Marko Leppä

PILVIPALVELUIDEN KÄYTTÖÖNOTTOPÄÄTÖKSEN KESKEISIÄ TEEMOJA - NÄKÖKULMIA TIETOHALLINTOON JA -TURVALLISUUTEEN VALTIONHALLINNOSSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Leppä, Marko
Pilvipalveluiden käyttöönottopäätöksen keskeisiä teemoja - näkökulmia tietohallintoon ja -turvallisuuteen valtionhallinnossa
Jyväskylä: Jyväskylän yliopisto, 2020, 90 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Siponen, Mikko

Pilvipalvelut (engl. cloud computing) on luonteeltaan kehittyvä viitekehys kattamaan laajan kirjon monipuolisia internet-välitteisiä tietoteknisiä palveluita erilaisten toimijoiden käyttötarpeisiin. Pilvipalveluiden käytöllä tavoitellaan kustannustehokkuutta, skaalautuvuutta sekä joustavaa käyttöä. Käytön tietoturvallisuuskysymykset, vastuiden jakautuminen sekä läpinäkyvyys läpi koko palveluketjun askarruttavat toimijoita heidän harkitessaan liiketoimintansa kannalta keskeisimpien tietojärjestelmiensä siirtämistä pilveen.

Pro gradu -tutkielmassa käytetään menetelmänä käsiteanalyyttista tutkimusotetta, joka sisältää myös kirjallisuuskatsauksen. Tarkastelun kohteena ovat valtionhallinnon organisaatioiden kannalta keskeiset näkökulmat otettaessa käyttöön pilvipalveluita osaksi tietoteknistä palvelutuotantoarkkitehtuuria. Kirjallisuuskatsauksessa selvitetään käyttöönottopäätökseen valmistelun taustalla vaikuttavia osa-alueita. Tutkielman keskiössä ovat tietoturvallisuuden osa-alueet arvioitaessa liiketoimintaan vaikuttavia riskejä pilviteknologioiden tunnistettujen vahvuuksien, heikkouksien ja uhkien kautta. Keskeisimpänä taustateoriana tutkielmassa on innovaatioiden diffuusio (engl. Diffusion of Innovation) ja TOE-kehysmalli, jonka kehys sisältää teknologisten, organisaatioon liittyvien ja toimintaympäristön vaikutusten tarkastelun (engl. Technology, Organization and Enviroment).

Pilvipalveluiden käyttöönotto ja käyttö vaativat organisaation ylimmän johdon tuen, johdonmukaisen hallintamallin, organisaatiotasoisen arkkitehtuurikehyksen sekä hyväksytyn toteutusprosessin toimintaohjeineen. Hallittua käyttöönottoa varten nähdään välttämättömäksi kehittää organisaatioiden omaa osaamista pilvipalveluiden sisältämien teknologioiden ja palveluratkaisujen osalta. Organisaation tarpeisiin nähden sovelletun monialaisen osaamiskeskittymän perustaminen tukisi ja varmistaisi käyttöönottojen onnistumisen. Tietojärjestelmien sijoittaminen erilaisiin palveluympäristöihin perustuu käsiteltävän tietoaineiston luokitteluun, sekä järjestelmäkohtaisiin riskiarviointeihin. Pilvipalveluiden auditointi sellaiselle tasolle, jossa pilveen voidaan sijoittaa myös käyttö rajoitettu -tasoista tietoaineistoa, vaikuttaa tarkoituksenmukaiselle tavoitteelle. Tällöin pilven hyödyt saataisiin optimoitua ja saavutettaisiin riittävän laajat käyttömahdollisuudet pilviarkkitehtuurille. Valmistelutyö vaatii merkittäviä ponnisteluja eri toimijoiden tuottamien tietojärjestelmäratkaisuiden yhteensovittamisessa.

Asiasanat: pilvipalvelut, pilvilaskenta, tietohallinto, tietoturvallisuus, riskiarviointi, päätöksenteko.

ABSTRACT

Leppä, Marko
Key themes for the adoption of cloud services - perspectives on information management and security in a government agency
University of Jyväskylä, 2020, 90 pp.
Information Systems, Master's Thesis
Supervisor: Siponen, Mikko

Cloud computing is an evolving framework to cover a wide range of Internet-based IT services for the use needs of different actors. The use of cloud services aims at cost efficiency, scalability and flexible use. Operational security issues, the division of responsibilities and transparency throughout the service chain are of particular concern when considering the migration of business-critical information systems to the cloud.

The method used in the master's thesis is a conceptual analytical research approach, which also includes a literature review. The focus is on the key aspects for government organizations when introducing cloud services as part of the IT service production architecture. The literature review examines the issues that influence the decision making when considering the adoption of cloud services. The most important parts of the review are the areas of information security in assessing business risks through the identified strengths, weaknesses, and threats of cloud technologies. The main background theory in the master's thesis is the Diffusion of Innovation theory and the TOE model, which includes the examination of technological, organizational, and environmental impacts.

The establishment of a multidisciplinary center of expertise appropriate to the needs of the organization would support and ensure the success of the implementations. The placement of information systems in various appropriate service environments is based on the classification of the data as well as risk assessments. The preparatory work also requires efforts to coordinate the multi-cloud solutions produced by the group of service providers.

The successful deployment and use of cloud services requires the top management support, a consistent management model, an organizational-level architectural framework, and operational guidelines with approved implementation models. In addition, building the organizations' own expertise in cloud services technologies and service solutions is essential. The chosen information management approach was just a scratch on the surface of an entity with a wide range of cloud computing dimensions.

Keywords: cloud services, cloud computing, information management, information security, risk assessment, decision making.

ESIPUHE

Pro gradu -tutkielmani tavoitteena on tuottaa tausta-aineistoa tietohallinnon päätöksenteon tueksi pohdittaessa tarkoituksenmukaisia, kustannustehokkaita ja arkkitehtuurivaatimukset täyttäviä pilvipalveluvaihtoehtoja viranomaisen käytössä oleville tietojärjestelmille. Työskentelen valtionhallinnon organisaatiossa. Aihepiiri tälle pro gradulle alkoi muotoutua erään työpalaverin jälkeen, jossa kollegani käsittelivät pilvipalveluihin liittyviä teemoja. He tiesivät, että opiskelen Jyväskylän yliopiston Informaatioteknologian tiedekunnassa, ja ehdottivat pilvipalveluita pro graduni aiheeksi.

Henkilökohtaisella tasolla pro gradu -tutkielman tekeminen oli opettavainen ja hyödyllinen kokemus. Aihepiirin löydyttyä varsinainen kirjoitusvaihe kesti yli vuoden sisältäen huomattavia ponnisteluja sekä epätoivon hetkiä mutta myös oivaltamisen iloa. Iltaisin, viikonloppuisin ja lomakausina tehty työ käynnistyi alkuun hitaasti ja vaati kokonaisuudessaan enemmän aikaa, kuin olin osannut odottaa. Oman osaamisen kehittäminen houkutteli keski-ikäisenä työvuosien lomassa maisteriopintoihin. Melkoinen ponnistus kaiken kaikkiaan. Tämä matka kannatti kuitenkin ehdottomasti tehdä.

KUVIOT

KUVIO 1 Kuinka ICT luo liiketoiminta-arvoa: Prosessiteoriaa mukaillen (Soh & Markus 1995, 37) 25
KUVIO 2 TOE-kehysmalli – mukaillen Tornatzky ja Fleischer 1990 29
KUVIO 3 Kirjallisuuskatsauksen vaiheistus Finkiä (2005) mukaillen 33

TAULUKKO

TAULUKKO 1 Kirjallisuuskatsauksen artikkelit jaoteltuina kategorioittain 39

SISÄLLYS

TIIVISTELMÄ 2

ABSTRACT 3

ESIPUHE 4

KUVIOT 5

TAULUKKO 5

SISÄLLYS 6

1 JOHDANTO 8
1.1 Lainsäädäntö, asetukset ja ohjeet määrittävät toimintaa 8
1.2 Tutkielman tavoite ja tutkimuskysymykset 10

2 KÄSITTEET, TEOREETTINEN TAUSTA JA TIETOHALLINTOTOIMIALAN ROOLI 11
2.1 Pilven ominaispiirteet palvelu- ja tuotantomalleineen 11
2.2 Pilvipalveluiden tietoturvallisuuden riskienhallinta 13
2.3 Tietohallintoala tukee päätöksentekoa 16
2.4 Luottamus koetuksella 18
2.5 Pilviadoption valmistelun haasteet 21

3 TIETOTURVALLISUUDEN TUTKIMUS JA TEOREETTINEN TAUSTA . 23
3.1 Pilvilaskennalla tavoitellaan kustannustehokkuutta 24
3.2 Innovaatioiden diffuusio ja TOE-kehysmalli 26

4 KIRJALLISUUSKATSAUS MENETELMÄNÄ 30
4.1 Menetelmän tausta ja soveltaminen tietojärjestelmätieteessä 32
4.2 Aineiston valintakriteerit 35

5 KIRJALLISUUSKATSAUKSEN AINEISTON KÄSITTELY JA HAVAINNOT 39
5.1 Teknologiaan liittyvät vaikutukset 41
5.2 Organisaatiotekijät 47
5.3 ICT-alan osaaminen ja -kyvykkyydet 50
5.4 Liiketoimintaympäristön vaikutuksista 51
5.5 Pilvipalveluihin kohdistuvaa kritiikkiä 53

6 TULOKSET JA JOHTOPÄÄTÖKSET 55
6.1 Riskien tunnistamisella ratkaisuihin 56
6.2 Laadukkaat sopimukset ja poistumissuunnitelma 58
6.3 Ohjeet ja sisäisen hallintomallin merkitys 59

6.4 Miten pilvi otetaan hallintaan? 60
6.5 Tutkimustulosten luotettavuus ja pätevyys 62

7 POHDINTA 64

LÄHTEET 66

LIITE 1 LUVUSSA 5 KÄYTETYT ARTIKKELIT 78

1 JOHDANTO

Tutkielmassa tarkastelen ja selvitän pilvipalveluiden (pilvilaskennan) käyttöönoton kannalta sellaisia keskeisiä seikkoja, joita alan tutkimus on käsitellyt ja joista voi ammentaa taustatietoa julkishallinnon toimijoiden tietohallintotoimialan työn tueksi.

Pilvipalveluiden ja pilvilaskennan hyödyntämisestä on olemassa runsaasti artikkeleita ja kirjallisuutta jo yli kymmenen vuoden ajalta, mutta kotimaisten valtionhallinnon toimijoiden näkökulmasta aihetta on tarkasteltu vielä melko vähän. Tämän tutkielman tarkoituksena ei ole pureutua tietotekniikkaan, eikä aihetta käsitellä myöskään IoT-näkökulmasta. Tutkielmassa on olennaista tietohallintonäkökulmalla tehtävä tarkastelu. Tieteellistä aineistoa tarkastellaan pilvipalveluiden käyttöönottopäätöksiin liittyen riskiarvioinnin ja tietoturvallisen käytön näkökulmista. Tutkielmassa arvioidaan myös pilvipalveluiden käyttöönoton onnistumisen kannalta hyödyllisiä toimintatapoja organisaation sisäisten ohjausmekanismien tarpeisiin. Tutkimuksen myötä kertyneitä havaintoja voidaan käyttää apuna laadittaessa tietoturvaohjeistusta sekä kehitettäessä sisäisiä toimintamalleja ja rakenteita tietojärjestelmien palveluympäristövaihtoehtoja arvioitaessa.

Tämän tutkielman haasteena on tietohallintonäkökulmalla tehtävään tarkasteluun soveltuvan tutkimusaineiston rajoittuneisuus. Cegielski, Jones-Farmer, Wu ja Hazen (2012) toteavat, että teoreettisesta näkökulmasta tarkastelevaa pilvipalvelututkimusta on vähän. Pilvipalveluita tarkastelevassa tutkimuksessaan he arvioivat suurimman osan tutkimuksista keskittyvän joko pilvipalveluympäristöjen arkkitehtuurien tai sovellusten tutkimukseen. Aihetta käsitellään yleensä arvioiden, millaisia esteitä tai mahdollisuuksia käytölle tunnistetaan. (Cegielski, Jones-Farmer, Wu & Hazen, 2012.)

1.1 Lainsäädäntö, asetukset ja ohjeet määrittävät toimintaa

Kansallinen lainsäädäntö ja ministeriöiden ohjaus luovat puitteet, jotka ohjaavat virastojen toimintaa myös tietojärjestelmäarkkitehtuurin näkökulmasta. Valtionhallinnon toimijat on velvoitettu yhteisten kansallisten tietojärjestelmä-

palveluiden käyttäjiksi. Tämä tuo mukanaan riippuvuuksia muihin kansallisiin alan toimijoihin, sekä se vaikuttaa lisäksi keskeisesti virastojen omiin arkkitehtuurivalintoihin ja -ratkaisuihin. Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015) velvoittaa valtion viranomaiset turvallisuusverkkopalveluiden (TUVE) käyttäjiksi.

> Turvallisuusverkon käyttövelvoite koskee sellaista valtion johtamiseen ja turvallisuuteen, maanpuolustukseen, yleiseen järjestykseen ja turvallisuuteen, rajaturvallisuuteen, pelastustoimintaan, meripelastustoimintaan, hätäkeskustoimintaan, maahanmuuttoon ja ensihoitopalveluun liittyvää viranomaisten sisäistä, välistä ja ulkoista yhteistoimintaa ja viestintää, joissa noudatetaan korkean varautumisen tai turvallisuuden vaatimuksia. (Finlex, 2015.)

Turvallisuusverkko on tarkoitettu varmistamaan kaikissa turvallisuustilanteissa valtion johdon ja yhteiskunnan turvallisuuden kannalta tärkeiden viranomaisten ja muiden toimijoiden häiriötön viestintä sekä turvata johtamisessa ja päätöksenteossa tarvittavan tiedon tietoturva. Viranomaisten turvallisuusverkko sisältää viestintäverkon laitetiloineen ja laitteineen, muun infrastruktuurin sekä yhteiskäyttöiset palvelut. (Kyberturvallisuuden sanasto, 2018.) Valtionhallinnon organisaatiot tuottavat tietoteknisiä palveluita itse, hankkivat lain velvoittamina yhteisiä tietojärjestelmäpalveluita tuottavilta organisaatioilta sekä tulevaisuudessa yhä kasvavassa määrin myös laajemmin vaatimukset täyttäviltä viranomaisten hyväksymiltä pilvipalveluyrityksiltä. Valtiovarainministeriöllä (VM) on lakisääteinen tehtävä ohjata julkishallinnon tietoturvallisuutta. VM on laatinut tietoliikennepalvelulinjauksia sekä Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjeita, joiden avulla ohjataan julkisen sektorin tietoliikennepalveluiden käyttöä, hankintaa ja tuotantoa. Ohjeilla ei ole lakiin perustuvaa asemaa, mutta käytännössä niistä on muodostunut tietynlainen de facto -tulkinta lainsäädännöstä. VM:n tarkoituksena on luoda ohjaus valtionhallinnon, maakuntien ja kuntien ICT-johdolle tarkoituksenmukaisten, turvallisten, kustannustehokkaiden tietoliikennepalveluratkaisuiden hankkimiseksi. (Liikenne- ja viestintävirasto Traficom, 2019.)

EU:n yleinen tietosuoja-asetus (GDPR) on ollut lainvoimainen 25.5.2018 alkaen. GDPR määrittelee vaatimukset organisaatioiden ja yritysten henkilötietojen keräämiseen, säilyttämiseen ja hallinnointiin. Yleistä tietosuoja-asetusta sovelletaan, mikäli yritys käsittelee henkilötietoja ja sijaitsee EU:ssa, tapahtuipa itse henkilötietojen käsittely missä tahansa. Asetusta sovelletaan myös silloin, jos EU:n ulkopuolella sijaitseva yritys käsittelee henkilötietoja, jotka liittyvät palveluiden tai tavaroiden tarjoamiseen henkilöille EU-alueella. Henkilötietoja ovat esimerkiksi: nimi, osoite, henkilökortin tai passin numero, tulot, kulttuurinen profiili, IP-osoite ja terveydenhuollon hallussa olevat henkilön yksilöivät terveystiedot. (European Parliament and Council of European Union, 2016.)

Valtiovarainministeriön mukaan pilviteknologiaa tulisi suosia, mikäli se tarjoaa parhaan palveluhyödyn ja -takuun (Valtiovarainministeriö, 2018). Julkiseksi luokitellun tietoaineiston käsittelyä pilvipalvelussa ei rajoiteta, mutta suojaamistarpeet eheyden ja saatavuuden näkökulmasta on kaikissa tapauksissa huomioitava. Henkilötietoja voidaan sijoittaa sellaiseen pilvipalveluun, joka tuotetaan tietosuojasääntelyn mahdollistamalla EU/ETA-alueella. Korkeampien

turvallisuusluokkien tietojen osalta vaatimuksena on palvelun sijainti Suomessa. Kukin viranomainen vastaa tietojenkäsittelynsä riittävästä turvallisuudesta ja on viime kädessä itse vastuussa kulloisenkin käyttötapauksen riittävän kattavasta ja luotettavasta arvioinnista. Nämä arviointihavainnot tulee myös käsitellä riskiperustaisesti. Mikäli kyseessä on useamman valtionhallinnon viranomaisen käyttämä, keskityn palveluntuottajan tuotantoympäristö, tulee jäännösriskien olla kaikkien palvelua käyttävien viranomaisten hyväksymiä. (Liikenne- ja viestintävirasto Traficom, 2020.)

Viranomaisten käsittelemä luokiteltava tietoaineisto tuottaa vaatimuksia tiedon käsittelylle ja tietojenkäsittely-ympäristöille. Viranomaistyössä tiedon luokittelu vaatii jatkuvaa huolellista arviointia ja tämä edellyttää käyttämään vaatimukset täyttäviä auditoituja sekä akkreditoituja tietojärjestelmäympäristöjä. Viranomaisten tietojärjestelmien arviointityössä käytetään apuna muun muassa Kansallista turvallisuusauditointikriteeristöä (KATAKRI), jonka avulla voidaan arvioida kohdeorganisaation kykyä suojata turvallisuusluokiteltua tietoa.

Pilvipalveluiden käyttöönotto perinteisten palvelutuotantomallien rinnalle on edennyt Suomessa viranomaistoimijoilla varsin verkkaiseen tahtiin. Kiinnostus ja käyttötarve pilvipalveluita kohtaan ovat merkittävässä kasvussa, jonka vuoksi hallittuun käyttöönottoprosessiin vaikuttavat tekijät vaativat huomiota ja käyttöönottovaihetta voidaan tukea tuottamalla tausta-aineistoa tietohallinnon käyttöön. Kansallisella tasolla virastojen käyttöön laadittua pilvipalvelusiirtymää ohjaavaa materiaalia kehitetään eri hallinnonaloilla parhaillaan.

1.2 Tutkielman tavoite ja tutkimuskysymykset

Tutkielman keskeinen tavoite on tukea valtionhallinnon organisaatioiden tietohallintoalan toimijoiden työtä kokoamalla akateemiseen tutkimukseen perustuvaa taustatietoa pilvipalveluista. Tuloksia voidaan hyödyntää organisaatioissa tehtävässä päätöksentekotyössä arvioitaessa erilaisia vaihtoehtoisia ratkaisuja pilvipalveluiden käyttömahdollisuuksista. Tässä pro gradu -tutkielmassa tuodaan esille sellaisia pilviteknologioiden käyttöön liittyviä osa-alueita, joita organisaatioissa tulisi ottaa huomioon riskiarviointiprosessin kehittämiseksi. Organisaatioiden sisäisiä arviointityön menetelmiä tai päätöksentekoprosesseja ei käsitellä yksityiskohtaisemmin minkään tietyn toimijan näkökulmasta.

Tässä tutkielmassa pyritään vastaamaan seuraaviin tutkimuskysymyksiin:

- Millaisia teemoja tulee huomioida tietoturvariskien arvioinnissa pilvipalveluiden käyttöönottopäätöksiä valmisteltaessa?
- Millaisia ohjeita tai toimintamalleja valtion viraston tietohallintotoimialan olisi hyödyllistä laatia arvioidessaan luokiteltua tietoaineistoa sisältävien tietojärjestelmien sijoittamista erilaisten toimijoiden pilvipalveluympäristöihin?

2 KÄSITTEET, TEOREETTINEN TAUSTA JA TIETOHALLINTOTOIMIALAN ROOLI

Tässä luvussa esitellään aluksi tämän tutkielman keskeisimpiä käsitteitä. Käsitteiden määrittely on välttämätöntä pohjatietoa tutkielman aihepiirin ymmärtämiselle. Määrittely sisältää pilvipalveluita käsittelevissä teksteissä yleisesti esiteltyjä pilvilaskennan ominaispiirteitä sekä pilven keskeisimmät palvelu- ja tuotantomallit. Muissa alaluvuissa käsitellään tietohallintotoimialan roolia organisaation johtamisen tukiprosessina sekä riskiarviointityön merkitystä pilvipalveluiden soveltuvuutta arvioitaessa.

2.1 Pilven ominaispiirteet palvelu- ja tuotantomalleineen

Pilvipalvelut tai siitä usein suomeksi käytetty termi pilvilaskenta ovat luonteeltaan kehittyvä ajattelumalli tai viitekehys. Pilvipalveluille ei kuitenkaan ole olemassa yleismaailmallista tai standardoitua määritelmää, vaikka se on jo ollut käytössä melko pitkään. Vertauskuvallisesti pilvellä viitataan sen laajaan tietojenkäsittelyresurssien saatavuuteen internet-teknologioita hyödyntäen. (Oliveira, Thomas & Espadanal, 2014.) Pilvipalvelut ovat tulevaisuutta, jonka päätavoite on vähentää ICT-palvelujen kustannuksia ja lisätä samalla tietojenkäsittelyn suorituskykyä, luotettavuutta, käytettävyyttä ja joustavuutta, aiempaa tehokkaammin ja nopeammin. Tietoturvaintegraatiot ovat kuitenkin haastavia, eivätkä siirtymät pilvipalveluihin ole tapahtuneet organisaatioissa niin nopeasti, kuin olisi ennakkoon voitu olettaa. (Low, 2011.)

Pilvipalveluilla tarkoitetaan joko internetin välityksellä tarjottavia datakeskusten palveluina tarjottavia sovelluksia tai palveluina tarjottavia laitteisto- ja järjestelmäohjelmistoja. Datakeskusten palveluiden tuottamista varten käytettävää laitteistoa ja ohjelmistoa kutsutaan pilveksi. Pilvipalveluilla mahdollistetaan verkon välityksellä tarjottavien jaettujen skaalautuvien tietojenkäsittelyresurssien joustava käyttö. Kapasiteettia voidaan ottaa käyttöön tai vapauttaa helposti itsepalveluperiaatteella vähäisillä hallinnointitoiminnoilla. (Armbrust, 2010.)

Pilvipalveluita käsittelevissä tieteellisissä teksteissä aihepiirin määrittelyissä viitataan lähes poikkeuksetta yhdysvaltalaisen National Institute of Standards and Technology (NIST) esittämään luokitteluun pilvipalveluiden ominaispiirteistä, sekä niiden palvelu- ja tuotantomalleista. NIST:n määrittelyä mukaillen pilvipalveluiden ominaispiirteet ovat seuraavat:

- Käyttöön perustuva itsepalvelu (engl. on-demand self-service). Palveluita hankkinut taho voi asiakkaana itse säädellä hankkimansa palvelun tietojenkäsittelyresurssien ominaisuuksia, kuten esimerkiksi laskentatehoa, levytilaa tai palvelun käyttökapasiteettia ilman palveluntarjoajan henkilöstön toimia.

- Laaja pääsy verkkoon (engl. broad network access). Pilvipalveluiden kyvykkyydet ja toiminnallisuudet ovat koko laajuudessaan käytössä tietoverkon välityksellä.
- Resurssien jakaminen (engl. resource pooling). Palveluntarjoajien yhdistettyä resurssivarantoa (pooli) jaetaan käyttöön laajan asiakaskunnan käyttäjille dynaamisesti käyttötarpeen mukaan. Palveluiden tuottamiseen käytetyn kapasiteetin maantieteellinen sijainti ei ole tiedossa, ellei siitä erikseen sopimuksin sovita.
- Nopea joustavuus (engl. rapid elasticity). Palvelun kapasiteetin lisääminen tai sen vapauttaminen voidaan tehdä nopeasti, jopa automaattisesti, käyttötarpeen niin vaatiessa.
- Mitattava palvelu (engl. measured service). Pilvipalveluiden resurssien asiakaskohtaista käyttöä voidaan valvoa, kontrolloida ja raportoida, jolloin pystytään tarjoamaan läpinäkyvyyttä sekä palveluntarjoajalle että palvelua käyttävälle taholle. Laskutuksen perusteena ovat palveluiden ja niiden sisältämien resurssien käytön tarkka mittaaminen kokonaisuudessaan. (Mell & Grance, 2011.)

Vakiintuneeksi muodostuneen jaottelun mukaisesti pilvipalveluiden yleisimmät palvelumallit (service models) esitellään seuraavasti:

- Ohjelmisto palveluna (engl. Software as a Service, SaaS). Palvelumallissa asiakas ostaa kokonaispalvelun, esimerkiksi selainkäyttöisen sähköpostijärjestelmän, jossa toimittaja vastaa kaikesta palveluntuottamiseen liittyvästä ja palvelun käyttäjä vain käyttää sitä. Asiakas ei yleensä edes tunne palveluntuottamiseen liittyviä yksityiskohtia, kuten verkkoratkaisuja, palvelimia, käyttöjärjestelmiä tai muita teknisiä ratkaisuja hankkimansa palvelun taustalla. Palvelu laskutetaan esimerkiksi käyttäjien lukumäärään ja käytössä olevaan levytilaan sekä palvelutasosopimuksessa määriteltyjen tukipalvelun vasteaikojen tuottaman hinnoittelun perusteella.
- Alusta palveluna (engl. Platform as a Service, PaaS). Pilvipalvelun tuottaja tarjoaa asiakkaan käyttöön palveluna sovellusalustan, kapasiteetin, jonka tuottamisesta se vastaa. Palveluun yleensä sisältyvät verkkoyhteydet, palvelimet, käyttöjärjestelmä ja varusohjelmistot. Asiakkaan omalle ylläpitovastuulle jää sovelluskerros päivityksineen ja sen tietoturva.
- Infrastruktuuri palveluna (engl. Infrastucture as a Service, IaaS). Infrastruktuuri palveluna on malli, jossa palveluntuottaja tarjoaa pilvi-infrastruktuurin, alustan, jota käytetään kapasiteetin tuottamiseen. Muut osat, kuten palvelimet, konfiguraatiot ja hallinnointi jäävät asiakkaan omalle vastuulle. Asiakkaalle tarjotaan vain hallintaliittymä, jolla voidaan hallinnoida palvelimien kapasiteettia, verkkoyhteyksiä ja tietoliikenneavauksia. Tässä palvelumallissa ei tarvitse välttämättä olla datakeskusosaamista asiakkaan omassa organisaatiossa. (Mell & Grance, 2011.)

Pilvipalveluiden tuotantomallit (engl. Deployment Models) ovat:

- Yksityinen pilvi (engl. private cloud). Tässä mallissa palvelut tuotetaan itse omasta konesalista (engl. on-premises) vain sisäisesti oman organisaation käyttäjien ja mahdollisesti rajatusti kumppaniyritysten tarpeisiin. Tällaisten palveluiden tuottamiseen vaadittava osaamistarve on suurimmillaan, mutta lisäksi koko palveluntuottamiseen liittyvä teknologiakerrokset ja järjestelmän sisältämä data ovat omissa käsissä. Tästä mallista on olemassa myös vaihtoehtoinen malli, hosted on-premises, jossa konesali on organisaation omistama, mutta sen ylläpitotyö on ostettu ulkoiselta palveluntuottajalta.
- Yhteisön pilvi (engl. community cloud). Yhteisöpilvi tuotantomallina rakentuu jonkin palvelutuotanto-organisaation ylläpitämästä palveluympäristöstä, jonka yhteisiä resursseja käyttävinä asiakkaina ovat kyseisen yhteisön rajattu käyttäjäkunta. Yhteisöön kuuluvilla käyttäjäorganisaatiolla on yleensä pääosin yhteiset turvallisuusstandardit ja käyttöpolitiikat palveluiden suhteen. Suomessa tällaisia palveluita tuottaa viranomaisille esimerkiksi Valtion tieto- ja viestintätekniikkakeskus Valtori.
- Julkinen pilvi (engl. public cloud). Julkinen pilvi tarkoittaa palvelua, jonka palveluinfrastruktuuri on kenen tahansa asiakkaan käytössä ja palvelun hinta muodostuu käytön mukaa. Palvelut ovat usein standardoituja, joten ne ovat tarjolla sellaisenaan, ja palvelun sisältö voi myös muuttua.
- Hybridipilvi (engl. hybrid cloud). Hybridipilvi yhdistää edellä kuvattujen tuotantomallien ominaisuuksia palvelukokonaisuudeksi voiden tarjota mahdollisesti monipuolisempia mahdollisuuksia palveluiden käyttäjille. Hybridipilvi voi mahdollistaa palvelun laajennuksen lisäkapasiteettia tarvittaessa tai se voi tarjota tietoaineiston mahdollisen hajasijoittamisen eri pilvituotantoratkaisuiden kesken. (Mell & Grance, 2011.)

