LAPIN AMK
Lapland University of Applied Sciences

LAINSÄÄDÄNNÖN VAIKUTUS JULKISTEN PILVIPALVELUIDEN KÄYTTÖÖN JULKISELLA SEKTORILLA

Kangas Mikko

Opinnäytetyö

Tietojenkäsittelyn koulutus
Tradenomi (AMK)

2023

LAPIN AMK
Lapland University of Applied Sciences

Opinnäytetyön tiivistelmä

Tietojenkäsittelyn koulutus
Tradenomi (AMK)

Tekijä	Mikko Kangas	Vuosi	2023
Ohjaaja	Marko Leinonen		
Työn nimi	Lainsäädännön vaikutus julkisten pilvipalveluiden käyttöön julkisella sektorilla		
Sivumäärä	49		

Tässä kuvailevassa kirjallisuuskatsauksessa käsiteltiin pilvipalveluiden hyödyntämistä julkishallinnossa. Opinnäytetyön tarkoituksena oli selvittää lainsäädännön vaikutusta julkishallinnon mahdollisuuksiin käyttää julkisia pilvipalveluita. Tavoitteena oli selvittää mitä rajoituksia lainsäädäntö asettaa salassa pidettävän ja turvaluokitellun tiedon käytölle julkisissa pilvipalveluissa ja millaisia palveluita on pystytty ottamaan käyttöön hyödyntäen julkisia pilvipalveluita. Opinnäytetyössä tutkittiin julkishallinnon pilvipalveluiden käyttöä liittyen seuraaviin tietotyyppeihin salassa pidettävä, henkilötieto, turvallisuusluokiteltu IV luokan tieto.

Opinnäytetyössä tutkittiin julkishallinnon pilvipalveluiden käyttöä sitä ohjeistavien dokumenttien ja lakien pohjalta. Pääasiallisena materiaalina käytettiin valtioneuvoston, valtiovarainministeriön sekä Traficomin ohjeistuksia.

Kirjallisuuskatsauksessa selvisi, että julkishallinnossa ei ole vielä juurikaan hyödynnetty julkisia pilvipalveluita salassa pidettävän ja turvallisuusluokitellun tiedon kohdalla. Julkishallinnon pilvipalvelut rajoittuvat tällä hetkellä julkisen tiedon, pieniriskiseksi todetun tiedon sekä erilaisten testiympäristöjen käyttöön. Kirjallisuuskatsauksessa selvisi myös, että julkisia pilvipalveluita on mahdollista käyttää tietotyypeillä salassa pidettävä, henkilötieto sekä turvallisuusluokiteltu IV luokan tieto, mutta palveluiden käyttöönottoa on hidastanut turvallisuusluokitellun tiedon säilytykseen liittyvät erityisvaatimukset sekä ohjeistuksien keskeneräisyys.

Avainsanat Pilvipalvelut, Julkishallinto, IaaS, PaaS, SaaS, PiTuKri

LAPIN AMK
Lapland University of Applied Sciences

Abstract of Thesis

Business Information Technology
Bachelor of Business Administration

Author	Mikko Kangas	Year	2023
Supervisor	Marko Leinonen		
Subject of thesis	The impact of legislation on the use of public cloud services in the public sector		
Number of pages	49		

This thesis' descriptive literature review handles the utilization of cloud services in public administration. The purpose of the thesis was to find out the impact of legislation on the possibilities of public administration to use public cloud services. The goal was to find out what restrictions the legislation places on the use of confidential and security classified information in public cloud services and what kinds of services were executed using public cloud services. The thesis examines the use of public administration cloud services in relation to the following types of data, confidential, personal data, security-classified IV class data.

The thesis studied the use of public administration cloud services based on the documents and laws that guide it. The guidelines of the Government, the Ministry of Finance and Traficom were used as the main material.

The literature review revealed that the public administration had not yet made much use of public cloud services for confidential and security classified information. The public administration's cloud services where then limited to the use of public data, data identified as low risk, and various test environments. The literature review also revealed that it was possible to use public cloud services with the information types of confidential, personal data and security classified class IV information, but the implementation of the services had been slow due to the special requirements related to the storage of classified data and the incompleteness of the instructions.

Keywords Public Cloud, IaaS, PaaS, SaaS, PiTuKri

SISÄLLYS

KÄYTETYT LYHENTEET

IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service
DoS	Denial of Service
PiTuKri	Pilvipalveluiden turvallisuuden arviointikriteeristö
KataKri	Kansallinen turvallisuuden arviointikriteeristö

1 JOHDANTO

Pilvipalveluiden kasvu on voimakasta, ja IDC:n (2021) julkaiseman tutkimuksen mukaan pilvipalveluiden markkina (infrastruktuurin, laitteet, ohjelmat ja palvelut) nousisi vuoden 2021 706,6 miljardista vuoteen 2025 mennessä 1 300 miljardiin dollariin vuotuisen kasvun pysyessä samana (16,9 %). Valtiovarainministeriön (2020a) Tuottavuutta pilvipalveluilla -ohjeen mukaan pilvipalveluista on muodostumassa keskeinen palvelumuoto ja on odotettavissa, että jo muutaman vuoden kuluttua paikalliseen konesaliin toteutettava palvelu tai teknologinen alusta ei ole enää oletusarvo vaan poikkeustapaus.

Tämän opinnäytetyön tarkoituksena on selvittää miten ja millaisilla ehdoilla julkiseen pilvipalveluun siirtyminen julkishallinnossa voidaan tehdä ja millaisia mahdollisuuksia ja haasteita pilvipalvelut tuovat julkishallinnolle. Tavoitteena on selvittää mitä rajoituksia lainsäädäntö asettaa sensitiivisen datan käytölle julkisissa pilvipalveluissa ja millaisia palveluita on jo otettu käyttöön hyödyntäen julkisia pilvipalveluita. Opinnäytetyössä tutkitaan julkishallinnon pilvipalveluiden käyttöä kokonaisuudessaan pääpainon ollessa kuitenkin salassa pidettävän ja turvallisuusluokitellun datan käytössä. Opinnäytetyö vastaa julkisen sektorin toimijoiden tietotarpeeseen tuomalla esiin pilvipalveluihin siirtymisessä tarvittavaa tietoa.

Opinnäytetyön tutkimuskysymys on:

- Miten lainsäädäntö ohjaa pilvipalveluiden käyttöä julkishallinnossa?

Apukysymyksiä ovat:

- Mitä palveluita on pystytty siirtämään julkiseen pilvipalveluun?
- Miltä tulevaisuus pilvipalvelujen osalta näyttää julkishallinnossa?

2 PILVIPALVELUIDEN HYÖDYNTÄMINEN

On-premisellä tarkoitetaan yrityksen omissa tiloissa olevia fyysisiä palvelimia ja ohjelmistoja. Yritys voi hoitaa ylläpidon itse tai ylläpito on voitu ulkoistaa kolmannelle osapuolelle, jolloin puhutaan hosted on-premise palvelusta. On-premise-palveluiden etuna ovat parempi turvallisuus ja hallittavuus, koska data pysyy kaikissa tilanteissa omissa tiloissa ja yrityksellä on täysi kontrolli omaan dataansa. Huonoja puolia ovat esimerkiksi korkeammat ylläpitokustannukset, kustannusten heikompi ennustettavuus sekä heikompi skaalautuvuus. On-premise ympäristössä on myös enemmän huoltokatkoja fyysisten palvelinten uusimisien, huoltojen sekä päivitysten yhteydessä. (Empower 2022.)

Pilvipalvelulla tarkoitetaan erilaisten laskentapalvelujen tarjoamista internetin kautta. Palveluita voivat olla esimerkiksi palvelinten, tallennustilan, tietokantojen ja ohjelmistojen tarjoaminen. Laskutus voi perustua käytettyyn levytilaan, käytettyihin suorittimen sykleihin tai käytettyyn kaistan leveyteen. (Microsoft 2022a.) Pilvipalveluiden etuja ovat esimerkiksi edullisuus, hyvä skaalautuvuus, luotettavuus ja tuottavuuden parantuminen huoltokatkojen jäädessä vähäiseksi (Microsoft 2022b). Pilvipalveluiden kustannukset on myös helpompi ennakoida koska laitteiden uusimistarve poistuu palvelinympäristön osalta palvelun käyttäjän näkökulmasta (Empower 2022).

2.1 Pääasialliset pilvipalveluiden toimitusmallit

Julkinen pilvipalvelu on kolmannen osapuolen julkisessa internetissä tarjoama palvelu, joka on kaikille avoin. Julkista pilvipalvelua voi ylläpitää yritys, akateeminen organisaatio tai valtio. (NIST 2011.) Yksityinen pilvi on yhden organisaation käyttöön tarkoitettu pilvi. Yksityisen pilven käyttäjiä voivat olla esimerkiksi saman yrityksen eri liiketoimintayksiköt. Yksityinen pilvi voi olla yrityksen omassa ylläpidossa tai sen ylläpito on voitu ulkoistaa. Yksityinen pilvi voi olla pilvipalvelu tai on-premise-palvelu. (NIST 2011.) Hybridipilvi on kahden tai useamman pilvi-infrastruktuurin yhdistelmä. Pilven eri osat muodostavat oman kokonaisuutensa, mutta ne ovat toisiinsa sidottuja mahdollistaen datan siirtymisen eri pilvien välillä. Hybridipilvi sisältää aina yksityisen pilven tai on-premise-palvelun sekä julkisen

pilven. Hybridipilven tarkoituksena on yhdistää molempien ympäristöjen etuja esimerkiksi tuomalla parempaa skaalautuvuutta ja matalampia kustannuksia julkisen pilven kautta sekä mahdollistaa yksityisen pilven ja on-premisen tarjoama parempi turvallisuus ja hallittavuus Usein vähemmän kriittiset palvelut on siirretty pilveen, ja yritykselle kriittiset palvelut ovat yksityisessä pilvessä. (Murugesan & Bojanova 2015, 9–10.)

2.2 Muut toimitusmallit

Monipilviympäristö on malli, jossa on useampia toisistaan erillään olevia julkisia tai yksityisiä pilvipalveluita. Tärkein ero monipilviympäristön ja hybridipilven välillä on se, että monipilviympäristössä eri pilvipalvelut eivät ole yhteydessä toisiinsa. Syitä monipilviympäristön käyttöön on monia kuten esimerkiksi halu välttää riippuvaisuutta yhteen palvelun tuottajaan, kustannusten optimointi, työkuormien jakaminen eri ympäristöihin, globaalin yrityksen halu käyttää lähellä sijaitsevaa palvelun tuottajaa, palveluiden hajauttaminen liiketoiminnan jatkuvuuden varmistamiseksi sekä se seikka. että yksikään palvelun tuottaja ei pysty täyttämään yrityksen kaikkia tarpeita. (Cloudian 2022.)

Yhteisöpilvi tarkoittaa tietyllä toimialalla toimivan yhteisön käytössä olevaa pilvipalvelua. Yhteisöpilviratkaisussa saman tavoitteen ja vaatimukset jakavat yritykset käyttävät ja ylläpitävät yhteisiä resursseja. Yleiset julkisen pilvipalveluiden ratkaisut eivät yleensä täytä osapuolten turvallisuus tai suorituskykyvaatimuksia, ja tästä syystä valitaan yhteisöpilvipalvelut, jotka räätälöidään vastaamaan yhteisön tarpeita. (Murugesan & Bojanova 2015, 42.)

