Taulukko koottu PiTuKri:stä keväällä 2023 SaaSec-hankkeessa.

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) - Vaatimukset ja vastuut	
Pilvipalveluntarjoajan on vastattava kaikkiin vaatimuksiin, kun kyseessä on SaaS-mallin pilvipalvelu. *Asiakasympäristön eli kunnan vastuulla olevat vaatimukset on merkitty taulukossa oikeanpuoleiseen sarakkeeseen.*	
Vaatimus	**Vastuu / asiakasympäristö**
Osa-alue 1: Esiehdot	
EE-01 - Järjestelmäkuvaus	
1) Pilvipalvelusta on järjestelmäkuvaus. Pilvipalveluntarjoajan kuvauksen perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Järjestelmäkuvauksesta tulee käydä ilmi vähintään: a) Pilvipalvelun palvelu- ja toteutusmallit, sekä näihin liittyvät palvelutasosopimukset (Service Level Agreements, SLAs). b) Pilvipalvelun tarjoamisen elinkaaren (kehittäminen, käyttö, käytöstä poisto) periaatteet, menettelyt ja turvatoimet, valvontatoimet mukaan lukien. c) Pilvipalvelun kehittämisessä, ylläpidossa/hallinnassa ja käytössä käytettävän infrastruktuurin, verkon ja järjestelmäkomponenttien kuvaus. d) Muutostenhallinnan periaatteet ja käytännöt, erityisesti turvallisuuteen vaikuttavien muutosten käsittelyprosessit. e) Käsittelyprosessit merkittäville normaalikäytöstä poikkeaville tapahtumille, esimerkiksi toimintatavat merkittävissä järjestelmävikaantumisissa. f) Pilvipalvelun tarjoamiseen ja käyttöön liittyvät roolit ja vastuunjako asiakkaan ja pilvipalveluntarjoajan välillä. Kuvauksesta on käytävä selvästi esille ne toimet, jotka kuuluvat asiakkaan vastuulle pilvipalvelun turvallisuuden varmistamisessa. Pilvipalveluntarjoajan vastuisiin tulee sisältyä yhteistyövelvollisuus erityisesti poikkeamatilanteiden selvittelyssä. g) Alihankkijoille siirretyt tai ulkoistetut toiminnot.	Ei
EE-02 - Lainsäädäntöjohdannaiset riskit	
1) Pilvipalveluun liittyvät lainsäädäntöjohdannaiset riskit ja velvoitteet on kuvattuna. Palveluntarjoajan tuottamien kuvausten perusteella on pystyttävä arvioimaan kyseisen pilvipalvelun yleistä soveltuvuutta kyseiseen asiakkaan käyttötapaukseen. Kuvausten tulee kattaa palvelun käytön ja palvelussa käsiteltävien tietojen koko elinkaaren. Kuvauksista on käytävä ilmi vähintään: a) Palvelussa käsiteltävän tiedon fyysinen sijainti koko tiedon elinkaaren ajalta, kattaen myös mahdolliset alihankinta-/ulkoistusketjut. b) Palvelun eri toimintojen (esimerkiksi ylläpito-/hallintaratkaisut, varmistukset) ja komponenttien fyysinen sijainti koko tiedon elinkaaren ajalta. c) Mahdolliset muut palvelun tuottamiseen osallistuvat tahot, esimerkiksi mahdolliset alihankinta-/ulkoistusketjut. d) Palvelun käyttöön ja palvelussa käsiteltäviin tietoihin sovellettava lainsäädäntö ja oikeuspaikka. e) Toimijat, joilla voi sovellettavasta lainsäädännöstä johtuen olla pääsy palvelussa käsiteltäviin tietoihin. 2) Lainsäädäntöjohdannaiset riskit eivät rajoita kyseisen pilvipalvelun soveltuvuutta kyseiseen käyttötapaukseen. 3) Pilvipalvelun asiakkaan tiedot sijaitsevat koko elinkaarensa ajan vain sopimuksessa kuvatuissa fyysisissä sijainneissa. Poikkeuksena tilanne, jossa pilvipalvelun asiakas on kirjallisesti etukäteen hyväksynyt tietojen siirron tai käsittelyn muissa fyysisissä sijainneissa. 4) Pilvipalveluntarjoajan sopimusehdot eivät rajoita kyseisen pilvipalvelun soveltuvuutta kyseiseen käyttötapaukseen.	Kyllä: kohdat 2 ja 4 (soveltuvuuden arviointi)
Osa-alue 2: Turvallisuusjohtaminen	
TJ-01 - Turvallisuusperiaatteet	
1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. 3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan johdolle ja niiden toteutumista seurataan säännöllisesti.	Kyllä
TJ-02 - Turvallisuuden vastuut	
1) Pilvipalvelun turvallisuuden hoitamisen tehtävät ja vastuut on määritelty ja dokumentoitu. 2) Pilvipalvelun tarjoamiseen ja käyttöön liittyvä vastuunjako asiakkaan ja palveluntarjoajan välillä on kuvattu. Vrt. EE-01. 3) Pilvipalvelun tietoturvallisuudesta vastaava henkilö on nimetty.	Kyllä
TJ-03 - Turvallisuusriskien hallinta	