ICT-alalla palvelumallien kirjoa on laajennettu ja useita muitakin toteutuksia kuvataan ilmaisten ne ”as a service” -tyyppisesti. Esimerkkinä edellisten lisäksi voidaan mainita eräänlainen palveluiden yhdistelmä, jossa palveluntuottaja täydentää palveluaan tietoturvallisuuskomponenteilla. Sellaista kuvataan termillä tietoturvallisuus palveluna (engl. Security as a Service, SECaaS). Tutkielmassa käytetään myös termiä adoptio (adoption), joka on hyvin yleisesti käytetty termi ICT-alaa käsittelevissä tieteellisissä teksteissä kuvaamaan organisaatioiden päätöksentekoa ja ratkaisua teknologiapalvelun käyttöönotosta.

2.2 Pilvipalveluiden tietoturvallisuuden riskienhallinta

Riskiarvioinnin merkitys on keskeinen pilvipalveluiden käyttöönottoa valmisteltaessa. Pilviteknologioiden käytön vahvuudet ja heikkoudet on tunnistettava ja otettava huomioon riskiarviointityössä aina tapauskohtaisesti. Tunnistettujen uhkien aiheuttamien riskien toteutumisen todennäköisyys on pystyttävä pienentämään siedettävälle tasolle.

Tutkielman yhtenä teemana käsitellään riskienhallintatyön tärkeyttä tehtäessä pilvipalveluiden käyttöönottopäätöstä. Kansallinen tietoturva-auditointi-

työkalu määrittelee organisaation riskienhallintaa seuraavasti: Riskienhallinta on organisaation johtamiseen ja toimintaa sisältyvä prosessi, jota sovelletaan organisaation toiminnassa. Riskienhallinnan tavoitteena on tunnistaa ja hallita toimintaedellytyksiä vaarantavia tekijöitä ja pitää riskit sellaisella tasolla, ettei organisaation toiminta ja tavoitteet ole uhattuina. Epäedullisia ja haitallisia tapahtumia pyritään välttämään vaikuttamalla tapahtuman todennäköisyyteen sekä pienennetään niiden seurauksia. Riskienhallinnan uhka-arvion perusteella mitoitetaan turvallisuusjärjestelyt oikealle tasolla. Arvioinnissa tunnistetaan organisaation riippuvuudet ulkoisista tekijöistä sekä niiden vaikutukset omaan toimintaan unohtamatta arvioida omaa vaikutusta muihin toimijoihin nähden. Hyvin toteutettu riskienhallinta on ennakoivaa, tietoista, suunnitelmallista ja dokumentoitua. (Puolustusministeriö, 2015.)

Riskianalyysi on tietoturva-ammattilaisten käyttämä tekniikka, jota käytetään tietojärjestelmien toteutettavuuden määrittämiseen. Tekniikkaan on ollut yhdistelmä kvantitatiivisia analyysejä sovellettuna tulkitsevaan dataan. Riskianalyysin avulla tietoturvamenetelmien laatijat perustelevat valvonnan toteutuksesta muodostuvat kustannukset organisaation johdolle. Koska riskianalyysiltä tekniikkana ajatellen puuttuu tilastollinen tarkkuus, se on tieteellisenä menetelmänä puutteellinen, joten sen tuottama arvaus voi johtaa kalliiden ja tarpeettomien tietojärjestelmäturvallisuuskontrollien toteuttamiseen. Riskianalyysin merkitys tiedonvälityksen linkkinä tietoturvallisuusammattilaisten ja organisaation johdon välillä onkin merkittävämpi käyttötarkoitus, kuin riskianalyysi pelkästään ennakoivana toimenpiteenä tietoturvakontrolleja suunniteltaessa. (Baskerville, 1991; Siponen, 2005.) Päätöksenteon tueksi tuotettavat tietoturva-arvioit ovat johdolle hyödyllisiä. Pilvipalveluiden riskiarviointi vaatii aiempaa monimutkaisemman ja kattavamman tarkastelun etenkin silloin, kun käyttäjäorganisaatio on esimerkiksi valtiollinen turvallisuusalan toimija. Viranomaisten käyttämiin tietojärjestelmiin kohdistuvien uhkien seuraukset tuottaisivat sekä taloudellisia että kansalliseen turvallisuuteen liittyviä tappioita. Järjestelmien monimutkaisuus sekä niiden sisältämä tietoaineisto edellyttävät arviointimenetelmien perusteellista ja järjestelmällistä suunnittelua. Tällöin riskienhallinnan menneiden vuosikymmenien strukturoimattomat tai pelkästään riskien laadulliseen arviointiin perustuneet varhaisemmat lähestymistavat eivät ole enää riittäviä. Riskianalyysien tekemiseen käytettävien työkalujen menetelmineen täytyy perustua loogiseen mallintamiseen ja kvantitatiiviseen arviointiin, jotta voidaan käsitellä monimutkaisille tietojärjestelmäkokonaisuuksille ominaisten uhkien tyypit ja niiden seuraukset. Tällaista lähestymistapaa käytetään muun muassa Livermoren riskianalyysimenetelmässä, jonka juuret juontavat Yhdysvaltojen ilmavoimien toimintaan. Menetelmä tarjoaa päätöksentekijöille arviointielementtejä riskien vaikutusten vähentämiseen sekä kustannustehokkuuden arviointiin. Yksittäiset valvonta- tai suojaustoimenpiteet voidaan liittää riskiskenaarioihin, valita niitä käyttöön tai jättää huomioimatta, lisäksi arvioida priorisoinnin vaikutuksia syntyviin kustannuksiin nähden. (Guarro, 1987; Siponen, 2005.)

Kuten edellä todettiin, tieteellisenä menetelmänä riskianalyysi on riittämätön, koska siltä puuttuu kyky saada todistettua suunnittelun, määrittelyn ja toteutuksen tehokkuudesta. Riskienhallinnan ympärillä on osuutensa aina myös tuurilla, joten tehtyjen ennakoivien toimien suorituskyvyn todistamisen

komponentti jää puuttumaan. Aihepiiri myös jää usein hallinnollisten toimien kokonaisvaltaisessa tarkastelussa vähäiselle prioriteetille siihen saakka, kunnes jotain tapahtuu. Ellei katastrofi toistu, organisaation johto ei välttämättä saa tehokasta palautetta osoittamaan, olivatko tehdyt toimet tarjonneet todellista turvallisuutta ja millainen osuus tapahtumien kulussa oli tuurilla. (Baskerville, 1991.)

Riskienhallinta on prosessi, joka tunnistaa organisaation liiketoiminnan kannalta olennaisiin tietovarantoihin kohdistuvat haavoittuvuudet ja uhkat. Tietoturva-ajattelun peruspilareita ovat luottamuksellisuus, eheys ja käytettävyys. Riskiperusteinen malli lisää edellisiin kolme keskeistä täydentävää elementtiä, jotka ovat autentikointi, kiistämättömyys sekä riskienhallinta. Tietoturvan peruselementtien tarkastelu on lähtökohta myös pilvipalveluiden arvioinnissa. Pilvipalveluiden käyttöönoton myötä siirtyy tyypillisesti laitteistojen, sovellusten ja tietoliikenteen hallintakyvykkyys vastuineen pois organisaation omalta henkilöstöltä. Pilvipalveluiden myötä aletaan käyttää palveluntuottajan yleensä usealle asiakkaalleen jakamaa kapasiteettia ja luovutetaan data palveluntuottajan vastuulle. Syntyvät riskit tulee etukäteen tunnistaa ja arvioida niiden vaikutuksia liiketoiminnalle. Riskiarvioinnin tuloksena on tiedossa jäännösriski, jonka määrä on tasapainoilua kustannusten kanssa. Ratkaistavaksi jää, millaisilla toimienpiteillä ja kustannuksilla saavutetaan tasoltaan hyväksyttävä jäännösriski. (Raggad, 2010.)

Rao ja Selvamani (2015) ovat pohtineet pilvipalveluiden turvallisuuden teemoja, joita joudutaan arvioimaan palveluiden käyttöönoton valmistelussa, ja jotka ovat havaittu keskeisimmiksi estäen etenemisen käyttöönotossa. Tietoturvan varmistaminen ja yksityisyyden turvaaminen tunnistettiin kriittisimmiksi tekijöiksi. Myös vaatimusten toteutuminen sekä lainopilliset ja toimijoiden välisiin sopimuksiin liittyvät yksityiskohdat vaativat paljon huomiota. Tietoturvallisuuden päähaasteiksi pilvipalveluita käytettäessä arvioitiin tietovuotojen ennaltaehkäisystä huolehtiminen sekä datan hallittu erottelu ja suojaus. Yhden pilvipalveluntuottajan tietovarastossa on tyypillisesti monen eri asiakkaan omistamaa luokiteltua dataa, jotka täytyy pitää erillään. Riskien välttämiseksi on välttämätöntä suojata tietovarastot ja niiden sisältämä data, liittyypä se sitten tallennukseen, siirtoon kuin sen prosessointiinkin. (Rao & Selvamani, 2015.)

Pilvipalvelun käyttö tuottaa osittain erilaisia riskejä verrattuna palveluiden tuottamiseen organisaation omasta konesaliympäristöstä. Keskeistä onkin kehittää soveltuva IT-hallintomekanismi, joka pystyy tunnistamaan, arvioimaan ja vähentämään sellaisia riskejä, jotka liittyvät pilvipalveluiden käytön ympärille. Pilvipalveluiden hallinta ja valvonta on monimutkaista vaatien lisäksi myös vahvoja palvelusopimuksia sekä osaamista asioidessa palveluntuottajien kanssa. (Paquette, Jaeger & Wilson, 2010.) Chang ym. (2016) arvioivat myös kehityssuuntaa, jossa jatkuvasti yhä useampi organisaatio ottaa käyttöön pilvipalveluita. Tietoturvallisuus ja yksityisyys pitäisi pystyä varmistamaan. Tutkijoiden mielestä turvallisuusteemat pitäisi implementoida, ennen kuin mitään pilvipalvelua otetaan käyttöön. (Chang & Ramachandran, 2016.)

Pilviteknologioiden arviointia käsittelevässä kirjoituksissa korostuvat yleensä riskeihin ja uhkiin liittyvät teemat. Samalla on hyvä muistaa myös kolikolla olevan aina kaksi puolta. Zissis ja Lekkas (2012) puntaroivat molempia puolia, mutta haluavat ensin korostaa pilviympäristöjen vahvuuksia.

Pilvipalveluiden arkkitehtuurin vuoksi niiden käytöllä saavutetaan myös monia turvallisuuteen vaikuttavia etuja. Tällaisia ovat muun muassa tietoturvallisuuden keskittyminen, datan ja sen prosessoinnin segmentointi, korkea käytettävyys ja tarpeettomien palveluiden käytöstä luopuminen (engl. redundancy). Hyötyjen kääntöpuolena ovat riskiarviointia vaativat teemat kuten palvelujen käytettävyys, luotettavuus, tietojen eheys, palauttaminen, sekä tietoturvallisuus ja -auditointikysymykset. (Zissis & Lekkas, 2012.) Kun palveluita tuotetaan organisaation itse hallinnoiman ympäristön ulkopuolella tai hybridivaihtona, sekä omasta että palveluntuottajan ympäristöstä, riskien arvioinnin osaamistarve laajenee merkittävästi.

Turvallisuusnäkökohtien arvioiminen on monitahoinen prosessi. Prosessi alkaa yleisen käytännön mukaisesti sillä, että pilvipalvelun arvioinnin perustiedot kootaan järjestelmäkuvausdokumenttiin, jonka tulee sisältää arviointia varten sellaiset taustatiedot, jotka mahdollistavat palvelun yleisen soveltuvuuden ja riskien arvioinnin suhteessa loppukäyttäjän käyttötapaukseen. Myös lainsäädäntöjohdannaiset riskit arvioidaan. Arvioitavia seikkoja ovat muun muassa tiedon fyysinen sijainti ja palvelun tuottamiseen osallistuvat tahot, sisältäen myös kaikki palveluntuottajan käyttämät alihankkijat. Välttämätöntä olisi myös tunnistaa, millaiset viranomaistoimijat voivat ulkomailla sikäläisen kansallisen lainsäädännön perusteella päästä käsiksi palvelussa käsiteltäviin asiakkaan tietoihin. Tietoturvallisuuden arviointiprosessi etenee riskiarvioinnin myötä kohti akkreditointia ja käyttöönottopäätöstä. (Liikenne- ja viestintävirasto Traficom, 2020.)

2.3 Tietohallintoala tukee päätöksentekoa

Organisaation tietohallintotoimialan yksi tehtävä on tukea päätöksentekoa ohjaamalla toimialaansa sisältyvien tietoteknisten järjestelmien valintaa ja hankintaa. Pilvilaskenta mahdollistaa yritysten keskittymisen ydinliiketoimintaansa, jolloin mahdollisesti koko ICT voidaan ulkoistaa innovatiivisuuden ja tuottavuuden kärsimättä. Pilviulkoistus tuottaa huomattavia säästöjä, koska omasta IT-infrastruktuurista voidaan luopua ja keskittyä oman asiakaskunnan tarpeisiin. (Khan & Al-Yasiri, 2016.) Pilvipalveluiden houkuttelevuuteen ovat johtaneet viime vuosikymmenen johtavat teknologiat, kuten virtualisointi, palvelusuuntautunut arkkitehtuuri (engl. service-oriented architecture) ja verkossa tapahtuva laskenta. Pilvialustoilla voidaan tuottaa suuren kapasiteetin ansiosta tällaisia palveluita tehokkaasti. Toisaalta pilvilaskenta on vielä kuitenkin varsin uusi viitekehys, jolta puuttuvat yhteneväiset käytännöt. Pilvipalveluiden hyödyntämisen keskeisiksi menestystekijöiksi on nimetty kolme osa-aluetta, jotka ovat strateginen, taloudellinen, ja tekninen. Näiden hallitsemiseen vaadittavia kyvykkyyksiä tulisi tavoitella. Strategisessa tarkastelussa saavutetaan hyöty ulkoistamalla osia tietoteknisistä töistä alihankkijalle, jolloin voidaan paremmin keskittyä omaan ydinliiketoimintaan. Taloudelliset hyödyt voidaan saavuttaa pilvitarjoajan skaalautuvan kapasiteetin ja toimittajan korkeatasoisen osaamisen avulla. Teknologinen hyöty muodostuu palveluntarjoajan omistaman huipputeknologian ja ammattitaidon yhdistelmänä, jolloin eliminoidaan oman palvelutuotannon

teknologian vanheneminen, riskit ja kustannukset. (Garrison, 2012.) Pilvipalveluita käyttävät organisaatiot ovat raportoineet saavuttaneensa jopa 30 %:n taloudellisia säästöjä samalla hyötyen tehostuneesta liikkuvan työn mahdollisuudesta, korkeammasta tuottavuudesta sekä prosessien standardisoinnin eduista (Rebollo, 2015).

Ulkoistettaessa strategisesti tärkeitä ICT-hankkeita kohdataan merkittäviä riskejä, joita täytyy kyetä vähentämään. Soveltuvat tietoturvan hallintamenetelmät ja optimaalinen riskien käsittely ovat keskeisimpiä ratkaistavia ongelmia tietohallinnossa. Tietohallintotoimialalle tarvitaankin tietoturvallisuuden hallintamalli, joka sisältää selkeän turvallisuusstrategian. Valittiinpa millainen pilvimalli tahansa, on tietohallintotyöllä ohjattava organisaation pilvipalveluiden käyttöönottoa. Tietoturvapolitiikan noudattaminen edellyttää aktiivista hallintotapaa ja organisaation oman henkilöstön osaamista ja valvontakykyä. Ulkoistettaessa palveluita kolmansia osapuolia hyödyntäen kyky säilyttää kontrolli on keskeinen seikka. (Rebollo, 2015.)

Etenkin valtiollisten organisaatioiden on usein ajateltu olevan joustamattomia ja tehottomia prosesseissaan. Garrison (2012) ennustaa vaikeuksia viitaten siihen, että organisaatioilta, joilla on joustamaton IT-infrastruktuuri, puuttuu kyky ottaa täysi hyöty irti pilvistrategiasta. Sellaiset IT-johtajat, joilla ei ole riittävää liiketoimintaosaamista eikä tietoteknistä ymmärrystä pilvipalveluiden hyödyntämisestä, hankaloittavat menestyksekästä käyttöönottoa. Tavoiteltua suorituskyvyn paranemista sekä kustannussäästöjä voidaan tästä huolimatta saavuttaa, mutta tutkijoiden mielestä puutteellisilla taidoilla ei tavoiteta kilpailuetua markkinoilla. Organisaation oma tietohallinnollinen kyvykkyys sekä hyvät suhteet palveluntuottajiin nähdään pilvipalveluita käyttöönotettaessa tärkeiksi ennakkoedellytyksiksi. (Garrison, 2012.)

Oliveira ym. (2014) nostavat esiin pilvikäyttöönoton onnistumiseen vaadittavia seikkoja korostaen organisaation ylimmän johdon tuen, sitoutumisen, osallistumisen ja rahoituksen varmistamisen merkitystä. Nämä ovat edellytyksiä, jotka vaaditaan ja nähdään välttämättöminä onnistuneen pilvikäyttöönoton mahdollistamiseksi. Organisaation isompi koko nähdään tutkimuksen mukaan suosivan pilvipalveluiden käyttöönoton onnistumista. Tämä johtuu tutkijoiden arvion mukaan siitä, että pienemmissä yrityksissä jää puuttumaan oma osaaminen tietämyksen rakentamiseen ja uudenlaisten palveluiden testaamiseen sekä käyttöönottoon liittyen. Yrityksen toimintaympäristön vaikutuksia puntaroidessa alan toimijoiden välinen kilpailupaine, varsinkin teknologiayrityksissä, ajaa kohti pilvipalveluiden käyttöönottoa. Kilpailutilanne näkyy lähinnä sellaisissa yrityksissä, joiden toiminnalle keskeistä oli esimerkiksi verkkokauppatoteutuksien rakentaminen. Lainsäädännölliset tekijät eivät näkyneet merkittävinä tekijöinä estämään tai toisaalta edistämäänkään pilvipalveluiden käyttöönottoa. (Oliveira ym., 2014.)

Organisaation ICT-henkilöstön uudenlaisen osaamisen kehittämistarpeen ovat tunnistaneet myös Lian ym. (2017). He tuovat esiin terveydenhuoltoalan toimijoiden huolen, koskien organisaation oman ICT-osaston riittävää kykyä ja osaamista pilvikäyttöönottoa suunniteltaessa. Ulkopuolisen asiantuntija-avun tarvetta ja kokemuksia aikaisemmista pilvikäyttöönotoista pidetään välttämättöminä, jotta virheiltä omassa käyttöönottoprosessissa voitaisiin välttyä. (Lian,

Jiunn-Woei, 2014.) Kuten yleisemminkin palveluita ulkoistettaessa myös pilvipalveluiden tapauksessa onnistuneen käyttöönoton vaatimuksina ovat organisaation johdon tuki ja sitoutuminen, taloudellisten resurssien turvaaminen, uudenlaisten sopimusten hallinnointikyky sekä ICT-henkilöstön riittävä osaaminen uudenlaisia teknologiaratkaisuja ja tietoturvaosaamista koskien.

Cegielski ym. (2012) summaavat päätöksen pilvipalveluiden käyttöönotosta perustuvan useisiin toisiinsa liittyviin päätöksentekomenetelmiin. Organisaatioiden täytyy punnita epävarmuustekijöitä olemassa oleviin tietojenkäsittelykapasiteetteihin nähden. Tutkijat lisäävät vielä, että erilaisista sisäisistä ja ulkoisista toimintaympäristön epävarmuustekijöistä johtuen on vaikea tunnistaa yleistettäviä piirteitä. Tämän vuoksi arviointi tulisi tehdä aina tapauskohtaisesti. (Cegielski ym., 2012.) Pilvipalvelut ovat kuitenkin tulevaisuutta, jonka päätavoite on vähentää IT-palvelujen kustannuksia. Käyttöönotolla halutaan lisätä tietojenkäsittelyn suorituskykyä, luotettavuutta, käytettävyyttä ja joustavuutta. (Low, 2011.)

2.4 Luottamus koetuksella

Pilvipalveluiden käyttöönoton yksi keskeisimmistä kysymyksistä on, miten saavutetaan luottamus palveluntuottajiin. Esiin nousevat tunnetut tietoturvallisuutta kuvaavat teemat: tietoturvallisuus, yksityisyys ja luottamus. Tietoturvallisuus käsittää järjestelyt, joilla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuudella tarkoitetaan sitä, että järjestelmät ja palvelut tietoineen ovat käytettävissä haluttuna aikana. Eheys tarkoittaa yhtäpitävyyttä alkuperäisen tiedon kanssa. Eli tietoa voivat lisätä, poistaa ja muokata vain henkilöt, joilla siihen on oikeutus. Luottamuksellisuus puolestaan tarkoittaa sitä, ettei sivullinen taho saa tietoa käyttöönsä. (Sanastokeskus, 2018.)

Luottamus tietotekniikkaan on tärkeä tarkastelun kohde, koska ihmiset luottavat ICT-järjestelmiin enemmin kuin koskaan aiemmin. Internet-verkko itsessään on avoimen suojaamattoman rakenteensa vuoksi kuitenkin haaste luottamukselle. Jos luottamusta pohditaan konseptina, se koostuu kolmesta käsitteestä. Luotetaan uskomuksiin, aikomuksiin ja toimintaan. Sovellettaessa näitä luottamukseen informaatioteknologiaa kohtaan, tarkoitetaan sitä, että luotetaan käytössä olevaan teknologiseen ratkaisuun sen sijaan, että yritettäisiin itse kontrolloida sitä. Järjestelmän uskotaan olevan luotettava, turvallinen ja toteuttavan tehtävän oikea-aikaisesti. Luottamuksen ihmisiin ja teknologisiin ratkaisuihin voidaan ajatella koostuvan samankaltaisista elementeistä. Luottamus syntyy, mikäli sen kohteen voidaan sanoa toimivan ennustettavalla ja johdonmukaisella tavalla, tekee sen mikä on suunniteltu eikä se tuota odottamattomia tuloksia. Luotettava tietotekniikkaa ja hyvä kokemus sen käytettävyydestä vaikuttaa myös sen omaksumiseen ja käyttöönottoon. (McKnight, 2005.)

Luottamuksen käsitteeseen liitetään persoonallisuuspsykologiasta tunnistettu lähtökohtainen yleinen tendenssi luottaa muihin. Informaatioteknologiaa käytettäessä tämä tarkoittaa luottamusta yleisesti erilaisten teknisten ratkaisuiden toimimiseen. Institutionaalinen luottamus puolestaan on sosiologinen käsite,

joka hiukan yleistäen tarkoittaa luottamuksen rakentuvan siitä, että tekniikan onnistuminen on todennäköistä, olosuhteet ovat suotuisat ja sopimukset, takuut sekä suojatoimet ovat kunnossa. Tämä rakenteisiin luottaminen on tunnistettu olevan keskeinen osa tutkittaessa luottamuksen muodostumista IT-artefakteihin. Institutionaalinen luottamuskäsite on juuri se, jolla on suotuisa vaikutus kuluttajien mielikuvaan verkkopalveluiden luotettavuudesta. Tietojärjestelmän laatuominaisuudet ja esimerkiksi käyttöliittymän visuaalinen vetovoima vaikuttavat luottamuksen rakentumiseen IT-artefaktia kohtaan. Myös ympäröivällä kulttuurilla on todettu olevan vaikutusta yksilöiden luottamukseen ja halukkuuteen alkaa käyttää uutta teknologiaa tai internet-sovellusta. (McKnight, 2005; Vance, 2008.) IT-artefaktit eivät ole kulttuurisesti neutraaleja. Eri kulttuureista tulevilla henkilöillä voi olla hyvin erilaisia asenteita muodostaessaan luottamusta IT-artefakteja kohtaan. Tällä voi olla hyvinkin merkittäviä vaikutuksia luottamuksen rakentumisessa uutta teknologiaa kohtaan. (Vance, 2008.)

Pilvipalveluissa asiakkaiden tiedot tallennetaan palveluntuottajan ympäristöön, jonne asiakkaalla ei ole pääsyä eikä näkyvyyttä. Alhanahnah, Tari ja Zahir (2017) toteavat luottamuksen olevan monimutkainen käsite, joka vaatii monitieteellistä lähestymistä. Tietotekniikassa luottamuksen määrä tarkoittaa tilannetta, jossa A uskoo B:hen tiettynä ajanjaksona tietyssä kontekstissa, suhteessa palveluun X. Luottamus voi täten kompensoida kontrollointimahdollisuuksien puutteen, vakuuttaen pilvipalvelun käyttäjän palveluntuottajan turvallisuus- ja yksityisyysratkaisuiden kelvollisuudesta. (Alhanahnah, Bertok & Tari, 2017.)

Luottamuksen rakentumisen esteeksi pilvipalveluita kohtaan on nähty tietoturvaan liittyvät haasteet. EU:n kyberturvallisuusvirasto (ENISA) ja yhdysvaltalainen National Institute of Standard and Technology (NIST) ovat vuosien ajan listanneet erilaisia tietoturvallisuuskysymyksiä, myös pilviteknologioiden käyttöä koskien. Coppolino, D'Antonio, Mazzeo ja Romano (2017) nostavat keskeisimmiksi tuvallisuushaasteiksi viisi aihealuetta:

1. Jaettujen teknologioiden haavoittuvuudet. Hyökkääjä voi päästä hypervisor-ohjelmiston haavoittuvuuden kautta käsiksi fyysiseen isäntäkoneeseen (engl. host) ja sitä kautta vaarantuu koko jaettu ympäristö. Hypervisor-ohjelmistolla allokoidaan fyysisen palvelimen laskentaresurssit useiksi virtuaalisiksi palvelimiksi tarpeen mukaan.
2. Tietovuoto, eli tapahtuma, jossa käyttäjän data luovutetaan tahallisesti tai tahattomasti. Sensitiivistä tietoa menetetään.
3. Käyttäjätilin tai palvelun tietoliikenteen kaappaus, jolloin tunkeutujalle avautuu pääsy palvelun kriittiselle alueelle ja tiedon luottamus, eheys ja saatavuus voivat kärsiä.
4. Palvelunestohyökkäys (engl. Denied-of Service, DoS). Yksi hälyttävimmistä skenaarioista, joka voi tarkoittaa pilvipalveluissa sitä, että skaalautuva ympäristö tarjoaa kuormituksen alla enemmin laskentatehoa torjuen hyökkäyksen vaikutusta, mutta samalla tukee hyökkääjää tämän ilkeämielisessä toiminnassa tarjoamalla enemmän resursseja.
5. Haitallisesti toimiva sisäpiiriläinen on uudempi kasvava skenaario, jossa esimerkiksi palvelua tuottavan yrityksen työntekijä yrittää käyttää

> etuoikeutettua asemaansa pyrkien pääsemään arkaluontoisiin tietoihin käsiksi hyötymistarkoituksissa. (Coppolino, D'Antonio, Mazzeo & Romano, 2017.)

Tietotekniikkaan keskittyvät julkaisut esittelevät runsaasti ratkaisuja edellä listattuihin turvallisuushaasteisiin. Tämän tutkielman rajauksen takia teknisiä ratkaisuja ei käsitellä eikä arvioida tarkemmalla tasolla. Luottamuksella ja luottamuksen hallinnalla, erityisesti kaupallisissa pilvipalveluympäristöissä, on keskeinen merkitys. Pilvipalveluntuottajat ovat ottaneet käyttöön mainepohjaisen luottamuksenhallintajärjestelmän, joka auttaa palvelun käyttäjää löytämään luottamuksenarvoisen palveluntuottajan sähköisen liiketoimintansa kumppaniksi. Pilviympäristöjen arviointiin on käytössä useita viitekehysmalleja, joilla voidaan selvittää luottamuksen osa-alueita sekä luvattujen palveluiden ja niiden vasteaikojen toteutumista. (Manuel, 2015.)

Turvallisuusuhkien ja niiden vastatoimien ymmärtäminen auttaa organisaatioita arvioimaan ja laatimaan kustannushyötyanalyysejä arvioidessaan pilvisiirtymän toteutuskelpoisuutta. Pilvipalveluiden toteutukset sisältävät sekä perinteisiä tietoteknisiä ratkaisuja, mutta myös niille ominaisia uusia teknologisia ratkaisuita, tuoden mukanaan sekä niiden heikkouksia että vahvuuksia tietoturvanäkökulmasta katsottuna. Mikäli kriittistä infrastruktuuria kuten esimerkiksi energiatuotannon hallintajärjestelmiä ulkoistetaan kaupallisille palveluntarjoajille, on ymmärrettävä, mitä tarkoittaa vastuun siirtäminen organisaation oman henkilöstön valvonnan ulkopuolelle. Tällöin myös tietoturvaongelmat voivat eskaloitua. (Ali, M., Khan & Vasilakos, 2015.)

Pilvipalveluiden käyttöönoton seula vaatii liiketoiminnallisten vaikutusten ja riskien arviointia. Palvelinten virtualisointi ja usean käyttäjän datan sijaitseminen jaetussa ympäristössä synnyttävät pilvikohtaisia tietoturvauhkia, jotka on huomioitava, mutta myös ymmärrettävä pilven ominaisuuksina. Viranomaistoiminnassa arvioidaan kaikkia palveluntuottamisen taustatekijöitä koko tietojärjestelmän elinkaaren ajan. Tiedon kriittisyyden mukaan on huomioitava tiedon saatavuus normaaliolojen lisäksi myös poikkeusoloissa. Viranomaistoimijoiden tiedonhallinta ja tiedon sijainti on toteutettava niin, että vaikka pilvipalvelun tarjoajan palvelimet olisivat toisella puolella maapalloa, palvelun käyttäjien täytyy päästä siihen käsiksi aina Suomesta. Kattavien yksiselitteisten sopimusten laatimisen merkitys ja niiden ymmärtäminen korostuu.