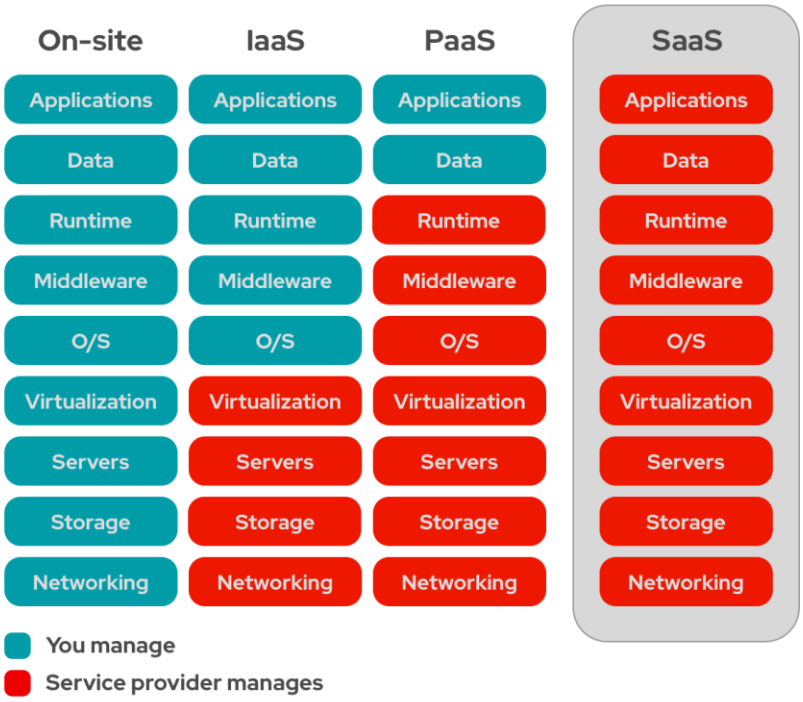
2.3 Pilvipalveluiden palvelumallit

Software as a Service tarkoittaa kuluttajalle tarjottavaa kykyä käyttää ohjelmistoja, jotka pyörivät palveluntarjoajan pilvi ympäristössä. Palveluita voidaan käyttää esimerkiksi nettiselaimen tai ohjelmiston käyttöliittymän kautta. Tässä mallissa sovelluksen taustalla olevan infrastruktuurin ja sovelluksen ominaisuuksien hallinta kuulu palvelun tuottajalle, palvelun käyttäjän vastuulle voi jäädä rajoitet-

tujen perusominaisuuksien hallinta. (NIST 2011.) SaaS-palveluita ovat esimerkiksi Microsoftin O365-palvelut, pilvipohjaiset CRM-palvelut kuten esimerkiksi HubSpot sekä pilvitallennuspalvelu Dropbox.

Platform as a Service tarkoittaa kuluttajalle tarjottavaa kykyä luoda erilaisia sovelluksia palveluntarjoajan toimittamia työkaluja käyttäen. PaaS-mallissa palvelun toimittaja tarjoaa infrastruktuurin ja työkalut, joita palvelun käyttäjä hyödyntää esimerkiksi sovelluskehityksessä. Vastuu taustalla olevasta infrastruktuurista kuten esimerkiksi palvelimista ja tallennuskapasiteetista sekä verkoista on palvelun tuottajalla. Palvelun käyttäjä vastaa tuottamistaan sovelluksista sekä mahdollisesti myös joistain alustan perusasetuksista. (NIST 2011.) PaaS-palveluita ovat esimerkiksi Microsoftin tarjoama Azure SQL Managed Instance, jossa Microsoft tarjoaa servereiden ja tallennus kapasiteetin lisäksi työkalut tietokantatyökalut (SQL Server Management Studio) palvelun käyttäjälle. (Microsoft 2022c.)

Infrastructure as a Service tarkoittaa palvelua, jossa palvelun tarjoaja toimittaa palvelun käyttäjälle infrastruktuurin kuten palvelimet, tallennustilan ja verkon. Palvelun käyttäjä vastaa käyttöjärjestelmistä ja asennettavista ohjelmistoista kokonaisuudessaan. Palvelun tuottajalla on vastuullaan ainoastaan taustalla oleva pilvi infrastruktuuri. (NIST 2011.) IaaS palveluja ovat esimerkiksi Microsoftin Azure ja Amazon Web services (AWS). Eri palvelumallien vastuiden jakautuminen on havainnollistettu kuviossa 1. Turkoosilla on merkattu palvelun käyttäjän vastuut ja punaisella palvelun toimittajan vastuut.



Kuvio 1. Vastuun jakautuminen eri palvelumalleissa (Red Hat 2022)

Kuvio 1 havainnollistaa miten vastuu alustan ja sovelluksien hallinnasta siirtyy palveluntuottajalle siirryttäessä on-premise palveluista pilvipalveluun. On huomattava, että alustan ja sovellusten hallinnan vastuun siirtyminen tarkoittaa palvelun tiilaajan kohdalla heikentynyttä mahdollisuutta vaikuttaa palveluihin sekä niiden turvallisuuteen.

2.4 Pilvipalvelun käyttämisen edut

Pilvipalveluissa on lukuisia etuja käyttäjille. Näitä etuja ovat esimerkiksi pienempi pääomantarve, pienemmät ylläpitokustannukset, käyttötarpeen mukainen skaalautuvuus sekä parantunut käytettävyys. Yksi tärkeimmistä eduista on pienempi pääoman tarve, sillä uutta pilvipalvelua perustettaessa yrityksen ei tarvitse sijoittaa pääomaa it-infrastruktuuriin, koska pilvipalveluiden maksut perustuvat yleensä käyttöön eli maksetaan esimerkiksi tallennustilasta ja suoritinkäytöstä sen sijaan, että maksettaisiin palvelimista ja ohjelmistolisensseistä. Pilvipalveluiden käyttö tuo mukanaan myös pienemmät operointikustannukset ja pienemmän ylläpitotarpeen palvelimien ja ohjelmistojen ylläpitovastuun siirtyessä palvelun-tuottajalle. (Murugesan & Bojanova 2015, 10.)

Ohjelmistojen sekä laitteistojen päivitykset tapahtuvat käyttäjän kannalta katsottuna automaattisesti, eivätkä ne aiheuta ylimääräisiä käyttökatkoja. Pilvipalvelut skaalautuvat myös yrityksen käyttötarpeen mukaan vastaamaan hetkellisten piikkien aiheuttamaan lisääntyneeseen kuormaan tai epävarmaan laskentatarpeeseen. Pilvipalvelut mahdollistavat myös pääsyn laajoihin pilvipalveluiden laskenta resursseihin Perinteisessä on-premise-ratkaisussa palvelimien resursseja on jälkeenpäin kallista lisätä, joten palvelimen valinta on osattava suunnitella ennalta vastaamaan käyttötarvetta. Pilvipalvelut mahdollistavat myös pääsyn dataan ja sovelluksiin mistä tahansa mahdollistaen datan jakamisen ja tiimityöskentelyn paikkariippumattomasti. Pilvipalveluissa tietoturvallisuus on yleensä paremmalla tasolla kuin perinteisissä on-premise järjestelmissä, joten iso toimija pystyy tarjoamaan parempitasoista turvaa ja reagoimaan erilaisiin tietoturvapoikkeamiin pientä organisaatiota nopeammin. (Murugesan & Bojanova 2015, 10–11.)

2.5 Turvallisuus ja riskit

Vaikka pilvipalveluihin on panostettu valtavasti ja suurten toimijoiden kohdalla palvelut ovat turvallisia käyttää, liittyy pilvipalvelun käyttöön myös riskejä. Suurimmat huolet liittyvät palvelun turvallisuuteen, datan yksityisyyteen, palvelun saatavuuteen sekä palvelun luotettavuuteen. Datan menettäminen, tietovuodot sekä ohjelmistojen tai datan hallinnan menettäminen sekä DoS-hyökkäykset ovat yleisimpiä huolenaiheita. (Murugesan & Bojanova 2015, 11.)

Turvallisuusongelmat voidaan luokitella CIA menetelmällä (confidentiality, integrity, availability). Luottamuksellisuudella (confidentiality) tarkoitetaan sitä, että luottamuksellista dataa käsitellään ja säilytetään tavalla, joka takaa riittävän suojauksen. Suojaustason vaatimukset voivat vaihdella eri ympäristöissä ja vaatimukset voivat koskea koko dataa tai vaan osaa siitä. Vaatimuksia ovat esimerkiksi dataan käsittelemään pääsevien käyttäjien määrittely sekä heidän datanmuokkaus oikeuksiensa määrittely. Eheydellä (integrity) tarkoitetaan sitä, että data on korruptoitumatonta ja että vain siihen valtuutetut voivat käyttää tai muokata sitä. Saatavuudella (availability) tarkoitetaan palvelun tuottajan lupausta palvelun saatavuudesta. Palvelun tarjoaja voi esimerkiksi luvata, että palvelun SLA on 99.9 %. SLA tulee sanoista Service Level Agreement eli palvelun tason sopimus. SLA: 99.9 % taso tarkoittaa käytännössä sitä, että vuoden aikana palvelussa voi olla katkoksia 8 tuntia 46 minuuttia. (Murugesan & Bojanova 2015, 208–209.)

Käyttäjätunnuksien joutuminen vääriin käsiin tai autentikointiin liittyvät puutteet voivat johtaa tietovuotoihin tai pahimmassa tapauksessa koko palvelun hallinnan menettämiseen. Palvelunestohyökkäyksillä voidaan myös lamauttaa palvelun toiminta kokonaan. Pilvipalveluun siirryttäessä on myös kiinnitettävä huomiota sopimuksiin. On erityisen tärkeää varmistaa, että datan omistajuus säilyy palvelun käyttäjällä ja data voidaan niin haluttaessa poistaa palvelusta siirtää toiseen palveluun. Tiedostojen salaukseen on myös kiinnitettävä huomiota. Tiedostot on pystyttävä salaamaan sekä siirrettäessä että levossa kun ne ovat tallennettuna kovalevylle. Salausavaimien hallinta on myös syytä säilyä palvelun käyttäjällä, jotta datan luottamuksellisuus voidaan taata. (Murugesan & Bojanova 2015, 210.)

3 TUTKIMUSMENETELMÄ JA AINEISTON KERÄÄMINEN

3.1 Kirjallisuuskatsaus

Kirjallisuuskatsaukset jaetaan useampiin eri tyyppeihin näitä tyyppejä ovat kuvaileva kirjallisuuskatsaus, systemaattinen kirjallisuuskatsaus, kvalitatiivinen meta-analyysi sekä kvantitatiivinen meta-analyysi (Salminen 2011, 6–14). Tähän opinnäytetyöhön valitsin menetelmäksi kuvailevan kirjallisuuskatsauksen. Kuvailevaa kirjallisuuskatsausta pidetään eräänlaisena yleiskatsauksena, jolle ei ole määritelty tarkkoja sääntöjä. Kuvailevassa kirjallisuuskatsauksessa käytetään laajoja aineistomääriä ja aineiston valintaa ei rajata tarkoilla metodisäännöillä vaan kuvaileva kirjallisuuskatsaus toimii itsenäisenä metodina. Kuvailevan kirjallisuuskatsauksen eri muodot ovat narratiivinen ja integroiva, valitsin näistä muodoista narratiivisen muodon ja toteutustavaksi kolmesta narratiivisen katsauksen muodoista laajimman eli yleiskatsauksen. Narratiivinen kirjallisuuskatsaus on metodillisesti kevyin kirjallisuuskatsauksen muoto. Narratiivissa yleiskatsauksessa pyritään tiivistämään suuria aineistomääriä yhteen ja pyritään luomaan helppolukuinen dokumentti, jossa kuvataan ja luokitellaan tutkittavan ilmiön ominaisuuksia. (Salminen A 2011, 7.)

Opinnäytetyössä kuvataan salassa pidettävän ja turvaluokitellun tiedon käyttömahdollisuuksia julkisissa pilvipalveluissa erilaisten dokumenttien kautta. Työssä käydään läpi julkisen hallinnon pilvipalvelu linjauksia ja pilviperiaatteita, tietotyyppien luokittelua sekä esitellään erilaisten ohje dokumenttien ja työkalujen käyttöä pilvipalvelun eri vaiheissa. Tämän kirjallisuuskatsauksen tavoitteena on löytää vastaukset tutkimus kysymyksiin hakemalla tietoa useista eri dokumenteista ja luoda eräänlainen tiivistelmä käsiteltävästä aiheesta useista lähteistä kerätyn tiedon pohjalta. Narratiivinen kirjallisuuskatsaus sopii tähän tarkoitukseen hyvin vapaampana tutkimusmenetelmänä. Tämä kirjallisuuskatsaus kuvaa tutkittavaa aihetta ja siihen vaikuttavia ilmiöitä ja siten mahdollistaa vastausten löytämisen asetetuille tutkimuskysymyksille. Lainsäädäntö on alan nopean kehityksen vuoksi jatkuvassa muutoksessa lakeja ja ohjeistuksia on muutettu vastaamaan uusien palvelumuotojen vaatimuksia. Narratiivisen kirjallisuuskatsauksen avulla tästä aiheesta voidaan tuoda esiin uuttakin tietoa.