1) Organisaatiolla on käytössä riskienhallintaprosessi. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi. Riskienhallintapäätökset vastuutahoineen dokumentoidaan. 2) Riskien analysoinnissa on käytettävä järjestelmällistä ja ymmärrettävää menetelmää. 3) Riskienhallinnan on katettava vähintään turvallisuusjohtamisen, tila- ja tietoturvallisuuden osa-alueet. 4) Tunnistetut riskit otetaan huomioon tarvittavien sidosryhmien osalta. Pilvipalveluntarjoajan tulee varmistaa, että asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Vrt. TJ-08. 5) Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvallisuustavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. 6) Turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon luokitteluperuste, määrä, muoto ja sijoitustilat suhteessa arvioituun vihamielisen tai rikollisen toiminnan uhkaan. 7) Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet.	Kyllä
TJ-04 - Turvallisuushäiriöiden hallinta	
1) Organisaatiolla on menettelytavat turvallisuushäiriöiden asianmukaiseen käsittelyyn. 2) Organisaatiolla on käytössään selkeät prosessit turvallisuushäiriöiden ilmoittamisesta. Organisaatiolla on määritettynä henkilöt/tahot, joille turvallisuushäiriöistä tai niiden epäilyistä tulee ilmoittaa. 3) Turvallisuushäiriöiden määrää ja tyyppejä seurataan. Toteutuneiden häiriöiden uusiutuminen on pyrittävä estämään korjaussuunnitelmissa. 4) Asiakastiedon käsittelyyn liittyvät turvallisuushäiriöt tai niiden epäilyt ilmoitetaan kyseiselle asiakkaalle.	Kyllä: kohdat 1-3

TJ-05 - Jatkuvuudenhallinta	
1) Jatkuvuudenhallinnan prosessit ja menettelyt on suunniteltu, toteutettu, testattu ja kuvattu siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Järjestelyissä huomioidaan erityisesti, että a) toipuminen ja jatkuvuuden varmistaminen toimintavaatimuksiin nähden riittävässä ajassa on huomioitu suunnittelussa, b) toiminnan jatkuvuussuunnitelmiin on sisällytettävä ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset tietojen käsittelyyn ja säilyttämiseen, c) poikkeamista tehdyt havainnot tuodaan osaksi riskienarviointia, ja toipumis- ja jatkuvuussuunnitelmia päivitetään tehtyjen havaintojen ja saatujen tulosten perusteella, ja d) jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai saatavuuden menettäminen.	Kyllä (soveltuvin osin, esimerkiksi toiminta tilanteessa, jossa verkkoyhteys pilvipalveluun ei käytettävissä)
TJ-06 - Tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä	
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.)	Kyllä: kohta 2, kohta 5 (käytettävien sovellusten asiakkaan vastuulla olevien osuuksien omistaja/vastuutaho, kohta 6 (käytettävien sovellusten ja niiden asiakkaan vastuulla olevien osuuksien kirjanpito ja muutoshallinta)
TJ-07 - Vaatimustenmukaisuus ja tietosuoja	
1) Pilvipalveluun sovellettavien lakien ja säädösten määräykset sekä menettelyt näiden noudattamiseksi on tunnistettu ja dokumentoitu, sekä säännöllisesti päivitetty. 2) Riippumattomat kolmannet osapuolet arvioivat vähintään vuosittain pilvipalveluun liittyvän toiminnan, prosessit ja tietotekniikkajärjestelmät soveltuvin osin, erillisessä arviointisuunnitelmassa määritellyn kuvauksen mukaisesti. Arvioinnin tulee pyrkiä tunnistamaan mahdolliset tapaukset, joissa lakeja tai säädöksiä ei noudateta. Arviointisuunnitelma kattaa palvelun turvallisuuden siten, että kaikki keskeiset turvallisuuteen vaikuttavat kokonaisuudet arvioidaan korkeintaan kolmen vuoden välein. Havaitut poikkeamat dokumentoidaan, priorisoidaan ja korjataan niiden kriittisyyden mukaisesti. 3) Pilvipalvelun toimintaan kohdistetaan vähintään vuosittain sisäinen tarkastus, jonka tavoitteena on selvittää kuinka palvelu kokonaisuutena vastaa turvakäytäntöjensä ja sopimus- sekä lainsäädännöllisten vastuiden täyttämiseen. 4) Ylin johto vastaa siitä, että havaitut poikkeamat priorisoidaan ja korvaavat suojaukset tai korjaukset toteutetaan riittävän nopeasti.	Kyllä (sovellusten käytön vaatimustenmukaisuuden ja tietosuojan arviointi)
TJ-08 - Palveluntarjoajien ja toimittajien turvallisuus	
1) Asiakkaiden tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiannosta. Varmistettava erityisesti, että a) ennen palveluntarjoajan/toimittajan henkilöstön pääsyä suojattaviin kohteisiin, henkilöstö on läpikäynyt vastaavat suojaustoimenpiteet (sopimukset, salassapitositoumukset, turvaselvitykset, koulutukset), kuin pilvipalveluntarjoajankin henkilöstö, b) palveluntarjoajat/toimittajat on kirjallisesti ohjeistettu ja sopimuksin velvoitettu noudattamaan vähintään vastaavantasoisia suojauksia, kuin organisaatiokin, c) sopimusvelvoitteiden noudattamisen varmistamiseen ja valvontaan on käytössä luotettavat menettelyt, d) turvallisuusluokitellun tiedon käsittelyyn suoraan tai epäsuoraan osallistuvat palveluntarjoajat ja toimittajat ovat voimassa olevan viranomaishyväksynnän, tai vastaavan menettelyn piirissä. Menettely kattaa soveltuvin osin sekä hallinnollisen (turvallisuusjohtamisen), fyysisen että teknisen tietoturvallisuuden kokonaisuudet.	Kyllä