Organisaation tietohallinnon koordinoimat vastuualueet ovat keskeisiä tietoteknisten ratkaisuiden ja valintojen taustalla myös pilvikäyttöönottoja valmisteltaessa. Pilvilaskennan käyttöönottopäätös vaatii perinteisten toimintamallien kehittämistä ja laajentamista siten, että ne mukautuvat tukemaan uudenlaisen ulkopuolisiin hankintoihin pohjautuvan toimintamallin kehittämistä ja käyttöönottoa.

2.5 Pilviadoption valmistelun haasteet

Pilvipalveluadoption onnistuneeseen etenemiseen on tunnistettu osatekijöitä, joilla on merkittävä vaikutus ja hyödyllisyys käyttöönoton onnistumisessa. Näitä tekijöitä Priyadarsihinee, Raut, Jha ja Gardas (2017) kokoavat tutkimuksessaan seuraavasti:

- Luottamuksen rakentuminen osoittautui tärkeimmäksi tekijäksi onnistuneelle pilvipalveluiden käyttöönotolle. Luottamus ja luottamuksellisuus määriteltiin sisältävän sellaisia käsitteitä, kuten esimerkiksi rehellisuus, totuus, oikeudenmukaisuus, aikomus pitää kiinni solmituista sopimuksista sopusoinnussa periaatteiden, ohjeiden ja lakien kanssa.
- Tietoturvallisuuden osa-alueet nähtiin toiseksi tärkeimmäksi seikaksi luottamuksen jälkeen. Palveluntarjoajan vastuu on hyvin merkittävä tarkastelun kohde palvelun saatavuutta ja turvallisuutta arvioitaessa. Tunnistettuja riskejä olivat suunnittelemattomat katkokset palveluiden käytössä, tietojen saatavuuden menetys tai hakkerihyökkäykset.
- Johtamistyylin kehittäminen edellyttää johtamiskäytäntöjen, menettelyjen ja rakenteiden kehittämistä tukemaan organisaation tulevia liiketoiminnan tavoitteita ja päämääriä. Johtaminen oli kolmanneksi merkittävin tekijä tutkimuksessa. Pilvipalveluiden hallintamallissa tulee kyetä yhdistämään IT-osaaminen ja liiketoimintakyvykkyydet. Informaatioteknologian pätevä hallintamalli edellyttää organisaatiolta kyvykkyyttä varmistaa ja tehdä aktiivisia toimia IT-omaisuutensa rakenneosien tarkoituksenmukaisessa ja tehokkaassa hyödyntämisessä.
- Uudenlaisesta teknologisesta innovaatiosta hyötyminen nähtiin seuraavaksi merkityksellisemmäksi. Uudenlainen innovaatio tuottaa organisaatiolle liiketoiminnallista hyötyä parantaen toiminnan tehokkuutta ja siten edelleen kilpailukykyä.
- Näyttöä oli myös sille, että pilviadoptiolla on voimakas suora vaikutus liiketoiminnan suorituskykyyn, joka edistää markkinointitoimia ja liiketoiminnan tulosten kasvua. (Priyadarshinee, Raut, Jha & Gardas, 2017.)

Palveluntarjoajat tuottavat omia ratkaisujaan ja rajapintojaan palveluiden ja resurssien saatavuudelle (Puthal, Sahoo, Mishra & Swain, 2015). Pilvipalveluita tuotetaan ympäri maailmaa, joten turvallisuus on keskeinen huolenaihe. Turvallisuusriskejä pidetäänkin merkittävimpinä estävinä syinä pilvipalveluiden käyttöönotolle. Arkkitehtuuri, jossa useampi asiakas jakaa samat resurssit, herättää epäilyksiä datan etävarastointia sekä omien resurssien hallinnan menettämistä kohtaan. Asiakkaan pitäisi pystyä luottamaan palveluntuottajaan. Palvelutasosopimuksiin kirjatut palvelut ja niiden käyttöä koskevat velvoitteet muodostavat ainoan juridisesti pätevän sitoumuksen palveluntuottajan ja asiakkaan välillä. Pilvipalveluiden tuottajat tarjoavat kuitenkin toisinaan heikkoja palvelusopimuksia asiakkaille. Sen vuoksi palveluntuottaja voi jopa välttyä sanktioiden maksamiselta asiakkaille, mikäli tapahtuu tietoturvarikkomus tai dataa menetetään. (El-Gazzar, Hustad & Olsen, 2016.)

Perinteiset IT:n turvallisuuskontrollit ja -mekanismit ovat hyvin samankaltaisia kuin mitä pilvipalveluiden toimitusmalleissa käytetään. Pilvipalveluilla on kuitenkin erilaisia organisaatiotason riskejä perinteiseen on-premises -tuotantomalliin verrattuna. Riskit liittyvät palveluiden käyttöönottotapoihin ja toiminnot mahdollistaviin tekniikoihin. Tietoturvalliset integraatiot perinteisen IT:n ja pilvipalveluiden välillä ovat usein haastavia ratkaista. Organisaation kriittisten, arkaluontoista tietoa sisältävien sovellusten siirtäminen pilvipalvelukapasiteettiin tuottaa huolen hallinnan menettämisestä organisaation omistamaan dataan. Palveluntuottajan pitää pystyä vakuuttamaan asiakas siitä, että hänelle tarjotaan edelleen samanlaisia suojausmekanismeja ja hallintamahdollisuus sovelluksille, kuin ne olisivat asiakkaan omasta IT-infrastruktuurista tuotettuina. Auditointien merkitys korostuu läpinäkyvyyden ja hallintamallien todentamisessa. (Khan & Al-Yasiri, 2016.)

Arvioitaessa tilannetta valtionhallinnon ja turvallisuusviranomaisten näkökulmasta, organisaation tietoaineiston fyysistä sijoituspaikkaa joudutaan arvioimaan viranomaistoiminnan erityisvaatimuksien kautta. El-Gazzar, Hustad ja Olsen (2016) arvioivat myös erityistarpeita todeten, että mikäli palvelun pitää olla käytettävissä 24/365, on syytä harkita tarkoin, minne ne fyysisesti sijoitetaan. Kriittisten sovellusten kohdalla palvelunestohyökkäyksestä, toimittajan konkurssista tai datakeskuksen vauriosta aiheutuu suuria ongelmia palvelun käyttäjille. Pilvipalveluita käyttöönotettaessa pitäisi aina tehdä myös poistumissuunnitelma sellaista tilannetta varten, jossa palvelu joudutaan kutsumaan takaisin ja sijoittamaan se jonnekin toiseen kapasiteettipalveluun. Tutkijat toivat esille yhtenä huomioitavana piirteenä myös kansallisten lainsäädäntöjen erilaisuuden ja paikallisten viranomaisten valtuudet alueellaan sijaitseviin datakeskuksiin. Asiakkaan tietoaineistoon voi sikäläisen kansallisen lainsäädännön valtuuttamana päästä käsiksi myös paikallinen viranomainen. Niin kutsutun Snowden-efektin jälkeen Yhdysvaltoja datan tallennuspaikkana halutaan jopa välttää. (El-Gazzar ym., 2016.) Snowden-efektillä viitataan Edward Snowdenin vuonna 2013 paljastamiin salaisiin asiakirjoihin, joista kävi ilmi muun muassa Yhdysvaltojen kansallisen turvallisuuspalvelun (NSA) harjoittama maailmanlaajuinen joukkovalvonta. Ali, Khan ja Vasilakos (2015) toteavat, että organisaation käyttäjien identiteetin ja käyttöoikeuksien hallinta on myös tarkasteltava ja ymmärrettävä sen toteutusmalli suhteessa pilvipalveluntuottajan hallintamalliin. (Ali ym., 2015.) Tässä alaluvussa toin esiin teorioita hyödyntävää tutkimusnäkökulmaa täydentäviä pilvipalveluiden käyttöönoton edellytyksiä ja riskiarviontiin vaikuttavia teemoja.

3 TIETOTURVALLISUUDEN TUTKIMUS JA TEOREETTINEN TAUSTA

Tässä luvussa käsitellään lyhyesti tietojärjestelmäturvallisuustutkimuksen kehitystä sekä esitetään tämän pro gradu -tutkielman taustalla vaikuttavat teoriat ja kehysmalli. Tietojärjestelmien tietoturvatutkimus sai alkunsa 1970-luvulla, jolloin tuli tarpeelliseksi ratkaista tietoturvallisuuden ongelmia ja kehittää käytännön prosesseja. Alkuvaiheen tietoturvallisuuden tarkastuslistoista siirryttiin vähitellen kypsyysstandardeihin, joista kehittyi myöhemmin nykyisinkin tunnettu ISO / IEC 27002. Tarkistuslistat sekä standardit keskittyivät ongelmiin ja niiden ratkaisuihin. Niiden avulla koottiin parhaita käytäntöjä ja ratkaisuja tietojärjestelmien turvallisuuden hallintaongelmiin. (Siponen & Baskerville, 2018.) Siponen (2005) mainitsee standardien eroavan tarkistuslistoista esimerkiksi siten, että ne yrittävät tarjota kansainvälisiä, auktorisoituja yleisiä kriteerejä. Käytännön tekemisen tasolla standardit sisältävät luettelon käytännöistä, joita organisaatioiden olisi toteutettava. Tarkastuslistat eivät olleet yhtä kunnianhimoisia listatessaan vain tehtäviä, joita pitäisi toteuttaa tietojärjestelmien turvaamisessa. Tietojärjestelmien turvatarkastuksissa korostetaan sitä, että tapauskohtaisesti tulee tarkastella kulloisessakin tarkastuksessa relevantit seikat, eikä pelkästään seurata tiettyä listausta asioista. Vakioituja tietoturvatarkastuskäytäntöjä noudattaen varmistetaan, että juuri oikeanlaisia tietoturvallisuusratkaisuja on tehty varmistamaan organisaation riittävä kypsyys ja osaamistaso. Tällä tavoin voidaan osoittaa asiakkaille ja liikekumppaneille luotettavuus aina kun on kyse tietoturvallisuudesta. Yleiset tietoturvastandardit eivät sellaisenaan tarjoa kaikille soveltuvaa tapaa arviointiin, vaan pitää ymmärtää turvallisuuden olevan monimutkainen organisaatiokysymys. Mikäli halutaan varmistua, että suojaus on tarkoituksenmukainen, tulee pystyä allokoimaan suojattavien kohteiden kriittisyys ja organisaation koon vaikutus. Tämä tarkoittaa sitä, että turvallisuustarpeet ovat erilaisia verrattaessa pienyrityksen tarpeita esimerkiksi valtionhallinnon turvallisuuskriittiseen virastoon. Tietoturvallisuuden arviointi on kehittynyt edelleen ottamaan huomioon organisaation tekemän tietoturvallisuusarviointityön kypsyystason sekä laajentanut tarkasteluaan erilaisiin käsitteellisiä malleja ja matemaattista mallinnusta hyödyntäviin riskienhallintamenetelmiin. (Siponen, 2006.)

Tietojärjestelmätieteen tutkimus on sovellettua tutkimusta siinä mielessä, että tietotekniikkaa ja organisaatioita koskevia ongelmia ratkaistaan käyttäen muiden tieteenalojen teorioita. Tällaisia tieteenaloja ovat esimerkiksi taloustiede, tietojenkäsittelytiede ja yhteiskuntatiede. Käytössä olevat vallitsevat tutkimusparadigmat ovat usein edelleen kuvaavan tutkimuksen mallia, joka on lainattu yhteiskunta- ja luonnontieteistä. (Peffers, Tuunanen, Rothenberger & Chatterjee, 2007.)

Baskervillen ja Mayerin (2002) tulkinnan mukaan tietojärjestelmätiede on kuitenkin saavuttanut myös aseman, jossa se itsenäisenä tieteenalana toimii referenssialana muille, eikä ole enää pelkästään muita tieteenalojen varassa. Kehityksen vuosikymmeninä hyödynnettiin tekniikkaa, tietojenkäsittelytiedettä, kyberneettisten järjestelmien teoriaa, matematiikkaa, johtamistiedettä ja

käyttäytymistiedettä. Tällä hetkellä tietojärjestelmätieteen tutkimus toimii perustana oman alansa uudelle kehittyvälle tutkimukselle, joka on osoitus kehittymisestä ja kypsymisestä. Viittauksia muiden tieteenalojen tutkimuskirjallisuuteen ei välttämättä tarvita. Alan oman tutkimusperinteen vakiintumisen osoittaa myös se, että tietojärjestelmätiede on kehittänyt oman aihepiirinsä, selkeän tutkimusnäkymänsä sekä myös tieteellisen kommunikaatiojärjestelmänsä. (Baskerville & Myers, 2002.)

Siponen ja Baskerville (2018) muistuttavat, että nykyisessä tietojärjestelmien turvallisuutta koskevassa tutkimuksessa tietojärjestelmätieteen panosta teorian kehittämiseksi pidetään hyvin arvokkaana. Yli 30-vuotisesta tutkimusperinteestä huolimatta tiedetään kuitenkin edelleen varsin vähän niistä olosuhteista ja tilanteista, joihin uudet teoriat tai rakenteet eivät sovellu. Ei tunneta myöskään sitä, miten tietoturvallisuuden ongelmia ratkaistaessa mikäkin teorioista toimii tai millainen on sen vaikutus suhteessa tarkasteltavaan kohteeseen. Edellisten lisäksi mainitaan, ettei ole kattavaa näyttöä siitä, pystyykö parhainkaan tutkimus tai teoreettinen panos voittamaan alan parhaat käytännöt tai ammattilaisten intuitioon perustuvan tietämyksen. (Siponen & Baskerville, 2018.)

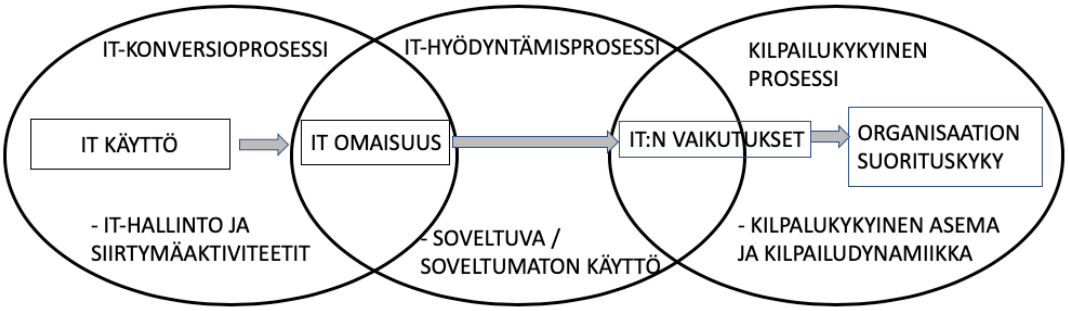
Tietojärjestelmien hallinnan kehittämisessä on paljon tavoiteltavaa myös tutkimuksen alalla. Tämä käy ilmi laajoista raporteista ympäri maailmaa, joissa kuvataan merkittävät taloudelliset menetykset, joita tietoturvaloukkaukset yrityksille aiheuttavat ja joiden vaikutukset ulottuvat myös järjestelmien käyttäjiin erilaisten sensitiivistenkin tietojen menettämisenä. Siponen ja Baskerville (2018) myöntävät tieteenalalla tunnistetun riittämättömän relevanssin suhteessa tietoturvallisuutta toteuttavien käytännön ammattilaisten työhön nähden. Erilaisten interventioiden vaikutusten tutkiminen nähdään kiinnostavana. Tutkimuksen kautta tarkastellaan, miten taustalla tunnistettu käytännön ongelma vähenee tehdyn toimenpiteen vaikutuksesta. Tällaiset tutkimustulokset voivat tuoda tietojärjestelmien tutkijat lähemmäs organisaatioiden ohjaavaa ja johtavaa käytännön toimintaa. (Siponen & Baskerville, 2018.) Voitaneen ajatella niin, että tietojärjestelmätieteen tutkimuksen vakiinnuttama asema muiden tieteenalojen joukossa vahvistuu entisestään, kehittymisen mahdollisuuksia tunnistetaan uusille sovellutusalueille ja tarve tietoturvallisuutta työkseen tekevien ammattilaisten kanssa tehtävälle yhteistyölle on hedelmällinen asetelma myös tulevaisuudessa.

3.1 Pilvilaskennalla tavoitellaan kustannustehokkuutta

Tilastokeskuksen (2019) mukaan maksullisia pilvipalveluita käyttää suomalaisista yrityksistä 74 prosenttia. Viidessä vuodessa käyttö on lisääntynyt 23 prosenttiyksikköä. Toimialoittain tarkasteltuna pilvipalveluita käytetään eniten ammatillisen, tieteellisen ja teknisen toiminnan aloilla (92 %), toiseksi eniten informaatio- ja viestintäaloilla (91 %), kolmantena tukkukaupan alalla (77 %) ja vähiten käyttöä oli vähittäiskaupan alalla (50 %). Suurimmista yrityksistä, jotka työllistävät yli sata henkilöä, käytti pilvipalveluita yli 90 prosenttia. Suosituimpia pilvipalveluina käytettäviä sovelluksia ovat sähköposti, tiedostojen tallennus ja toimisto-ohjelmat. Kaikista yrityksistä suurin osa, eli 64 prosenttia, käyttää julkista

pilveä, eli palvelut ostetaan samoilta palvelimilta, joita muutkin palvelun asiakkaat käyttävät. (Tilastokeskus, 2019.)

Pilvilaskennan suosion taustalla on kustannustehokkuuden tavoittelu. Organisaation adoptoidessa uutta teknologiaa päätöksen taustalla vaikuttavat aina liiketoimintaympäristö, teknologiset seikat sekä organisaation ominaisuudet ja kyvykkyydet. Soh ja Markus (1995) ovat kuvanneet IT:n luomaa liiketoimintahyötyä yleisellä tasolla prosessiteoriassaan (KUVIO 1). ICT:n vaatimien taloudellisten panostusten tuottama lisäarvo esitetään IT-johtamisen käynnistämänä kolmivaiheisena prosessina, jossa IT-voimavarat oikein hyödynnettynä ja käytettynä parantavat positiivisen vaikutuksensa kautta yrityksen suorituskykyä sekä kilpailuasetelmaa markkinoilla (Soh & Markus, 1995).



KUVIO 1 Kuinka ICT luo liiketoiminta-arvoa: Prosessiteoriaa mukaillen (Soh & Markus 1995, 37)

Wade ja Hulland (2004) esittelevät tutkimuksessaan resurssiperusteisesta näkökulmasta (engl. resource based view) saman aihepiirin tarkasteluun soveltuvan, mutta tarkemmalle tasolle jäsennellyn mallin. Resurssiperusteinen näkökulma tarjoaa tietojärjestelmätieteilijöille arvokkaita tapoja suhteuttaa tietojärjestelmiä organisaation strategiaan ja suorituskykyyn. Se tarjoaa viitekehyksen tutkia tietojärjestelmäresurssien strategista arvoa organisaatioille. Tietojärjestelmien resurssit harvoin kuitenkaan tuottavat suoraa vaikutusta kestävälle kilpailuedulle, joka olisi ideaali ominaisuus resurssiperusteisen teorian kannalta arvoituna. Sen sijaan resurssit muodostavat monimutkaisen varojen, vahvuuksien ja kyvykkyyksien ketjun, joka voi johtaa kestävään kilpailuetuun. (Wade & Hulland, 2004.) Baskervillen (2011) toteaa ICT-hyötyjen arvioimisen olevan ongelmallista. Tietojärjestelmiä koskevilta hankintaehdotuksilta edellytetään yleensä taloudellisen toteutettavuustutkimuksen tai kustannus-hyöty-analyysin. Järjestelmien tuottamaa, osin aineetonta hyötyä on vaikea perustella päätöksentekijöille niin, että he ymmärtäisivät miksi kannattaa sijoittaa pääomaa tietojärjestelmähankkeisiin. Arvioitujen hyötyjen kvantifiointi missä tahansa muodossa olisi toivottavaa, jotta päätöksentekoprosessi helpottuisi. (Baskerville, 1991.)

Organisaatioiden ICT-menot ovat alati kasvava kuluerä ja suuruusluokaltaan sellainen, että etenkin laskusuhdanteiden aikana myös IT-menoja arvioidaan hyvin tarkasti. Toimintaa halutaan tehostaa sekä lisäksi tietää sijoitetun pääoman tuotto. DeLonen ja McLeanin tietojärjestelmän menestysmallissa (Information Systems Success Model) arvioidaan käyttöönotettujen

tietojärjestelmien mittaamista niillä osatekijöitä, jotka vaikuttavat onnistumiseen. Mallissa yhdistetään ja vertaillaan eri ulottuvuuksien välisiä vaikutuksia toisiinsa. (Petter, 2013.)

Petter (2013) tunnistaa tutkimuksessaan joukon teemoja, joiden vaikutuksia arvioidaan toisiinsa nähden. Nämä loppukäyttäjän kokemuksiin sisältyvät tekijät nousivat esiin myös tämän tutkielman artikkeliaineistoa analysoitaessa. Tarkastelussa tunnistettuja tietojärjestelmien menestyksen osa-alueita ovat:

1) Tietojärjestelmän laatu. Sisältää toivottuina ominaisuuksina käytön helppouden, mukautuvuuden, luotettavuuden ja nopeat vasteajat.
2) Informaation laatu. Tietojärjestelmän tuotoksien relevanssi, ymmärrettävyys, tarkkuus, ajantasaisuus ja käytettävyys.
3) Järjestelmän tukipalveluiden laatu. ICT-henkilöstön reagoimiskyky, osaaminen, tarkkuus ja empatia.
4) Järjestelmän käyttömahdollisuudet. Ominaisuuksien hyödyntäminen, käyttöasteet ja -tavat, käytön laajuus sekä tarkoituksenmukaisuus.
5) Käyttäjien tyytyväisyys tietojärjestelmän käyttöön.
6) Järjestelmän käytöstä yksilölle, ryhmälle, organisaatiolle, teollisuudenalalle ja kansakunnan toiminnalle saatu nettohyöty, jonka myötä saavutetaan parempi päätöksentekokyky, tuottavuus, lisääntynyt myynti ja tehokkuus. (Petter, 2013.)

Tässä alaluvussa taustoitettiin yleisellä tasolla ICT:n merkitystä organisaation liiketoiminnan mahdollistajana. Kustannukset sekä tehokkuuden tavoittelu leimaavat myös tietoteknisten järjestelmien osalta tehtäviä linjauksia ja ratkaisuja. Pilvipalveluiden onkin nähty olevan seuraava askel tuottaa palveluita kustannustehokkaammin ja joustavammin.

3.2 Innovaatioiden diffuusio ja TOE-kehysmalli

Tämän tutkielman tieteellinen selkäranka sekä empiirisen osuuden käsittelyn pohja rakentuvat tietojärjestelmätieteelle ominaisista tunnetuista teorioista ja yhdestä sovellettavasta kehysmallista. Aluksi on hyödyllistä perehtyä hieman siihen, mitä innovaatiolla tarkoitetaan. Laajassa merkityksessä innovaatio voi olla mikä tahansa uusi idea käyttäjäjoukolle. Innovaation on todettu olevan idea, käytäntö tai esine, jonka yksilö tai uusi omaksujajoukko mieltää uudeksi. Ei ole merkittävää, onko se lajissaan objektiivisesti uusi, olennaista on omaksujajoukon käsitys uutuudesta. Innovaation ei myöskään tarkoita välttämättä paremmuutta tai sitä, että uusi innovaatio olisi hyödyllisempi käyttäjilleen kuin aikaisemmin käytetty. Innovaatio voi viitata johonkin abstraktiin, vaikkapa ideaan, mutta se voi olla myös konkreettisempi, kuten uusi käyttöönotettava teknologia. (Rogers, 2003; Straub, 2009.)

Adoptioteoria tutkii yksilöä ja tämän valintoja tietyn innovaation hyväksymiseksi tai hylkäämiseksi. Adoptioteoria on muutosta tarkasteleva mikroperspektiivi, joka kokonaisuuden tarkastelun sijaan keskittyy osatekijöihin, jotka

muodostavat kokonaisuuden. Diffuusioteoria puolestaan kuvaa, kuinka innovaatio leviää populaation keskuudessa. Se voi tarkastella esimerkiksi sellaisia tekijöitä kuin aika tai sosiaaliset paineet selittäessään tapahtumasarjaa, jossa populaatio sopeutuu, omaksuu tai hylkää jonkin tietyn innovaation käytön. Diffuusioteorian tarkastelu tapahtuu makroperspektiivistä havainnoiden innovaatioiden leviämistä ajan kuluessa. (Straub, 2009.)

Pilvipalveluiden käyttöönoton siirtymävaiheeseen liittyy keskeisesti uuden omaksuminen sekä kyky sopeutua palveluiden käyttäjäksi. Käyttöönottopäätösten ennakkovalmisteluun sisältyy laaja-alainen vaikutusten arviointi. Oliveira, Thomas ja Espadanal (2014) nimeävät kaksi teoriaa, jotka ovat yleisesti käytettyjä adoptiomalleja käsiteltäessä. Ne ovat innovaatioiden diffuusio (Diffusion of Innovations) ja TOE-kehysmalli, joka tarkastelee teknologian, organisaation sekä toimintaympäristön vaikutuksia. Myös Venkatesh, Morris, Davis ja Davis (2003) esittelemä Unified Theory of Use and Acceptance of Technology (UTAUT) mainitaan, mutta sen sanotaan liittyvän ja soveltuvan lähinnä yksilön valintojen tekemiseen (Oliveira ym., 2014.; Venkatesh, Morris, Davis & Davis, 2003). IT-käytön mallit saavat osakseen myös muunlaista kritiikkiä puutteellisuudestaan. Pahnila, Siponen ja Zheng (2011) eivät kiistä UTAUT:n ansioita, mutta tunnistavat puutteiksi sen, ettei teoria käsittele lainkaan ihmisten tapojen merkitystä käyttäytymisessä. Tutkijat ovat vakuuttuneita siitä, että tapojen tarkastelu tulee integroida osaksi tutkimusta, jossa tarkastellaan tietojärjestelmien tai palveluiden käyttöön vaikuttavia tekijöitä. Tekniikan tai palvelun käyttö jatkuu, koska sen käyttö on vakiintunut tavaksi. (Pahnila, Siponen & Zheng, 2011.) UTAUT teoriana näyttääkin näin kehittyvän edelleen saaden perustellun ja tarpeellisen näkökulman täydentämään ja laajentamaan aiempaa tarkastelua. Tässä tutkielmassa ei käytetä eikä esitellä UTAUT:ta laajemmin, koska tietohallintotoimialan näkökulma edellyttää organisaatiokontekstissa tehtävää tarkastelua, eikä tällöin yksilökeskeisen kuluttajanäkökulman vaikutus ole yhtä keskeinen.

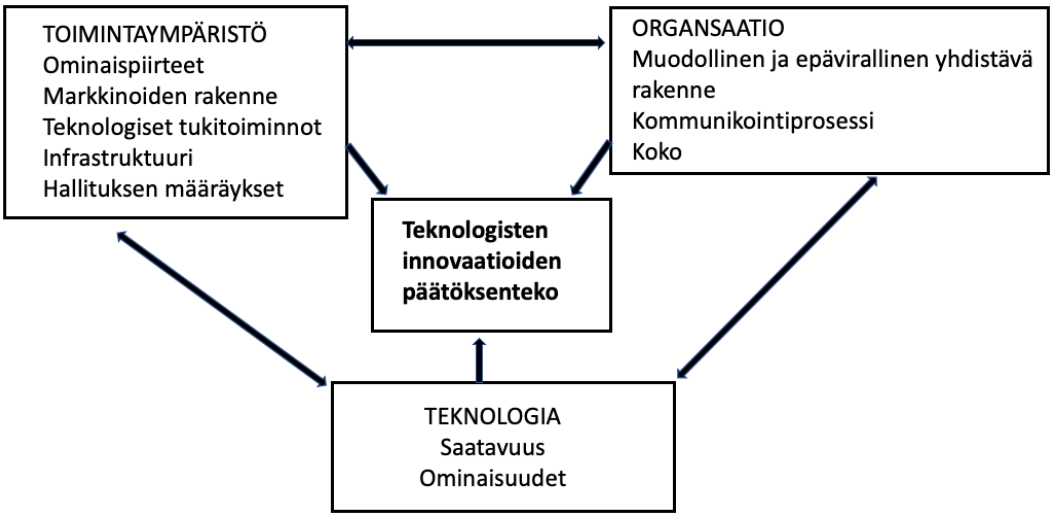
Innovaatioiden diffuusio -teoria käsittelee idean, tekniikan tai käytännön yleistymistä ja leviämistä. Teoria sisältää viisi ominaisuutta, joilla on vaikutusta innovaatioiden leviämiseen ja hyväksymiseen.

- Suhteellinen hyöty
    - Taso, joka saavutettaisiin uuden innovaation käyttöönoton myötä suhteessa aiempaan vastaavaan.
- Yhteensopivuus aiempien kokemusten, tarpeiden ja arvojen suhteen
    - Missä määrin uusi innovaatio voidaan rinnastaa esimerkiksi olemassa oleviin liiketoimintaprosesseihin?
- Kompleksisuus
    - Kuinka vaikeaa uutta innovaatiota on käyttää tai kuinka helppoa siihen on sopeutua?
- Näkyvyys
    - Missä määrin innovaatio on näkyvä toimintaympäristössään? Innovaation näkyvyys aktivoi aihetta käsittelevien keskusteluiden syntymistä vertaisverkostoissa.
- Kokeiltavuus

- Onko uutta innovaatiota helppo kokeilla? Vaivattomasti kokeiltava innovaatio edustaa pienempää epävarmuutta, kuin sellainen, johon ei voi tutustua kokeillen. (Rogers, 2003.)