3.2 Aineistonkeruu ja analysointi

Aloitin materiaalin keräämisen hakemalla tietoa hakukoneen avulla useilla eri hakusanoilla. Tarkoituksena oli löytää luotettavia lähteitä opinnäytetyössä käytettäväksi materiaaliksi. Luotettavia lähteitä voisivat olla asiantuntijaorganisaatioiden julkaisut, viranomaisten julkaisemat materiaalit ja tieteelliset tutkimusartikkelit. Kaupallisten toimijoiden materiaalit jätin pois koska niiden puolueettomuutta ja luotettavuutta ei voi taata. Kirjallisuuskatsauksessa käytettävän materiaalin tuli sisältää julkishallinnon pilvipalveluihin liittyvää ohjeistusta, nykyisiä käytäntöjä kuvaavaa materiaalia sekä materiaalia pilvipalveluiden käyttöä ohjaavasta lainsäädännöstä. Luonnollisesti materiaalin tuli käsitellä aihetta Suomen lainsäädännön ja julkisen hallinnon näkökulmasta koska opinnäytetyö rajoittuu käsittelemään ainoastaan julkisen hallinnon julkisten pilvipalveluiden käyttöä Suomessa. Materiaalin tulee olla tuoretta koska ala muuttuu nopeasti. Rajasin materiaalin siten, että se saa olla maksimissaan viisi vuotta vanhaa.

Alustavien hakujen perusteella luotettaviksi materiaalin lähteiksi valikoitui Traficomin sekä valtioneuvoston sivustot molemmilta sivustoilta löytyi runsaasti materiaalia opinnäytetyön pohjaksi. Hain materiaalia Traficomin verkkosivuilta https://www.traficom.fi/fi, sekä valtioneuvoston verkkosivuilta osoitteesta https://julkaisut.valtioneuvosto.fi. Traficomin sivustolla käytin hakusanaa pilvipalvelu, lisäksi rajasin hakutuloksia sisältämään ainoastaan tilastoja ja julkaisuja. Tällä haulla tuli kaksi dokumenttia, pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) sekä Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille näistä jälkimmäisen rajasin pois koska PiTuKri dokumentissa käsitellään samat aiheet yksityiskohtaisemmin. Valtioneuvoston sivuilla käytin hakusanaa pilvipalvelu ja rajasin hakutuloksia asiasanalla julkinen hallinto. Tällä haulla sain neljä dokumenttia, jotka ovat julkisen hallinnon pilvipalvelu linjaukset, pilvipalveluiden soveltamisohje, turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa sekä tuottavuutta pilvipalveluilla. Näiden hakujen jälkeen tutustuin alustavasti materiaaleihin ja totesin, että nämä aineistot riittävät tämän opinnäytetyön materiaaliksi. Näiden hakujen lisäksi materiaaliksi valikoitui tietoturvallisuuden auditointityökalu Katakri, johon viitattiin PiTuKri dokumentissa sekä Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä, johon viitataan

dokumentissa turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa. Taulukossa 1 on listattuna kirjallisuuskatsaukseen valitsemani materiaali.

Taulukko 1. Kirjallisuuskatsaukseen valittu aineisto

Nimi	Julkaisija	Julkaisu-vuosi
Tuottavuutta pilvipalveluilla	Valtiovarainministeriö	2020
Julkisen hallinnon pilvipalvelu linjaukset	Valtiovarainministeriö	2018
Pilvipalveluiden soveltamisohje	Valtiovarainministeriö	2020
Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa	Valtiovarainministeriö	2020
Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä	Valtiovarainministeriö	2021
Pilvipalveluiden turvallisuuden arviointi kriteeristö (PiTuKri)	Traficom	2020
Tietoturvallisuuden auditointityökalu viranomaisille (Katakri)	Traficom	2020

3.3 Käytettävän aineiston esittely

Tuottavuutta pilvipalveluilla on lyhyehkö perusdokumentti, joka käsittelee pilvipalveluiden kehitystä ja eri pilvipalvelu malleja. Dokumentissa käsitellään julkisen hallinnon pilviperiaatteita, pilvipalveluiden tuomia hyötyjä sekä haasteita. Dokumentin tarkoituksena on kuvata keskeisiä seikkoja, joita tulee ottaa huomioon uusia pilvipalveluita suunniteltaessa ja käytettäessä.

Julkisen hallinnon pilvipalvelulinjaukset dokumentti on myös lyhyehkö perusdokumentti, joka käsittelee pilvipalvelu linjauksia ja niiden tavoitteita sekä tiedonkäsittelyn vaatimuksia ja pilvipalveluiden käytön haasteita. Dokumentissa käydään läpi myös pilvipalveluiden palvelu ja toteutus mallit.

Pilvipalveluiden soveltamisohje on jatkoa Tuottavuutta pilvipalveluilla dokumentille. Soveltamisohjeessa kuvataan pilvipalveluiden hyödyntämisen koko elinkaari

suunnitteluvaiheesta palvelun päättämiseen asti. Kaikille elinkaaren vaiheille on tehty yksityiskohtaiset kuvaukset, jotka sisältävät esimerkiksi roolitukset, vastuualueet ja muut huomioon otettavat asiat kuten esimerkiksi kyseisen osa-alueen riskitekijät. Dokumentti sisältää selkeitä soveltamisohjeita ja mallipohjia, jotka auttavat esimerkiksi palvelustrategian luomisessa ja pilvipalvelun soveltuvuuden tarkastamisessa.

Suositus turvallisuusluokiteltujenasiakirjojen käsittelystä dokumentissa käydään läpi turvallisuusluokittelun lähtökohtia ja merkitsemistä sekä asiakirjojen käsittelyyn ja suojaamiseen liittyviä vaatimuksia. Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalvelussa dokumentti puolestaan keskittyy riskeihin ja vaatimuksiin, jotka liittyvät pilvipalvelussa säilytettäviin turvallisuusluokiteltuihin asiakirjoihin. Dokumentissa käsitellään myös pilvipalveluiden ja pilvipalvelun tuottajien luotettavuuden arvioimista sekä pilvipalveluiden ja pilvipalveluntuottajien palvelusopimuksiin liittyviä säädöksiä.

Pilvipalveluiden turvallisuuden arviointi kriteeristö (PiTuKri) ja Tietoturvallisuuden auditointityökalu viranomaisille (Katakri) ovat auditointityökaluja, joita voidaan käyttää myös yrityksen tai viranomaisen toimesta tietoturvallisuuden arviointiin ja kehittämiseen.

4 PILVIPALVELUT JULKISHALLINNOSSA

4.1 Julkisten pilvipalveluiden käyttö Suomessa

Valtiovarainministeriö on tuottanut useita dokumentteja edistämään ja ohjeistamaan pilvipalveluiden käyttöä. Tässä luvussa käsitellään pilvipalveluiden käyttöä dokumenttien tuottavuutta pilvipalveluilla sekä julkisen hallinnon pilvipalvelulinjaukset pohjalta. Molemmat dokumentit ovat lyhyitä ja tarjoavat perustietoa julkisen hallinnon pilvipalveluiden tilasta ja pilvipalveluiden käyttöönoton vaatimuksista ja haasteista.

Suomessa käytössä olevista pilvipalveluista ja pilvipalveluiden hyödyntämisen kasvusta ei ole täsmällistä tietoa saatavilla. Valtiovarainministeriön arvion mukaan Suomi on kuitenkin edelläkävijämaihin verrattuna takamatkalla pilvipalveluiden hyödyntämisessä. Pilvipalveluiden hitaan käyttöönoton syyksi mainitaan julkisen palvelun kohdalla turvallisuusluokitellun tiedon säilytykseen liittyvät erityisvaatimukset sekä ohjeistuksien keskeneräisyys. (Valtiovarainministeriö 2020a, 15.)

Tuottavuutta pilvipalveluilla dokumentissa mainitaan tyypillisiksi jo käytössä oleviksi julkisen hallinnon palveluiksi lähinnä julkista tietoa sisältävät palvelut, pieni riskiseksi todetut palvelut sekä testauspalvelut, joissa käytetään itse luotua testi aineistoa, joka ei sisällä salattavaa tietoa. Alla on listattuna Tuottavuutta pilvipalveluilla dokumentissa mainitut käytössä olevat pilvipalvelut (Valtiovarainministeriö 2020a, 22).

- Internet-sivustojen julkaisualustat sekä julkiset yleisneuvontapalvelut tai näiden tukipalvelut (ns. julkiset tiedot ilman asiakasdataa/henkilötietoja) ovat usein toteutettu pilvipalvelualustalla.

- Tietohallinnon ja tietojärjestelmäkehityksen välineistöt (ns. julkiset

- aineistot kehittämisessä, rajatusti salassa pidettävät kehitysaineistot ja itse kehittämisvälineet ilman että tuotantodata tai tuotantoympäristö paljastuu).

- Tietyt testauspalvelut tai niiden osat, joissa julkista, tai luotua testiaineistoa (ei-todellista), erityisesti kehittämisputken automaattitestauksessa.
- Tietyt sisäiset palvelut, joissa tietosuojavaikutusten arvioinnin
- perusteella on pienet riskit (ns. oman henkilöstön henkilötiedot, ei
- kansalaisten tietoja eikä erityisiä henkilötietoryhmiä henkilöstöstä –
- esim. taloushallinnon tietyt järjestelmät).
- Tietyt viestintäpalvelut, joissa on tietosuojavaikutusten arvioinnin
- perusteella pienet riskit.
- Tietyt tukipalvelut edellisiin liittyen.
- Tallennus- ja prosessointikapasiteetti pilvestä.

4.2 Pilvipalveluiden linjaukset ja periaatteet

Tuottavuutta Pilvipalveluilla dokumentissa mainitaan, että pilvipalveluista on muodostumassa keskeinen palvelumuoto ja että jo muutaman vuoden kuluttua uusien teknologisten alustojen ja palveluiden toteuttaminen paikallisiin konesaleihin on poikkeustapaus. Dokumentissa todetaan myös, että useimpia valmisjärjestelmiä ei ole enää saatavilla paikallisesti asennettavina, vaan ne toimitetaan pilvipalveluna. Dokumentissa korostetaan myös pilvipalveluiden tuomaa merkittävää hyötyä skaalautumisen, joustavuuden sekä jatkuvan kehittymisen kautta sekä korostetaan pilvipalveluiden merkitystä integroituvuuden edistäjänä. Julkiselle hallinnolle ehdotetaan roolia sujuvampien palveluiden luomiseen kansalaisille julkisten pilvipalveluiden avulla. Rajallisten kehityspanosten vuoksi ehdotetaan, että on syytä valita millä osa alueilla tehdään räätälöityä kehittämistä ja millä osa alueilla käytetään valmiita ratkaisuja. (Valtiovarainministeriö 2020a, 9–16.)

Julkisen hallinnon pilvipalvelulinjaukset dokumentissa on lueteltu julkisen hallinnon keskeiset pilvipalvelu linjaukset julkisen hallinnon organisaation omistaman

tiedon käsittelylle. Nämä linjaukset antavat hyvän kuvan siitä, miten julkisen hallinnon pilvipalveluiden käyttöä halutaan edistää. Alla on listattuna keskeiset pilvipalvelu linjaukset (Valtiovarainministeriö 2018, 9–10).

- Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta.
- Pilvipalveluissa on kiinnitettävä erityistä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen.
- Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset.
- Mikäli pilvipalvelu tai pilvipalveluteknologia tarjoavat parhaan palveluhyödyn ja -takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita.
- Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti sekä oleellisten sopimusehtojen muuttuessa.
- Julkisen tiedon käsittelyä ei rajoiteta.
- Ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu.