Osa-alue 3: Henkilöstöturvallisuus	
HT-01 - Työsuhteen elinkaaren huomioiminen	
1) Organisaatiolla on käytössä turvallisuuden huomioon ottava menettely työsuhteen elinkaaren eri vaiheissa. Erityisesti huomioidaan toimenpiteet rekrytoitaessa, työtehtävien muutoksissa ja työsuhteen päättyessä.	Kyllä
HT-02 - Henkilöstön luotettavuuden arviointi	
1) Pilvipalvelun asiakkaiden tietoja tai yhteistä IT-infrastruktuuria käyttämään pääsevien sisäisten ja ulkoisten työntekijöiden taustat tarkistetaan paikallisen lainsäädännön mahdollistamien menettelyjen mukaisesti ennen työsuhteen alkua. Lainsäädännön sallimissa rajoissa tarkistukseen sisällyttävä vähintään: a) Henkilöllisyyden todentaminen. b) Työhistorian todentaminen. c) Koulutustaustan todentaminen. 2) Turvallisuusluokiteltujen aineistojen käsittelyyn liittyvien henkilöiden luotettavuus selvitetään ja sitä seurataan asianmukaisen tason turvallisuusselvitysmenettelyin.	Kyllä
HT-03 - Salassapito- ja vaitiolositoumukset	
1) Salassapito- tai vaitiolositoumusmenettely on käytössä. Salassapitosopimukset on allekirjoitettava ennen sopimussuhteen alkamista tai ennen kuin pilvipalvelun asiakkaiden tietoja koskeva käyttöoikeus myönnetään.	Kyllä
HT-04 - Turvallisuustietoisuus	
1) Keskeiset turvallisuuteen liittyvät periaatteet ja toimintatavat on kuvattuna. 2) Turvalliset toimintatavat on henkilöstölle jalkautettuna siten, että henkilöstön riittävästä turvatietoisuudesta pystytään varmistumaan. 3) Turvallisuuteen liittyvien kuvausten/ohjeistusten ajantasaisuus sekä jalkautuminen käytäntöön varmistetaan säännöllisesti, vähintään vuosittain. 4) Turvallisuuteen liittyvät ohjeet kattavat henkilötietoihin ja salassa pidettävään tietoon liittyvät prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta. 5) Turvallisuusohjeiden noudattamista valvotaan ja ohjeiden muutostarpeita arvioidaan säännöllisesti.	Kyllä

HT-05 - Tiedonsaantitarpeet ja tehtävien erottelu	
1) Salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ylläpidetään luetteloa. Tällaisiksi työtehtäviksi tulkitaan kuuluvaksi myös sellaiset kehitys- ja ylläpitotehtävät, joissa on suora tai epäsuora mahdollisuus päästä salassa pidettävään tietoon, tai muuten oleellisesti vaikuttaa salassa pidettävän tiedon suojauksiin. 2) Pääsy salassa pidettävään tietoon voidaan myöntää vasta, kun henkilön työtehtävistä johtuva tiedonsaantitarve on selvitetty. 3) Luetteloa turvallisuusluokiteltujen tietojen käsittelyoikeuksista ylläpidetään luokittain. 4) Tehtävät ja vastuualueet on mahdollisuuksien mukaan eriytetty, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Mikäli vaarallisia työyhdistelmiä syntyy, on niitä varten oltava valvontamekanismi. 5) Turvallisuusluokan III kasaumalle lisäksi: Kriittiset tehtävät ja vastuualueet on eriytetty eri henkilöille, jotta vähennetään suojattavien kohteiden luvattoman tai tahattoman muuntelun tai väärinkäytön riskiä. Erityishuomiota kiinnitettävä siihen, että yksittäinen henkilö ei pysty poistamaan toimiensa jälkiä tai merkittävästi estämään poikkeavien toimien havaitsemista.	Kyllä
Osa-alue 4: Fyysinen turvallisuus	
FT-01 - Monitasoinen suojaaminen ja riskienhallinta	
1) Fyysiset turvatoimet on toteutettu monitasoisen suojaamisen periaatetta noudattaen. 2) Suojattavat tilat rakennuksessa on luokiteltu turvallisuusalueiksi (hallinnollinen alue, turva-alue) ja niillä on selkeästi määritellyt ja näkyvät rajat. 3) Korkeintaan turvallisuusluokan IV salassa pidettävää tietoa sisältävät tietovarannot ja tietojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle. 4) Turvallisuusluokan III kasauman muodostaneet tietovarannot ja tietojen pääsynrajauksiin ja -valvontaan käytettävät tietojärjestelmät on sijoitettava turva-alueelle. 5) Hallinnollisilla alueilla on selkeästi määritetyt näkyvät rajat ja joihin vain organisaation valtuuttamilla henkilöillä on pääsy ilman saattajaa. 6) Turva-alueilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle. 7) Turvatoimet on mitoitettu riittävälle tasolle siten, että ne vastaavat riskienarvioinnissa todettuja riskejä.	Ei
FT-02 - Rakenteet ja turvallisuusjärjestelmät	
1) Arkaluonteisia tai kriittisiä tietoja, tietojärjestelmiä tai muuta verkkoinfrastruktuuria sisältävien tilojen tai rakennusten ulkorajat suojataan fyysisesti kestävällä tavalla sekä nykyaikaisilla ja asianmukaisilla turvatoimilla.	Ei