Edellä kuvatut ominaisuudet soveltuvat tarkasteluun etenkin yksilön, mutta myös organisaation tietohallinnollisesta näkökulmasta. Rogers (2003) laajentaa arviotaan edelleen myös organisaatiotason päätöksentekoprosesseihin paremmin soveltuvaksi. Tarkastelua laajentavat ominaisuuksina tietämyksen hankkiminen innovaation olemassaolosta ja siitä, kuinka se toimii. Houkuttelevuus on muodostunut mielikuva uuden innovaation soveltuvuudesta tai soveltumattomuudesta. Päätös syntyy silloin, kun sitoudutaan sellaisiin aktiviteetteihin, jotka johtavat innovaation hyödyntämiseen. Implementointivaiheessa innovaatio otetaan käyttöön. Konfirmaatio ilmenee käytön jatkumisena myös myöhemmissä arviointipisteissä, tai vaihtoehtoisesti käytön lopettaminen, jos ei olla enää tyytyväisiä tuotteeseen ja jokin korvaava tuotevaihtoehto vastaa paremmin käyttäjäkunnan tarpeisiin. (Rogers, 2003.) Oliveira, Thomas ja Espadanal (2014) kritisoivat innovaatioiden diffuusioteoriaa todeten sen jättävän huomiotta muut toimintaympäristöön sisältyvät tekijät, jotka vaikuttavat kuitenkin yrityksen päätöksentekoon uuden teknologian käyttöönoton suhteen. Sellaisia tekijöitä ovat esimerkiksi ulkoinen paine ja lainsäädännöllinen tuki. (Oliveira ym., 2014.) Näiden tekijöiden vaikutus johti etsimään täydentävää mallia myös tässä tutkielmassa.

Soveltaessaan organisaatioiden päätöksentekoprosesseihin innovaatioiden diffuusioteoriaa Oliveira ym. (2014) tukeutuvat Tornatzkyyn ja Fleischeriin (1990), jotka ovat kuvanneet TOE-kehysmallin (KUVIO 2). TOE-kehysmalli kuvaa päätöksentekoprosesseihin vaikuttavaa kolmea ulottuvuutta, kontekstia, joilla on merkitystä uuden innovaation käyttöön johtavassa päätöksentekoprosessissa. Kontekstit ovat teknologia, organisaatio ja toimintaympäristö. Teknologiakonteksti sisältää organisaation kannalta merkitykselliset teknologiset ratkaisut ja valmiudet uuden innovaation adoptointiin. Organisaatiokonteksti sisältää organisaatiorakenteen, yrityksen koon, hallinnollisen rakenteen, sekä mukaan luettuna resurssit ja viestintäkulttuurin vaikutukset. Kolmas konteksti on ympäristö, sisältäen organisaation asemoitumisen liiketoimintaympäristössä suhteessa kilpailijoihin, ja toimintaa ohjaavan vallitsevan yhteiskunnallisen toiminnan sääntelyyn. (Tornatzky & Fleischer, 1990.)



KUVIO 2 TOE-kehysmalli – mukaillen Tornatzky ja Fleischer 1990

Oliveira ym. (2014) ehdottavat, että yhdistämällä DOI ja TOE saadaan kattavampi perspektiivi teknologioiden käyttöönoton tarkastelua varten, jolloin teoriat täydentävät toisiaan. Oliveiran ym. (2014) tutkimuksessa toimialoina olivat valmistava teollisuus ja palvelualat, joilla kummallakin pilvipalveluiden käyttöön siirtymiseen vaikuttavat muutosvoimat olivat hieman toisistaan poikkeavat. Tuloksissa havaittiin muun muassa, että teknologinen valmius helpottaa pilvipalveluiden käyttöönottoa. Vakiintunut teknologiainfrastruktuuri ja ICT-henkilöstön osaaminen ovat edellytys pilvipalveluiden integrointiin. Perinteinen teknologiaosaaminen ei riitä, vaan vaatimuksena on kyky pystyä varmistamaan oikeanlainen osaaminen juuri pilvipohjaisten ratkaisuihin siirryttäessä. Ellei niin tehdä, on odotettavissa hallinnointihaasteita. (Oliveira ym., 2014.) Organisaation ICT-henkilöstön uudenlaisen osaamisen kehittämistarpeen ovat tunnistanut myös Lian (2017), joka tuo esiin terveydenhuoltoalan toimijoiden huolen koskien organisaation oman ICT-osaston riittävää kykyä ja osaamista pilviadoptiota suunniteltaessa. Lainsäädännölliset tekijät eivät näkyneet merkittävinä tekijöinä estämään tai toisaalta edistämäänkään pilvipalveluiden käyttöönottoa. (Oliveira ym., 2014.)

Priyadarsihinee, Raut, Jha ja Kamble (2017) haluavat korostaa sitä, että TOE-kehysmallin tarkasteluun tulee lisätä kaksi ulottuvuutta. Nämä ovat koettu tietoturvariski ja laadittava riskiarvio, joita ilman heidän mukaansa ei tulisi tehdä hallinnollisia päätöksiä pilvipalveluiden käyttöönotosta. Tutkimuksensa tulosten perusteella he toteavat, että havaituilla riskeillä ja tietoturvariskien arvioinnilla on merkittävä vaikutus pilvipalveluiden käyttöönottoon. Vielä tärkeämmäksi nousee luottamuksen käsite. Luottamuksen tulkitaan tarkoittavan pilvipalvelutuottajaan kohdistuvaa vahvaa luottamuksellisuutta, rehellisyyttä, oikeudentajua, oikeutta sekä hyvää tahtoa pyrkiä toteuttamaan solmittuja sopimuksia. (Priyadarshinee, Pragati, Raut, Jha & Kamble, 2017.)

4 KIRJALLISUUSKATSAUS MENETELMÄNÄ

Tässä luvussa esitellään tutkielmassa käytetty menetelmä, tutkimusaineiston valintaperusteet rajauksineen sekä tutkimusaineiston käsittelyn vaiheet käytettyyn menetelmään perustuen. Tutkimuksen kvalitatiivinen luonne soveltuu tämän pro gradu -tutkielman tarpeeseen ja tavoitteeseen. Siponen ja Klaavuniemi (2020) haastavat käsityksen siitä, että vain luonnontieteiden perinteiden kvantitatiivinen tutkimusote olisi soveltuva tietojärjestelmätieteen tutkimukseen. Yleinen käsitys on ollut sellainen, että luonnontieteiden tutkimus on kvantitatiivista, objektiivista ja tarkkaa, kun taas yhteiskuntatieteiden tutkimus on kvalitatiivista ja soveltavaa. Tietojärjestelmien tutkimuksessa kvantitatiivisia menetelmiä käyttäen voidaan muodostaa jopa virheellinen tulkinta oletettua totuutta ja sen hallittavaksi tekemistä koskien. Tämä voi näkyä esimerkiksi tulkintana tutkitun ilmiön oletetusta lineaarisesta luonteesta, jota sillä ei kuitenkaan todellisissa olosuhteissa ole. Tällaisessa tapauksessa tulosten sovellettavuudesta voitaisiin vakuuttua vain muilla menetelmillä tehtävillä jatkotutkimuksilla. Siponen ja Klaavuniemi (2020) korostavat sitä, että parhaat tietojärjestelmätieteen käyttämät mallit ja teoriat antavat oikein asetettuina pätevät ennusteet ja ovat yleisesti tarkkoja. Tietojärjestelmien tutkimuksen ja luonnonteiden välillä on monia eroavaisuuksia, mutta luonnontieteellisestä tutkimuksesta voidaan toki ottaa oppia. (Siponen & Klaavuniemi, 2020.)

Tässä tutkielmassa käytetään menetelmänä käsiteanalyyttistä (engl. conceptual analytical) tutkimusotetta (Järvinen, 2000; Siponen, 2002), joka sisältää myös kirjallisuuskatsauksen (engl. literature review). Kirjallisuuskatsauksessa selvitetään miten ja millaisista näkökulmista aihetta on aiemmin tutkittu tuoden aineiston pohjalta tehdyt havainnot ja johtopäätökset osaksi tämän tutkielman lopputuloksia. Aineisto haetaan ja valitaan keskeiseksi määriteltyjä käsitteitä käyttäen sekä rajataan niin, että aineiston vastaavuus palvelee tutkielman tavoitetta. Kirjallisuuskatsaus on metodi, jossa tutkitaan aiempaa tutkimusta. Kokoamalla aiemmin tehtyjen tutkimusten tuloksia, syntyy pohja uusille tutkimustuloksille. Johdonmukaisen tarkastellen analysoidaan ja yhdistellään aiempaa tutkittua tietoa ja tietämys aihepiiristä lisääntyy. Kirjallisuuskatsauksen tavoite on kehittää olemassa olevaa teoriaa luoden myös uutta, sekä muodostaa mahdollisimman kattava kuva tarkasteltavasta kokonaisuudesta. (Salminen, 2011.) Lähdeviitteet mahdollistavat lukijalle tietojen tarkastamisen sekä arvioinnin. Lähdeviitteiden perusteella voidaan myös arvioida, millaiselta pohjalta tutkijan tuottama uusi tieto on muodostettu (Hirsjärvi, Remes, Sajavaara & Sinivuori, 2009).

Salminen (2011) muistuttaa, että suomenkielinen termi kirjallisuuskatsaus (engl. literature research review, literature review) on osittain harhaanjohtava, koska kyse ei ole pelkästään lyhyt tai tiivis katsaus aihepiiriin, vaan tieteellisen aineiston analyyttinen, kriittinen ja perusteellisella otteella suoritettava arviointi (Salminen, 2011). Kirjallisuuskatsaus on laaja käsite, joka tyypillisesti tarkoittaa tutkimusraportin lyhyttä primaarin tietoaineiston esittelyjaksoa. Kirjallisuuskatsauksella itsessään voi olla lukuisia erilaisia kohteita, päämääriä tai näkökulmia. Sen kohteena voivat olla tutkimustulokset, menetelmät, teoriat, sovellutukset tai se voi yhdistää kaikkia edellä lueteltuja. (Cooper, 1988.) Kirjallisuuskatsaus

menetelmänä on luoteeltaan itsenäinen ja soveltuu laaja-alaisiin käyttökohteisiin tuoden näkyväksi monialaiset käyttötavat ja merkityksen osana tieteellistä tutkimusta (Bruce, 1994).

Koska tutkielman yhtenä tavoitteena on tuottaa pilvipalveluita käsittelevää tausta-aineistoa tietohallintotoimialalle osaamisen ja tietämyksen lisäämisen taustaksi organisaatiossa, soveltuu kirjallisuuskatsaus hyvin käytettäväksi menetelmäksi. Asiaankuuluvan aiemman kirjallisuuden katsaus ja arviointi ovat olennainen piirre kaikissa akateemisissa projekteissa luoden vankan perustan uuden tiedon edistämiselle. Se helpottaa teorian kehittämistä, muodostaa käsityksen aihepiireistä, joista on jo hyvin runsas määrä tutkimusta ja paljastaa toisaalta alueita, joista tutkimusta kaivataan lisää. Kirjallisuuskatsaus on onnistunut, kun se auttaa lukijaansa ymmärtämään käsiteltävästä aiheesta kertyneen tietämyksen. (Webster & Watson, 2002.) Kirjallisuuskatsauksella tuotetaan systemaattinen kokoava näkemys pro gradu -tutkielman tulosten sekä tulkintojen muodostamiseksi, joita voidaan edelleen jatkotyönä jalostaa viraston sisäisten päätöksentekoa ohjaavien päätösten ja ohjeiden tausta-aineistona.

Kirjallisuuskatsaus toteutetaan systemaattisen kirjallisuuskatsauksen periaatteita noudattaen. Fink (2005) määrittelee kirjallisuuskatsauksen olevan systemaattinen, täsmällinen, toistettava menetelmä, jolla tunnistetaan, arvioidaan ja syntesoidaan aiempi valmis julkaistu tutkimustyö (Fink, 2005). Kirjallisuuskatsauksessa keskitytään tutkimuksen kannalta keskeisen kirjallisuuteen esitellen, miten ja mistä näkökulmista aihepiiriä on aiemmin tutkittu ja miten valmisteilla oleva tutkimus liittyy aikaisemmin tehtyihin tutkimuksiin. Lukija voi lähdeviitteiden avulla tarkistaa niiden alkuperän sekä sen, miten niitä on käytetty tutkimuksessa. (Hirsjärvi ym., 2009.)

Systemaattisen kirjallisuuskatsauksen laatiminen nähdään hyödylliseksi menetelmäksi monien ominaispiirteittensä takia. Johdonmukaisen prosessin avulla saadaan koottua tutkimuksen kannalta olennaiset tutkimukset ennalta määrättyjen sisäänotto ja poissulkukriteereiden ansioita. Pyrkimys tarkastella alkuperäistutkimuksia tuottaa mahdollisimman laadukkaan aineiston. Valintojen avulla rajataan kohtuullinen määrä lähteitä, sisällyttäen mukaan kuitenkin olennaiset. Metodin vaiheiden asianmukainen noudattaminen tuo uskottavuutta aineistosta nousseille tulkinnoille ja tutkimustuloksille. (Metsämuuronen, 2005.)

Metsämuuronen (2005) pohtii lisäksi tutkimuksen kautta tuotetun näyttöön perustuvan ajattelun merkitystä. Näyttöön perustuvassa ajattelussa selvitetään, onko jokin malli tai toimintatapa tutkimukseen perustuen toista parempi. Tieteellisellä näkökulmalla parannetaan best practices tai benchmarking ajattelua ja tuotetaan tietoa esimerkiksi valintoja tehtäessä päätöksenteon tueksi. (Metsämuuronen, 2005.) Käytettävissä olevan tiedon määrä lisääntyy koko ajan ja tätä tietoa tarvitaan johtamistoiminnassa päätöksenteon tueksi. Tällöin systemaattisen kirjallisuuskatsauksen keinoin tuotetun tiedon jalostamiselle on kasvava tarve (Salminen, 2011). Organisaatioiden tietohallintotoimiala ja päätöksentekoprosessit hyötyvät tällaisista tarkasteluista. Menetelmää hyödyntäen tutkimusaineistosta tehdään meta-analyysi, jonka avulla luodaan synteesi ja haetaan vastaukset tutkimuskysymyksiin. Seuraavissa alaluvuissa esittelen tarkemmin kirjallisuuskatsauksen vaiheet sekä käytännön toteutuksen.

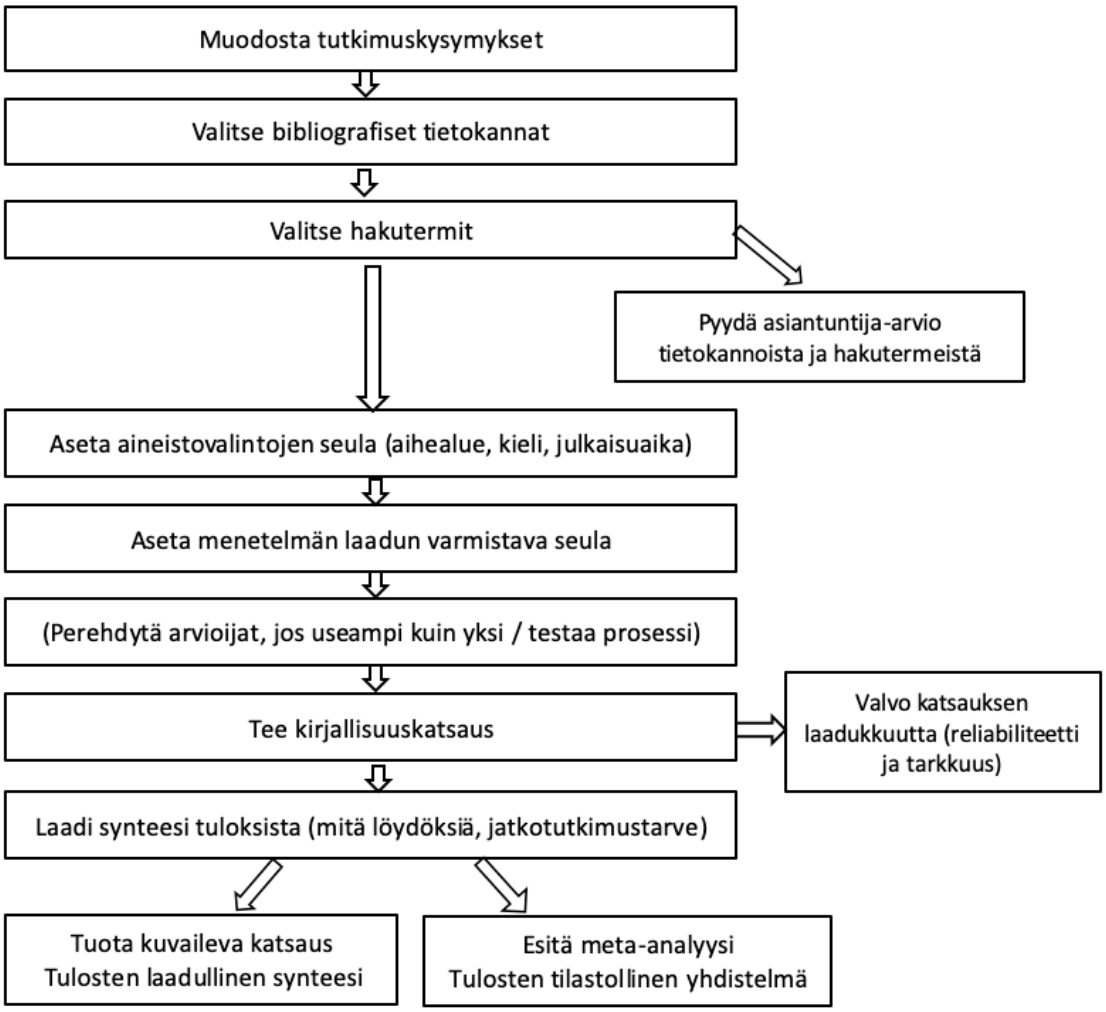
4.1 Menetelmän tausta ja soveltaminen tietojärjestelmätieteessä

Kirjallisuuskatsauksen toteutusta tietojärjestelmien tutkimuksessa ovat soveltaneet Okoli ja Schabram (2010), jonka taustalla on Finkin (2005) alkujaan terveydenhuoltoalan tutkijoille luoma malli (KUVIO 3). Tämä on yksi yleisimmistä rakenteista, jota sovelletaan kirjallisuuskatsauksia laadittaessa. Kirjallisuuskatsauksen laatimista Fink (2005) esittelee alla olevalla tavalla.

Ensin muodostetaan täsmälliset tutkimuskysymykset, jotka ohjaavat kirjallisuuskatsauksen tekemistä. Toisessa vaiheessa valitaan käytettävät tiedonlähteet, kuten tietokannat ja kirjallisuus, jotka sisältävät sellaista aineistoa, joista voidaan löytää vastaukset tutkimuskysymyksiin. Jo tässä vaiheessa tulee valita tutkimuksen aihealuetta hyvin tuntevien asiantuntijoiden laadukasta materiaalia lähdeluetteloineen. (Fink, 2005.)

Kolmannessa vaiheessa muodostetaan tiedonhaussa käytettävät hakusanat ja lausekkeet, jotka pohjautuvat tutkimuskysymyksien kehystämään tutkimuksen aihealueeseen. Seuraavissa kahdessa vaiheessa (vaiheet 4 ja 5) keskitytään seulomaan hakuja harkittujen kriteereiden avulla, jotta laajaan ensivaiheen hakutulokseen saadaan sisällytettyä olennaiset ja poissuljettua tarpeettomat aineistot. Käytännön seulontakriteereitä voivat olla aineiston julkaisukieli ja julkaisun tyyppi sekä julkaisuajankohta. Seulontavaiheisiin kuuluu myös aineiston tieteellisen laadun arviointi, jonka tuloksena pyritään valitsemaan tieteellisin kriteerein mahdollisimman korkeatasoinen aineisto. (Fink, 2005.)

Kuudennessa vaiheessa toteutetaan itse kirjallisuuskatsaus reliabiliteetin ja validiuden edellyttämillä tavoilla käyttäen vakiomuotoista tapaa tietojen koostamiseksi artikkeleista. Mikäli aineistoa arvioi useampi henkilö, tulisi heidät tässä vaiheessa opastaa tehtäväänsä ja monitoroida prosessin kulku sekä sen laadukkuus. Viimeinen vaihe on kootun aineiston tulkinta, yhteenveto ja kokonaisnäkemyksen muodostaminen. Synteesi on joukko kirjallisuuskatsauksen havaintojen tulkintoja, joissa yhdistyvät sen laatijan aiempi kokemus ja tulkinnat saatavilla olleen aineiston sisältöön liittyen. (Fink, 2005.) Kirjallisuuskatsauksen toteutus kirjataan tutkielmaraporttiin, jotta tutkimuksen tekemisestä syntyy lukijalle selkeä käsitys ja jotta se olisi myös toistettavissa.



KUVIO 3 Kirjallisuuskatsauksen vaiheistus Finkiä (2005) mukaillen

Okoli ja Schabram (2010) antavat tunnustusta Finkin esittelemälle ohjeelle tehdä kirjallisuuskatsauksia, mutta haluavat täydentää ja tarkentaa tiettyjä kohtia, joita pitävät puutteellisina. Heidän mielestään Finkin ohje keskittää huomionsa terveystieteiden tutkimukseen ja siten siinä käsitellään vain pintapuolisesti laadullisen tutkimuksen tekemistä. Tämä rajoittaa kirjoittajien mukaan huomattavasti Finkin laatiman ohjeen sovellettavuutta liiketalouden ja sosiaalitieteiden tutkimuksessa. (Okoli & Schabram, 2010.)

Toteutan kirjallisuuskatsaus Okolin ja Schabramin (2010) tietojärjestelmätieteen tutkimukseen sovittamaa mallia mukaillen. Kirjallisuuskatsauksen tarkoitus ja tavoitteet ovat Okolin ja Schabramin (2010) listaamina seuraavat:

1. **Kuvaillaan ensin selkeästi kirjallisuuskatsauksen tarkoitus ja päämäärä.** Kuvailu on tarpeellista, jotta kirjallisuuskatsaus olisi selkeä lukijoille.
2. **Menettelytapojen yhdenmukaistaminen ja perehdytys tutkijaryhmälle.**

Tutkijaryhmän työn alkaessa on tärkeä vaihe sopia käytännöistä ja menettelytavoista kaikkien tutkimuksen toteutukseen osallistuvien kesken. Työn edetessä tulee myös valvoa menettelytapojen noudattamista ja laadukasta toteutusta.

3. **Aineiston hakuun liittyvät yksityiskohdat perusteluineen.**
   Kirjallisuuden haun yksityiskohdat on kuvattava selkeästi. Tulee myös selittää ja perustella, kuinka haun kattavuus on varmistettu. Perinteisten oppikirjatyyppisten lähteiden sijaan suositellaan käyttämään tieteellisen tutkimuksen vaatimukset täyttäviä erilaisia sähköisiä hakupalveluita. (Okoli & Schabram, 2010.)
4. **Sisällön seulontavaihe, rajaukset ja perustelut valinnoille.**
   Seuraavaksi tehdään haetun aineiston seulontaa, jossa sisällytetään soveltuvat tutkimukset mukaan sekä rajataan ulkopuolelle sellaiset, jotka eivät täytä vaatimuksia. Arviointia voidaan tehdä esimerkiksi otsikon ja abstraktin perusteella. Tehdyt ratkaisut on kuvattava raporttiin täsmällisesti ja perusteltava valinnat. Poissuljettujen tutkimusten osalta on selitettävä syyt, miksei niitä käsitetty ja perusteltava miten kirjallisuuskatsauksen tulos voi olla silti kattava. Okoli ja Schabram (2010) toteavat kuitenkin, että aineistovalintojen seulominen on hyvin subjektiivinen ja tutkijan itsensä tekemistä valinnoista riippuva vaihe kirjallisuuskatsauksen tekemisessä. Heidän mukaansa ei ole absoluuttisesti oikeita tai vääriä valintoja, mutta tehtyjen valintojen perusteluun tulee kiinnittää merkittävästi huomioita. Aineiston tulee olla riittävän laaja ja tarkoituksenmukainen vastattaessa tutkimuskysymyksiin, mutta toisaalta se on suhteutettava käytettävissä olevaan aikaan, rahaan ja henkilöstöresursseihin. Valinnan onnistumisella on aivan olennainen merkitys sille, voidaanko kirjallisuuskatsausta pitää luotettavana. Tässä vaiheessa ei vielä arvioida tutkimusraporttien laatukysymyksiä, vaan pyritään valitsemaan sisällöltään tutkimukseen aihealueeseen soveltuvaa aineistoa. (Okoli & Schabram, 2010.)
5. **Valitun aineiston kelvollisuus, laadukkuus ja kriteerit.**
   Kirjallisuuskatsauksen seuraava vaihe on asettaa kriteerit aineiston tieteellisen laadun arvioinnille. Edellisessä vaiheessa seulottua aineistoa on tarpeen tarkastella tarkemmin kunkin artikkelin tieteellisen laadukkuuden näkökulmasta. Okoli ja Schabram (2010) pohtivat tämän seulontavaiheen merkitystä todeten, että vaikka se yleensä nähdään soveltuvan määrällisen tutkimuksen kirjallisuuskatsauksiin paremmin, on sen käyttö myös laadullisessa tutkimuksessa perusteltua. Vain siten voidaan tukea tieteellisen tutkimuksen yleisiä periaatteita, joita ovat muun muassa pyrkimys tarkkuuteen, järjestelmällisyyteen ja tutkimuksen toistettavuuteen. (Hirsjärvi ym., 2009; Okoli & Schabram, 2010.) Myös tutkimusaineiston metodologisen laadun osoittaminen on hyvin tärkeää, koska lopputuloksen laatu on suuresti riippuvainen tutkimuksessa tarkasteltavien aiempien tekstien laadukkuudesta. Seulonnan kaksi vaihetta olisi syytä kuvata erikseen, vaikka ne liittyvätkin myös kriteereiden osalta vahvasti toisiinsa. Seulonnan metodologisen vaiheen yhteismitallinen toteuttaminen ei ole kuitenkaan yksiselitteistä, sillä laatua on voitu arvioida eri tavoin. Okoli ja Schabram (2010) myöntävät, etteivät voi tuottaa kattavaa opasta laadun

arvioinnin suorittamiselle, eivätkä voi antaa määritelmää myöskään sille, milloin artikkeli on riittävän laadukas käytettäväksi tutkimuksessa. Erilaisia laatuarviokriteereiden perusteita on olemassa eri tutkijoiden kirjaamina ja heidän suosittelemiaan teemoja voidaan soveltaa kulloisenkin kirjallisuuskatsauksen protokollaa laadittaessa. Perusteet tulee kirjata niin selkeästi, että toteutettu kirjallisuuskatsaus olisi toistettavissa. Laadullisen tutkimuksen alalla yhteiskunnallisessa tutkimuksessa käsittelytapa on luonteeltaan hieman erilainen, mutta silti kriteereiden määrittelyä, kuvaamista ja niiden noudattamista pidetään soveltuvana käytäntönä, jota tulee noudattaa. (Okoli & Schabram, 2010.)

6. **Järjestelmällinen läpikäynti ja havaintojen luokittelu.**
   Aineiston jokaista tekstiä tulisi tarkastella ainakin seuraavia seikkoja arvioiden: mitä väitteitä tutkimuksessa esitetään, mitä todisteita näiden väitteiden tueksi esitetään, ovatko todisteet vakuuttavia, ja jos ovat, miten niitä tuetaan ja taustoitetaan. Laadullisen tutkimuksen osalta arviointikriteerit tulisi kuvata erilliseen taulukkoon, josta lukija voisi ne nähdä. Taulukkoon tulisi myös pystyä kommentoimaan tehtyjä valintoja. Aineiston metodologisen laadun osoittaminen on hyvin tärkeää, koska toteutettavan kirjallisuuskatsauksen lopputuloksen laatu on suuresti riippuvainen siinä tarkasteltavien aikaisempien tutkimuksien laadusta. (Okoli & Schabram, 2010.)
7. **Tutkimusaineiston analysointi ja synteesin laatiminen**
   Analyysivaiheessa yhdistetään tutkimuksista kerätyt faktat käyttämällä tarkoituksenmukaisia tekniikoita, jotka voivat laadullisia tai määrällisiä tai molempia. (Okoli & Schabram, 2010.)
8. **Katsauksen kirjoittaminen ja työn raportointi toistettavuuden varmistamiseksi.** Viimeisessä vaiheessa kirjallisuuskatsauksesta kirjoitetaan raportti tutkimuspapereiden yleisiä periaatteita noudattaen. Systemaattisen kirjallisuuskatsauksen prosessi on kuvattava niin yksityiskohtaisesti, että muut tutkijat voivat toistaa tutkimuksen itsenäisesti ja saada samat tutkimuksen tulokset. (Okoli & Schabram, 2010.)