Nämä pilvipalvelulinjaukset on tarkennettu pilvipalvelu periaatteiksi, joita kaikkien julkisen hallinnon toimijoiden tulisi soveltaa (Valtiovarainministeriö 2020a, 31–32). Pilvipalvelu periaatteissa annetaan yleisiä perusperiaatteita, joita tulee noudattaa pilvipalveluiden suunnittelussa ja käytössä. Näitä ovat esimerkiksi oman toiminnan ja tarpeiden ymmärtäminen ja niiden huomioiminen valintaa tehdessä sekä tiedonhallintaan liittyvien riskien ja vaatimusten selvittäminen. Periaatteissa ohjeistetaan lisäksi pilvipalvelutyypin ja ominaisuuksien valintaa sekä korostetaan valvonnan, siirrettävyyden sekä sopimusehtojen huomioinnin merkitystä. Taulukossa 2 on listattu pilvipalvelu periaatteet.

Taulukko 2 Julkisen hallinnon pilviperiaatteet (Valtiovarainministeriö 2020a, 31–32)

#	Periaate	Kuvaus
1	Tunnista ja analysoi toiminnallinen tarpeesi, johon etsit ratkaisua	Tekninen ratkaisumalli ei ole itseisarvo vaan keskeisintä on löytää joustava ratkaisumalli tunnistettuun ja määritettyyn tarpeeseen. Ensimmäiseksi on hyvä ymmärtää toiminnan ja käyttäjien toiminta, tavoitteet ja tarpeet, johon ratkaisua haetaan. Aloita tunnistamalla, ketkä käyttävät tulevaa palvelua. Tunnista myös tiedot, joita tarpeen mukaisessa toiminnassa käsitellään.
2	Tunnista tietoosi liittyvät keskeiset riskit, tee ratkaisu pilvipalvelun käytöstä faktaperusteisesti	Arvioi edellisen kohdan perusteella, mitä riskejä ja vaatimuksia tarpeen mukaiseen toimintaan ja sen tiedonhallintaan liittyy eri käyttötilanteissa. Arvioi objektiivisesti ja faktaperusteisesti, mitkä ovat kyseisen toiminnan olennaiset riskit. Tutustu pilvipalvelutarjontaan, tee markkinatutkimusta ja laadi faktapohjainen analyysi pilvipalvelujen soveltuvuudesta tunnistettuihin riskeihin sekä toiminnalliseen tarpeeseesi nähden.
3	Suunnittele ratkaisusi ja siihen liittyvät palvelut alusta asti pilvipalveluja silmälläpitäen	Suunnittele palvelusi siten, että ratkaisusi arkkitehtuuri ja teknologiavalinnat sekä kehittämis- ja ylläpitokäytännöt heti alusta asti soveltuvat hyödyntämään pilven tuottamia palveluja täysimääräisesti.
4	Hyödynnä oletusarvoisesti julkisia pilvipalveluja	Hyödynnä ensisijaisesti ja lähtökohtaisesti julkisia pilvipalveluja. Älä toteuta yksityisiä tai yhteisön pilvipalveluja, ellei tähän ole perusteltua ja todennettavaa syytä tai julkisia pilvipalveluja ei ole saatavissa.
5	Huolehdi strategisen tiedon ja toimintojen siirrettävyydestä	Huolehdi alusta asti siitä, että keskeiset tiedot ja toiminnot ovat siirrettävissä pilvipalveluista toisaalle tarpeesi mukaan. Mikäli tietojen tai toimintojen siirtoa ei pystytä täysimääräisesti toteuttamaan, tee riskiarvio, miten toimit ja mitä tapahtuu, jos siirtotarve kuitenkin myöhemmin ilmenee. Mieti riskiarviosi perusteella, mihin tieto sijoitetaan.
6	Hyödynnä pilvipalvelun vakio-ominaisuuksia ja automaatiota täysimääräisesti	Käytä ja hyödynnä pilvipalvelussa olevia erilaisia palveluja, ominaisuuksia ja moduuleja. Vältä pilvipalvelujen räätälöintiä, pyri hyödyntämään olemassa olevia ominaisuuksia. Pilviratkaisujen ideologia perustuu siihen, että käytämme valmiita moduuleita ja vältämme tiettyjen uudelleen rakentamista. Kun ratkaisu myös koostetaan näistä valmiista palasista, on niihin helpompi hankkia vakioitu tuki palveluntarjoajalta. Pilvi ei ole pilvi ilman automaatiota. Tutkimusyhtiö Gartnerin selvitysten mukaan n. 90 % pilvipalvelujen vikatilanteista johtuu siitä, ettei käytetä julkipilven valmiita palveluja tai työkaluja jatkuvuuden varmistamiseksi. Mikäli valmisratkaisu ei täytä keskeisiä tarpeita, on parempi toteuttaa räätälöinti valmisalustalla (PaaS) kuin räätälöidä SaaS-palvelua.
7	Valvo pilvipalvelun käyttöä	Valvo pilvipalvelun teknistä toimivuutta sekä hallinnoi pilvipalvelujen parametrointia, hankintaa, provisiointia ja poistamista. Valvo erityisesti aitoa loppukäyttäjän palvelun ja toimintaprosessien laatua ja saatavuutta. Pilvipalvelujen käyttö ei sulje pois perinteisen valvonnan ja hallinnan vaatimuksia.
8	Varmista sopimusehtojen soveltuvuus ja varaudu niiden tuomiin riskeihin	Varmista, että pilvipalvelusopimus mahdollistaa myös palvelujen skaalaamisen alaspäin (erityisesti SaaS-palvelut) ja palvelujen jatkuvuuden. Tunnista pilvitoimittajien omat edut takaavien sopimusten riskit ja varaudu riskien realisoitumiseen.

4.3 Haasteet ja riskienhallinta

Valtiovarainministeriön selvityksen mukaan pilvipalveluiden käyttöönottamiseen liittyy ennakkokäsityksiä ja valmiuksien puutteita. Haasteiksi valtionhallinnossa

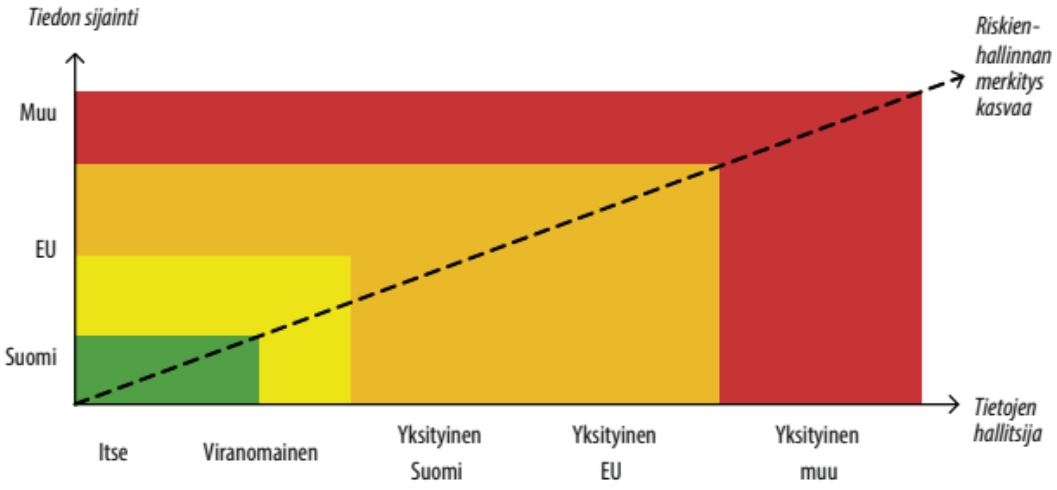
koetaan muun muassa osaamisen puute epäilyttävä tietoturva, erityislainsäädännön tiukat tulkinnat, palvelujen kokonaishallinta sekä hankala kilpailuttaminen. Pilvipalvelua hankittaessa on osattava ottaa huomioon useita seikkoja, esimerkiksi miten palvelu voidaan tarvittaessa kotiuttaa tai miten vältetään toimittajalukkoon joutuminen. On huomioitava myös se riski, että omistajarakenteen muuttuessa voi palveluun vaikuttava lainsäädäntö muuttua. (Valtiovarainministeriö 2020a, 26–27.)

Julkisen hallinnon pilvipalvelu linjauksissa käytön haasteiksi mainitaan lisäksi eijulkisten tietojen käsittely, toiminnan jatkuvuuden varmistaminen, riskien hallinnan moniulotteisuus, yksipuoliset sopimusehdot, riittävän tietosuojan ja tietoturvan tason takaaminen tiedon sijainnista ja hallinnasta riippuen. Tietoturvan toteutuminen pilvipalvelussa on haastavampi toteuttaa, kun on-premise toteutuksessa. luottamuksellisuuden, eheyden, saatavuuden ja kiistämättömyyden varmistaminen vaatii muun muassa tietoliikenne yhteyksien ja lainsäädännön tarkempaa huomioonottamista. Riskienhallinnan moniulotteisuudella tarkoitetaan tietojen hallintaan ja omistamiseen liittyvät seikat palvelun käytön aikana ja palvelun päättyessä, kuka omistaa tiedot ja kuka saa käyttää niitä. Sopimusehtoihin tulee tutustua huolellisesti, varsinkin isojen kansainvälisten toimijoiden kohdalla sopimusehdot voivat olla yksipuoliset, sopimusehtojen vaikutukset palvelulle ja siellä säilytettävälle tiedolle on ymmärrettävä. Organisaation tulee tunnistaa palvelun kriittisyys käyttäjille ja varmistaa toiminnan jatkuvuus vaaditulla tasolla myös poikkeusolosuhteissa. (Valtiovarainministeriö 2018, 19–20.)

4.4 Tiedon käsittelyn vaatimukset

Salassa pidettävälle, turvallisuusluokitellulle sekä henkilötiedoille asetetaan useita vaatimuksia tiedon sijainnin ja hallinnan suhteen. Lainsäädäntö määrittää kuka näitä tietoja voi hallinnoida ja missä näitä tietoja voidaan fyysisesti säilyttää. Julkisen hallinnon pilvipalvelulinjauksissa määritetään maantieteellisiksi sijainneiksi Suomi, EU/ETA-alue sekä muut maat. Tiedon ja palvelun tuotannon hallitsijoita voivat olla organisaatio itse, muu viranomainen tai julkinen toimija, kotimainen yksityinen toimija, EU/ETA alueella toimiva yksityinen toimija sekä EU/ETA alueen ulkopuolinen yksityinen toimija. Kuviossa 2 havainnollistetaan tiedon si-

jainnin ja hallinnan merkitystä riskien suhteen. Kuten kuvasta voi päätellä, riskienhallinnan merkitys kasvaa hallinnan siirtyessä pois itseltä sekä sijainnin siirtyessä pois Suomesta ja EU:n alueelta. (Valtiovarainministeriö 2018,17–19.)



Kuvio 2 Tiedon sijainnin ja hallinnan merkitys riskienhallinnassa (Valtiovarainministeriö 2018, 17)

Tiedon käsittelyssä on otettava huomioon lukuisia näkökohtia kuten tietosuoja asetukset, luottamuksellisuus, eheys, saatavuus, autentikointi sekä kiistämättömyys. Luottamuksellisuudella tarkoitetaan sitä, että tiedon käsittelyyn on oikeus vain siihen hyväksytyillä henkilöillä, luottamuksellisuuden toteutuminen vaatii käyttöoikeuksien hallinnan ja autentikoinnin toteuttamisen. Luottamuksellisuuden toteutuminen voi vaatia myös tietojen salaamisen joissain ympäristöissä. Eheydellä tarkoitetaan tiedon muuttumattomuuden varmistamista, käytännössä tämä tarkoittaa sitä, että tieto on ajantasaista ja oikeaa eikä sitä ole muutettu sellaisten henkilöiden toimesta, joilla ei ole siihen oikeuksia. Saatavuudella tarkoitetaan sitä, että tieto on käytettävissä aina kun sitä tarvitaan. Autentikoinnilla tarkoitetaan käyttäjän sekä palvelun identiteetin varmistamista esimerkiksi kirjautumisen yhteydessä. Kiistämättömyydellä tarkoitetaan sitä, että tietoa käsitellyt henkilö pystytään jälkikäteen tunnistamaan, tämä voidaan toteuttaa esimerkiksi lokien avulla. (Valtiovarainministeriö 2018, 17–18.)