FT-03 - Luvattoman pääsyn estäminen	
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.	Ei
FT-04 - Palveluntuottajat ja vierailijat	
1) Vierailijat tunnistetaan, varustetaan vierailijakortilla ja kirjataan. Organisaatiolla on dokumentoitu vierailijapolitiikka. Vierailijoiden suhteen sovelletaan aina isäntäperiaatetta. 2) Siivous-, huolto- ja muu palveluntuottajien henkilöstö tunnistetaan, varustetaan vierailijakorteilla ja kirjataan. Säännölliset palveluntuottajat varustetaan kuvallisella henkilökortilla. 3) Alueella itsenäisesti liikkuvat tai suojattaviin kohteisiin käsiksi pääsevät palveluntuottajat on turvallisuusselvitetty. Henkilöt, joita ei pystytä tai ei ole vielä turvallisuusselvitetty liikkuvat saatettuna. Vrt. HT-02. 4) Huoltoihin, päivityksiin ja ylläpitoon liittyvät käytännöt on kirjallisesti kuvattu ja dokumentoitu.	Ei
FT-05 - Varautuminen ja jatkuvuudenhallinta	
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/ikkunarakenteiden palonkestävyys sekä läpivientien tiivistäminen paloluokkaa vastaavilla tuotteilla). b) Tekniset turvatoimet: i. Tila tai rakennus on kytketty automaattiseen paloilmoitinjärjestelmään, jonka hälytys välittyy hätäkeskukseen. ii. Suojattava tila on varustettu muusta kiinteistöstä erillisellä ilmanvaihtojärjestelmällä ja automaattisilla palonrajoittimilla (esim. automaattiset savupellit). iii. Tilaan on asennettu suojattavasta tiedosta riippuen riittävät olosuhde-, lämpötila- ja kosteusanturit (verkkovirran- tai paineenvaihtelut, kuumuus/kylmyys, vesivuodot). iv. Käytössä on automaattiset sammutusjärjestelmät, jotka havaitsevat esim. tulipalon aikaisessa vaiheessa ja aloittavat alkusammutuksen. v. Sähkön häiriötön saanti on varmistettu sähkönsyötön turvaavilla laitteilla (UPS, varavoima). vi. Tietoliikenteen varmistukset, ja jäähdytysjärjestelmän kahdennus. c) Organisatoriset turvatoimet: i. Pelastussuunnitelman laatiminen ii. Nimetty vastuuhenkilö tai taho, kenelle tieto hälytyksistä välittyy iii. Säännölliset pelastusharjoitukset ja paloturvallisuustarkastukset paloturvallisuusmääräysten noudattamisen toteamiseksi iv. Jatkuvuussuunnittelu	Ei
Osa-alue 5: Tietoliikenneturvallisuus	
TT-01 - Tietoliikenneverkon rakenne	
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.	Ei
TT-02 - Yleisiä verkkohyökkäyksiä vastaan suojautuminen	
1) Organisaatio ylläpitää riskienarviointia, joka kattaa yleisiltä verkkohyökkäyksiltä suojautumisen. 2) Suojaukset on mitoitettu siten, että yleiset verkkohyökkäykset eivät vaaranna palvelun tai siinä käsiteltävien tietojen luottamuksellisuutta, eheyttä tai saatavuutta.	Ei

Osa-alue 6: Identiteetin ja pääsyn hallinta	
IP-01 - Käyttöoikeushallinta	
1) Käyttöoikeuksien hallinnointi toteuttaa vähimpien oikeuksien periaatetta: a) Käyttäjätilien luontiin, hyväksymiseen ja ylläpitoon on ennalta määritelty prosessi. b) Tietojenkäsittely-ympäristön käyttäjille annetaan vain ne tiedot, oikeudet tai valtuutukset, jotka ovat tehtävien suorittamiseksi välttämättömiä. c) Järjestelmän käyttäjistä ylläpidetään listaa. Jokaisesta myönnetystä käyttöoikeudesta jää merkintä. d) Käyttöoikeuden myöntämisen yhteydessä tarkistetaan, että oikeuden saaja kuuluu henkilöstöön tai on muutoin oikeutettu. e) Käyttöoikeuksien käsittely ja myöntäminen on ohjeistettu. f) Käyttö- ja pääsyoikeudet pidetään ajan tasalla. Tarpeettomat käyttäjätilit ja oikeudet poistetaan, kun niitä ei enää tarvita (esimerkiksi käyttäjän lähtiessä organisaatiosta tai kun käyttäjätiliä ei ole käytetty ennalta määritettyyn aikaan). g) On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseen välittömästi asiankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen. h) Käyttö- ja pääsyoikeudet katselmoidaan säännöllisesti, vähintään puolivuosittain.	Kyllä
IP-02 - Käyttäjätunnistus	
1) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjät sekä palvelun käyttäjät tunnistetaan ja todennetaan luotettavasti ennen pääsyä suojattavaan tietoon: a) Käytössä on yksilölliset henkilökohtaiset käyttäjätunnisteet. b) Kaikki käyttäjät tunnistetaan ja todennetaan. c) Tunnistamisessa ja todennuksessa käytetään tunnettua ja turvallisena pidettyä tekniikkaa tai se on muuten järjestettävä luotettavasti. d) Käyttäjätunnukset lukittuvat tilanteissa, joissa tunnistus epäonnistuu liian monta kertaa peräkkäin. e) Järjestelmien ja sovellusten ylläpitotunnukset ovat henkilökohtaisia. Mikäli tämä ei kaikissa järjestelmissä tai sovelluksissa ole teknisesti mahdollista, edellytetään sovitut, dokumentoidut ja käyttäjän yksilöinnin mahdollistavat hallintakäytännöt yhteiskäyttöisille tunnuksille. f) Käyttäjien todennus tehdään vahvasti, vähintään kahteen tekijään nojautuen (esimerkiksi salasana + token). Yhteys on salattu käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. i. Poikkeuksena tilanne, jossa todennus tehdään fyysisesti suojatun turvallisuusalueen (Vrt. FT-01) sisällä vähintään salasanaa käyttäen. Mikäli käytetään salasanatodennusta, 1. käyttäjiä on ohjeistettu hyvästä turvallisuuskäytännöstä salasanan valinnassa ja käytössä, 2. käyttöä valvova ohjelmisto asettaa salasanalle tietyt turvallisuuden vähimmäisvaatimukset ja pakottaa salasanan vaihdon sopivin määräajoin. 2) Tilanteissa, joissa yhteys kulkee fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan konesalin ja ylläpidon/asiakkaan päätelaitteen välillä), tieto/tietoliikenne on suojattu viranomaisen hyväksymällä salausratkaisulla. 3) Pilvipalvelun tuottamiseen liittyvät palveluntarjoajan ja asiakkaan ylläpitäjien päätelaitteet ja järjestelmät tunnistetaan riittävän luotettavasti ennen pääsyä suojattavaan tietoon.	Kyllä (yleensä keskittyen turvallisten asetusten konfigurointiin ko. palvelun asetuksista, sekä asiakkaan päätelaitteiden turvallisuuteen)
IP-03 - Hallintayhteydet	
1) Hallintapääsy tapahtuu pilvipalveluympäristössä rajattujen, hallittujen ja valvottujen pisteiden (esimerkiksi hyppykoneet, hallintaportaalit ja vast.) kautta. Hallintapääsyn mahdollistavat pisteet eriytetään toisistaan vähintään siten, että pilvipalveluntarjoajan ja eri asiakkaiden hallintapisteet, sekä niiden kautta saavutettavat palvelut, ovat toisistaan luotettavasti eroteltuna (vrt. JT-03). 2) Hallintapääsy edellyttää vahvaa, vähintään kahteen todennustekijään (esimerkiksi salasana + token) pohjautuvaa käyttäjätunnistusta. 3) Hallintaliikenne on salattua käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. 4) Hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (vrt. FT-01) ulkopuolelle viedyt asiakastietoa sisältävät päätelaitteet ja muut tietovälineet (kiintolevyt, USB-muistit ja vastaavat) säilytetään salattuina käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja, tai tietovälineitä ei jätetä valvomatta. Vrt. SA-01 ja FT-01. 5) Viranomaisen turvallisuusluokitellun tiedon hallinta on mahdollista vain kyseisen turvallisuusluokan mukaisilta päätelaitteilta ja ympäristöistä sekä fyysisiltä alueilta (vrt. FT-01). 6) Viranomaisen turvallisuusluokitellun tiedon hallintaan on pääsy vain viranomaisen hyväksymällä menettelyllä salatulla hallintayhteydellä. 7) Turvallisuusluokiteltua tietoa sisältävien päätelaitteiden ja muiden tietovälineiden (kiintolevyt, USB-muistit ja vastaavat) salaus on viranomaisen hyväksymä.	Kyllä: kohdat 2-7 (yleensä keskittyen turvallisten asetusten konfigurointiin ko. palvelun asetuksista, sekä asiakkaan päätelaitteiden turvallisuuteen)

Osa-alue 7: Tietojärjestelmäturvallisuus	
JT-01 - Jäljitettävyys ja havainnointikyky	
1) Luotettavat menetelmät turvallisuuteen liittyvien tapahtumien jäljitettävyyteen on toteutettu. Erityisesti: a) Tallenteet ovat riittävän kattavia tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen. b) Keskeiset tallenteet säilytetään vähintään 6 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. c) Lokitiedot ja niiden kirjauspalvelut suojataan luvattomalta pääsyltä (käyttöoikeushallinto, looginen pääsynhallinta) vähimpien oikeuksien periaatteen mukaisesti. d) Lokitietojen välitys lokilähteiden ja lokikeräimen välillä on toteutettu suojatusti. Välityksen osapuolet tunnistetaan. Lokitiedot välitetään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. Vaihtoehtoisesti lokitiedot voidaan siirtää erillisen hallintaverkon kautta. e) Kellot on synkronoitu sovitun ajanlähteen kanssa. f) Turvallisuusluokan III kasaumalle lisäksi: Keskeiset tallenteet säilytetään vähintään 24 kk, ellei lainsäädäntö tai sopimukset edellytä pitempää säilytysaikaa. g) Turvallisuusluokan III kasaumalle lisäksi: Keskeiset lokitiedot ohjataan lokilähteistä erilliselle lokikeräimelle (tai erillisille lokikeräimille). 