4.2 Aineiston valintakriteerit

Tässä alaluvussa kuvaan tarkemmin tutkimusaineiston kokoamisen ja käsittelyn vaiheet. Tutkielman keskeisimmät osa-alueet ovat pilvipalveluiden käyttöönottopäätösten taustalla vaikuttavat teemat, sekä pilviadoption onnistunutta läpivientiä varmistavat hyödylliset havainnot. Informaatioteknologian alojen tutkimukselle kansainväliset tieteelliset aikakauslehdet ja konferenssijulkaisut ovat merkittäviä julkaisukanavia. Kirjallisuuskatsauksen aineisto on haettu yliopiston kirjaston ohjeiden mukaisesti informaatioteknologian alan keskeisistä tietokantoista Elsevier Scopus ja IEEE Xplore Digital Library. Täydentäviä hakuja varten käytettiin myös Google Scholaria. Hakuehtojen mukaiset haut on suoritettu kirjautumalla Jyväskylän yliopiston opiskelijan käyttäjätunnuksilla JYKDOK-

palveluun, jonka kautta yliopisto tarjoaa käyttöön sähköiset ja painetut aineistot. JYKDOK on osa kansallista Finna-palvelukokonaisuutta.

Aineiston valinnassa tulee muistaa lähdekritiikki. Vaikka tieteellisten julkaisuiden kirjoittajien pitäisi olla alansa asiantuntijoita, aineistoa on lähestyttävä harkiten pyrkien objektiivisuuteen. Tulee kiinnittää huomioita mahdollisiin vinoumiin, joita voidaan tunnistaa kielenkäytössä ja tekstin painotuksissa. (Hirsjärvi, 2009.) Testihakujen perusteella haastavaksi muodostui aineistohakujen rajaaminen tarkoituksenmukaisella tavalla pro gradu -tutkielman laajuus huomioiden. Esimerkiksi cloud computing hakusanana tuotti kymmeniin tuhansiin yksittäisiin julkaisuihin nousevan määrän potentiaalista aineistoa. Aihepiiriä kohdennettiin tarkemmin seuraavin termein: security, security issue, adoption ja governance. Hakuvaihe päättyi, kun tietokantahaut eivät tuottaneet enää mainittavasti uusia tuloksia valitusta aihepiiristä.

Hyväksymiskriteerit määrittelevät ne edellytykset, joiden puitteissa aineistovalinnat on tehty. Käytetyt kriteerit ovat:

- Aineistossa käsitellään tämän tutkielman näkökulmasta relevantteja aiheita, kuten pilvipalvelut, adoptio, tietoturva, organisaatiot ja tietohallinto.
- Julkaisut ovat verrattain uusia tieteellisiä artikkeleita tai konferenssijulkaisuja. Julkaisuvuodet ovat aikaväliltä 2014–2020.
- Aineisto on julkaistu IEEE Xplore tai Elsevier Scopus -tietokannoissa.
- Tekstit liitteineen ja lähdeluetteloineen ovat kokonaisuudessaan saatavissa luettavaksi veloituksetta Jyväskylän yliopiston opiskelijan käyttäjätunnuksilla.
- Artikkelit ovat vertaisarvioituja.
- Julkaisukielenä on englanti. Pääosa alan tieteellisistä julkaisuista on englanninkielisiä.
- Saatuja hakutuloksia rajattiin tietokantojen käyttöliittymien valinnoilla. Hakutuloksia rajattiin tutkielman aihepiirin mukaisesti ja sisällytettiin hakutuloksiin seuraavia tarkentavia attribuutteja: cloud computing, security of data, organizational aspect, risk management, governance, decision making, data protection.
- Ulkopuolelle jäivät: IoT, cyber security, forensic, big data, edge computing ja mobile network.

Hakulausekkeita ei ollut testihakujen perustella tarpeellista monimutkaistaa, vaan pysyttäydyin hyvin yksinkertaisessa hakukaavassa. Tietokantojen haut noudattivat seuraavia hakuehtoja, joita täydensin hakuportaaleiden lisävalinnoilla, jotka edellä hyväksymiskriteereissä on lueteltu. Hakulausekkeita olivat: cloud computing AND adoption AND security, cloud computing AND adoption AND survey, cloud computing AND governance, cloud AND security AND governance.

IEEE Xplore -tietokannan hakutuloksena oli aluksi 208 tekstiä, joista hakuportaalin puplication topics -valinnoilla määräksi kaventui 104 tekstiä. Tämä tulos sisältää myös konferenssijulkaisut. Scopus-tietokannan hakulausekkeet tuottivat useita satoja kappaleita soveltuvaa aineistoa. Määrää oli rajattava, joten

Scopuksen osalta konferenssijulkaisut jäivät jatkokäsittelyn ulkopuolella. Tämän karsinnan jälkeen Scopuksen aineistoa päätyi tarkempaan tarkasteluun 105 tekstiä. Hakuportaaleiden työkaluilla valittiin mukaan englanninkieliset tekstit ja niistä sellaiset, jotka ovat saatavissa kokonaisuudessaan veloituksetta luettavaksi Jyväskylän yliopiston Informaatioteknologian tiedekunnan opiskelijoiden käyttäjätunnuksiin sisältyvillä käyttöoikeuksilla.

Tietokanoista haetun ja rajausten jälkeen jäljelle jääneen aineistokokonaisuuden (209 kpl) karsinta jatkui tiivistelmien lukemisella. Teksteistä luettiin ensin tiivistelmä ja mikäli siinä ei mainittu tutkielman teemaan liittyvää sisältöä tai käsittely painottui ulkopuolelle rajattuihin aiheisiin, tekstiä ei valittu mukaan kirjallisuuskatsauksen tutkimusaineistoon. Teksteistä jatkoanalyysin ulkopuolelle jäivät sellaiset, joiden käsittelyn pääpaino näytti olevan otsikon tai artikkelikannassa näkyvän abstract-kuvauksen perusteella datan salaustekniikka, IoT, Edge-computing, mobiiliverkon palvelut, rahoitustoimialan ratkaisut tai terveydenhuoltoalan pilvijärjestelmät. Kirjallisuuskatsauksen aineistoksi tarkempaan läpikäyntiin päätyi yhteensä 78 tieteellistä tekstiä, joiden sisältö käsitteli tämän tutkielman tavoitteiden kannalta relevantteja teemoja.

Tietojen poiminta oli tärkeä vaihe ja se kohdennettiin niihin artikkeleihin, jotka sisällytettiin edellisten seulontavaiheiden kautta lopulliseen tarkasteluun. Aineiston käsittelyä varten luotiin lomakepohja, johon kirjattiin jokaisen artikkelin sisällöstä havainnot. Artikkelit käytiin kokonaisuudessaan läpi ja saatuja vastauksia tutkimuskysymyksiin kirjattiin muistiin systemaattisesti. Muistiinpanoja rikastettiin lisäksi kirjaamalla yleisemmän tason havaintoja ja kommentteja sisällöistä, joita voitiin hyödyntää yhteenvedossa ja lopputuloksia koostettaessa. Tutkimuksen yhteenveto syntyi järjestellen ja vertaillen kirjattuja havaintoja.

Okolin ja Schabramin (2010) mukaan analysointivaiheen tulisi olla suoraviivainen prosessi. Esimerkiksi terveydenhuoltoalan tutkimuksessa tyypillisen meta-analyysin tekeminen vastaavalla tarkkuudella ei ole mahdollista yhteiskunnallisen tutkimuksen kirjallisuuskatsauksissa. Tämä johtuu siitä, että tutkimukset tietojärjestelmätieteessäkään eivät yleensä ole homogeenisia eivätkä toistettavissa sellaisella tarkkuudella, jota edellytetään välttämättömyytenä lääketieteentutkimuksessa. (Okoli & Schabram, 2010.)

Tutkimusosuudesta tässä pro gradu -tutkielmassa muodostuu lähinnä laadullinen synteesi, joka raportoitiin. Hakukriteereiden rajaamasta aineistosta laadittiin erillinen yksilöivä taulukko tutkielman liitteeksi (liite 1).

Kirjallisuuskatsauksen laadullisen metasynteesin piirteitä noudattaen aineisto analysoitiin pyrkien ymmärtämään ja selittämään tutkittavaa aihepiiriä, eli pilvipalveluiden käyttöönottoon liittyviä teemoja tietohallinnon näkökulmasta. Salmisen (2010) mukaan metasynteesissä yhdistetään samaa aihepiiriä käsittelevä aineistokokonaisuus, pyrkien löytämään erovaisuuksia, mutta toisaalta myös yhtäläisyyksiä (Salminen, 2011). Havaintojen luokittelun ja ryhmittelyn pohjana olivat innovaatioiden diffuusioteoriaan ja TOE-kehysmalliin perustuva jaottelu. Lopuksi koostettuja havaintoja sekä niistä muodostettuja johtopäätöksiä peilattiin riippumattomien tutkimuslaitosten pilvipalveluiden tietoturvasta ja käyttöönotoista julkaisemiin raportteihin.

Okoli ja Schabram listaavat viimeisen vaiheen kirjallisuuskatsauksessa olevan löydösten raportoinnin kirjoittaminen. He muistuttavat vielä, että mikäli

edelliset vaiheet on tehty järjestelmällisesti, työ sujuu loppuun systemaattisesti ja sujuvasti. Kaikkein tärkeimmäksi ohjeeksi todetaan raportoiminen niin yksityiskohtaisesti, että muut tutkijat pystyisivät toistamaan koko proseduurin ja saamaan samat tulokset. Prosessia kuvatessa ei saa kuitenkaan unohtaa kirjata tuoreita uusia jopa odottamattomiakin tuloksia. (Okoli & Schabram, 2010.) Tässä luvussa kuvattiin tutkimusmenetelmänä käytetyn kirjallisuuskatsauksen toteutus.

5 KIRJALLISUUSKATSAUKSEN AINEISTON KÄSITTELY JA HAVAINNOT

Tässä luvussa esittelen kirjallisuuskatsaukseen käytetyn aineiston käsittelyn ja kokoan yhteen aineiston artikkeleiden ja konferenssijulkaisuiden keskeisimmät teemat. Teknologia-, organisaatio- ja ympäristövaikutukset käsitellään omissa alaluvuissaan. Omissa alaluvuissaan käsitellään lisäksi myös organisaation osaamisen merkitys sekä pilvipalveluiden osakseen saama kritiikki. Luvussa mainittujen lähteiden tiedot on listattu tutkielman liitteenä olevassa taulukossa (kts. liite 1). Liitteen sisältämään taulukkoon on kirjattu kriteerit täyttävistä teksteistä artikkelin yksilöivä numero, tekijätiedot, otsikko, julkaisuvuosi, käytetty tutkimusmenetelmä sekä keskeisin tulos tai havainto.

Aluksi havainnollistan tutkimusaineiston teemojen sisällöllistä jakaumaa. TOE-kehysmallin jaottelun mukaisesti jokainen artikkeli on sijoitettu taulukkoon sen sisällössä eniten korostuneen piirteen tai tutkimistulosten keskeisimpien havaintojen perusteella. Pääteemoihin sisältyvät alakohdat tarkentavat esiintyneitä osa-alueita. Analysoitujen tekstien kokonaismäärä on 78 kappaletta ja kuhunkin teemaan sisältyvien tekstien lukumäärä on kirjattu yhteenlaskettuna sulkeisiin kyseisen osa-alueen yhteyteen (taulukko 1).

TAULUKKO 1 Kirjallisuuskatsauksen artikkelit jaoteltuina kategorioittain

Teknologiaan sisältyvät teemat:		
	Suhteellinen hyöty verrattuna korvattavaan tekniikkaan sisältäen myös kustannushyötyvertailut (14 kpl)	(Ahmed, Alhadi & Seliaman, 2015; Almazroi, Shen, Teoh & Babar, 2016; Arpaci, 2017; Arvanitis, Kyriakou & Loukis, 2017; Boillat & Legner, 2014; Butt ym., 2019; Hsu, Ray & Li-Hsieh, 2014; Kuiper, Van Dam, Reiter & Janssen, 2014; Kuo & Kang, 2018; Masana & Muriithi, 2019; Senyo, Effah & Addae, 2016; Shee, Miah, Fairfield & Pujawan, 2018; Shin, Jo, Lee & Lee, 2014; Stieninger, Nedbal, Wetzlinger, Wagner & Erskine, 2018)
	Tietoturvallisuus- ja riskinäkökulma (24 kpl)	(Aissaoui, Ait idar, Belhadaoui & Rifi, 2017; Alkhwaldi, Kamala & Qahwaji, 2017; Andriole, 2017; Attasena, Darmont & Harbi, 2017; Balaaooriya, Wibowo & Wells, 2017; Bhajantri & Mujawar, 2019; Caldarelli, Ferri & Maffei, 2017; Candel Haug, Kretschmer & Strobel, 2016; Chang & Ramachandran, 2016; Chiba, Abghour, Moussaid, El Omri & Rida, 2016; Esposito, Castiglione, Martini & Choo, 2016; Ghorbel, Ghorbel & Jmaiel,

		2017; Lim, Grönlund & Andersson, 2015; Liu, Sun, Ryoo, Rizvi & Vasilakos, 2015; Luna, Suri, Iorga & Karmel, 2015; Mishra & Jena, 2019; Opara-Martins, Sahandi & Tian, 2015; Rahi, Bisui & Misra, 2017; Sabi, Uzoka, Langmia & Njeh, 2016; Sfondrini, Motta & Longo, 2018; Sharma & Srivastava, 2016; Sirohi & Agarwal, 2015; Sun, 2018)
	Järjestelmien yhteensovittamistekijät ja kompleksisuus (2 kpl)	(Minhaj & Islam, 2016; Opara-Martins ym., 2015)
	Teknologioiden käyttökelpoisuus ja -valmius (6 kpl)	(Ali, O., Soar, Yong & Tao, 2016; Almanea, 2014; Gangwar, Date & Ramaswamy, 2016; Lian, J. -W, 2015; Ratten, 2015; Sfondrini, Motta & You, 2015)
	IT-hallintamallit, politiikat, strategiat (14 kpl)	(Alassafi, Alharthi, Walters & Wills, 2017; Alemeye & Getahun, 2015; Alkhater, Wills & Walters, 2015; Chang, Ramachandran, Yao, Kuo & Li, 2016; Garg ym., 2014; Hiran, Henten, Shrivas & Doshi, 2018; Kyriakou & Loukis, 2019; Lansing, Siegfried, Sunyaev & Benlian, 2019; Miorandi, Rizzardi, Sicari & Coen-Porisini, 2019; Papadopoulos ym., 2019; Porrawatpreyakorn, Nuchitprasitchai, Viriyapant, Tangprasert & Chaipunyathat, 2019; Prieto-González, Tamm & Stantchev, 2015; Priyadarshinee ym., 2017; Wang, Wood, Abdul-Rahman & Lee, 2016)
Organisaatioihin liittyvät teemat:		
	ICT-osaaminen ja kyvykkyydet (3 kpl)	(AlKharusi & Al-Badi, 2016; Bouaynaya, 2020; Senarathna, Wilkin, Warren, Yeoh & Salzman, 2018)
	Organisaation koon vaikutus (2 kpl)	(Loukis & Kyriakou, 2015; Loukis, Arvanitis & Kyriakou, 2017)
	Ylimmän johdon tuki (5 kpl)	(Dincă, Dima & Rozsa, 2019; Hiran & Henten, 2020; Palos-Sanchez, Robina-Ramirez & Velicia-Martin, 2019; Yigitbasioglu, 2015)
Toimintaympäristön vaikutukset:		
	Toimijoiden luoma kilpailupaine (2 kpl)	(Gutierrez, 2015; Kumar, Samalia & Verma, 2017)
	Ulkoiset säännökset, määräykset tai ohjaus (2 kpl)	(Oredo, Njihia & Iraki, 2017; Oredo, Njihia & Iraki, 2019)

	Sosiaaliset ulottuvuudet (4 kpl)	(Alsmadi & Prybutok, 2018; Sabi, Uzoka, Langmia, Njeh & Tsuma, 2018; Singh, Sharma, Kumar & Yadav, 2016; Tariq, Tayyaba, Rasheed & Ashraf, 2017)

Teknologiset teemat oli yleisin käsitelty aihekokonaisuus. Noin 80 %:a teksteistä käsitteli pilvipalveluita teknologian tai kustannushyötyjen näkökulmasta. Teknologianteeman sisällä kaksi tekstiä kolmesta käsitteli pääsisältönään tietoturvallisen käytön vaatimuksia, riskejä tai teknisiä haasteita sekä ratkaisuja epävarmuuden lievittämiseksi. Organisaatioista lähtöisin oleviin vaikutuksiin keskittyi teksteistä noin 15 %:a ja toimintaympäristö sai vähiten huomioita jääden noin 5 % suuruiseksi. Edellä koostetut lukumäärät ovat karkeasti jaotteluja ja perustuvat tutkielman tekijän omiin tulkintoihin, mutta ne osoittavat kuitenkin suuntaa antavasti hyvin sen, miten teemat näyttäytyvät pilvipalveluita käsittelevässä tutkimuksessa. Seuraavissa alaluvussa esitellään aineistosta poimitut havainnot TOE-kehysmallia hyödyntäen.

5.1 Teknologiaan liittyvät vaikutukset

Lähes kaikissa tarkastelluissa teksteissä kirjoittajat toivat esille jollakin painotuksella teknologiaan liittyvien seikkojen vaikutukset pilvipalveluita arvioitaessa tai käyttöönotettaessa. Pääasiallinen epävarmuus ja huoli kohdistuivat turvallisen käytön mahdollistamiseen ja tietoturvallisuuden todentamiseen. Pilviympäristö, erityisesti SaaS-mallissa, siirtää palveluntuottamisen kerrosten vastuut kokonaan ulkoistettuna hankittavaan palveluun. Kaikki palvelun tuottamiseen vaadittavat teknologiakerrokset ja ratkaisut ovat siten palveluntuottajan vastuulla ja hallinnassa. Luottamuksen saavuttaminen on haastavaa, koska tilaajalla ei ole läpinäkyvyyttä palveluntuottajan tekniseen ympäristöön. Ehkä juuri siksi monista eduista huolimatta organisaatiot ovat edelleen hyvin varautuneita ottamaan käyttöön pilviratkaisuja.

Turvallisuus, palvelun saatavuus ja riskit arveluttavat käyttäjäorganisaatioita. Eri palvelumalleista SaaS-palveluiden suosio on jo korkealla, mutta edellä mainittujen syiden takia lähinnä sähköposti, kollaboraatiopalvelut tai sisällönhallintajärjestelmät viedään ulkopuoliselle palveluntuottajalle. Tärkeämpiä yrityksen varsinaisen ydinliiketoiminnan sovelluksia ei strategisen arvonsa vuoksi ole siirretty pilveen. Yritysjärjestelmien nähdään kuitenkin olevan seuraava suurempi askel pilvipalveluiden käyttöönotossa. Liiketoimintakriittisyyden, suorituskyvyn ja yksityisyyden valvonnan haasteiden vuoksi liiketoimintasovellusten siirtäminen pilveen on vaikeampaa. Pilvilaskenta voi tuottaa kuitenkin merkittävää hyötyä monessakin mielessä, koska pilvituottajien infrastruktuuri on käytettävyydeltään hyvää, ammattitaidolla ylläpidettyä ja se voi tuottaa säästöä muun muassa lisenssikustannuksissa. Esimerkiksi toiminnanohjausjärjestelmien vieminen pilviympäristöön on yleistyvä trendi yritysmaailmassa. Sovellusten laaja saavutettavuus erilaisten palveluiden osalta internetissä, myös mobiililaitteilla, puoltaa käyttöönottoa. Tämä näkyy varsinkin kuluttajakäyttäjille tuotettavissa

palveluissa. SaaS-palveluiden lisäksi PaaS ja IaaS-malleilla tuotetut pilviyritysjärjestelmät ovat aiempaa yleisemmin täydentämässä kokonaisuutta erilaisten sisäisten ja ulkoisten sovellusten järjestelmäintegraatioiden muodossa. (Boillat ja Legner, 2014.)

Pilvipalveluiden koetut edut sisältävät teknisessä mielessä vastuunsiirtoa palveluntuottajalle sellaisista tehtävistä kuten: helpottunut käyttöönotto, versionnostojen ja ylläpitotehtävien sujuvuus, datan varmuuskopioinnin hoituminen, pilvituottajan ammattitaitoinen tekninen tukipalvelu, loppukäyttäjien käyttötapojen laajeneminen internetin kautta käytettäväksi ja lyhentynyt käyttöönottoaika palveluita perustettaessa. Liiketoiminnan saavuttamista hyödyistä huolimatta toisessa vaakakupissa joudutaan arvioimaan riskejä liittyen palveluiden vasteaikojen toteutumiseen, palveluiden odottamattomiin epäkäytettävyystilanteisiin, tietoturvallisuusnäkökohtiin sekä hankalaan integroitavuuteen suhteessa muihin yrityksen käyttämiin tietojärjestelmiin. Miettimään joudutaan myös sitä, mitä merkitsee lukkiutuminen yhdelle toimittajalle sellaisissa tapauksissa, joissa teknologiat eri palveluntuottajien kesken eivät ole yhteensopivia migraatioita ajatellen. (Hsu ym., 2014.) Siirrettävyysongelma ja lukkiutuminen yhden palveluntuottajan palveluun (engl. vendor lock-in) syntyvät tilanteessa, jossa yhdellä pilvialustalla toimiva sovellus haluttaisiin asiakkaan toimesta siirtää toiselle palveluntuottajalle. Sovelluksen tai datan migraatio ei välttämättä onnistu, koska käytössä olevien resurssien ja palveluiden semantiikka ovat eri palveluntuottajilla erilaiset. Tyypillisimmin tähän törmätään SaaS-palveluissa, joissa koko tuotantotekninen osuus kaikilta osiltaan on palveluntuottajan hallinnassa. Tämän nähdään olevan yksi keskeisimmistä syistä sille, miksi organisaatiot eivät vielä ole valmiita ottamaan pilvipalveluita käyttöön.

Asiakasyritykset eivät ole aina edes tietoisia datan omistajuuskysymyksistä palveluiden käyttöönottotilanteissa. Siirron monimutkaisuus ja siitä aiheutuvat kustannukset saattavat selvitä vasta migraatiosuunnittelun myötä. Opara ym. (2017) ehdottavat strategista lähestymistapaa lukkiutumisen välttämiseksi. Pilvipohjaisten ratkaisuiden monimutkaisuudesta ja riippuvuuksista olisi muodostettava selkeä käsitys jo etukäteen. Palveluntarjoajien sovellusrajapinnat ja sopimusten mahdolliset lukitusta koskevat osa-alueet tulisi arvioida ennakkoon. Suureksi hyödyksi olisi valita sellaiset toimittajat palveluineen, jotka käyttävät tarjonnassaan vakiomuotoisia formaatteja ja protokollia. Tällöin voitaisiin myös varmistua riittävästä siirrettävyyskyvykkyydestä. (Opara ym., 2017.)

Gangwar ja Date (2016) tutkivat koetun käyttökelpoisuuden ja käytön helppouden merkitystä pilviadoptioon todeten niiden olevan merkittäviä välillisiä muuttujia käyttöönottoaikomuksen edeltäjinä (Gangwar & Date, 2016). Boillat ja Legner (2014) näkevät pilvipalveluiden hyödyntämisen olevan jo paljon muutakin kuin pelkästään tähän asti yleisin IT-vetoinen siirtymä, jossa yritysten käyttämistä vanhoista järjestelmistä siirrytään SaaS-palveluihin. Yleistyvä suuntaus on myös liiketoimintalähtökohdista toteutettava migraatio. Liiketoimintaprosesseja halutaan innovoida ja optimoida mobiili- ja verkkoteknologioiden pohjalta hallinnoimalla samalla IT:n monimutkaisuutta. Yrityskäyttöön rakennettuja pilvijärjestelmiä otetaan käyttöön yhtenäisinä tietojärjestelminä hajautetuissa myynti- ja palveluverkostoissa. Edellä mainittujen lisäksi yritysten pilvikäyttöönottoja on jalostettu edelleen SaaS-mallin lisäksi myös kattamaan iPaaS ja

aPaaS, joissa perinteisiä malleja laajennetaan esimerkiksi niin, että toimitetaan ohjelmistokehityspalveluita helpottamaan web-sovelluskehittäjien työskentelyä. Pilvipalveluina tuotettavat yritysjärjestelmät halutaan liittää täydentämään organisaatioiden on-premises-ratkaisuja sen sijaan, että pilvi korvaisi ne kokonaan. Pilvipalveluita halutaankin käyttää myös palvelualustana, jonka avulla integroidaan organisaation sisäisiä ja ulkoisia sovelluksia toisiinsa. Mobiili- ja pilviteknologiat nähdään yhdentyvän sekä tuottavan merkittävää taloudellista etua monipuolisempien käyttömahdollisuuksiensa ja standardoitujen liiketoimintaprosessiensa muodossa. (Boillat ja Legner, 2014.)

Kehittyvien teknologioiden yleistymiseen liittyy Andriolen (2017) mukaan uudenlainen nopeasyklinen käyttöönottoperiaate, toisin kuin on ollut tapana perinteissä tietojärjestelmämaailmassa. Uusi teknologia otetaan usein käyttöön jopa liiankin helposti. Yritysten sisällä osastojen omista pilottikäyttöönotoista ja innostuksesta seuraa se, että uuden teknologian käyttöönotot tehdään ilman minkäänlaista perinteistä määrittelyvaihetta. Tästä on syntynyt toisinaan niin kutsuttu uusi normaali ICT-maailmassa. Käytön pilotointiin ryhdytään ilman ennakoivia liiketoimintasuunnitelmia tai vaatimusmäärittelyitä. Pilotointia voi seurata edelleen nopea laajamittaisempi käyttöönotto, koska uusiin ominaisuuksiin on jo totuttu. (Andriole 2017.) Joissain tapauksissa kirjoituksissa on tuotu esille tietynlaisen harmaan alueen eli varjo-ICT:n syntyminen, jolla on negatiivinen kaiku. Tämä voi johtaa haastavaan tilanteeseen kokonaisarkkitehtuuria ajatellen ja vaikeuttaa tietohallinnon työtä pitää yritystasoinen ICT-kokonaiskuva hallinnassa.

Tutkimusaineistossa esiintyi useita pyrkimyksiä helpottaa hallitusti yritystasoisia käyttöönottoja erilaisten viitekehysten, hallintamallien ja täytäntöönpanomallien avulla. Hyvin yksiselitteinen lähtökohta oli strategiatyön merkitys ja vaatimus sen olemassaolosta. Chang ym. (2016) muistuttavat nykyisestä tilasta, jossa tietoturvahaasteet pilviteknologian yhteydessä ovat valtavat. Tutkijaryhmä esittää tätä selkeyttämään viitekehystä, jonka avulla pilven suorituskykyä voidaan tutkia ennen käyttöönottopäätöstä. Ehdotettu kymmenen kohdan etenemismalli on tutkijaryhmän kehittämä ja sinällään vain yksi monista, mutta sisältää yhdenlaisen loogisen etenemispolun huomioitavista seikoista:

1. Työhön osallistuvat sidosryhmät sopivat domainin ja yhteiset käsitteet.
2. Tunnistetaan ja yksilöidään tietoturvatavoitteet.
3. Kehitetään artefaktit erilaisten skenaarioiden ja väärinkäyttötapausten kuvaamiseksi.
4. Suoritetaan riskiarviointi ja analysoidaan uhkat turvallisuustavoitteille
5. Valitaan käytettävä elisitaatiotekniikka, jolla sidosryhmien tietoturvavaatimukset voidaan systemaattisesti tunnistaa ja analysoida.
6. Suoritetaan tiedonkeruu sovitun tekniikan mukaisesti kohdentaen se vaiheen kaksi tavoitekartoituksen kohteisiin.
7. Tehdään luokittelu tietoturvavaatimuksille yrityskohtaisen vaatimusmäärittelypohjan perusteella. Tästä muodostuu työkalu järjestelmäylläpitohenkilöstön käytettäväksi. Vaatimukset tulee myös validoida (saattaa voimaan) ja verifioida (näyttää toteen).

8. Tunnistetaan systeemidatan tietoturvavaatimukset alijärjestelmineen, kuten datakeskusten ja palvelinten virtualisointi siltä osin, kuin se on relevanttia.
9. Tietoturvavaatimukset priorisoidaan arvioiden niitä liiketoiminnallisiin tavoitteisiin verraten ja kustannushyötyanalyysejä käyttäen.
10. Tarkastetaan tietoturvavaatimukset suorittaen vaatimusten validointiprosessi auditointeineen. (Chang ym., 2016.)