4.5 Pilvipalveluiden käytön elinkaarimalli

Tässä luvussa käsitellään pilvipalvelun soveltamisohjetta. Pilvipalvelun soveltamisohje on suunnattu henkilöille, joiden vastuulla on esimerkiksi pilvipalvelu ratkaisuiden järjestäminen, suunnittelu, hankinta, toteuttaminen, kehittäminen ja ylläpito. Ohjeessa käydään läpi pilvipalvelun elinkaaren kaikki vaiheet ja annetaan ohjeita eri vaiheiden läpikäyntiin. Pilvipalveluiden soveltamisohje ikään kuin luo rungon pilvipalvelun elinkaaren vaiheille, ohjeistaa ja opastaa sekä tuo erilaisia työkaluja kuten malli ja asiakirjapohjia tukemaan pilvipalvelun hankita ja käyttö prosesseja (Valtionvarainministeriö 2020b, 9–10).

Pilvipalvelun elinkaaren prosessi jakautuu kuuteen vaiheeseen, sekä kaikkiin vaiheisiin liittyvään yleiseen osaan A pilvipalveluvalmiuksien kehittäminen ja pilvipalvelujen johtaminen. Vaiheessa A perehdytään pilvipalvelun hyödyntämisen mahdollisuuksiin, etuihin ja riskeihin. Tavoitteena on organisaation valmiuksien ja toimintaedellytyksien luominen, johtamisen rakenteiden luominen sekä kehittämisen tukemisen järjestäminen (Valtionvarainministeriö 2020b, 16–17).

Vaiheissa 1 ja 2 rajataan kohdetta ja määritellään vaatimuksia, tässä vaiheessa ei vielä tiedetä voiko palvelua viedä julkiseen pilvipalveluun. Vaiheissa 3 ja 4 etsitään mahdollisia ratkaisuja pilvipalvelun toteuttamiseksi ja tehdään hankinta. Vaiheissa 3 ja 4 käytetään apuna PiTuKria, tässä vaiheessa selviää pilvipalvelun käytön mahdollisuus. Vaiheessa 5 käydään läpi palvelun toteuttamista ja sen hallintaa koko pilvipalvelun käytön ajalta. Viimeisessä vaiheessa 6 käydään läpi pilvipalvelun päättämiseen ja siirtoon liittyviä seikkoja. Taulukossa 3 on kuvattu pilvipalvelun elinkaaren eri vaiheet ja kuvaukset niiden sisällöstä sekä niiden käyttöön tehdyistä dokumenttipohjista. (Valtionvarainministeriö 2020b, 14–15.)

Taulukko 3 pilvipalvelun elinkaaren vaiheet (Valtionvarainministeriö 2020b, 15)

A: Pilvipalveluvalmiuksien kehittäminen ja pilvipalvelujen johtaminen					
Pilvistrategia-pohja Pilvipalvelujen tietoturvapolitiikka					
1. Kohteen määrittely ja rajaus	2 Kohteen vaatimusten määrittely	3 Ratkaisuvaihtoehtojen arviointi	4 Hankinta ja sopimus	5 Palvelun toteutus ja muutosten hallinta	6 Palvelun päättäminen / siirto
Kehitettävän kohteen rajausten ja reunaehtojen dokumentointipohja	Pilvipalvelujen yleiset riskit ja niiden kontrollit – esimerkki/pohja Pilvipalvelujen riskienhallinnan vaatimusten tunnistamispohja.	Pilvipalvelujen soveltuvuuden tarkistuslista Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)	Pilvipalvelujen soveltuvuuden tarkistuslista – keskeiset sopimusehdot Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)		Pilvipalvelujen päättämisen tarkistuslista

5 TURVALLISUUSLUOKITTELU JA TIETOTYYPIT

Tässä luvussa käsitellään asiakirjojen turvallisuusluokittelua ja tietotyyppejä. Turvallisuusluokitellun tiedon käyttöä pilvipalvelussa ohjaavat laki julkisenhallinnon tiedonhallinnasta (906/2019 18§) sekä valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Valtiovarainministeriö on julkaissut kaksi ohjeistusta, jotka auttavat täyttämään nämä lait ja asetukset, kun suunnitellaan uutta pilvipalvelua. Nämä ohjeet ovat Turvallisuusluokiteltavien asiakirjojen käsittely pilvipalveluissa (Valtiovarainministeriö 2020a) ja Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (Valtiovarainministeriö 2021).

Asiakirjat jaetaan erilaisiin tietotyyppeihin, jonka perusteella voidaan määritellä missä palvelussa kutakin asiakirjaa voidaan käyttää. Eri tietotyyppejä ovat julkinen, salassa pidettävä, henkilötieto, varautumisen näkökulmasta suojattava sekä neljä eri turvaluokiteltua luokkaa I–IV. Turvallisuusluokkia määritettäessä on otettava huomioon myös niin sanottu kasautumisvaikutus. Kasautumisvaikutuksella tarkoitetaan ilmiötä, jossa suuren tiedostomäärän muodostama asiakokonaisuus on yksittäistä dokumenttia merkittävämpi ja voi siten antaa aihetta korottaa turvallisuusluokkaa. (Valtiovarainministeriö 2021, 34.)

Julkisella tiedolla tarkoitetaan kuten jo nimikin kertoo, julkista kaikille saatavilla olevaa tietoa, jota on tarve suojata ainoastaan eheyden ja saatavuuden kannalta. Salassa pidettävällä tiedolla tarkoitetaan viranomaisen turvallisuusluokittelematonta salassa pidettävää tietoa, jos nämä tiedot sisältävät henkilötietoa, kuuluvat ne silloin myös tietotyypin henkilötieto alle. Henkilötiedolla tarkoitetaan tietosuojalain (2018/1050) sekä EU:n tietosuoja-asetuksen (2016/679) alaista tietoa. Varautumisen näkökulmasta suojattavilla tiedoilla tarkoitetaan sellaista tietoa, joka on oltava saatavilla sellaisessakin tilanteessa, että verkkoyhteydet rajoittuvat Suomen rajojen sisäpuolelle.

Turvallisuusluokiteltavat asiakirjat jaetaan neljään turvallisuusluokkaan (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019 3 §). Alla on listattuna kuvaukset turvallisuusluokista.

- Turvallisuusluokan I asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa tiedonhallintalain 906/2019 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle

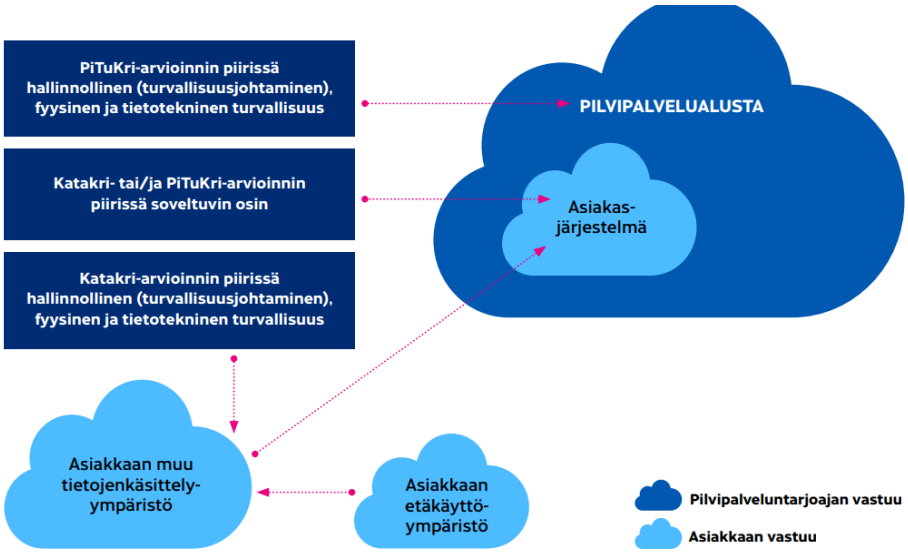
- Turvallisuusluokan II asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa tiedonhallintalain 906/2019 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle

- Turvallisuusluokan III asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa tiedonhallintalain 906/2019 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle

- Turvallisuusluokan IV asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa tiedonhallintalain 906/2019 18 §:n 1 momentissa tarkoitetulle suojattavalle edulle.

6 PILVIPALVELUIDEN TURVALLISUUDEN ARVIOIMINEN

Tässä luvussa käsitellään pilvipalveluiden turvallisuuden arvioimista Pilvipalveluiden turvallisuuden arviointi kriteeristö (PiTuKri) ja Tietoturvallisuuden auditointityökalu viranomaisille (Katakri) dokumenttien pohjalta. Luvussa esitellään PiTuKri työkalun käyttöä ja viranomaisarviointi ja hyväksyntäprosessien kulkua. PiTuKri on tarkoitettu pilvipalveluiden turvallisuuden arvioinnin työkaluksi. Kriteeristöä voidaan hyödyntää uutta palvelua suunniteltaessa tai olemassa olevan palvelun turvallisuutta arvioitaessa. Dokumentissa käydään läpi PiTuKri työkalun käyttöä aihe alueittain korttien avulla. Korttien avulla käydään läpi palvelulle asetetut vaatimukset ja arvioidaan vaatimusten toteutumista. Dokumentti sisältää esimerkkitapauksia sekä kuvaa eri tietotyypit sekä viranomaisarviointi ja hyväksyntä prosessit. Pilvipalvelun turvallisuuden arviointi jaetaan yleensä palveluntarjoajan osuuksiin ja asiakkaan osuuksiin. Kuviossa 4 havainnollistetaan miten nämä osuudet yleensä jakautuvat.



Kuvio 4 Ympäristöjen vastuunjako ja auditointityökalujen käyttö (Traficom 2020, 4)

PiTuKri ottaa kantaa salassa pidettäviin sekä turvallisuusluokitettuihin IV-luokan tietoihin. Korkeampien turvallisuusluokkien osalta työkalu ottaa kantaa ainoastaan pilvipalveluiden yleisen soveltuvuuden osalta. (Traficom 2020, 3.)

Tietoturvallisuuden auditointityökalu viranomaisille dokumentti kuvaa kansallisen turvallisuusauditointikriteeristö Katakrin käyttöä. Katakri-dokumentti on PiTuKrin tapaan auditointi työkalu, jota käytetään yritysturvallisuusselvityksissä sekä tietoturvallisuuden auditoinneissa. Dokumentissa käydään läpi Katakrin eri käyttötapauksia ja Katakri-työkalun käyttöä. Dokumentti jakautuu kolmeen osa-alueeseen, jotka ovat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. PiTuKrin tavoin eri aihealueita käsitellään korttien ja esimerkkien avulla. Katakri työkalulla arvioidaan organisaation kykyä suojata kansalista tai kansainvälistä turvallisuusluokiteltua tietoa. Katakri työkalua käytetään esimerkiksi yritysturvallisuusselvityksessä, kun yritys tarvitsee oikeuden käsitellä turvallisuusluokiteltuja kansallisia tai kansainvälisiä viranomaistietoja. Yritysturvallisuusselvityksen tekee suojelupoliisi. Katakriin sisältyvät tietoturvan vaatimukset perustuvat olemassa olevaan lainsäädäntöön ja velvoitteisiin. Kuvio 4 havainnollistaa palveluntarjoajan ja asiakkaan vastuunjakoa sekä PiTuKri ja KataKri työkalujen käyttömahdollisuuksia pilvipalvelu ympäristössä. (Traficom 2020b, 5–6.)