2) Pilvipalveluntarjoaja toimittaa asiakkaan pyynnöstä, pilvipalveluntarjoajan vastuualueeseen kuuluvien järjestelmäkomponenttien osalta, asiakkaaseen vaikuttavat lokitiedot muodossa, josta asiakas voi tutkia häneen vaikuttavia tapauksia. 3) Pilvipalveluntarjoaja tarjoaa mahdollisuuden (teknisen rajapinnan) reaaliaikaiseen tiedonvaihtoon asiakkaan kanssa asiakkaan tietojen turvallisuuteen liittyvien tapahtumien välittämiseen (lokitiedot, tapahtumatiedot, tietoturvahavainnot). 4) Luotettavat menetelmät turvallisuuspoikkeamien havaitsemiseksi on toteutettu. Erityisesti: a) On olemassa menettely, jolla kerätyistä tallenteista (vrt. KT-04) pyritään havaitsemaan poikkeamia (erityisesti tietojärjestelmän luvaton käyttöyritys on kyettävä havaitsemaan). b) Verkkoliikenteen normaali tila (liikennemäärät, protokollat ja yhteydet) on tiedossa. c) On olemassa menettely, jolla verkkoliikenteen normaaliin tilaan nähden eroavat tapahtumat (esimerkiksi poikkeavat yhteydet tai niiden yritykset) pyritään havaitsemaan. d) On olemassa menettely, jolla pilvipalveluun kuuluvista palvelimista ja muista kohteista (hosts) voidaan havainnoida poikkeamia. e) Turvallisuusluokan III kasaumalle lisäksi: On olemassa menettely, jolla yritykset päästä valtuuttamattomasti laajempaan osaan tietosisällöstä pyritään havaitsemaan. 5) On olemassa menettely havaituista poikkeamista toipumiseen.	Ei
JT-02 - Järjestelmäkovennus	
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.	Ei
JT-03 - Tiedon erottelu	
1) Asiakkaiden salassa pidettävät tiedot säilytetään luotettavasti toisistaan eroteltuna yhteiskäyttöisissä virtuaalisissa ja fyysisissä järjestelmissä.	Ei
JT-04 - Haittaohjelmasuojaus	
1) Pilvipalvelussa, mukaan lukien sen hallinnointiin käytettävissä järjestelmäympäristöissä, toteutetaan luotettavat menetelmät haittaohjelmauhkien ennaltaehkäisyyn, estämiseen, havaitsemiseen, vastustuskykyyn ja tilanteen korjaamiseen.	Ei
JT-05 - Suojattavien kohteiden siirtäminen	
1) Laitteita, ohjelmistoja, siirtomedioita tai vastaavia saa siirtää fyysisesti suojattujen toimitilojen ulkopuolelle vain erilliseen valtuutukseen pohjautuen. 2) Fyysisesti suojatun toimitilan ulkopuolella tapahtuva siirto ja käsittely tapahtuu siirrettävän suojattavan kohteen (luokituksen) mukaisesti. 3) Siirrettäessä asiakkaan salassa pidettävää tietoa fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolella, tieto on salatussa muodossa (vrt. SA-02) tai suojattava kohde on pilvipalveluntarjoajan henkilöstön jatkuvan valvonnan alaisuudessa. 4) Viranomaisen turvallisuusluokitellun tiedon suojaamisessa käytetään viranomaisen hyväksymiä salauskäytäntöjä, -vahvuuksia ja -tuotteita (vrt. SA-01).	Ei
Osa-alue 8: Salaus	
SA-01 - Salauskäytännöt ja avainhallinta	
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.	Kyllä (voi soveltua asiakkaan konfigurointimahdollisuuksien osalta)
SA-02 - Salaus fyysisen turvallisuusalueen ulkopuolella	
1) Siirrettäessä asiakkaan salassa pidettävää tietoa hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (esimerkiksi palveluntarjoajan konesali, vrt. FT-01) ulkopuolella, tai matalamman turvallisuustason verkon kautta, salassa pidettävä tieto siirretään käyttötilanteeseen soveltuvalla menetelmällä salattuna, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-01. 2) Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. 3) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. SA-01).	Kyllä (voi soveltua asiakkaan konfigurointimahdollisuuksien osalta)

SA-03 - Salaus fyysisesti suojatun turvallisuusalueen sisäpuolella	
1) Kun asiakkaan salassa pidettävää tietoa siirretään hyväksyttyjen fyysisesti suojattujen turvallisuusalueiden (vrt. FT-01) ja kyseisen turvallisuustason verkon sisäpuolella, alemman tason salausta tai salaamatonta siirtoa voidaan käyttää, mikäli tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin. Vrt. JT-03. 2) Asiakkaiden salassa pidettävät tiedot tallennetaan pilvipalveluun salatussa muodossa, mikäli käytetään yhteiskäyttöistä laitteistoa. Vrt. JT-03. 3) Salausavaimistot ovat asiakaskohtaisesti eroteltuja. 4) Viranomaisen turvallisuusluokitellun aineiston salaus toteutetaan viranomaisen hyväksymällä menetelmällä (vrt. SA-01).	Kyllä: kohdat 2-4 (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)
Osa-alue 9: Käyttöturvallisuus	
KT-01 - Järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi	