Garg ja Stiller (2015) luonnehtivat organisaatioiden haasteita pilvipalvelun käyttöönottopäätöstä tehtäessä varsin monimutkaiseksi arkkitehtuuritason pohdinnaksi, joten ennakkosuunnittelu ja evaluointi tulee tehdä perusteellisesti. Pilvipohjaisten ratkaisuiden kohdalla arviointi on pakko jakaa osiin ja suorittaa ne moduuli kerrallaan. Siten voidaan muodostaa käsitys vaikutuksista käyttökustannuksiin, pystytään tunnistamaan ja minimoimaan epävarmuustekijät sekä saadaan turvattua turvallisuus, yksityisyys ja luotettavuus. (Garg ja Stiller, 2015.) Riskiarviointeihin pohjautuva lähestymistapa tietojärjestelmien hallintaan on kokonaisvaltaista toimintaa. Sen tulisi olla sisällytetty organisaation kaikkiin toiminteisiin systeemisuunnittelusta ja järjestelmäkehityksen elinjaksonhallinnan prosesseista aina tietoturvallisuuden valvontavastuiden kohdentamiseen saakka. (Luna ym., 2015.) Pilvipalveluiden tietoturvan teknisten ratkaisuiden ohella tietohallinnon vastuualueeseen liittyvät toimet on myös hyvin tärkeää saattaa kuntoon. Liu ym. (2015) muistuttavat, että tekniset ratkaisut pilviturvallisuuden haasteisiin ovat riippuvaisia siitä, miten hyvin teknisiä vastatoimia hallitaan ja johdetaan. Tietoturvakulttuuria analysoitaessa ja kehitettäessä esimerkiksi salauksen hallinnointinäkökulma on kriittinen. Mikäli tietoturvakulttuurin puutteista johtuen käyttäjät eivät kanna vastuutaan salausavaimien suojauksesta, ei ole enää merkitystä sillä salataanko tiedostot vai ei. Jotta voidaan kehittää tehokas pääsynhallintajärjestelmä, on äärimmäisen tärkeää ensin määritellä tarvittavat politiikat ja tunnistaa suojattavan IT-omaisuuden komponentit. Priorisointi liittyy myös pääsynhallintaan, koska kaikkea ei voi suojata yhtä korkealla prioriteetilla. Politiikkojen kehittäminen, omaisuuden luettelointi ja priorisointi vaativat tietohallintohenkilöstön työtä. Se on merkittävä osa turvallisuuden hallintaprosessia. (Liu ym., 2015.)

Sekä tietohallinnon että teknologisen osaamisen yhteistyö osoittautuu välttämättömäksi kokonaisuuden kannalta. Esimerkkinä tästä pilvipalveluiden teknologisia ja hallinnollisia riskitekijöitä organisaationäkökulmasta arvioivat Alassafi ym. (2017) tuoden esiin seuraavia ongelmakohtia ja niistä muodostuvia kehityskohteita:

- IaaS-palveluiden suunnittelua ja toteutusta ei usein ole tehty kaikilta osiltaan täyttämään jaetun arkkitehtuurin tietoturvavaatimuksia ja tästä voi aiheutua tietoturvaongelmia.
- Käyttöliittymät ja sovellusohjelmointirajapinnat voivat olla epäluotettavia. Tämä on merkittävä ongelma, sillä asiakkaat hallinnoivat pilvipalveluitaan niiden kautta. Palveluntuottajan olisi pystyttävä takaamaan turvallisuus, mutta silti käyttäjien on oltava tietoisia tästä riskistä.

- Käyttäjäidentiteetti voidaan varastaa ja sitä kautta voidaan kaapata palvelun tietoliikenne. Skenaariota pidetään hyvin korkeana riskinä ja sitä vastaan voidaan puolustautua vain käyttämällä monivaiheista tunnistautumismenetelmää.
- Valtion virastojen pitää olla selvillä lainsäädännöstä ennen kuin otetaan käyttöön pilvipalveluita, vaikka se tapahtuisikin palveluntarjoajan välityksellä. Tietoturvarikkomuksen tapahduttua mikään laki tai ohje ei enää tue organisaatiota.
- Tietoaineiston omistajuus ja vastuisiin liittyvät riskit on kyettävä harkitsemaan tarkkaan ja miettimään niiden lievittämiskeinot. Omistamaansa tietoaineistoa on kyettävä puolustamaan.
- Tietoaineiston vuotaminen heijastaa pääsyoikeusratkaisun, fyysisen siirtoväylän tai varmuuskopiointitoteutuksen heikkoutta. (Alassafi ym., 2017.)

Opara ym. (2015) mainitsevat, ettei liiketoiminnan näkökulmasta kolmea tietoturvan merkittävää arvoa voida aliarvioida tai korostaa liikaa käytäessä keskustelua yritysten tietoaineiston käsittelystä pilviympäristöissä. Lainopillisesti tietoturvan ehkä keskeisin eroavaisuus ja huolenaihe on datan tallentaminen tuntemattomalle, oman hallintovallan ulottumattomiin olevalle, täysin erilaiselle lainkäyttöalueelle, kuin missä yritys muutoin sijaitsee. (Opara ym., 2015.) Pilvipalveluiden tietosuojan toteutuminen jättää avoimia kysymyksiä ilmaan, jotka olisi ratkaistava. Ghorbel ym. (2017) muistuttavat, että käyttäjähallinnan puutteellisuudet pilviparadigmassa johtavat epäilykseen siitä, onko tietoaineiston suojaus riittävällä tasolla? Toistaiseksi kun läpinäkyvyys puuttuu, eikä tietojen käsittelyssä ole avoimuutta, jää epäselväksi ovatko tiedot suojattuja ja hallittuja hyvin. Toinen mainittu haaste liittyy tietoturvapolitiikan toteutumiseen dynaamisessa pilvi-infrastruktuurissa. Datan käyttö pilvessä synnyttää siitä useita kopioita, joilla tulisi jokaisella olla sama suojaustaso kuin alkuperäisellä. Mikäli yksi kopio joutuu tietovuoden kohteeksi, on sama kohtalo kaikilla datakopioilla. Tämä on hyvin haastava aihe, koska monille organisaatioille tietovuoto merkitsee erittäin merkittävän taloudellisen menetyksen ja maineenhallintatappion konkretisoitumista. (Ghorbel ym., 2017.)

Arkaluoteinen sensitiivinen tietoaineisto täytyy suojata luvattomalta käytöltä ja aiheettomalta datan palauttamiselta. Tyypillisesti pilviympäristössä allokoidaan resursseja dynaamisesti eri asiakkaille heidän käyttötarpeensa mukaan. Jäännösdatan käsittely on herättänyt runsaasti aiheellista keskustelua pilviympäristöjen käyttäjillä, vaikka ilmiö itsessään teknisessä mielessä on ollut aina olemassa myös on-premises-ratkaisuissa. Mitä pilvipalvelun datalle tapahtuu, kun käyttäjä poistaa tiedoston itseltään käytöstä sovelluksessa? Vaikka sovellus ei sitä enää käytä, on teknisesti mahdollista, että se voidaan palauttaa muistista tai levypinnalta. Tämä on merkittävä kysymys luottamuksellisten tietojen, kuten esimerkiksi salasanojen, terveystietojen, liikesalaisuuksien tai viranomaisen turvallisuusluokitteleman tietoaineiston kohdalla. Aissaoui ym. (2017) ehdottavat ratkaisuja edellä kuvatulle datan remanenssi-ilmiölle. Perinteiset salausmenetelmät eivät ole enää tehokkaita tässä uudessa pilviviitekehyksessä. Tieto tallennetaan kolmansien osapuolten virtualisointitekniikoilla toteutetulle jaetulle

etäpalvelimelle, josta vastaa pilvipalvelun tarjoaja takaamalla myös ratkaisun luotettavuuden. Tunnetut pilvipalveluiden tarjoajat, kuten esimerkiksi Amazon tai Microsoft, ilmoittavat kyllä käyttämänsä NIST:n hyväksymät standardit, mutta yksityiskohtaisempaa lisätietoa toteutuksesta ei anneta. Jotkut pilvipalveluiden tarjoajat sivuuttavat koko jäännösdatakysymyksen. (Aissaoui ym., (2017.)

Aissaoui ym. (2017) listaavat ratkaisuvaihtoehtoja, joista kuitenkaan yhtäkään ei nähdä sellaisenaan ratkaisuksi datan hävittämiselle pilvipalveluntuottajan järjestelmästä. Datan ylikirjoittaminen ohjelmistoratkaisulla tallennusmedialta ei sovellu dynaamiseen ja virtuaaliseen pilviympäristöön. Magneettikentän poistaminen tai vähentäminen (degausser-laite) toimisi magneettisille kiintolevyille, mutta saattaa myös tehdä niistä kokonaan käyttökelvottomia estäen jatkokäytön mahdollisuudet. Tiedot voidaan salata ennen pilveen siirtämistä ja salausavaimet säilytetään organisaation itse hallinnoimalla yksityisellä palvelimella, mutta tämä tuottaa monimutkaisen avaintenhallintaratkaisun. Kryptattua dataa ei voida myöskään prosessoida pilvessä ilman salauksen purkua eivätkä fyysiset tai kemialliset tuhoamistekniikat ole sovellettavissa pilviympäristössä. Tästä seuraa tilanne, jossa ratkaisu jää edelleen avoimeksi, mutta on selvää, että datan sanitoimiseen pilvessä ei ole yksinkertaista soveltuvaa toimintatapaa. Luottamuksen rakentaminen palveluntuottajaan nousee jälleen esille merkittävänä haasteena, koska perinteisten auditointitekniikoidenkin käyttö nähdään pilvipalveluiden osalta hankalasti soveltuvaksi ja sovellettavaksi. (Aissaoui ym., 2017.)

Salausratkaisuilla voidaan lisätä luottamusta ja varmistaa ydinliiketoiminnan prosessien kannalta kriittisen tiedon eheys ja saatavuus. Palvelutasosopimusten merkitys korostuu, koska riippuvuus palveluntuottajan toimista on keskeistä. Sopimuksiin tulee sisältyä myös tuki sovellusten siirrettävyydelle, jotta asiakas voi vaihtaa pilvipalvelun tuottajaa tietoturvan perusperiaatteiden turvaamiseksi. Pilvipalvelun tuottaja voi helpottaa luottamuksen saavuttamista ilmaisemalla datakeskusten sijaintitiedot sekä tukea asiakasta tämän pilvisiirtymässä myös lainopillisin neuvoin. Käyttöönottopäätösten tekemisessä korostetaan käyttäjäorganisaation osaamisen merkitystä. Merkittäväksi ponnistukseksi todetaan haaste varmistaa hyvän hallintotavan ja turvallisuuden noudattaminen. Pilvipalveluiden tarjoajien kanssa asioidessa voidaan lieventää riskejä varmistamalla, että tarjoaja noudattaa hyväksyttyjä standardeja tietoturva- ja tietosuojakysymyksissä. Noudattamalla standardeja ja vakuuttamalla asiakas toiminnan laadukkuudesta palveluntuottaja voi sujuvoittaa asiointia ja herättää näin asiakasorganisaation luottamuksen. (Opara ym., 2015.)

Pilviteknologioita käyttävän asiakasorganisaation varmuus ja riskinsietokyky riippuu siitä, kuinka suuren luottamuksen se osoittaa pilviekosysteemiä kohtaan. Riskienhallintaprosessi varmistaa, että luottamuksen rakentamiseen vaadittavat uhkien yksityiskohdat on tunnistettu, niiden todennäköisyyttä on vähennetty sekä pienennetty mahdollisesti aiheutuvaa vahinkoa. Tämä kaikki tulee tehdä riittävän ajoissa käyttöönottoa valmistellessa sekä seurata säännöllisesti vaikutuksia myös palvelun elinkaaren aikana. Liiketoimintakriittisten prosessien osalta on välttämätöntä tunnistaa pilvestä johtuvien riskien mukaan sovitetut turvallisuuskontrollit. Niiden osalta on hyödynnettävä

sopimustenmukaisia palveluntuottajan tai pilvipalveluvälittäjän vastuita turvavalvonnan toteuttamisesta ja raportoinnista. (Luna ym., 2015.)

Kuiper ym. (2014) ovat huomanneet pilviadoption etenevän hitaasti julkisella sektorilla Euroopassa. Julkisen sektorin toimijoiden tulee toiminnassaan noudattaa lakeja, ylläpitää yksityisyyttä ja taata riittävä turvallisuus. Tutkijat toteavat tosin lainsäädännön olleen pitkään varsin puutteellista ja arvelevatkin toisen syyn palveluiden hitaaseen käyttöönottoon olleen sen, että johtajat eivät ole olleet varmoja pystytäänkö julkisille toimijoille määritellyt arvot takaamaan toiminnassa. Liiketoimintatapausten arviointi julkisella sektorilla on tutkijoiden mielestä ongelmallista. Millaisilla perusteilla osoitetaan realistinen oikeutus projektille vai onko turvallisempaa olla tekemättä toistaiseksi mitään muutoksia. TOE-kehysmallin mukainen vertailu tuo esille lähinnä kustannusnäkökulman, jonka kääntöpuolella tulee arvioida mahdollista tietoturvariskiä. Riskiarvio tulee kuitenkin huomioida käyttöönottopäätöstä tehdessä, vaikka se tuottaakin silloin vähemmän positiivisen näkökulman pilvilaskennan käyttökelpoisuutta kohtaan julkisen sektorin toimijoilla. (Kuiper ym., 2014.)

Julkishallinnon tarjoamat sähköiset asiointipalvelut kansalaisille ovat lisääntymässä ympäri maailmaa. Viranomaiset haluavat tarjota korkealaatuisia ja tehokkaampia palveluita kansalaisille. Pilvipalvelut käyttöönottohaasteistaan huolimatta nähdään ratkaisuna sähköiseen asiointiin. Pilvitekniikka edustaa varsin perusteellista muutosta julkisen sektorin tavoissa tuottaa palveluita ja harjoittaa omaa liiketoimintaansa. Sähköinen hallinto ja viranomaispalvelut edustavat käyttäjäkeskeistä palvelukokonaisuutta, johon halutaan ja johon kansalaisten edellytetään kasvavissa määrin siirtyvän. Taustalla tavoitteena on tuoda myös viranomaistoimintaan parempaa kustannustehokkuutta. Palveluiden turvallisuushuolet ovat keskeinen piirre sekä palveluita tuottavilla julkishallinnon organisaatioilla kuin kansalaisilla käyttäjinä. (Alkhwaldi ym., 2017.)

Alassafi ym. (2017) ovat tunnistaneet muutamia valtion virastoihin liittyviä riskejä pilvipalveluiden käyttäjinä. Maineenhallinnan riski on suuri, mikäli viranomaisten palvelut eivät ole luotettavasti käytössä pilvipalvelun katkoksen vuoksi. Vielä edellistäkin vakavampi tilanne on silloin, jos tietoja pääsee vuotamaan palvelun ulkopuolelle. Virastolle koituu huomattava vahinko ja samalla luotettavuus viranomaistoimintaan kärsii. Tutkijat toteavatkin yleisimmin esille tuoduksi riskiskenaarioksi myös valtionhallinnossa tietoturvallisuuteen liittyvät ongelmat. (Alassafi ym., 2017.) Valtiollisen toimijan hyödyistä, kuten kustannussäästöistä, joustavasta resurssien mitoittamisesta ja ketteryydestä huolimatta kasvavien riskien vaikutuksen tarkastelu tulee ulottaa liiketoimintaprosesseihin, turvallisuuskulttuuriin sekä hallintomalleihin. Riskien vaikutuksia voidaan lieventää lisäämällä tietämystä ja kehittämällä riskitietoisuuskulttuuria myös käyttäjien keskuudessa. (Porrawatpreyakorn ym., 2019.)

5.2 Organisaatiotekijät

Organisatorisilla tekijöillä on havaittu olevan vaikutusta pilviadoptiopäätöksen syntymiseen, vaikka niiden sisältämät aihealueet eivät olekaan yhtä merkittäviä

vaikutukseltaan kuin edellä käsitellyt teknologiset teemat. Organisaation koko, sisäisen ICT-osaamisen laajuus ja ylimmän johdon tuki nähtiin vaikuttavan merkittävästi pilviadoptiopäätösten tekemiseen.

Loukis ja Kyriakou (2015) ovat havainneet yrityksen pitkälle kehittyneen infrastruktuurin aiheuttavan korkeat käyttö- ja ylläpitokustannukset. Sen vuoksi pilvipalveluiden käyttöönottoa pidetään tarkoituksenmukaisena kustannusten vähentämiseksi. Liiketoiminnalliset strategiat asettavat tavoitteita myös tietohallintotoimialalle. Strategiapapereihin on kirjattu tavoite ja pyrkimys tieto- ja viestintätekniikan investointien vähentämiseen. Ulkoa ostetuissa palveluissa voidaan huolellisella käyttöönotolla saavuttaa kustannussäästöjä. Pilviteknologiat ovat vastaus myös bisnesanalytiikkajärjestelmien tai vaikkapa CRM-järjestelmän ostamiseen palveluina. Organisaation omiin ICT-järjestelmiin ei tarvitse rakentaa uutta ja kuitenkin pilvestä saadaan käyttöön palveluina uusia kehittyviä teknologioita liiketoiminnan tehostamisen tarpeisiin. Erilaiset innovaatiokeskeiset strategiat puoltavat myös pilvipalveluiden käyttöä, koska niiden käyttöönotto on nopeaa ja kustannusten osalta ne nähdään edullisina. Henkilöstöpolitiikan kohdalla tämä voi näkyä myös pyrkimyksenä palkata lisää sellaista ICT-henkilöstöä, jolla on jo aiempaa kokemusta tieto- ja viestintätekniikan ulkoistamisesta tai aiempaa pilviteknologioiden tuntemusta. (Loukis ja Kyriakou (2015.)

Organisaation koon vaikutus pilvipalveluiden käyttöönottoon näkyi aineistossa siten, että kooltaan suuremmilla yrityksillä oli pieniä laajempi kiinnostus ja valmius pilvipalveluiden käyttöönottoon. Tämä johtuu pääsääntöisesti siitä, että isoilla yrityksillä on jo lähtökohtaisesti enemmin ICT-henkilöstöä palkkalistoillaan. Pieniltä yrityksiltä puuttuu soveltuvaa, manageerointikykyistä ICT-osaamista omaava henkilöstöä. Pilviosaamista vaaditaan tutkimaan ja ymmärtämään olemassa olevia pilvipalveluita ja valitsemaan sieltä tarkoituksenmukaisimmat ratkaisut yrityksen käyttöön. Lisäksi tarvitaan kaupallista, lainopillista ja tietohallinnollista kykyä valvoa ja hallinnoida asiakassuhdetta pilvipalveluiden tuottajayrityksiin. (Loukis ym., 2015.) Hsu ym. (2014) tunnistavat yrityksen koon vaikuttavan selkeästi sen aikomukseen käyttää pilvipalveluita. Tämä näkyy siten, että henkilöstömäärältään suuremmissa yrityksissä myös erilaisissa rooleissa toimivaa ICT-henkilöstöä on enemmän. Käyttöönotoissa tarvitaan teknologian ominaisuuksia tuntevia IT-osaajia, myös sellaisia, joilla on laajasti ICT-hallintotaitoja ja projektiosaamista. Kokemuksella ja osaamisella voidaan selviytyä uuden teknologian käyttöönotossa ilmenevistä odottamattomista turbulenssitilanteista jopa ilman merkittäviä taloudellisia vaikutuksia. (Hsu ym., 2014.) Samansuuntaiseen tulokseen päätyivät myös Senarathna ym. (2018) todeten, että keskisuuret ja suuret yritykset ovat todennäköisempiä käyttämään pilviteknologialla tuotettua palvelua kuin pienet (Senarathna ym., 2018).

Masana ja Muriithi (2019) näkevät julkishallinnon toimijoiden osalta tilanteen siten, ettei organisaatioyksikön koolla olisi samanlaista vaikutusta käyttöönottopäätökseen, kuten yksityisellä sektorilla. Tämän selitetään johtuvan siitä, että kaikki virastot ovat ministeriöiden ohjauksen alaisia ja tämän seurauksena kansallisella tasolla ohjaus on samansuuntaista. Virastokohtaisia eroja eri toimialojen yksityiskohtaisemmissa toteutuksissa voi kuitenkin olla. Julkishallinnon yhden toimijan tekemä päätös, innovaatio tai positiivinen kokemus, voivat olla hyödyksi myös muille julkishallinnon toimijoille. Tämä pitänee paikkansa ainakin

saman hallinnonalan ohjaukseen kuuluvilla virastoilla. (Masana ja Muriithi, 2019.)

Organisaation ylimmän johdon tuen ja sitoutumisen merkitystä korostetaan usein pilvipalveluita käsittelevässä kirjallisuudessa. Ylimmän johdon tuella varmistetaan visioiden toteutuminen, suorituskyvyn kehittyminen, resurssien sitouttaminen, sekä optimaalinen hallinta organisaation tavoitteisiin nähden. Mikäli IT-hankkeilla ei ole ylimmän johdin tukea, on niillä vain vähän mahdollisuuksia menestyä tai ne epäonnistuvat kokonaan (Hiran ym. 2020; Gangwar ym. 2014; Masana ja Muriithi 2019). Aihetta puntaroi myös Yigitbasioglu (2015) todeten, että ylimmän johdon tuen merkitys on kiistämätön uuden innovaation tai tekniikan omaksumisessa. Pelkästään ylhäältä alaspäin suuntautuva johtaminen lähestymistapana ei kuitenkaan ole ainut toimintamahdollisuus. Myös organisaatoissa alhaalta ylöspäin suuntautuva ratkaisuiden ehdottaminen, arviointi ja paikalliset kokeilut pilotointeineen voivat olla merkittäviä uusien kehityssuuntien valmistelussa. (Yigitbasioglu, 2015.)

Ylimmän johdon vaikutus on merkittävä tekijä koko toimitusketjun suorituskyvylle otettaessa käyttöön pilvipalveluita yrityksessä. Pilviteknologian käyttöönotto vaatii tarkastelun useamman toimijan välisten vaikutusten arvioinnista ja prosesseista. Tarkasteltavina ovat yrityksen sisäisten toimintojen, toimittajayrityksen ja asiakkaan väliset vaikutukset. (Shee ym., 2018.) Ylimmän johdon tuki on hyvin merkittävä tekijä pilvipalveluiden käyttöönottoon silloin, mikäli kehittyvissä maissa yrityksillä ei ole välttämättä selkeää organisaatiorakennetta ja kaikki päätökset tekee pk-yrityksen omistaja. Ylimmän johdon tuki esitettiin olevan tutkimuksessa keskeisempi tekijä, kuin muut käyttöönottoa puoltavat tekijät, kuten vaikkapa havaittu etu, joka uuden teknologian käytöstä nähdään muodostuvan aikaisempaan toimintatapaan verrattuna. (Kumar ym. 2017.) Al-Jabri ym. (2016) ovat tunnistaneet myös ylimmän johdon tuen oleva ratkaiseva tekijä pilvipalvelun käyttöönotolle ja käytölle myös päätöksentekoa vaatineen ratkaisuvaiheen jälkeen. Johdon tehtävä on edistää käyttöönottoa stimuloimalla muutosta ja tarjoamalla resursseja sekä palkitsemalla onnistuneita toteutuksia. Tutkijat muistuttavat myös siitä tosiasiasta, että ylin johto on todennäköisesti myös se, joka kantaa pilvitoteutuksen riskit. (Al-Jabri ym., 2016.)

Dinca ym. (2019) ovat tulkinneet johtajan roolin merkitseväksi kyselytutkimuksensa vastaajajoukossa, joka oli koottu Romanian pk-yritysten johtajien keskuudesta. Myös johtajien henkilökohtainen IT-alan tuntemus ja osaaminen korostuivat. Tutkijat toteavat, että mikäli johtaja ymmärtää pilvipalveluiden hyötyjä, uusi teknologinen toteutus voidaan ottaa helpommin käyttöön. Mikäli taasen johto ei ymmärrä teknologia-asioita, ei käyttöönottopäätöstäkään synny. (Dinca ym., 2019.) Tämä tukee sitä näkemystä, jossa kooltaan suurempien organisaatioiden oma IT-henkilöstö osaamisensa kautta olisi merkittävä tuki uusia teknologioita arvioitaessa.

Organisaation valmius omaksua uutta teknologiaa vaikuttaa innovaatioiden omaksumiseen. Taloudelliset ja teknologiset taustatekijät määrittävät, onko organisaation valmius omaksua uutta teknologiaa positiivinen tai negatiivinen. Mikäli organisaatiolla on valmiutta ja kyvykkyyttä omaksua uutta, seuraa siitä myös todennäköisemmin uuden innovaation käyttöönottopäätös. (Masana ja Muriithi, 2019.)

Kooltaan isommat organisaatiot ovat paremmassa asemassa pieniin verrattuna pilvipalveluiden käyttöönottoa ajatellen. Organisaation isompi koko edellyttää yleensä myös omaa ICT- ja tietohallinto-osaamista tietojärjestelmien hallinnointiin. Yrityksen ylimmän johdon tuki ja sitoutuminen pilviteknologioiden käyttöönottopäätöksiin on välttämätöntä. Ylin johto tarvitsee kuitenkin organisaation ICT-henkilöstön tukea päätöksenteon valmisteluun ja käytännön toteutukseen. Seuraavassa alaluvussa käsitellään ICT-osaamisen ja osaajien roolia tarkemmin.

5.3 ICT-alan osaaminen ja -kyvykkyydet

Pilvipalveluiden käyttöönotto asettaa yrityksen ICT-henkilöstön uudenlaisen ammatillisen osaamisen äärelle. Kirjallisuudessa on esitetty monenlaisia näkemyksiä siitä, millainen vaikutus on ICT-ammattilaisten suhtautumisella uuden teknologian käyttöönottoon. Bouaynaya (2019) näkee tilanteen sellaisessa valossa, että pilvipalveluihin siirtyminen edellyttää yritystasolla koko liiketoimintamallin muuttamista ja täten muuttaa myös tietohallinnon ja tietohallintojohtajan (CIO) roolia tietoteknisten ratkaisujen integraattorina. Tietohallintojohtajan työn sisältö laajenee toiminnallisesta johtajasta strategiseen arviointiin ja tulevaisuuden visiointiin. Pilvisuuntautuneen liiketoimintastrategian arvellaan tuottavan vaatimuksia ICT-kustannusten vähentämiseksi, koska ylläpitopalveluista siirrytään laajemmin koko palvelutuotantoratkaisujen infrastruktuurin uudistamiseen. Pilvipalveluiden kohdalla CIO:n roolissa pitäisi pystyä myös arvioimaan tietoturvavaikutuksia, koska etenkään pk-yrityksissä ei ole yleensä erillistä tietoturvajohtajaa (CISO). (Bouaynaya, 2019.)

ICT-tuotteiden ja -palveluiden toimitustapa on muuttunut pilvipalveluiden aikakaudella, toteavat Wang ym. (2016). Vahvat liiketaloudelliset näkökannat puoltavat pilvipalveluiden ketterää käyttöönottoa ja ICT-ratkaisut ovat mahdollistamassa tätä tavoitetta. Käyttöönottoprojektien tekninen monimutkaisuus kuitenkin lisääntyy ja turvallisuushaasteetkin on huomioitava. Vaikka pilveen siirtyminen on muuttanut ICT-hankkeiden luonnetta, projekteissa vaaditaan kuitenkin edelleen myös sosiaalisten elementtien hallintaan liittyvää johtamiskykyä. Tutkijat päätyvät toteamaan, että sellaiset kokeneet IT-projektipäälliköt, joilla on myös vahvat sosiaaliset taidot, ovat parhaita henkilöitä johtamaan siirtymää pilviteknologiaan. Sosiaalisilla ja kulttuurisilla johtamistaidoilla voidaan vähentää hankkeiden epävakautta ja tukea projektien onnistumista. (Wang ym. 2016.)

Pilvipalveluiden käyttöönotto on samalla myös palveluiden ulkoistamista. Ulkoistamisen tuottamalla epävarmuudella voi olla vaikutusta organisaation oman ICT-henkilöstön halukkuuteen olla tukemassa uudenlaisen teknologian käyttöönottoa. AlKharusi (2016) on tutkimuksessaan käsitellyt ICT-henkilöstön kokemuksia ja ihmisiin liittyviä tekijöitä. Hän toteaa, että mitä parempi tuntemus ICT-henkilöstöllä on pilvipalveluita kohtaan, sitä paremmin he ovat valmiita ottamaan niitä organisaatiossaan käyttöön. Aiemmat tiedot ja kokemukset ovat tutkimuksen mukaan merkittävin tekijä. Pilvipalveluiden käyttöönottoa ei myöskään koettu uhkakuvana oman työtehtävän jatkumiselle. (AlKharusi, 2016.)

Ganwar ym., 2014 muistuttavat henkilöstön sellaisen koulutuksen merkityksestä, jolla lisätään osaamista pilvipalveluiden tekniikkaan ja mahdollisuuksiin. Yrityksen johdon tulisikin kyetä vakuuttamaan henkilöstö uuden teknologian välttämättömyydestä. Lisäksi johdon tulisi sitoutua kehittämään tehokas koulutusohjelma, jonka tuloksena pilviteknologia voitaisiin ottaa mahdollisimman tuottavasti ja osaavasti käyttöön. Koulutusohjelmalla voidaan myös tukea henkilöstön sitouttamista työtehtäviinsä. (Gangwar ym., 2014.) Pilvipalveluiden käyttöönottoa harkitseva organisaatio tarvitsee myös tietoturvallisuuden hallitsevia ammattilaisia. Mitä laajemmin palveluita pilvestä aiotaan käyttää, sitä keskeisemäksi nousee tietoturvallisuuden toteuttaminen ja osaaminen talon sisällä. (Alassafi ym., 2017.) Organisaation oma ICT-henkilöstö on tärkeässä roolissa tukemassa pilvipalveluiden käyttöönottoa. Monimutkainen tuotantoympäristö ja hybriditoteutukset vaativat osaamista myös organisaation sisällä. Pelkästään pilvipalveluntuottajan apu tai muu ulkopuolelta hankittu osaaminen eivät riitä, sillä yrityksen toiminnan, tietoteknisten ratkaisuiden ja prosessien tuntemus ovat eduksi. (Kyriakou ym., 2019.) Pilvipalveluiden hallinnoinnin vastuu nähdään selkeästi IT-osastolle kuuluvaksi kokonaisuudeksi ja tehtäväksi, koska siellä on sellaiseen vaadittavaa erityisosaamista ja vastuu muidenkin ICT-toimintojen osalta (Prieto-Gontzales ym., 2015). AlKharusi ym. (2016) muistuttavat yhteenvetona teemaan liittyen yleistämisen antavan liian yksioikoisen käsityksen vertailtaessa IT-henkilöstön suhtautumista pilviteknologian hyväksymiseen. Niin kutsutut ihmisiin liittyviä tekijät vaihtelevat yksilöiden välillä, johtuen heidän persoonallisista piirteistään ja ominaisuuksistaan. Kunkin henkilön tietämys ja valveutuneisuus pilviteknologioita koskien vaikuttavat merkittävästi siihen, miten hän suhtautuu. Tämä korostuu varsinkin tietoturvallisuutta käsittelevien seikkojen kohdalla. (AlKharusi ym., 2016.) Organisaatioiden oma ICT-henkilöstö ei tämän tutkielman aineistoon viitaten vastusta pilvipalveluiden käyttöönottoa, mutta heidät olisi hyvä sitouttaa uusien teknologioiden käyttöönottoon mahdollistamalla soveltuva koulutusohjelma uuden oppimiseen.

5.4 Liiketoimintaympäristön vaikutuksista

Liiketoimintaympäristöön liittyvät tekijät näyttäytyivät useissa teksteissä luoden useimmiten osittaista painetta uusien innovaatioiden käyttöönotolle. Kuitenkin liiketoimintaympäristöön liittyviä seikkoja oli käsitelty melko niukasti. Joitain havaintoja löytyi normatiiviseen tukeen, kilpailuympäristön paineisiin sekä sosiokulttuurisiin seikkoihin liittyen.

Gutierrez ym. (2015) havaitsivat liiketoimintakumppaneiden muodostaman paineen vaikuttavan eniten pilvipalveluiden käyttöönottopäätökseen. Kilpailijat käyttävät pilvipalveluita omassa liiketoiminnassaan, joten samaan imuun halutaan päästä pian mukaan. Teknologiapalveluiden tarjoajilla on keskeinen merkitys myös käyttöönottopäätöksiin - aktiivinen toiminta markkinoinnin ja kohdennetun viestinnän muodossa edistää päätöksentekoa. Myös aikaisemmat hyvät kokemukset tietoteknisistä projekteista jonkin tietyn toimittajayrityksen kanssa lisäävät kiinnostavuutta. Liiketaloudellinen tavoite on lisätä operatiivisen

toiminnan tehokkuutta ja hyötyä siten myös pilvipalveluiden mahdollistamista säästöistä. Palveluntarjoajien aktiivisuus tarjoutumalla avuksi käyttöönottovaiheessa lakisääteisten määräysten täyttämisessä ja palveluiden räätälöinnissä havaittiin vakuuttavan päätöksentekijät helpommin ja käyttöönottopäätös syntyi. (Gutierrez ym., 2015.)

Tutkimusaineisto sisälsi myös tekstejä, jotka käsittelivät kehittyviä maita Aasiassa tai Afrikassa. Näissä tutkimuksissa toimintaympäristön tekijät tai sosiokulttuuristen seikkojen merkitys olivat korostuneemmin esillä kuin kehittyneiden maiden pilvipalveluita käsitelleissä tutkimuksissa. Almazroi ym. (2016) ovat havainneet toimintaympäristön vaikutuksen merkittävänä tiedonvälittäjänä ja kannustajana pilvipalveluiden käyttöönotossa myös yksilötasolla. He toteavat, että korkeakouluopiskelijoiden keskuudessa ei välttämättä tunnisteta niitä hyötyjä oppimiselle, verkostoitumiselle tai tutkimukselle, joita pilvipalveluiden käyttö tuo tullessaan. Tutkijoiden mielestä sekä palveluntarjoajien että yliopistojen johdon pitäisi tehdä yhteistyötä asiaa edistääkseen. (Almazroi ym., 2016.) Ulkoisen paineen raportoitiin olevan Pakistanin korkeakouluissa selkein tekijä pilvipalveluiden käyttöönoton suosioon. Tosin infrastruktuuri ja palveluiden käyttö oli vasta kehittymässä. (Tarig ym., 2017.) Sähköisten palvelujen käyttökulttuurin puute ja epäilys palvelujen luotettavuudesta johtavat kansalaiset mieluummin valitsemaan asioinnin virastossa paikan päällä kuin verkossa. Kaikenlaiset huhut ja epäilykset hidastavat ennestäänkin vaatimatonta sähköisten palveluiden käyttäjämäärää. (Alkhwaldi ym., 2017.)

Normatiivisen ohjauksen luomalla paineella todetaan olevan voimakas ohjaava vaikutus organisaatioille, joka näkyy myös uusien innovaatioiden ja teknologioiden käyttöönottoa edistäen. Kun normatiiviset paineet ovat korkeat, ympärillä olevien kilpailijoiden uusien teknologioiden käyttöönotot luovat paineen muillekin toimijoille hypätä samaan junaan. Tämän bandwagon-ilmiön on nähty olevan merkittävä vauhdittaja kehittyvissä maissa juuri pilvipalveluiden käyttöönotoissa. Tutkijat ehdottavatkin, että teknologioiden myyjien tulisi tehdä tiivistä yhteistyötä valtionvirastojen sekä kaupanalan toimijoiden kanssa myynnin edistämiseksi, sillä mainituilla toimijoilla on vakaan maineensa vuoksi merkittävä vaikutus myös muiden toimialojen päätöksentekijöiden käyttöönottopäätöksiin. Tietoteknisten innovaatioiden todetaan olevan osa laajempaa sosiaalista, taloudellista ja poliittista verkostoa, jonka laajemmat institutionaaliset voimat muodostavat. (Oredo ym., 2017.)

Kilpailijoiden luomalla paineella tai toimittajan tuella ei kuitenkaan aina havaittu merkittävää vaikutusta organisaation aikomukseen tehdä käyttöönottopäätös. Terveydenhuollon potilastietojärjestelmiä käsittelevä Etelä-Afrikkaan sijoittuva tutkimus ei tukenut tätä muutoin yleistä tutkimustulosta. Tutkimuksesta kävi tosin ilmi, että potilastietojärjestelmälle oli olemassa tietty akkreditoitu palveluntuottaja, joten tulos on kyseisessä tilanteessa ymmärrettävä. (Masana ja Muriithi, 2019.) Ympäristökysymyksiä teknologisella painotuksella vetivät yhteen Hsu ym. (2014), joiden tutkimuksessa kansallisen internet-infrastruktuurin paikallinen saatavuus oli IT-ammattilaisten merkittävin pohdinnan aihe. Toki verkkovälitteisten palveluiden tapauksessa perusinfrastruktuurin toimivuus on olennainen huoli. Muut teemat olivat hallituksen määräämien asetusten

yhtenäisyys ja kilpailijoiden edistymisen arviointi uusien palveluiden käyttöönotossa. (Hsu ym., 2017.)

Liiketoimintaympäristön vaikutukset vaihtelevat selkeästi sen mukaan millaiseen valtioon tutkimuksen kohteena ollut tapaus sijoittui ja millainen oli sikäläinen kansallinen ohjaus ja kehittyneisyyden taso. Länsimaisessa tarkastelussa kilpailijoiden tai kumppaneiden pilvikäyttöönotot tuottivat imua lähteä mukaan, jotta pysytään mukana kilpailussa. Palveluiden tuottajat ovat ilmeisen aktiivisia ja halukkaita kaikkialla esittelemään ja tarjoamaan apuaan pilvipalveluiden käyttöönottoa harkittaessa.

5.5 Pilvipalveluihin kohdistuvaa kritiikkiä

Organisaatioiden innostus pilvipalveluiden käyttöönottoon on herättänyt myös kriittisemmän joukon tutkijoita pohtimaan millaisessa vaiheessa ja millaisten haasteiden edessä toimiala on. Sfondrini ym. (2015) summaavat tilannetta todeten, etteivät ydinliiketoiminnan sovellukset ole vielä siirtyneet julkiseen pilveen. Yritykset käyttävät pilven palveluita ydinliiketoiminnan osalta lähinnä ei-tuotannollisiin tarkoituksiin, kuten kehitys- ja testausympäristöjen tuottamiseen. Näin voidaan hyödyntää pilven parhaat ominaisuudet ja välttyä tuotantoympäristön epäkäytettävyyden aiheuttama riski, joka kohdentuisi liiketoiminnan jatkuvuuteen.

Kriittisestä suhtautumisesta ja kontrolloinnin välttämättömyydestä viestii Sfondrini ym. (2015) tutkimuksensa tuloksissa. IaaS:n on ottanut käyttöön suurin osa organisaatioista, koska palvelumallina se mahdollistaa koko tuotantopinon kerrosten hallinnan omin toimin. PaaS kärsii eniten luottamuspulasta, joten sen käyttö on vähäisintä. Palvelutason hallinta on toinen kokonaisuus, joka tuottaa kitkaa. Pilviympäristöjen käyttöön soveltuvien hallintamallien kehittyminen vie aikaa. ICT-toimialan perinteiset viitekehykset kuten esimerkiksi Control Objectives for Information and Related Technology (CoBIT) ja IT Infrastructure Library (ITIL) ovat levinneet palvelutason hallinnointiin pilvituotantomaailmaan melko verkkaisesti. Pilvipalveluntarjoajien ehdottamia palvelutasosopimuksia pidetään puutteellisina, eikä sellaisia perusasioita kuten vasteajat tai tietoturvan toteuttaminen ole lausuttu selkeästi. Palvelutasosopimusten puutteellisuuksien pelätään johtavan tilanteisiin, joissa pilvipalvelun tuottajat voivat sivuuttaa vastuunsa ongelmatilanteissa. Tämä on käyttäjäorganisaatioille huomattava riskitekijä ja uhkaa liiketoiminnan jatkuvuutta. Erityinen piirre on myös se, että palvelun valvontakyky myös suorituskyvyn osalta on vain palveluiden tarjoajalla. Yleensä asiakasyrityksellä ei ole läpinäkyvyyttä liiketoimintasovellustensa tilanteeseen, eikä varmuutta palvelutasosopimuksen yksityiskohtien toteutumisesta. Juridisessa mielessä ajatellen, mikäli poikkeamia ei voi havaita tai todentaa, niistä ei voida myöskään reklamoida riittävällä tasolla. Tällöin ei voida myöskään vaatia korvauksia, mikäli sellaisia on edes palvelutasosopimuksissa määritetty. (Sfondrini ym., 2015.)

Prieto-Gonzales ym. (2015) näkevät myös tietohallinnon käytäntöjen kehittämisen välttämättömäksi. Palvelusopimuksessa tulee määritellä tasot

palveluille, vasteajat palvelun palauttamiselle vikatapauksissa, tiedonsiirtonopeus palvelun käytössä sekä tukipalvelun vasteaika sen reagoidessa palvelupyyntöön. Näiden palvelulupausten avulla tehdään palvelusta avoimia asiakkaalle ja tärkeät näkökohdat tulevat ajoissa määritellyiksi. Vastuu pilvipalveluiden hallinnasta nähdäänkin sisältyväksi IT-osaston toimialaan. (Prieto-Gontzales ym., 2015.)

AlKharusi ym. (2016) kuvaavat arjen realismia tuoden esille sen, että mikäli pilvipalveluissa esiintyy epäkäytettävyyttä tai jotain menee pieleen, lankeaa suurin osa vastuista ja riskienhallinnan epäonnistumisesta siinä tilanteessa organisaation oman ICT-osaston, eikä palveluntuottajan harteille. Sellaisissa organisaatioissa, joissa on korkeampi hallinnon osaamistaso ja kypsyys, ajatellaan palvelunhallintaan liittyviä seikkoja tarkemmin ja odotetaan sitä myös organisaation omalta tietohallinnolta.

Pilvipalveluiden hallinnointikäytännöissä on kuitenkin hyvin yleistä osaamisen ja hallinnointityön ostaminen pilvipalveluvälittäjältä. Pilvipalveluvälittäjän vastuulle halutaan tyypillisesti sen tarjoaman pilvipalvelun käyttöön liittyvä riskienhallinta ja erilaiset pilviympäristön hallintaan liittyvät tehtävät. Nähdäänkin, että liikesuhde pilvipalveluvälittäjän kanssa olisi pikemminkin kestävämpää strategista kumppanuutta, kuin kertaluonteinen palvelutehtävä. (Prieto-Gonzales ym., 2015.)

Julkisen pilven luottamuskysymykset edellyttävät laajamittaista käyttöönottoa varten pilven tuottajilta standardien ja jaettujen sovellusrajapintojen luomista. Standardien mukaiset sovellusrajapinnat mahdollistaisivat myös palveluiden siirtäminen palveluntuottajalta toiselle. Läpinäkyvyyden tuottamiseksi pitäisi toteuttaa asiakasorganisaation sisäisten valvonta- ja hallintajärjestelmien yhdistäminen palveluntuottajan järjestelmiin. Toteutukset ovat edenneet hitaasti ja niiden puutteellisuuksien on todettu olevan yksi pilvipalveluiden luottamuksen saavuttamisen esteistä. Globaalisti toimivien palvelutuottajien yhteistoimintaa tarvitaan tämän kehityssuunnan mahdollistamiseksi. (Sfondrini ym., 2015.)

Kirjallisuuskatsauksen aineiston analysoinnin myötä on selkiytynyt käsitys siitä, että pilvipalveluiden käyttöönottopäätöksien taustalla puhuttavat eniten tietoturvallisuuteen liittyvät haasteet, vaikka arvoidut kustannussäästöt ICT-kustannuksissa puoltavatkin voimakkaasti palveluiden käyttöönottoja. Vaikka mitään varsinaisesti uutta ei adoptiota ja osin tietoturvallisuuden teemoja sisältävässä aineistossa esiintynytkään, syntyi hyvin selkeä näkemys pilvipalveluiden käyttöönottopäätöksiin eniten vaikuttavista tekijöistä. Tietoturvallisuuden toteutuminen ja luottamus olivat tutkimuksissa läsnä. Selvää oli myös se, ettei kaikkia palveluiden luottamuksen lisäämiseen tähtääviä ratkaisuja ole valmiina ja standardointikysymykset ovat edelleen ainakin osin avoimina. Standardit, valvontamahdollisuudet ja pitävät palvelutasosopimukset luovat läpinäkyvyyden, jota pidetään ehdottomana edellytyksenä palveluiden käyttökelpoisuudelle. Tämä korostuu silloin, mikäli pilvipalveluihin sijoitetaan asiakkaan turvallisuusluokiteltua dataa. Tässä luvussa esittelin kirjallisuuskatsauksena toteutetun tutkielman empiirisen osuuden aineistosta poimitut keskeisimmiksi tulkitsemani havainnot.

6 TULOKSET JA JOHTOPÄÄTÖKSET

Tässä luvussa peilaan luvussa viisi esittelemiäni havaintoja tietoturva- ja käyttöönottonäkökulmista pilvipalveluiden nykytilaa käsitteleviin riippumattomien tutkimuslaitosten julkaisuihin. Kokoan lisäksi yhteenvetoa ja johtopäätöksiä tutkielmassa käsittelemistäni teemoista. Tulosten tavoitteena on tuottaa valtion viraston tietohallintotoimialan käyttöön tieteellisiin tutkimuksiin perustuvaa tausta-aineistoa, laadittaessa organisaation sisäistä toimintaa ohjaavaa, päätöksentekoa tukevaa materiaalia. Tietoturvanäkökulma huomioiden tuon esille sellaisia seikkoja, joihin olisi hyödyllistä kiinnittää huomiota pilvipalveluiden käyttöönottoa laajennettaessa. Nämä havainnot tukevat ja auttavat sujuvoittamaan pilvipalveluiden adoptointia organisaatiossa.

Tässä tutkielmassa haettiin vastauksia kysymyksiin:

- Millaisia teemoja tulee huomioida tietoturvariskien arvioinnissa ja pilviadoption onnistuneessa läpiviennissä?
- Millaisia ohjeita tai toimintamalleja valtion viraston tietohallintotoimialan olisi hyödyllistä laatia arvioidessaan luokiteltua tietoaineistoa sisältävien tietojärjestelmien sijoittumista erilaisten toimijoiden pilvi-palveluympäristöihin?

Kananen (2015) johdattelee tulosten kokoamisvaihetta kiteyttämällä, että tutkimuksessa saaduista tuloksista tehdään johtopäätökset. Tutkimustuloksille annetaan merkitys ja selitetään, mitä ne tarkoittavat. Näin tuotetaan ratkaisu tutkimusongelmaan ja vastataukset tutkimuskysymyksiin. (Kananen, 2015.)

Kirjallisuuskatsauksen myötä kävi ilmi, että tietohallintonäkökulmasta tehtyä tutkimusta on vielä melko vähän, joten siinä mielessä tämä tutkielma kohdistui aihepiirinsä osalta hyödylliseen tutkimuskohteeseen. Tutkielman tarkastelunäkökulmina teknologia, organisaatio ja ympäristö olivat kiinnostava lähtökohta luoda katsaus siihen, miten ne osa-alueineen tässä tutkielmassa näkyvät pilviteknologioiden käyttöönottopäätösten taustana. Pilvipalveluiden käyttöönoton kiistattomana etuna tuodaan yleensä aina esille ne potentiaaliset taloudelliset hyödyt, joita uusi teknologisesti moderni palvelutuotantoratkaisu tuottaa käyttäjilleen. Heti samaan hengenvetoon huoli käytön turvallisuudesta, riskeistä ja sopimuksiin perustuvasta luottamuksesta ovat vastavoimana edellyttämässä huolellista arviointia käyttöönottopäätöstä tehtäessä. Viranomaisen käsittelemän tietoaineiston asianmukainen ja oikein tehty luokittelu sekä kansalaisten odottama palveluiden luotettavuus ovat merkittäviä teemoja turvallisuustoimialan toimijoiden tuottamien palveluiden käytön näkökulmasta. Luottamus ja maineenhallinta ovat viranomaistoiminnan keskeisiä kulmakiviä, joihin ratkaisuilla pyritään.

Pilvipalveluiden käyttöönottopäätöstä valmisteltaessa arvioitaviksi teemoiksi nousivat luottamuksen saavuttamisen dilemma sekä monimutkaisen tuotantorakenteen tietoturvahaasteet monitoimittajaympäristössä. Merkittäviä tekijöitä pilviteknologioiden käyttöönotolle ovat lisäksi organisaation ylimmän

johdon tuen välttämättömyys sekä kyky pystyä kuvamaan valmisteluvaiheessa tekniset asiat riippuvuuksineen riittävällä tarkkuudella ja ymmärrettävästi päätöksentekoa varten. Kehitettäviä osa-alueita ovat myös organisaation oman pilviteknologiaosaamisen kasvattaminen sisältäen uudenlaisen palvelu-ulkoistuksen hallinnointi- ja operointikyky yhdessä osaavan toimittajakumppaniverkoston avulla.

Digitalisessa maailmassa luottamuksen rakentaminen ja ylläpitäminen on hyvin erilaista kuin mihin olemme perinteisesti tottuneet. Toiminnan osapuolet ovat toisilleen tuntemattomia, eri puolilta maailmaa, eikä kohteisiin tutustuminen tai havainnointi ole mahdollista. Luottamuksen käsite on monimuotoisempi ja mukautuvampi. Standardit ja sertifikaatit sekä niiden valvonta, ovat digitaalisen toimintaympäristön keino luoda yhteiset ja yleisesti tunnistetut käytännöt, joilla varmistetaan turvallisuus ja luottamus osapuolten välillä. (Liikenne- ja viestintävirasto Traficom, 2019.)

Koska tietoturva oli kirjallisuuskatsauksen perusteella keskeisin huoli ja kehitettävä kohde, onkin perusteltua pohtia, miten pilvipalveluiden käyttöönotossa olisi hyödyllistä edetä. Kirjallisuuskatsauksen perusteella voidaan tulkita, että tietoturvallisten järjestelmien rakentaminen pilvialustoille vaatii hallitun prosessin ja uudenlaisen palvelurakenteen luomisen, kehittämisen ja omaksumisen.

6.1 Riskien tunnistamisella ratkaisuihin

Cloud Security Alliance (2020) on listannut ja asettanut järjestykseen vakavuuden mukaan 11 tämän hetken pilvipalveluihin liittyvää uhkaa. Käsittelen niistä kahdeksaa tässä alaluvussa hieman tarkemmin.

1. Tietomurrot
2. Virheelliset konfiguraatiot ja puutteellinen muutoshallinta
3. Pilviturvallisuusarkkitehtuurin ja strategian puute
4. Puutteellinen identiteetin-, pääsyn-, tai salausavainhallinta
5. Käyttäjätilien kaappaukset
6. Sisäpiiriläisten aiheuttama uhka
7. Turvattomat rajapinnat ja sovellusliittymät
8. Heikko hallintakerros (control plane)
9. Meta- ja sovellusrakenteen puutteellisuudet
10. Rajoitettu näkyvyys pilven käyttöön
11. Vääränlainen tai rikollinen pilvipalveluiden käyttö

Tietomurrot ovat yleisimpiä uhkia ja kyberturvallisuuden tapahtumia (incident) vuodesta toiseen, joissa sensitiivistä, suojattua tai luottamuksellista tietoa vapautuu kohdennetun hyökkäyksen tai tyypillisimmin inhimillisen virheen, sovellushaavoittuvuuden tai virheellisen konfiguroinnin seurauksena. Datasta on tulossa verkkohyökkäysten pääkohde, joten tietoaineiston liiketoiminnallisen arvon ja menettämisen vaikutusten arviointi on keskeistä tiedot omistavalle

organisaatiolle. Kryptaustekniikat suojaavat dataa mutta järjestelmän suorituskykyyn ja käyttäjäystävällisyyteen sillä on negatiivinen vaikutus. Häiriöiden torjuntasuunnitelma on ICT-henkilöstön työkalu tapahtumien havainnointiin, niihin reagointiin ja niistä palautumiseen. (Cloud Security Alliance, 2020.)

Pilviympäristö eroaa perinteisistä ICT-ratkaisuista ja johtaa muutoshallinnan kontrolloinnin monimutkaisuuteen, sillä pilviteknologiat perustuvat automaatioon sekä roolien ja pääsynhallintaoikeuksien laajentamiseen pikamuutosten toteuttamiseksi. Koska pilvipohjaiset resurssit ovat dynaamisia ja monimutkaisia, muutoshallinnan yksityiskohtien määrittäminen on haastavaa. Ratkaisuksi jää automaation omaksuminen ja sellaisten tekniikoiden käyttö, jotka skannaavat keskeytyksettä virheellisiä konfiguraatioita korjaustoimia varten. (Cloud Security Alliance, 2020.)

Ehkä merkittävin haaste siirrettäessä osia IT-infrastruktuurista pilveen on organisaation puutteellinen tietoturva-arkkitehtuuri kyberhyökkäysten sietämiseksi. Onnistuneella kyberhyökkäyksellä on vakavat taloudelliset ja mainehallinnan vaikutukset liiketoimintaan. Tietoturva-arkkitehtuuri tulee yhdenmukaistaa liiketoimintatavoitteiden kanssa sekä laatia tietoturva-arkkitehtuurikehys. Uhkamalleja pidetään ajan tasalla sekä seurataan yleistä turvallisuusympäristön tilaa. (Cloud Security Alliance, 2020.)

Uhkien listaukseen uutena teemana on nostettu puutteellinen identiteetin-, pääsyn-, tai salausavainhallinta. Identiteetin- ja pääsynhallinta asettuu pilviympäristössä perinteisiä tuotantomalleja tärkeämmäksi asiaksi varmistaa kuntoon. Identiteetin yhdistäminen pilvipalvelun tarjoajan kanssa, voidaan tehdä esimerkiksi SAML:lla (Security Assertion Markup Language), jolloin käyttäjähallinta helpottuu. Mikäli identiteetinhallinta aiotaan yhdistää palveluntarjoajan kanssa, on kyettävä sovittamaan yhteen turvallisuuteen liittyvät prosessit, infrastruktuuri ja segmentointi. Pilvessä käytettävän identiteetin osalta tuleekin soveltaa mahdollisimman tiukkoja identiteetin ja pääsynhallinnan käytäntöjä ja suosia tarkoituksenmukaista minimioikeuksien periaatteita käyttäjän työtehtävien edellyttämä tarve huomioiden. (Cloud Security Alliance, 2020.)

Käyttäjätilien kaappaukset ovat haitallisia, mutta erityisen vahingollisia niissä tapauksissa, jolloin paha-aikeinen hyökkääjä pääsee käsiksi pilvipalveluiden hallinnointi- tai tilaustileihin. Organisaatioiden tulisikin tiedostaa nämä uhkat ja pohtia strategiat niistä selviytymiseen. Tilin kaappaus on vakava uhka, josta ei selvitä salasanan palautuksella. Tätäkin uhkaan voidaan pienentää palveluiden ja käyttövaltuushallinnan valvonnalla. (Cloud Security Alliance, 2020.)

Sisäpiiriläisten tuottama uhka on varsin yleistä. Noin kaksi kolmasosaa tapauksista on huolimattomuudesta johtuvia tietoturvaloukkauksia, joten yksi kolmannes tapahtuneista on tarkoitushakuista rikollista toimintaa. Huolimattomuus ilmenee virheellisinä palvelinkonfiguraatioina tai turvattomissa henkilökohtaisissa laitteissa säilytettyinä salasanoina. Merkittävää parannusta saadaan aikaan turvallisuuskulttuurin kehittämisellä koulutuksen ja valvonnan avulla sekä rajoittamalla pääsynhallinta. (Cloud Security Alliance, 2020.)

Heikko hallintakerros johtaa siihen, ettei järjestelmäarkkitehdilla tai järjestelmäteknikolla ole täyttä hallintaa datainfrastruktuurin logiikkaan, turvallisuuteen ja varmentamiseen, eikä siten tiedetä, missä sokeat pisteet tai heikot kohdat ovat, joten tietovuodon mahdollisuus on olemassa. Tästä aiheutuu suuri riski

liiketoiminnalle, sillä organisaatioilla on vastuu datasta. Henkilötietojen menetys on esimerkiksi GDPR:ssa sanktioitu jopa 20 miljoonan euron suuruiseksi. Meta- ja sovellusrakenne ovat pilven kriittisiä komponentteja. (Cloud Security Alliance, 2020.)

Luottamuksen kehittämiseksi palvelutasosopimukset nousivat merkittäviksi myös tämän tutkielman tarkastelussa. Aineistossa tuotiin esille huoli asiakkaan rajoittuneesta näkyvyydestä käyttämiinsä pilvipalveluihin. Myös Cloud Security Alliance (2020) on tuonut tämän ongelman esiin. Tämä tarkoittaa tilannetta, jossa organisaatiolla ei ole mahdollisuutta visualisoida ja analysoida pilvipalveluiden käytön turvallisuutta. Valvontakyvyn puuttuessa työntekijät käyttävät pilvisovelluksia ja resursseja ilman yrityksen ICT- ja tietoturvaosastojen tukea ja lupaa. (Cloud Security Alliance, 2020.) Virallisen käyttöpolitiikan puuttuminen lisää riskialttiutta eritoten silloin, jos palvelussa on sensitiivistä yritysdataa. Sopimusten merkitystä ja sisältöjä käsitellään tarkemmin seuraavassa alaluvussa.

6.2 Laadukkaat sopimukset ja poistumissuunnitelma

Pilvipalveluita käyttävän asiakasorganisaation näkökulmasta luottamuksen edellytys ovat riittävän kattavat ja huolellisesti neuvotellut palvelusopimukset. Palvelusopimuksiin kirjataan roolit sekä vastuut, keskeiset termit ja suorituskykyasiat. Palvelun suorituskyky ja sen mittarit tulee määritellä selkeästi sekä sopia kenen vastuulla mittaaminen on. Sovittavia asioita ovat muun muassa: miten palvelu on asiakasorganisaation käytettävissä, kuinka suuri on samanaikaisten käyttäjien maksimimäärä ja millainen kyky palveluntuottajalla on laajentaa käyttäjämäärää, millainen on palvelun kapasiteetti, millaiset ovat vasteajat palvelun käytölle sekä tukipyynnöille. Lisäksi on määriteltävä miten ja milloin asiakkaalla on pääsy omistamaansa dataan, kuka hallinnoi verkkoja ja miten data saadaan pilvipalvelusta kokonaan takaisin asiakasorganisaatiolle, jos palvelu poistuu tai lopetetaan. Sopimuksesta on myös käytävä ilmi sellaiset palvelunhallintavaatimukset kuten: miten palveluntuottaja seuraa suorituskykyä ja miten raportoi sen asiakkaalle sekä miten palvelu voidaan auditoida ja vahvistaa sovittujen asioiden toteutuminen. Katastrofeista palautuminen ja toiminnan jatkuvuus on suunniteltava, testattava ja harjoiteltava. Palveluntuottajan tulee täyttää asiakasorganisaation vaatimukset tietosuojan osalta. On määritettävä, kenellä on pääsy organisaation luokittelemaan dataan ja miten ilmoitetaan, jos väärinkäytöksiä huomataan tapahtuneen. (Defense Acquisition University, 2019.)

Pilvipalveluiden tuottajat ovat epäonnistuneet historiansa kuluessa aina välillä ja tulevat todennäköisesti epäonnistumaan joissain tilanteissa myös tulevaisuudessa. Vaikka pilvipalvelun tuottajan tai minkä tahansa ICT-toimijan kanssa olisi hyvä pitkä asiakassuhde ja luottamuksellinen kumppanuus, on äärimmäisen tärkeää tietää jo sopimusta tehtäessä ne ehdot ja menettelyt, miten toimitaan kumppanuuden päättyessä. (Defense Acquisition University, 2019.)