6.1 Turvallisuuden arviointi

Pilvipalvelun turvallisuuden arviointiin on mahdollista käyttää useita eri menetelmiä. Näitä menetelmiä voivat olla esimerkiksi itsearviointi, sertifikaatit, sopimustekniset sitoumukset, ulkopuolisen riippumattoman tahon todennukset sekä jatkuva auditointi. Kun arvioidaan olemassa olevia viitekehyksiä ja sertifiointeja on huomioitava mitä asioita sertifioinnit mittaavat, jotta voidaan taata Pitukrissa kuvattujen vaatimusten täyttyminen. Viranomaisen vastuulla on järjestää riittävän kattava ja luotettava arviointi turvallisuuden takaamiseksi. (Traficom 2020, 5.)

Taulukossa 5 on Pitukri dokumentissa käytettävä tietotyyppien luettelo. Tietotyypit on jaettu suojaustarpeen mukaisiin luokkiin. Tietotyyppien julkinen, salassa pidettävä ja henkilötieto kohdalla voidaan käyttää julkista pilvipalvelua. Edellä mainituista julkisen ja salassa pidettävän kohdalla tietojen fyysistä sijaintia ei rajoiteta. Henkilötietojen kohdalla fyysinen sijainti täytyy olla EU/ETA maassa. Turvaluokan IV, Turvaluokan IV kasauma ja Varautumisen näkökohdasta suojattavat tiedot kohdalla fyysinen sijainti rajataan Suomeen. Lisäksi tietotyypin varautumisen näkökohdasta suojattavat tiedot kohdalla asetetaan ehto, että palvelun on

toimittava myös tilanteessa, jossa verkkoyhteydet on rajattu Suomen maantieteellisten rajojen sisäpuolelle. Kuvan kolmea alimmaista tietotyyppiä ei voi käyttää julkisessa pilvipalvelussa. (Traficom 2020, 16).

Taulukko 5 Tietotyypit (Traficom 2020, 8)

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

PiTuKri jakautuu 11 eri osa-alueeseen. Ensimmäinen osa-alue 1 esiehdot, on erityisasemassa muihin nähden. Esiehtojen avulla määritetään jatkoarvioinnin mahdollisuus. Esiehdot osio tukee myös vastuullisen viranomaisen riskienhallinta työtä. Esiehtojen perusteella määräytyy alustavasti mitä pilvipalvelua voidaan käyttää, on kuitenkin huomioitava, että vaikka esiehtojen perusteella voitaisiin käyttää esimerkiksi julkista monikansallista palvelua voi jatkoarvioinnissa ilmetä seikkoja, jonka vuoksi monikansallinen palvelu ei ole mahdollinen. Osa-alueet koostuvat teemoittain jaetuista vaatimus korteista. Kortteihin on kuvattu seuraavat aiheet: teema, konkreettinen vaatimus, vaatimuksen soveltamiskohteet, suojaustavoite sekä lisätietokenttä. (Traficom 2020, 7.) Esiehdot on jaettu kahdelle

eri kortille. Taulukossa 6 on esiehdot kortti EE-01 jota käytetään suunniteltavan järjestelmän kuvaamiseen. Kortti jakautuu osiin vaatimus, soveltuvuus, tietotyypit, suojaustavoite sekä lisätiedot. Kortin vaatimus kohta havainnollistaa millä tasolla järjestelmä pitää olla kuvattuna, jotta täytetään annetut vaatimukset. Lisätiedot kohdassa annetaan tarkempaa tietoa ja ohjeistusta vaatimusten täyttämiselle. Suojaustavoite kohdasta ilmenee kortin tarkoitus, joka on palvelun käyttötarkoitukseensa soveltumisen ja sen riskien arvioimisen mahdollistaminen Soveltuvuus, ja tietotyypit kohdat kertovat mitä tietotyyppejä ja mitä osa-aluetta kortti koskee.

Taulukko 6 Esiehdot kortti EE-01 (Traficom 2020, 14)

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

Taulukon 7 EE-02 korttia käytetään lainsäädäntöjohdannaisten riskien kuvaamiseen. EE-01 kortin tavoin EE-02 kortti jakautuu osiin vaatimus, soveltuvuus, tietotyypit, suojaustavoite sekä lisätiedot. EE-02 kortin tavoitteena on lainsäädäntöjohdannaisten riskien ja velvoitteiden kuvaaminen mahdollistaen palvelun soveltuvuuden ja riskien arvioinnin annetun kuvauksen pohjalta. EE-02 kortissa käsitellään palvelun fyysiseen sijaintiin, lainsäädäntöön ja sopimusehtoihin liittyviä asioita. Lisätiedoissa esitetään konkreettisia esimerkkejä palvelulle asetetuista vaatimuksista tiedon fyysiseen sijaintiin, sopimusehtoihin sekä tiedon käsittelyyn liittyen.

Taulukko 7 Esiehdot kortti EE-02 (Traficom 2020, 15)

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

Jatkoarvioinnin mahdollisuudet korttia (Taulukko 8), suositellaan käytettäväksi täytettyjen esiehtokorttien tiedon arvioimisessa. Kortin perusteella voidaan määritellä mitä rajoitteita palvelulle asetetaan pilvipalvelutyypin, fyysisen sijainnin ja palveluntarjoajan suhteen. Pelkästään jatkoarvioinnin mahdollisuudet kortin perusteella ei voida kuitenkaan arvioida palvelun ja tietojen käsittelyn soveltuvuutta pilvipalveluun. Jokainen pilvipalvelu hanke on käytävä läpi tapauskohtaisesti PiTuKri-työkalua käyttäen käyden läpi työkalun kaikki osa-alueet.

Taulukko 8 Jatkoarvioinnin mahdollisuudet (Traficom 2020, 16)

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

Tässä työssä en käy läpi kaikkien osa-alueiden kortteja vaan esittelen työkalun käyttöä PiTuKri dokumentin malli esimerkkien avulla. Taulukossa 9 on PiTuKri työkalun eri osa-alueet ja kortit. Kortteja on kaikkiaan 41 kappaletta.

Taulukko 9. PiTuKri työkalun osa-alueet

Osa-alue	Kortit	Nimi
1	EE01, EE02	Esiehdot
2	TJ01-TJ08	Turvallisuusjohtaminen
3	HT01-HT05	Henkilöstöturvallisuus
4	FT01-FT05	Fyysinen turvallisuus
5	TTO1-TT02	Tietoliikenneturvallisuus
6	IP10-IP03	Identiteetin ja pääsyn hallinta
7	JT01-JT05	Tietojärjestelmäturvallisuus
8	SA01-SA03	Salaus
9	KT01-KT04	Käyttöturvallisuus
10	SI01-SI02	Siirrettävyys ja yhteensopivuus
11	MH01-MH02	Muutostenhallinta ja järjestelmäkehitys

Taulukossa 10 näkyy esimerkki vaatimusten kohdentumisesta palveluntarjoajan ja asiakkaan kesken, kun asiakasjärjestelmä on pilvipalvelussa IaaS-palvelumallilla tuotettuna. Vastuut on jaoteltu korteittain siten, että saman kortin eri alakohta voi olla eri osapuolien vastuulla tai molempien vastuulla. Eri palveluntuottajien erilaisten teknisten toteutusten ja sopimusehtojen vuoksi alla olevaa taulukkoa ei voida yleistää tai verrata toisen toimittajan vastaavaan ratkaisuun. (Traficom 2020, 52–53.)

Taulukko 10 Vaatimusten kohdentaminen IaaS mallissa 1/2 (Traficom 2020, 53)

ID	Alakohta	Vastuu/Asiakasympäristön osuus	Vastuu/Pilvipalveluntarjoajan osuus
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (soveltuvuuden arviointi)	x
	3	-	x
	4	x (soveltuvuuden arviointi)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a-d	x (soveltuvin osin)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a-d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	x	x
JT-03	1	- (Ellei asiakasjärjestelmässä edelleen eri erottelutarpeisia asiakkaiden tietoja.)	x
JT-04	1	x	x
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d	x (mikäli asiakas toteuttaa siirron asiakasympäristön kautta/välityksellä)	x
	2 e-f	-	x
	3	x	x
KT-04	1 a-b	x	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (sopimuksen osalta)	x
	4-5	x (voi soveltua asiakkaan konfigurointimahdollisuuksien osalta)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x	x

6.2 PiTuKri:n käyttö vaatimuksenmukaisuuden arvioinnissa

Tässä esimerkissä kuvataan kriteeristön käyttöä turvallisuusluokitellun luokan IV tiedon arviointiin henkilöstöturvallisuuden kohdalla. Esimerkissä selviää, kuinka korttien avulla saadaan selkeämpi kuva vaatimuksista ja tarvittavista toimenpiteistä, kun pelkän lakitekstin perusteella. Tässä esimerkissä viranomainen on tunnistanut yhteyden lakitekstin ja Korttien HT-03, HT-04 ja HT-05 välillä. Alla siteeraan valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta (1101/2019 §8).

> Turvallisuusluokitellun asiakirjan käsittelyoikeus voidaan antaa vain sille, jolla työtehtäviensä tai muiden valtionhallinnon viranomaisen tehtävien hoitamiseen liittyvän tarpeen vuoksi on tarve saada tietoja asiakirjasta tai muutoin käsitellä sitä ja jolle on selvitetty turvallisuusluokiteltujen tietojen suojaamista koskevat ohjeet ja menettelyt ja joka tuntee asiakirjojen käsittelyä koskevat velvoitteet. Valtionhallinnon viranomaisen on pidettävä luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan I, II tai III asiakirjoja. Luettelossa on mainittava henkilön tehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu. Valtionhallinnon viranomaisen on pidettävä huolta, että se, joka ei enää toimi tehtävissä, joihin oikeus luokiteltujen asiakirjojen käsittelyyn perustuu, palauttaa asiakirjat tai tuhoaa ne asianmukaisella tavalla. (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019 §8.)

Taulukossa 11 on kortti HT-03 joka koskee salassapito- ja vaitiolo sitoumuksia. Kortissa HT-03 valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 §8) vastaa vaatimus 1 salassapito- tai vaitiolomenettelystä. Vaatimuksena on salassapito tai vaitiolositoumus menettelyn käyttäminen. Lisätietoja kentässä määritellään asiat, jotka tulee sisältyä salassapitosopimukseen, joka vaaditaan kaikille tiedon käsittelijöille. Vaadittaviin asioihin sisältyy salassa pidettävän aineiston määrittely, salassapitosopimuksen ehdot, sopimuksen päättymisen jälkeen vaadittavien toimien määrittely, tiedon omistajan määrittely, tietojen käytön ja luovuttamisen säädökset sekä sääntörikkomuksien seuraamukset. Kortilla HT-03 tavoitellaan henkilöstön luotettavuuteen liittyvien riskien pienentämistä lisäämällä tietoisuutta tietosuoja asioista.

Taulukko 11 Kortti HT-03 (Traficom 2020, 25)

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

Taulukossa 12 oleva kortti HT-04 käsittelee turvallisuustietoisuutta. Valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 §8) vastaa kaikki kortin vaatimukset pois lukien vaatimus 5 säännöllisestä valvonnasta. Vaatimuksena on turvallisuuteen liittyvien periaatteiden ja toimintatapojen kuvaaminen ja ohjeistaminen henkilöstölle, kuvausten ja ohjeistuksen ajantasaisena pitäminen, ohjeistuksen käyttöönottamisen ja käytön varmistaminen ja säännöllinen seuranta. Lisäksi vaaditaan, että ohjeistus kuvaa prosessit ja käsittely-ympäristöt koko tiedon elinkaaren ajalta. Lisätietokentässä tarkennetaan vaatimusten täyttämistä esimerkein. tavoitteena HT-04 kortilla on varmistaa turvallisten toimintatapojen suunnittelu ja henkilöstön kyky toimia turvallisesti kaikissa tilanteissa.

Taulukko 12 Kortti HT-04 (Traficom 2020, 25)

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

Taulukossa 13 on kortti HT-05. Kortissa HT-05 valtioneuvoston asetusta asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019 §8) vastaa vaatimukset 1–2 ylläpitotehtävien luetteloinnista ja tiedonsaantitarpeen selvittämisestä ennen pääsyn myöntämistä. Vaatimuksena on, että salassa pidettävän tiedon käsittelyä vaativat tehtävät määritellään ja niistä pidetään luetteloa. Lisäksi vaaditaan tiedonsaantitarpeen määrittely ennen, kun myönnetään oikeus salassa pidettävän tiedon käsittelyyn. Lisätietokentässä kerrotaan esimerkkien avulla, miten tiedonsaantitarpeen määrittelyn menettelyä voidaan helpottaa. Tavoitteena HT-05 kortilla on mahdollistaa salassa pidettävän tiedon päätyminen vain valtuutetuille henkilöille tiedonsaantitarpeeseen perustuen. Toisena tavoitteena on salassa pidettävään tietoon kohdistuvien riskien pienentäminen.

Taulukko 13 Kortti HT-05 (Traficom 2020, 26)

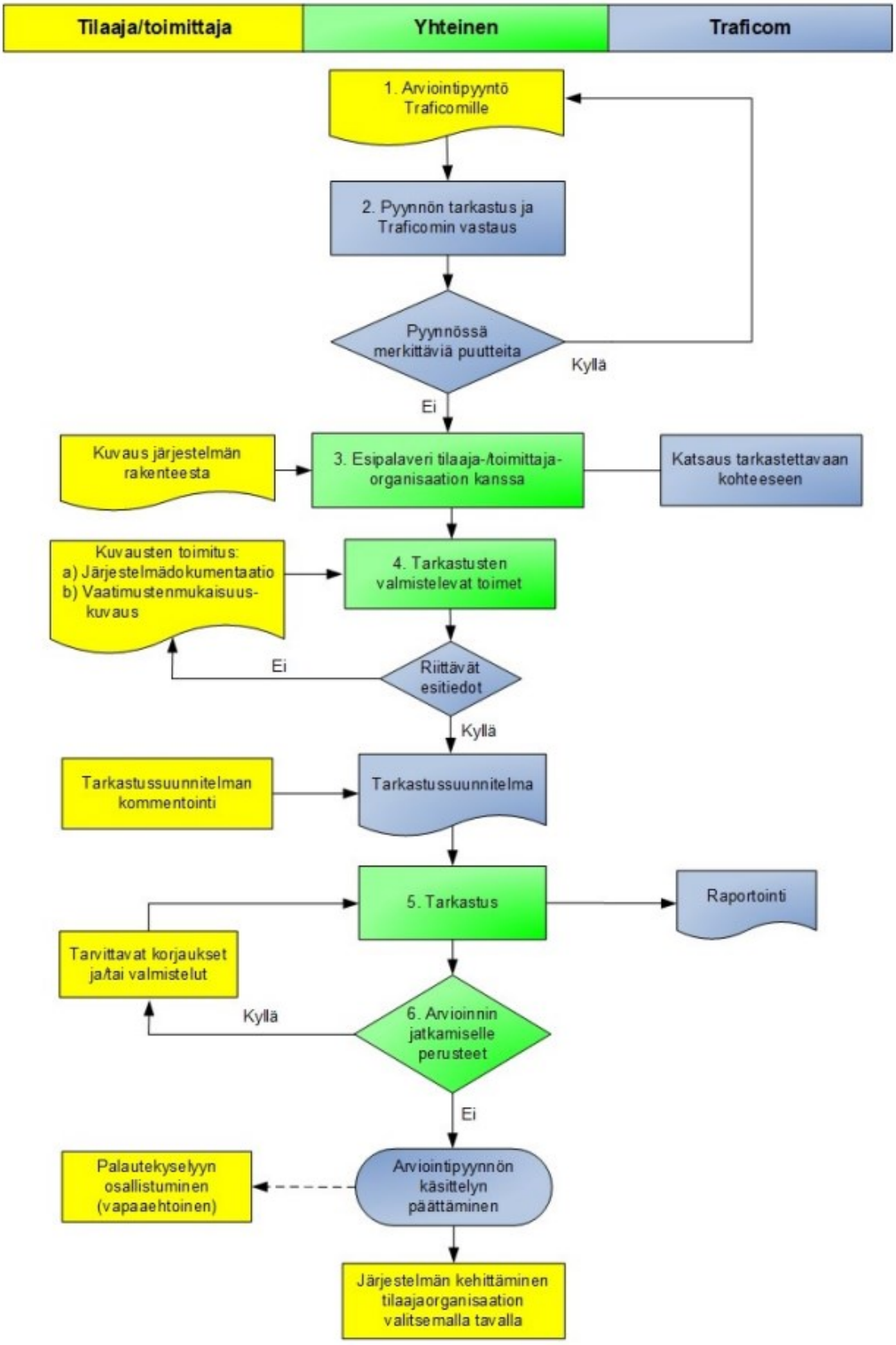
HT-05	Tiedonsaantitarpeet ja tehtävien erottelu
Vaatimus	1) Salassa pidettävän tiedon käsittelyä edellyttävistä työtehtävistä ylläpidetään luetteloa. Tällaisiksi työtehtäviksi tulkitaan kuuluvaksi myös sellaiset kehitys- ja ylläpitotehtävät, joissa on suora tai epäsuora mahdollisuus päästä salassa pidettävään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

Korttien avulla saadaan konkreettiset menettelyohjeet palvelun suunnittelemiseen ja toteutukseen. Pilvipalvelua suunniteltaessa on suositeltavaa käyttää PiTuKri kriteeristöä palvelun vaatimuksen mukaisuuden selvittämiseksi ennen kuin edetään Traficomin arviointi ja hyväksyntäprosessiin. Näin varmistetaan arviointiprosessin sujuva läpikäynti.

6.3 Viranomaisarviointi ja -hyväksyntä

Viranomaiset voivat käyttää tietojärjestelmiensä tietoturvallisuuden tarkastamiseen Traficomia tai sen hyväksymää tietoturvallisuuden tarkastamiseen erikoistunutta laitosta. Arviointiprosessia ja hyväksyntäprosessia ohjaa laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (2011/1406) sekä laki kansainvälisistä tietoturvallisuusvelvoitteista (2004/588). Arviointi prosessissa voidaan käyttää apuna PiTuKria (Traficom 2020, 61). Traficomin tietoturvallisuus arviointi ja hyväksyntäprosessiin pääseminen edellyttää perusteltua tarvetta käsitellä turvaluokiteltua tai salassa pidettävää tietoa (Traficom 2021, 1).

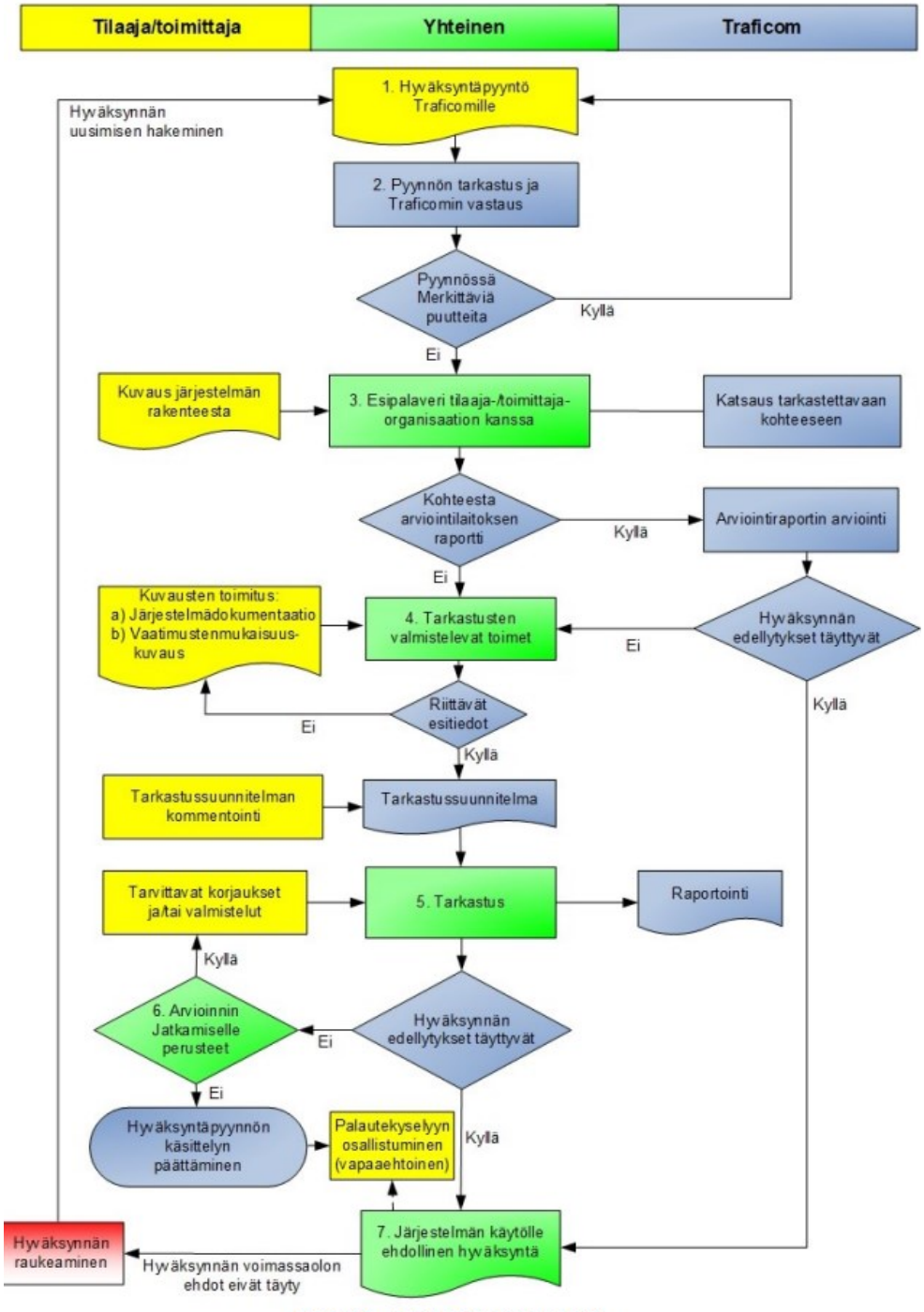
Arviointiprosessilla tarkoitetaan menettelyä, jossa Traficom tarkastaa tilaajan toimittaman dokumentaation perusteella täyttääkö järjestelmä lain sille asettamat vaatimukset. Arviointiprosessi alkaa, kun tilaaja toimittaa Traficomille arviointipyynnön. Arviointiprosessi koostuu useammasta eri vaiheesta, joissa tilaaja/ toimittaja sekä Traficom käsittelevät arvioitavaa järjestelmää tilaajan/toimittajan tuottaman materiaalin pohjalta. Arviointiprosessin päätteeksi Traficom antaa virallisen lausunnon, jossa todetaan miltä osin järjestelmä täyttää siihen kohdistuvat vaatimukset. Arviointiprosessista edetään hyväksyntäprosessiin, kun kaikki vaatimukset on täytetty. (Traficom 2021, 1.) Kuviossa 5 näkyy arviointiprosessin eteneminen kokonaisuudessaan.



Kuvio 5 Arviointiprosessi (Traficom 2021, 3)

Kun arviointiprosessi on käyty läpi ja virallinen lausunto järjestelmän soveltuvuudesta saatu, voidaan aloittaa hyväksyntäprosessi. Prosessi alkaa, kun tilaaja toi-

mittaa Traficomille hyväksyntä pyynnön. Hyväksyntäprosessi tarkoittaa menettelyä, jonka päätteeksi Traficom antaa virallisen lausunnon järjestelmän hyväksymisestä käytettäväksi siinä turvallisuus luokassa ja niillä turvallisuus menettelyillä, joita on käytetty hyväksyntäpyynnössä. Hyväksyminen edellyttää, luonnollisesti sen, että kaikki vaadittavat turvatoimet ovat käytössä ja kaikki tarkastuksessa ilmenneet puutteet on korjattu. (Traficom 2021, 1.) Hyväksyntäprosessi on arviointiprosessin tavoin monivaiheinen prosessi, jossa tilaaja/toimittaja sekä Traficom käsittelevät aineistoa yhdessä. Hyväksyntäprosessin vaiheet näkyy kuviossa 6.



Kuva 2. Hyväksyntäprosessi.

Kuvio 6 Hyväksyntä prosessi (Traficom 2021, 4)

Traficomin myöntämän hyväksynnän voimassa pysyminen edellyttää turvallisuuden tason pysymistä ennallaan. Merkittävät turvallisuuteen vaikuttavat muutokset voivat aiheuttaa hyväksynnän raukeamiseen. Tästä syystä merkittävämpien muutoksen kohdalla on suositeltavaa hyväksyttää muutokset ennakkoon. (Traficom 2020, 63.)

7 JOHTOPÄÄTÖKSET JA POHDINTA

Tämän opinnäytetyön tavoitteena oli selvittää miten lainsäädäntö ohjaa pilvipalveluiden käyttöä julkisessa hallinnossa, mitä palveluita on pystytty siirtämään julkiseen pilvipalveluun sekä miltä tulevaisuus pilvipalveluiden osalta näyttää julkishallinnossa.

Salassa pidettävien ja turvallisuusluokiteltujen tietojen käyttöä pilvipalvelussa rajoittaa monet kansalliset ja kansainväliset lait. Pilvipalvelua suunniteltaessa tarvitaan hyvää lakien tuntemusta, tarkkaa ennakkosuunnittelua ja perehtymistä, jotta lakien vaatimukset voidaan täyttää. Tähän tarkoitukseen on luotu useita dokumentteja ja työkaluja, joita voidaan hyödyntää pilvipalvelun kaikissa elinkaaren vaiheissa. Dokumentit ja työkalut helpottavat pilvipalvelun tietoturvallisuuden ja vaatimusten määrittelyssä suuresti ja auttavat viemään hankeprojektin koordinoidusti läpi.

Valtiovarainministeriön ohjeistuksissa kannustetaan pilvipalveluiden käyttöön ja tuodaan esille niillä saavutettavia etuja. Ohjeistuksista välittyy kannustava vaikutelma pilvipalveluiden käyttöä kohtaan. Pilvipalveluiden käyttöönotto vaikuttaa kuitenkin haasteelliselta, tiukan lainsäädännön ja osittain puutteellisen ohjeistuksen vaikeuttaessa palveluiden suunnittelua ja kilpailuttamista. Valtiovarainministeriön selvityksessä valtiohallinnon virastot kokivat haasteelliseksi pilvipalvelun käyttöönottoon liittyen erityisesti tietoturvan ja tietosuojan varmistamiseen, muita haasteita olivat esimerkiksi osaamisen riittämättömyys, hankala kilpailuttaminen sekä erikoislainsäädännön tiukat tulkinnat (Valtiovarainministeriö 2020a, 26). Vaikuttaa siltä, että nämä seikat hidastavat pilvipalveluiden käyttöönottoa julkisen hallinnon kohdalla.

PiTuKri ja muut ohjeistukset helpottavat ja selkeyttävät pilvipalveluiden hankinnan suunnittelua, mutta yksityiskohtaisempia soveltamisohjeita ja esimerkkitoteutuksia kaivattaisiin lisää. PiTuKrissa on määritelty selkeästi eri tietotyyppien kohdalla, voidaanko niitä viedä julkiseen pilvipalveluun ja millä maantieteellisellä alueella palvelu voi sijaita, tämän perusteella ei voida kuitenkaan suoraan päätellä pilvipalvelun käytön mahdollisuutta vaan palvelua täytyy aina tarkastella ko-

konaisuutena ja arvioida tapauskohtaisesti palvelun soveltuvuutta siihen tarkoitukseen luotujen työkalujen avulla. Haasteita aiheuttaa suuri työmäärä ja osaamisen tarve, joka vaaditaan määrittelyihin ja arviointeihin, jotta voidaan varmistua siitä, että suunniteltava palvelu täyttää vaatimukset ja hankkeessa voidaan edetä. Vaikka alustavien selvitysten perusteella palvelu täyttäisikin vaatimukset, voi myöhemmässä vaiheessa ilmetä seikkoja, jotka estävät suunnitellun palvelun toteutuksen tai jotka pakottavat tekemään muutoksia jo suunniteltuun toteutukseen. Hankintaprosessia helpottamassa olisi hyvä olla yksityiskohtaisempia ohjeita, joissa käytäisiin tarkemmin läpi mahdollisia toteutus vaihtoehtoja, eri pilvipalvelun tuottajien palveluehtoja ja niiden vaikutusta pilvipalvelun käyttöönottoon.

Tällä hetkellä Suomessa käytössä olevista julkisen hallinnon pilvipalveluista oli vaikea löytää tilastoitua tietoa. Valtiovarainministeriön oman arvion mukaan Suomi ei ole edelläkävijämaiden joukossa pilvipalveluiden käyttäjänä (Valtiovarainministeriö 2020a, 15). Suomessa julkinen hallinto käyttää tällä hetkellä julkisia pilvipalveluita lähinnä julkisen tiedon käsittelyyn, pieniriskiseksi todetun tiedon käsittelyyn sekä erilaisiin testi ympäristöihin, joissa käytetään itse tuotettua dataa (Valtiovarainministeriö 2020a, 22). Valtiovarainministeriön arvio on, että yleiskäyttöiset toimialariippumattomat valmisjärjestelmät siirtyvät lähes kokonaan SAAS-palveluiksi, yleisenä ohjeistuksena on annettu, että tällaisia yleiskäyttöisiä palveluita tulisi suosia aina kun mahdollista (Valtiovarainministeriö 2020a, 16). Ohjeistuksen kehittyminen saatujen kokemusten perusteella tulee helpottamaan valtion virastojen pilvipalveluiden käyttöönottoa tulevaisuudessa, joten uskon, että lähitulevaisuudessa tulemme näkemään enemmän myös IaaS ja PaaS palveluita, jotka on tuotettu julkisen pilvipalvelun päälle, nähtäväksi jää mitä palveluita pilveen siirtyy ja millä aikataululla. Kokonaisuudessaan pilvipalveluiden käytöstä julkisessa hallinnossa jäi hiukan ristiriitainen kuva. Työtä pilvipalveluiden käytön edistämiseksi on selvästi tehty tuottamalla erilaisia ohjeita ja työkaluja, toisaalta pilvipalveluita ei vielä ole laajasti käytössä. Uutisoinnit Kelan epäonnistuneesta pilvi projektista ja uusien fyysisten palvelimien hankinnasta jättää kuvan, että valtion virastoissa ei ole uskoa siihen, että pilvipalveluihin voitaisiin siirtyä lähitulevaisuudessa ainakaan laajassa mittakaavassa.

Opinnäytetyöprosessi eteni siten, että aineiston haun ja rajauksen jälkeen aloin tutustua materiaaliin. Luin ensin materiaalin läpi kokonaisuudessaan, jotta saisin

kokonaiskuvan aiheesta. Aineiston luettuani etenin pilvipalveluiden soveltamisohjeen mukaan pilvipalvelun hankinta prosessia käyden läpi PiTuKri-työkalun sekä Katakri-työkalun käyttöä sekä muita opinnäytetyön lähteinä käytettäviä materiaaleja. Materiaalia oli paljon, mutta sen perusteella muodostui hyvä kuva siitä, miten lainsäädäntö ohjaa julkisten pilvipalveluiden käyttöä ja miten esimerkiksi pilvipalvelun hankinta prosessi etenee. Haasteena oli aiheen laajuus ja monipuolisuus, jälkeenpäin ajateltuna aihetta olisi ollut hyvä rajata lisää, jotta olisi voinut perehtyä johonkin pienempään yksityiskohtaan tarkemmin. Ilman käytännön kokemusta on vaikeata muodostaa täydellistä kuvaa näin laajasta kokonaisuudesta, syvällisempi analyysi olisi vaatinut esimerkiksi mahdollisuutta olla mukana pilvipalvelun hankinta prosessissa tutustumassa prosessin eri vaiheisiin ja toteutuksiin käytännön tasolla. Pelkkä lainsäädännön ja auditointi työkalujen tunteminen ei vielä riitä muodostamaan kuvaa siitä, mitä palveluja voidaan viedä julkiseen pilvipalveluun vaan on tunnettava monia muita yksityiskohtia. Jatkossa voisi lähteä tutkimaan tätä samaa aihetta palvelun tarjoajan näkökulmasta siten, että selvitettäisiin esimerkiksi isojen pilvipalvelun tarjoajien palveluehtojen yhteensopivuutta Suomen lainsäädännön kanssa. Voitaisiin tutkia myös, onko eri palveluntarjoajien palveluehdoissa eroavaisuuksia ja mitkä ovat ne osa-alueet, jotka vaativat vielä yhteensovittamista, jotta pilvipalveluita voitaisi käyttää julkisen hallinnon toimesta.

LÄHTEET

Cloudian 2022. Multi-Cloud Management: 5 Critical Considerations. Viitattu 25.9.2022 https://cloudian.com/guides/hybrid-it/multi-cloud-management/#1.

Empower 2022. On-premises vs cloud - what does that actually mean? Viitattu 25.9.2022 https://www.empowersuite.com/en/blog/on-premise-vs-cloud.

EU:n tietosuoja-asetus 2016/679.

IDC 2021. IDC Forecasts Worldwide "Whole Cloud" Spending to Reach $1.3 Trillion by 2025. Viitattu 2.10.2022 https://www.idc.com/getdoc.jsp?containerId=prUS48208321.

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista 22.12.2011/1406.

Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588.

Laki julkisenhallinnon tiedonhallinnasta 906/2019.

Microsoft 2022a. What is public cloud? Viitattu 14.8.2022 https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-public-cloud/.

Microsoft 2022b. Top benefits of cloud computing. Viitattu 25.9.2022 https://azure.microsoft.com/en-in/resources/cloud-computing-dictionary/what-is-cloud-computing/#benefits.

Microsoft 2022c. Azure SQL Managed Instance. Viitattu 25.9.2022 https://azure.microsoft.com/en-us/products/azure-sql/managed-instance/.

Murugesan, S. & Bojanova, I. 2015. Encyclopedia of cloud computing. West Sussex: Wiley.

NIST 2011. The NIST Definition of Cloud Computing. Viitattu 25.9.2022 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Red Hat 2022. What is SAAS. Viitattu 8.10.2022 https://www.redhat.com/en/topics/cloud-computing/what-is-saas.

Salminen, A. 2011. Mikä kirjallisuus katsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasa: Vaasan yliopisto. Viitattu 18.03.2023 https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf.

Tietosuojalaki 5.12.2018/1050.

Traficom 2020a. Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri. Traficomin julkaisuja 13/2020. Viitattu 6.3.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf.

Traficom 2020b. Katakri 2020 Tietoturvallisuuden auditointityökalu viranomaisille. Traficomin julkaisusarja 232/2020. Viitattu 6.3.2023 https://um.fi/documents/35732/0/Katakri+-+2020_1218.pdf/ab9c2d4a-5031-3670-6743-3f8921dce8c9?t=1608302599246.

Traficom 2021. Liikenne- ja viestintävirasto Traficomin suorittamat tietojärjestelmien arviointi- ja hyväksyntäprosessit. Viitattu 6.3.2023 https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 1101/2019.

Valtiovarainministeriö 2018. Julkisen hallinnon pilvipalvelu linjaukset. Valtiovarainministeriön julkaisuja 35/2018. Viitattu 2.20.2022 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161294/VM_35_2018_Julk_hallinnon_pilvipalvelulinjaukset.pdf?sequence=1&isAllowed=y.

Valtiovarainministeriö 2020a. Tuottavuutta pilvipalveluilla. Valtiovarainministeriön julkaisuja 66/2020. Viitattu 6.3.2023 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162451/VM_2020_66.pdf?sequence=4.

Valtiovarainministeriö 2020b. Pilvipalveluiden soveltamisohje. Valtiovarainministeriön julkaisuja 73/2020.Viitattu 6.3.2023 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162453/VM_2020_73.pdf?sequence=1&isAllowed=y.

Valtiovarainministeriö 2021. Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. Valtiovarainministeriön julkaisuja 5/2021. Viitattu 6.3.2022 https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162649/VM_2021_5.pdf?sequence=1&isAllowed=y.