1) Pilvipalvelusta on kattavat järjestelmäkuvaukset sekä ohjeet palvelun turvalliseen ylläpitoon ja hallinnointiin. Kuvaukset ja ohjeistukset ovat sellaisella tasolla, että niiden avulla pystytään uskottavasti välttämään käytön aikaiset virheet sekä varmistumaan sopimusvelvoitteiden mukainen palautuminen häiriötilanteista. 2) Järjestelmäkuvaukset ja ohjeet pidetään ajan tasalla. 3) Järjestelmäkuvaukset ja ohjeet ovat henkilöstölle jalkautettuna ja saatavilla roolien mukaisesti.	Kyllä: kohta 3
KT-02 - Suorituskyvyn hallinta	
1) Pilvipalvelun suorituskyky (kapasiteetti) mitoitetaan siten, että palvelutasosopimusten mukainen palvelutaso pystytään luotettavasti tarjoamaan. Mitoitukseen on sisällyttävä toteutuneen suorituskykytarpeen seuranta sekä tulevien suorituskykytarpeiden ennusteet. 2) Pilvipalveluntarjoajan on mahdollistettava asiakkaalle annettujen järjestelmäresurssien (esim. tietojenkäsittely- tai tallennuskapasiteetin) käytön seuranta.	Ei
KT-03 - Varmistus- ja palautusprosessit	
1) Varmistus- ja palautusprosessit on suunniteltu, toteutettu, testattu ja kuvattu osana jatkuvuussuunnitelmaa siten, että pystytään vastaamaan palvelutasosopimusten ja lainsäädännön velvoitteisiin sekä pilvipalvelun muihin liiketoiminnallisiin vaatimuksiin. Erityisesti huomioitava: a) Varmistusten taajuus on riittävä varmistettavan tiedon kriittisyyteen nähden. Edellyttää selvitystä siitä, kuinka paljon dataa voidaan menettää (recovery point objective, RPO). b) Palautusprosessin nopeus on riittävä toimintavaatimuksiin nähden. Edellyttää selvitystä siitä, kuinka kauan palautuminen voi kestää (recovery time objective, RTO). c) Varmuuskopioinnin ja palautusprosessin oikea toiminta testataan säännöllisesti. d) Varmuuskopioiden fyysinen sijoituspaikka on riittävän eriytetty varsinaisesta järjestelmästä (eri sortuma-/palotila, välimatka varmuuskopion ja varsinaisen tilan välillä). 2) Varmuuskopiot suojataan niiden elinkaaren ajan vähintään vastaavan tasoisilla menetelmillä, kuin millä alkuperäinen tieto. Suuri määrä tietoa voi edellyttää tiukempia suojauksia (kasautumisvaikutus). Erityisesti huomioitava: a) Pääsy varmuuskopioihin on rajattu vähimpien oikeuksien periaatteen mukaisesti vain hyväksytyille henkilöille tai rooleille. b) Varmistus- ja palautusprosessit ovat jäljitettävissä (lokitus) ja valvottuja siten, että luvattomat toimet (esimerkiksi valtuuttamattomat palautukset) pyritään havaitsemaan. c) Tilanteissa, joissa varmuuskopioita säilytetään toisessa fyysisessä sijainnissa, myös tämän sijainti on fyysisen ja loogisen pääsynhallinnan osalta vähintään vastaavalla tasolla. d) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan toiseen konesaliin) verkon välityksellä, tieto/tietoliikenne on salattuna käyttötilanteeseen soveltuvalla menetelmällä, suosien oikeellisen toiminnan osalta varmistettuja (validoituja) ja standardoituja salausratkaisuja/-protokollia. Vrt. SA-02 ja SA-03. e) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle siirtomedialla (esimerkiksi varmistusnauhat tai -levyt), siirtomedia siirretään jatkuvan valvonnan alaisuudessa. Siirtomedialle tai sen sisältämälle tiedolle suositellaan salausta. f) Varmistusmediat hävitetään luotettavasti (vrt. SI-02). 3) Viranomaisen turvallisuusluokiteltua tietoa sisältävien varmuuskopioiden osalta lisäksi huomioitava: a) Tilanteissa, joissa varmuuskopioita siirretään fyysisesti suojatun turvallisuusalueen (vrt. FT-01) ulkopuolelle (esimerkiksi pilvipalveluntarjoajan toiseen konesaliin) verkon välityksellä, tieto/tietoliikenne on suojattu viranomaisen hyväksymällä salausratkaisulla. b) Käsiteltäessä samalla varmistusjärjestelmällä eri omistajien tietoja, erottelumenettelyt (esimerkiksi salaus tai/ja fyysisesti erilliset tallennejärjestelmät ja -mediat) on toteutettu varmistusjärjestelmän liittymien ja tallennemedioiden osalta. Vrt. JT-03 ja SA-03.	Ei
KT-04 - Haavoittuvuuksien hallinta	
1) Pilvipalvelun koko elinkaaren ajalle toteutetaan luotettavat menettelyt ohjelmistohaavoittuvuuksien hallitsemiseksi. Erityisesti huomioitava: a) Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja riskiperusteisesti tarpeellisiksi arvioidut turvapäivitykset asennetaan hallitusti (vrt. MH-01). b) Järjestelmät tarkistetaan tunnettujen haavoittuvuuksien varalta automaattisesti vähintään kuukausittain. Jos suunnitelluista asetuksista tai turvapäivitystasosta on poikettu, syyt analysoidaan, ja poikkeamat korjataan tai dokumentoidaan poikkeamahallintaprosessin mukaisesti (ks. TJ-04). c) Pilvipalvelun turvallisen toiminnan kannalta keskeiset komponentit tarkistetaan riippumattoman tahon tunkeutumistestauksella säännöllisesti, vähintään vuosittain. Merkittävät poikkeamat korjataan välittömästi. d) Pilvipalvelun asiakkaalle tiedotetaan merkittävistä haavoittuvuuksista ja niiden vaikutuksista asiakkaan tietojen suojaamiseen. Tiedotus on erityisen tärkeää tilanteissa, joissa haavoittuvuuden hallinta edellyttää toimia sekä pilvipalveluntarjoajalta että asiakkaalta.	Ei

Osa-alue 10: Siirrettävyys ja yhteensopivuus	
SI-01 - Siirrettävyys ja yhteensopivuus	
1) Pilvipalvelun ohjelmointirajapinnat (API, Application Programming Interface) on julkaistu siten, että ne mahdollistavat yhteentoimivuuden eri ohjelmistokomponenttien ja ohjelmistojen kanssa. 2) Pilvipalvelu tukee yleisesti käytettyjä muotoja ohjelmistojen siirrettävyyteen (esimerkiksi Open Virtualization Format, Docker, Kubernetes tai vastaavat). 3) Pilvipalveluntarjoaja tarjoaa teknisen rajapinnan tai muun menetelmän asiakkaan tietojen toimitukseen asiakkaalle soveltuvassa, käyttökelpoisessa ja yleisesti yhteensopivassa muodossa. Muodot on kuvattu riittävällä tasolla asiakkaan kanssa solmittavissa sopimuksissa. 4) Tietojen tuontiin ja vientiin sekä palvelun hallinnointiin käytetään turvallisia, vakiintuneita verkkoprotokollia siten, että siirrettävien tietojen luottamuksellisuudesta, eheydestä ja saatavuudesta voidaan varmistua. 5) Viranomaisen turvallisuusluokitellun tiedon siirrossa käytetään viranomaisen hyväksymiä salausratkaisuja.	Kyllä: kohta 3 (sopimuksen osalta), kohdat 4-5 (voi soveltua asiakkaan konfigurointi-mahdollisuuksien osalta)
SI-02 - Tietoaineistojen tuhoaminen	
1) Tietoaineistojen tuhoaminen on järjestetty riittävän luotettavasti. 2) Tuhoaminen kattaa koko salassa pidettävän tiedon elinkaaren siltä osin, kun tieto on ollut pilvipalvelussa. 3) Asiakkaan salassa pidettävät tiedot tuhotaan luotettavasti erityisesti seuraavissa tilanteissa: a) Asiakkaan pyytäessä tietojensa tuhoamista. b) Asiakkaan sopimuksen päättyessä. c) Laitteistohuollon, -ylläpidon ja -vaihdon tapauksissa (esimerkiksi asiakkaan salassa pidettävää tietoa sisältävän rikkoontuneen levyn vaihto). 4) Turvallisuusluokitellun tietoaineiston tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.	Kyllä (voi soveltua asiakkaan konfigurointimahdollisuuksien osalta)
Osa-alue 11: Muutostenhallinta ja järjestelmäkehitys	
MH-01 - Muutostenhallinta	
1) Pilvipalveluun tehtäviin muutoksiin on käytössä turvallisuuden huomioiva muutostenhallintamenettely. Muutostenhallintamenettely huomioi myös vaatimustenmukaisuuden (vrt. TJ-07) sekä sopimusvelvoitteet. 2) Muutoksiin liittyvät riskit arvioidaan ja hyväksytetään soveltuvilla tahoilla. 3) Muutokset testataan ennen niiden käyttöönottoa tuotantoympäristössä. 4) Testausympäristöt ovat eroteltuja tuotantoympäristöistä. 5) Testaus suunnitellaan ja toteutetaan siten, että se tuottaa luotettavan kuvan muutoksen vaikutuksista ennen siirtoa tuotantoympäristöön.	Kyllä: kohdat 1-2 (painotus yleensä hallinnollisissa menettelyissä), kohdat 3-5 (voi soveltua räätälöidyissä sovelluksissa, jossa testaukseen mahdollisesti myös asiakkaan osallistuminen tarpeen)
MH-02 - Järjestelmäkehitys	
1) Sovellukset ja ohjelmointirajapinnat (API:t) suunnitellaan, kehitetään, testataan ja otetaan käyttöön alan hyvien turvallisuuskäytäntöjen mukaisesti. Rajapintojen on kestettävä yleiset hyökkäysmenetelmät ilman, että käsiteltävien tietojen luottamuksellisuus, eheys tai saatavuus vaarantuu. 2) Tuotantoympäristö on eriytetty muista ympäristöistä (esimerkiksi kehitys-, testaus- ja laadunvarmistusympäristöistä). 3) Versionhallinnan turvallisuus on huomioitu vähintään siten, että menettelyt luotettavasti estävät valtuuttamattomien versioiden siirron tuotantoympäristöön. 4) Turvallisen ohjelmistokehitysprosessin käytännöt on jalkautettu organisaatioon jokaiseen osaan, joka on tekemisissä kyseisen ohjelmiston kanssa. 5) Tilanteissa, joissa pilvipalvelun (tai sen osan) lähdekoodin suunnittelu, kehittäminen, testaus tai provisiointi ulkoistetaan, sopimuksissa huomioidaan erityisesti: a) Turvallisen ohjelmistokehitysprosessin vaatimukset (erityisesti suunnittelun, kehitystyön ja testauksen osalta), b) näyttö riittävästä testauksesta, c) hyväksymistestaus sovittujen toiminnallisten ja ei-toiminnallisten vaatimusten mukaisesti, ja d) oikeus testata kehitysprosessia ja valvontatoimia, myös pistokokeina.	Ei