Kaikkiin pilvistrategioihin kuuluu osana myös huolellisesti suunniteltu ja säännöllisesti päivitetty SaaS-, IaaS- ja Paas -malleilla toteutettuja sovelluksia koskeva poistumisstrategia. Tätä osuutta riskienhallintatyön osana ei saa

unohtaa, vaikka sellaista on tapahtunutkin kiireellisemmiksi koettujen asioiden viedessä huomiota pilven käyttöönotoissa. Poistumisstrategiaa ajatellen IaaS palvelumallina on näistä yksinkertaisin, mutta SaaS ja PaaS ovat vaativampia. Vaihtoehtoina ovat pysyminen edelleen pilvessä, mutta lisäten palveluun korkean käytettävyyden vaatimukset. Toisena vaihtoehtona voidaan palata takaisin on-premises-ratkaisuun eli omaan palvelutuotantoon. Kolmas vaihtoehto on vaihtaa käyttämään jonkin muun palveluntuottajan palvelua. (Gartner, 2018.)

Suunnitelman pitäisi olla sovelluskohtainen ja eri vaihtoehtojen riskit ja kustannusvaikutukset pitää pystyä esittämään riittävällä selkeydellä sidosryhmille. Tärkeintä on varmistua jo ajoissa siitä, että käytettävissä on validoitu menetelmä datan ja metadatan poistamiseksi palveluntuottajalta. Selvitettynä tulee olla myös se, että mahdollisessa paluutapauksessa käytössä on soveltuvia alustoja ja sovelluksia, joiden avulla tuotu data otetaan käyttöön omassa palvelutuotantoympäristössä. Jos käyttökelpoista sovellusta tietoaineistolle ei ole, importoitu data on arvotonta. (Gartner, 2018.) Tästä voidaan tehdä hyvin yksiselitteinen tulkinta todeten se, ettei poistumisstrategian suunnittelua sovi unohtaa, vaikka pilvipalveluiden käyttöönottotilanteessa se saatetaankin jättää helposti vähemmälle huomiolle.

6.3 Ohjeet ja sisäisen hallintomallin merkitys

Tutkielman johdantoluvussa on mainittu viranomaistoimijoiden ja näille palveluja tuottavien yritysten liiketoiminnan suunnittelua sujuvoittavista ohjeista, kuten esimerkiksi KATAKRI tai VAHTI-ohjeet. Pilvipalveluiden käyttöönotto, varsinkin globaaleiden toimittajien palveluina, johtaa tilanteeseen, jossa kansainvälisessä toimintaympäristössä on välttämätöntä huomioida tietoturvallisuuden vaikutusta laajemmin, kuin vain kansallisesta näkökulmasta.

Tietoturvallisuuden hallintajärjestelmien kansainvälinen standardi on hallinnan ja johtamisen standardi ISO/IEC 27001, joka antaa viitekehyksen riskiperusteisten tietoturvallisuusasioiden hallintaan. Standardi on yleistasoinen joukko vaatimuksia, mutta siinä ei kuitenkaan määritellä kuinka ne pitää toteuttaa. Akkreditoinnin tarkoitus on osoittaa pätevyys puolueettomasti ja riippumattomasti. Liikenne- ja viestintävirasto Traficom hyväksyy ja valvoo arviointilaitoksia, jotka tarjoavat viranomaisille puolueetonta arviointipalvelua. Viranomaisille arviointeja tekevät toimijat joutuvat käymään läpi prosessin, jolla arviointikyvykkyys todennetaan. ISO/IEC 27001-sertifikaatteja myöntävät myös akkreditoimattomat arviointilaitokset. Tämä onkin syytä huomioida, sillä kansainvälisessä toiminnassa kansallinen arviointikriteeristö tai akkreditoimaton sertifiointi jäävät kovin heikoiksi painoarvoltaan. Oikein tehty puolueeton tarkastus ja hyväksyntä lisäävät olennaisesti sidosryhmien luottamusta vaatimusten noudattamiseen. KATAKRI:a ei ole tarkoitettu käytettäväksi julkisten hankintojen tietoturvallisuusvaatimuksena, vaan sitä tulisi kyetä soveltamaan. Julkisen hankinnan tarkat turvallisuusvaatimukset tulisi aina määrittää erikseen, niin että riskit ja erityistarpeet otetaan huomioon. (Liikenne- ja viestintävirasto Traficom, 2019.)

Tiedonhallintalaki astui voimaan 1.1.2020 ja uuden lain vanavedessä ministeriöiltä on odotettavissa erilaisten asiantuntijatyöryhmien tuottamana tällä hetkellä valmistelussa olevia ohjekokonaisuuksia. Digi- ja väestötietoviraston (DVV) asiantuntijatyöryhmä laatii soveltamis- ja arviointiohjeistusta, joka korvaa valmistuessaan VAHTI 2/2010 ohjeen. Tavoitteena uudistettavan ohjekokonaisuuden laatimisessa on viestinnän selkeys, jolla väärinymmärrykset vältetään. (Liikenne- ja viestintävirasto Traficom, 2019.) Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelman luonnoksessa on mainittu myös muita digitaalisen turvallisuuden kehittämiseen tähtääviä, vuosille 2020–2023 asetettuja työryhmiä. Tavoitteena on luoda hallinnon toimintaa ja prosesseja ohjaavia arkkitehtuuri-, yhteistoiminta- ja hallintomalleja sekä ohjeita, joissa tarkastellaan toimintaa sekä kansallisessa että kansainvälisessä toimintaympäristössä.

Selkeä viestiminen organisaation johdolle tietoturvallisuuden merkityksestä todetaan olevan vaativaa. Viestinnän tueksi kaivataan selkeää velvoittavaa kriteeristöä. Tarkemmalle tasolle kuvatut vaatimukset helpottavat auditointeja tehden niistä tasalaatuisia. Mitä väljemmin asiat ilmaistaan, sitä enemmin jää tulkinnanvaraa ja tarvitaan kokemusta tietoturvan toteuttamiseksi.

6.4 Miten pilvi otetaan hallintaan?

Gartnerin (2020) mukaan pilvi on näennäisesti helppo omaksua. Käyttö voi alkaa tyypillisesti siten, että teknologioita tuntemattomat henkilöt valitsevat mielestään tarpeisiinsa sopivan pilvipalvelun ja hankkivat sen luottokortilla käyttöönsä. Tässä kohtaa organisaation tietohallinnon on tunnistettava roolinsa ja astuttava hallinnoimaan palvelua, suojelemaan yrityksen liiketoimintaa ja alkaa edistämään tehokasta käyttöä. (Gartner, 2020.)

Gartner (2020) ehdottaakin pilviteknologioiden hallintaan perustettavaksi kolmesta työryhmästä muodostettavaa organisaation sisäistä toimielintä (engl. cloud center of excellence). Kolmen ryhmän yhteistyöllä hoidetaan organisaation pilvikokonaisuutta ja sen hallintaa. Esittelen seuraavaksi lyhyesti tiivistäen Gartnerin cloud center of excellence -mallin sovellettavuutta. Työryhmärakenne voisi olla tehtäviensä kautta nimetty esimerkiksi seuraavasti:

- Pilviratkaisuiden tuotteistusryhmä
- Pilviteknologioiden pääarkkitehdit
- Pilviosaamisen yhteisö.

Pilvipalveluiden käyttöönotto vaikuttaa laajasti organisaatiossa sen eri osiin ja toimialoihin. Sisäisten sidosryhmien tehtävä on kehittää asianmukaiset toimintamallit, ohjeet ja käytännöt, sekä kokoontua seuraamaan ja päivittämään niitä tarpeen mukaan.

Pilviratkaisuiden tuotteistusryhmä on luonteeltaan moniammatillinen eri toimialojen edustajista koostuva työryhmä. Ryhmä kokoontuu tarvittaessa kulloinkin ratkaistavissa olevan uuden liiketoimintatarpeen arvioimiseksi, mikäli esimerkiksi aiemmin luotu toimintamalli ja pilvivaihtoehdot kaipaavat laajennusta tai kokonaan uusia ratkaisuja. Ryhmään kuuluu edustajia tietohallinnosta

kuten esimerkiksi pilviarkkitehti, kaupallisten hankintojen ja talousseurannan asiantuntija, lainopillinen asiantuntija, tietoturvallisuuden vastuuhenkilö, ICT-palvelutuotannon ja tietojärjestelmäintegraation asiantuntija, sekä henkilöstöhallinnon asiantuntija. RACI-malliin perustuen ryhmä on vastuussa erilaisten tehtäviensä suorittamisesta, kuten prosessien kuvaamisesta organisaation käyttöön. Ryhmä on tilivelvollinen omasta osuudestaan pilviprosessien ja käytäntöjen toteutuksessa. Ryhmä valmistelee oman osaamisalansa asioissa taustatietoa pilviteknologioiden pääarkkitehdeille ja saa vastavuoroisesti tiedon pilviarkkitehtuurikeskuksen ratkaisuista ja konsernitason linjauksista. Ryhmä muodostaa vaihtoehdot eli ikään kuin palvelutarjottimen erilaisten tietojärjestelmien sijoittamiseksi pilviympäristöihin. Valmiit ratkaisuvaihtoehdot nopeuttavat ja helpottavat merkittävästi jatkossa organisaation eri toimialojen tietojärjestelmien pilvikäyttöönottoja. (Gartner, 2020.)

Pilviteknologioiden pääarkkitehdit vastaavat konsernitasoisesta pilvipolitiikasta ja määrittää linjaukset sekä laatii ohjaavan dokumentaation muille toimijoille. Ryhmä toimii organisaation ylimmän tietohallintojohtajan alaisuudessa. Se tekee tehtäväänsä yleensä muun organisaatiotasoisen tietohallinnollisen yritysarkkitehtuurityön ohessa luoden hallintomalleja muiden sisäisten toimijoiden työlle, mutta ei aktiivisesti osallistu pilvikäyttöönottojen toteutuksiin. (Gartner, 2020.)

Lähempänä loppukäyttäjiä olisi kolmas työryhmätaso eli **pilviosaamisen yhteisö.** Tämä on yhteisö, joka toimii aktiivisesti vuorovaikutuksessa, rakentaa yhteistoimintaa organisaation sisällä ja tuottaa yhteisöllisiä resursseja. Se edistää tiedonvälitystä pilviratkaisuiden osalta organisaation sisällä lisäten ymmärrystä mahdollisuuksista ja nopeuttaen käyttöönottoja sekä niiden tuottamaa liiketoiminnallista hyötyä. Ryhmän toiminta tiivistää osaamisellaan etenkin laajojen organisaatioiden hajanaisia pilvikäyttöönottoja levittäen hyviä käytänteitä sekä auttaa kehittämään pilviosaamista yhteen paikkaan organisaation sisällä. Ryhmään voi kuulua periaatteessa kuka tahansa pilvipalveluista kiinnostunut. Todennäköisimmin ryhmään osallistuvat kuitenkin pilviprojekteissa mukana olevat tai sellaiset, joiden työtehtäviin pilvijärjestelmien käyttöönotot tulevat vaikuttamaan myös jatkossa ja he haluavat siksi kehittää osaamistaan. (Gartner, 2020.)

Esitelty rakenne sisältää ja edellyttää tarkoituksenmukaisen dokumentaation tuottamista jokaisessa ryhmässä, jota voidaan hyödyntää eri tasoilla tietohallinnon päätöksenteosta aina loppukäyttäjäohjeisiin saakka. Luomalla käytäntöjä ja ohjeita valmiiksi keskitetyssä rakenteessa, vältytään tekemästä samoja asioita joka kerta uudestaan erillisissä käyttöönottoprojekteissa. Virtuaalityöryhmärakenne on ajateltu joustavaksi ja henkilöiden osallistuminen käynnistysvaiheen jälkeen perustuu kulloinkin käsiteltävien aiheiden perusteella tarveharkintaan. Ryhmien jäsenet olisivat omalle asiantuntemusalalleen organisaation palkkaamaa henkilöstöä. Työryhmärakenteen osallistujat ja tehtävät määräytyvät sitä soveltavan organisaation oman johtamis- ja hallintomallin mukaisesti. Ryhmien työskentelyä tukemaan tarvittaneen esimerkiksi luotettavia kumppaneita ulkopuolisten palveluvälittäjien puolelta. Organisaation luomat pilvipolitiikka- tai strategiapaperit eivät sellaisenaan riitä, vaan konkreettiset toimet

pilvipalveluiden käyttöönottoon vaativat jäsentyneet toimintamallin sekä siihen nimetyt henkilöt, joilla on työnsä tekemiselle mandaatti.

6.5 Tutkimustulosten luotettavuus ja pätevyys

Pro gradu -tutkielman tekeminen edellyttää pohdintaa tutkimuksen luotettavuuteen ja pätevyyteen vaikuttavista tekijöistä, eli millaisin keinoin on pyritty totuudenmukaiseen ja toistettavaan lopputulokseen. Reliabiliteetti laadullisessa tutkimuksessa tarkoittaa sitä, että tutkimustulokset vastaavat tutkittavia ilmiöitä. Tavoite pyritään varmistamaan riittävän tarkalla dokumentaatiolla. Lukijan tulisi pystyä arvioimaan tulkintojen paikkaansa pitävyys. Aineiston pohjalta myös muiden pitäisi tulla samaan lopputulokseen ja johtopäätösten tulisi olla selkeitä. (Kananen, 2015.)

Tutkimuksessa tulee pyrkiä virheettömyyteen, minkä vuoksi tehdyn työn luotettavuutta ja validiteettia tuleekin arvioida. Tutkimuksen reliaabelius tarkoittaa mittaustulosten toistettavuutta eli ne eivät saa sattumanvaraisia tuloksia. Luotettavuuden arviointiin pyritään kiinnittämään huomiota koko prosessin ajan perustelemalla tehdyt ratkaisut. Kvalitatiivisen tutkimuksen osalta raportoinnin selkeys prosessin kaikissa vaiheissa on hyvin tärkeää. Pyritään kertomaan selkeästi kaikkien vaiheiden eteneminen ja selkeyttämään analysointia luokitteluja tekemällä. Tämä toimintatapa jatkuu aina tulosten ja johtopäätösten esittämiseen saakka eli tutkijan tulee perustella, millaisilla perusteilla tulkintoja esitetään ja mihin tämä päätelmänsä perustaa. (Hirsjärvi ym., 2009.)

Tämän kirjallisuuskatsauksena toteutetun tutkimuksen luotettavuus pohjautuu aiemmin tehtyyn tieteelliseen tutkimukseen ja siitä kirjoitettuihin tieteellisiin artikkeleihin, jotka on julkaistu informaatioteknologian alan laadukkaiksi ja suositeltaviksi tunnustamissa tietokannoissa Scopus ja IEEE Xplore. Kirjallisuuskatsauksen toteutus eteni käytettävissä olevan ajan ja resursoinnin puitteissa Okolin ja Schabramin (2010) laatimaa mallia noudattaen sekä soveltaen sitä yhden henkilön tekemään pro gradu -tutkielmaan. Hakusanat valikoituivat tutkimuskysymysten tavoitteiden kautta testihakujen havaintoja hyödyntäen. Aineiston haku ja siihen kohdennettu seulominen on kuvattu luvussa neljä. Aineiston keruuvaiheen hakusanat, käytetyt tietokannat, sisäänotto- ja poissulkukriteereineen on kuvattu vaiheittain selkeästi. Tarkempaan läpikäyntiin valitut 78 tekstiä on taulukoitu tämän tutkielman liitteeksi, joten dokumentointi on tarkkaa ja tutkimus on toistettavissa. Edellä kuvatut toimet tukevat tutkimuksen luotettavuutta. Laadullisen tutkimuksen tulosten muodostamiseen on vaikutusta tutkimuksen tekijän omalla näkemyksellä ja kokemuksella tietohallintoalan tehtävistä valtionhallinnossa. Tästä on ollut etua, koska tutkittava aihepiiri on pääpiirteissään tuttua. Toki henkilökohtaiset valinnat painotuksineen tulee ottaa huomioon kokonaisuuden luotettavuutta arvioitaessa.

Tietohallintonäkökulmalla suoritettu tutkimusote on koko tutkielman punainen lanka. Kirjallisuuskatsaus oli hyvin soveltuva tällaiseen aiheen käsittelytavaksi ja tutkimuskysymyksiin saatiin vastauksia. Aineistojen väljempi rajaus, hakutermien tai tietokantojen lisääminen toisi huomattavan määrän lisäaineistoa

ja samalla myös kattavamman kuvan esimerkiksi tietoturvan toteuttamisen ratkaisuista. Tällä kertaa siihen ei ollut mahdollisuutta, koska aineiston määrä piti pitää kohtuullisissa rajoissa. Käsittelyn tarkempi kohdentaminen kotimaisiin turvallisuusalan viranomaistoimijoihin toisi kyselytutkimuksen myötä tuoreen pintatilanteen pilvipalveluiden hyväksymispäätöksiin ja käyttöönottojen ensi kokemuksiin virastoissa.

7 POHDINTA

Tässä pro gradu -tutkielmassa selvitin pilvipalveluiden käyttöönottopäätöksen taustalla vaikuttavia teemoja sekä sitä, millaisia ohjeita tai toimintamalleja olisi hyödyllistä laatia ja toteuttaa käyttöönottojen onnistumisen varmistamiseksi. Tarkastelussani keskeinen näkökulma oli valtionhallinnon organisaation tietohallinnon rooli ja sen tehtävät riskiarviointeineen pilven soveltuvuuden arvioinnissa tuotettaessa tietoa päätöksenteon tueksi.

Pilvipalveluiden käyttö laajenee myös valtionhallinnon organisaatioissa. Päätöksentekoa hidastaa kuitenkin epävarmuus pilviteknologioiden käytön turvallisuudesta, joka johtuu palvelu-ulkoistuksen myötä vastuun siirtymisestä omasta organisaatiosta merkittäviltä osin palveluntuottajalle. Vastuun jakautumiseen vaikuttaa valittu palvelu- ja tuotantomalli. Luottamuksen lisääminen vaatisi nykyisiä toteutuksia kehittyneempiä hallinta- ja valvontamenetelmiä läpinäkyvyyden parantamiseksi. Mitä kriittisempi sovellus on liiketoiminnan kannalta, sitä tärkeämpää olisi saavuttaa luottamus ja näkyvyys organisaation omistamaan dataan. Liiketoimintakriittisten prosessien osalta on välttämätöntä pystyä arviomaan riskit ja oppia tunnistamaan pilven edellyttämät turvallisuuskontrollit. Valtionhallinnon toimijoiden käyttämien tietojärjestelmien lisäksi myös sähköiset verkkopalvelut kansalaisille ovat lisääntymässä kaikkialla maailmassa ja ratkaistavat haasteet vaikuttavat olevan joka puolella samanlaisia. Viranomaispalveluiden tulisi olla turvallisia käyttää ja luotettavaksi koettuja, jotta kansalaiset rohkaistuvat niitä käyttämään. Viranomaistoimijan luotettavuuden menetys esimerkiksi tietovuototapauksessa olisi maineenhallintaa ajatellen huomattava vahinko. Riskiarviointikyvykkyyden laajentaminen tunnistamaan, arvioimaan ja vähentämään pilvipalveluiden tuottamat riskit siedettävälle tasolle, on keskeistä. Organisaation henkilöstön osaamisen kasvattaminen, niin pilviteknologioiden, palvelusopimusten, kuin hankintateknisten seikkojen suhteen, on niin ikään merkittävästi eduksi pilvikäyttöönoton onnistumisessa.

Mitä tämä pro gradu -tutkielma tuo mukanaan pilvipalveluiden tietoturvallista käyttöä ja käyttöönottopäätöksiä koskevaan tutkimukseen? Pilvipalvelut ovat aihepiirinä hyvin laaja sisältäen paljon erilaisia ulottuvuuksia tarkasteltavaksi. Aihepiirin laajuudesta huolimatta tämän tutkimuksen rajauksien puitteissa esittelemistäni tuloksista voidaan vetää suuntaa antavia johtopäätöksiä tietohallinnon työn tueksi valtionhallinnossa.

Johtopäätöksissä ja pohdinnassa kokosin listauksen sellaisista teemoista, joita pilvipalveluiden laajamittainen käyttö edellyttää ja joihin on hyödyllistä kohdistaa huomio. Tutkimukseni perusteella en luonnollisestikaan voi ottaa kantaa siihen, onko Suomessa valtionhallinnossa tehty oikeanlaisia asioita tai kuinka pitkällä erilaisten pilvipalveluratkaisuiden tiellä ollaan. Se vaatisi erillisen tarkastelun. Sen tämä tutkielma osoitti, että riippumatta organisaation toimialasta, samanlaiset tietoturvallisen käytön toteutumiseen liittyvät teemat askarruttavat kaikkialla.

Valtiollisten toimijoiden pilvikäyttöönottoihin liittyy toimintaympäristön vaikutuksia ajatellen merkittävästi kansallinen ministeriöiden ohjaus kuten myös EU-tasoinen lainsäädäntö vaikutuksineen. Tämä ei näkynyt merkittävässä

roolissa kirjallisuuskatsauksen tuloksissa. TOE-kehysmallin osa-alueita ajatellen toimintaympäristön merkitys tässä suhteessa kuitenkin korostuu valtionhallinnon organisaatioiden tietohallintotoimialan työssä. Pilviosaamisen jalkauttamista varten luvussa 6.4. esittelemäni pilviosaamisen keskus työryhmineen vaikuttaa houkuttelevalle tavalle keskittää päätöksentekoa ja osaamista organisaation sisälle sujuvoittamaan pilvikäyttöönottoja. Gartnerin materiaaleissa tämä cloud center of excellence -nimellä esitelty rakenne ja toimintamalli on viety varsin pitkälle yksityiskohtineen sellaisenaan sovellettavaksi. Mallin soveltaminen esimerkiksi turvallisuusviranomaisten toimintaympäristöön olisi kiinnostava kohde tarkastelulle ja mahdollisesti myös jatkotutkimuksille.

Tutkielman tulosten läpikäynti tuottaa erinomaisen mahdollisuuden tietohallinnon ammattilaiselle ja päätöksentekijöille arvioida millaisessa maturiteettivaiheessa oma organisaatio on. Onko mahdollisesti jotain vielä kesken ja olisiko kehitettävä tai luotava uusia prosesseja ja käytäntöjä? Tarkastelun tuloksen perusteella voisi laatia edelleen etenemispolkuja jatkotoimille perustellen niiden rahoituksen ja projektoinnin välttämättömyyttä esimerkiksi edustamansa organisaation johdolle. Käyttämäni lähdeaineiston välityksellä käsittelemiini teemoihin voi hakea myös lisää syvyyttä ja laajuutta haluamallaan tavalla, vaikkapa tehden erilaisia painotuksia tämän tutkielman käsittelyn ja tulosten laajentamiseksi.

Mielestäni tutkimusta voisi ulottaa jatkossa myös organisaatioiden erilaisissa rooleissa työskentelevien tietohallinnon ammattilaisten ja päätöksentekijöiden suuntaan. Olisi kiinnostavaa koota ja vertailla esimerkiksi eri valtionhallinnon toimijoiden kokemuksia ja toimintatapoja pilvikäyttöönotoissa. Myös erot tai yhtäläisyydet erilaisten valtionhallinnon toimijoiden tietohallinnon tavoissa ohjata pilviteknologioiden käyttöönottoa olisi kiinnostava tutkimusaihe. Tutkielman tekeminen osoitti sen, että sekä ICT-alan ammattilaiset että akateemiset tutkijat ovat tunnistaneet keskeiset turvallisuushaasteet ja niihin suhtaudutaan asian vaatimalla vakavuudella ja tehdään oikeansuuntaisia toimia asioiden kuntoon saattamiseksi.

LÄHTEET

Ahmed, T., Alhadi, N. & Seliaman, M. E. (2015). Acceptance of e-government services in Sudan: An empirical investigation. 2015 International Conference on Cloud Computing (ICCC). 26-29 April 2015. Riyadh, Saudi Arabia (1-4). IEEE.

Aissaoui, K., Ait idar, H., Belhadaoui, H. & Rifi, M. (2017). Survey on data remanence in cloud computing environment. 2017 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS). 19-20 April 2017. Fez, Morocco (1-4). IEEE.

Alassafi, M. O., Alharthi, A., Walters, R. J. & Wills, G. B. (2017). A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies. *Telematics and Informatics, 34*(7), 996-1010.

Alemeye, F. & Getahun, F. (2015). Cloud readiness assessment framework and recommendation system. (1-5). AFRICON Conference. Sept. 2015. Addis Ababa, Ethiopia (14-17). IEEE.

Alhanahnah, M., Bertok, P. & Tari, Z. (2017). Trusting cloud service providers: Trust phases and a taxonomy of trust factors. *IEEE Cloud Computing, 4*(1), 44-54.

Ali, M., Khan, S. U. & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences, 305*(C), 357-383.

Ali, O., Soar, J., Yong, J. & Tao, X. (2016). Factors to be considered in cloud computing adoption. *Web Intelligence, 14*(4), 309-323.

AlKharusi, M. H. & Al-Badi, A. H. (2016). IT personnel perspective of the slow adoption of cloud computing in public sector: Case study in Oman. (1-8). 2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC). 15-16 March 2016. Muscat, Oman. IEEE.

Alkhater, N., Wills, G. & Walters, R. (2015). Factors affecting an organisation's decision to adopt cloud services in Saudi-Arabia. 2015 3rd International Conference on Future Internet of Things and Cloud. 24-26 Aug. 2015. Rome, Italy (553-557). IEEE.

Alkhwaldi, A., Kamala, M. & Qahwaji, R. (2017). From e-govemment to cloud-government: Challenges of jordanian citizens' acceptance for public services. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST). 11-14 Dec. 2017. Cambridge, UK (298-304). IEEE.

Almanea, M. I. M. (2014). A survey and evaluation of the existing tools that support adoption of cloud computing and selection of trustworthy and transparent cloud providers. 2014 International Conference on Intelligent Networking and Collaborative Systems. 10-12 Sept. 2014. Salerno, Italy (628-634). IEEE.

Almazroi, A. A., Shen, H., Teoh, K. & Babar, M. A. (2016). Cloud for e-learning: Determinants of its adoption by university students in a developing country. 2016 IEEE 13th International Conference on e-Business Engineering (ICEBE). 4-6 Nov. 2016. Macau, China (71-78). IEEE.

Alsmadi, D. & Prybutok, V. (2018). Sharing and storage behavior via cloud computing: Security and privacy in research and practice. *Computers in Human Behavior, 85*, 218-226.

Andriole, S. J. (2017). The adoption of emerging technology: Technology before requirements. 2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC). 4-8 July 2017. Turin, Italy (709-713). IEEE.

Armbrust, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50-58.

Arpaci, I. (2017). Antecedents and consequences of cloud computing adoption in education to achieve knowledge management. *Computers in Human Behavior, 70*, 382-390.

Arvanitis, S., Kyriakou, N. & Loukis, E. N. (2017). Why do firms adopt cloud computing? A comparative analysis based on south and North Europe firm data. *Telematics and Informatics, 34*(7), 1322-1332.

Attasena, V., Darmont, J. & Harbi, N. (2017). Secret sharing for cloud data security: A survey. *VLDB Journal, 26*(5), 657-681.

Balaaooriya, L. N. P., Wibowo, S. & Wells, M. (2017). Factors influencing cloud technology adoption in Australian organisations. 2017 2nd International Conference on Information Technology (INCIT). 2-3 Nov. 2017. Nakhonpathom, Thailand (1-6). IEEE.

Baskerville, R. & Myers, M. (2002). Information systems as a reference discipline. *MIS Quarterly,* 26(1), 1-14.

Baskerville, R. (1991). Risk analysis: An interpretive feasibility tool in justifying information systems security. *European Journal of Information Systems, 1*(2), 121-130.

Bhajantri, L. B. & Mujawar, T. (2019). A survey of cloud computing security challenges, issues and their countermeasures. 2019 Third International

conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). 12-14 Dec. 2019. Palladam, India, India (376-380). IEEE.

Boillat, T. & Legner, C. (2014). Why do companies migrate towards cloud enterprise systems? A post-implementation perspective. 2014 IEEE 16th Conference on Business Informatics. 14-17 July 2014. Geneva, Switzerland (102-109). IEEE.

Bouaynaya, W. (2020). Cloud computing in SMEs: Towards delegation of the CIO role. *Information and Computer Security, 28*(2), 199-213.

Bruce, C. S. (1994). Research students' early experiences of the dissertation literature review. *Studies in Higher Education, 19*(2), 217-229.

Butt, S. A., Tariq, M. I., Jamal, T., Ali, A., Martinez, J. L. D. & De-La-Hoz-Franco, E. (2019). Predictive variables for agile development merging cloud computing services. *IEEE Access, Volume 7*, 99273-99282.

Caldarelli, A., Ferri, L. & Maffei, M. (2017). Expected benefits and perceived risks of cloud computing: An investigation within an italian setting. *Technology Analysis and Strategic Management, 29*(2), 167-180.

Candel Haug, K., Kretschmer, T. & Strobel, T. (2016). Cloud adaptiveness within industry sectors - measurement and observations. *Telecommunications Policy, 40*(4), 291-306.

Cegielski, C. G., Jones-Farmer, L. A., Wu, Y. & Hazen, B. t. (2012). Adoption of cloud computing technologies in supply chains. *The International Journal of Logistics Management, 23*(2), 184-211.

Chang, V. & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. *IEEE Transactions on Services Computing, 9*(1), 138-151.

Chang, V., Ramachandran, M., Yao, Y., