokomponentin sisäinen toimivuus, tai näiden toimivuuksien yhdistelmät.

Esimerkki 2: SaaS-palveluna toteutettu asiakasjärjestelmä

Tässä kuvataan tiiviisti esimerkki siitä, kuinka kriteeristöä voidaan soveltaa tilanteessa, jossa asiakas käyttää pilvipalveluntarjoajan SaaS-palveluna toteuttamaa ohjelmistoa. Kriteeristön käyttö voidaan tällaisessa tilanteessa jakaa kahteen käyttötapaukseen. Ensimmäinen käyttötapaus kohdistuu SaaS-mallilla tarjottavaan palvelukokonaisuuteen. Toinen käyttötapaus kohdistuu palvelukokonaisuuden asetusten ja käytön turvallisuuteen.

Palvelukokonaisuuden turvallisuus

SaaS-mallilla tarjottavan pilvipalvelukokonaisuuden turvallisuus voidaan jakaa pilvipalveluntarjoajan hallinnollisen ja henkilöstöturvallisuuden, sekä fyysisen ja teknisen tietoturvallisuuden osuuksiin. Mikäli viitearkkitehtuurina käytetään kuvan 1 (sivu 8) mukaista pinomallia, teknisen tietoturvallisuuden vastuut rajautuvat tyypillisesti aina sovelluskerroksen ohjelmointirajapintojen ja käyttöliittymän tasolle asti. Asiakkaan turvallisuusvastuut kohdistuvat tällöin tyypillisesti vain palvelukokonaisuuden turvalliseen konfigurointiin ja käyttöön.

Palvelukokonaisuuden asetusten ja käytön turvallisuus

Erilaisten palvelukokonaisuuksien konfigurointimahdollisuudet vaihtelevat merkittävästi palveluntarjoajasta ja kyseisen palvelukokonaisuuden toiminnallisuudesta riippuen. Esimerkiksi palvelukokonaisuuden käyttäjien käyttöoikeushallinto ja tunnistautumismenettelyjen valinnat kuuluvat tyypillisesti asiakkaan vastuisiin. Myös palvelukokonaisuuden asetusten konfigurointiin käytettävien päätelaitteiden turvallisuus kuuluu asiakkaan vastuulle.

Liite 2: Viranomaisarviointi ja -hyväksyntä

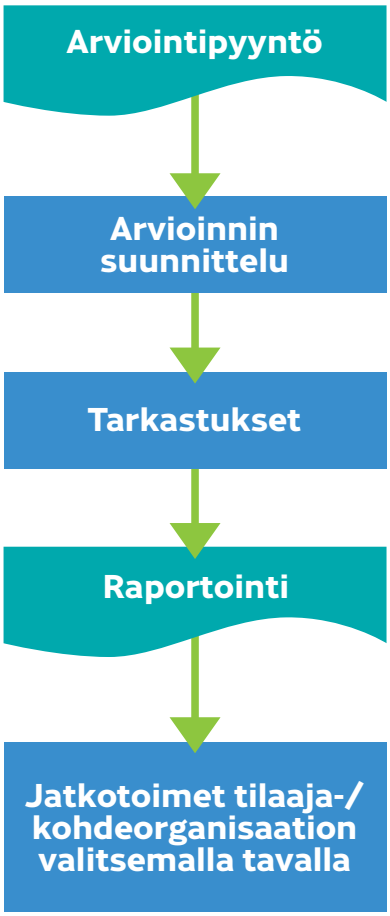
Tausta

Lain viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista[17] mukaisesti viranomaiset saavat käyttää tietojärjestelmiensä tietoturvallisuuden arvioinnissa Liikenne- ja viestintävirasto Traficomia tai sen hyväksymää tietoturvallisuuden arviointilaitosta[18]. PiTuKria voidaan käyttää työkaluna selvitettäessä, miten viranomaisen määräämisvallassa olevan tai hankittavaksi suunnitteleman pilvipalvelupohjaisen tietojärjestelmän tietoturvallisuudesta on huolehdittu suhteessa kansallisen tai kansainvälisen tiedon suojaustarpeisiin[19].

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 2. 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”[20].



Kuva 2. Arviointiprosessi yksinkertaistettuna

[17] 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.

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

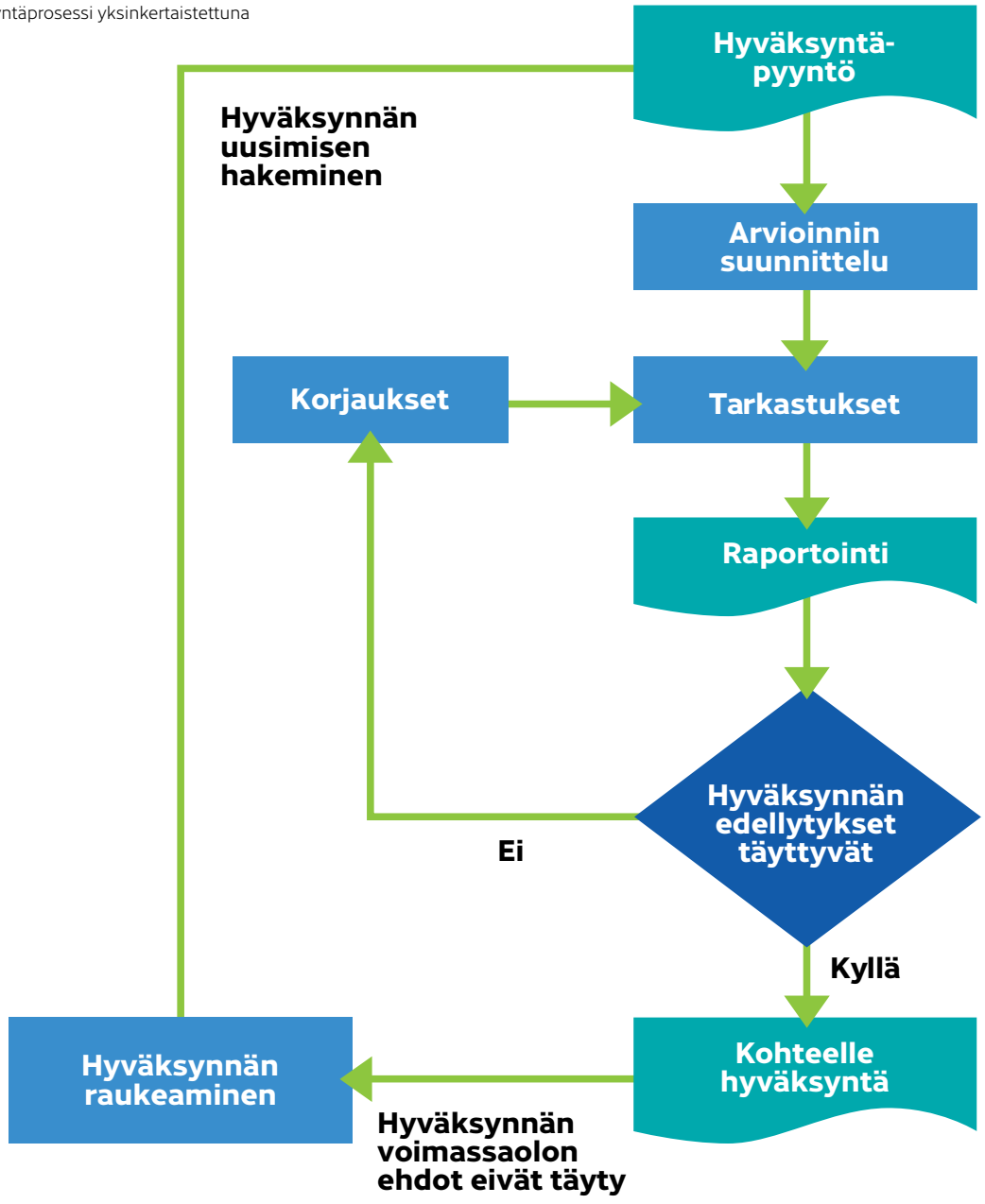
[19] Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), https://www.finlex.fi/fi/laki/alkup/2004/20040588. Turvallisuusselvityslaki (726/2014), https://www.finlex.fi/fi/laki/alkup/2014/20140726.

[20] Kyberturvallisuuskeskus. 2018. 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, L 726/2014 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 3. 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 3. Hyväksyntäprosessi yksinkertaistettuna



Viranomaishyväksyntä

Liikenne- ja viestintävirasto Traficom voi myöntää vaatimukset täyttävälle kansallista tai kansainvälistä salassa pidettävää tietoa käsittelevälle järjestelmälle hyväksynnän (accreditation). Hyväksynnän myöntäminen edellyttää, että tarkastuksen kohde sitoutuu turvallisuuden tason säilyttämiseen. Hyväksyntä edellyttää tyypillisesti 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.

Traficomilla on mahdollisuus myöntää järjestelmälle hyväksyntä pohjautuen hyväksytyn arviointilaitoksen suorittamaan arviointiin (L 1405/2011). Myöntämisen keskeisinä ehtoina ovat tehtyjen tarkastusten rajausten yhteneväisyydet haettavan hyväksynnän rajauksiin sekä toimitettujen arviointiraporttien sisältämien tietojen riittävyys. Hyväksyntää varten Traficom suorittaa tarvittaessa tarkentavia arviointeja tai pyytää tilaajaorganisaatiolta lisäselvitystä sen selvittämiseksi ja varmistamiseksi, että kohde täyttää soveltuvat tietoturvallisuusvaatimukset.

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

TRAFICOM
Kyberturvallisuuskeskus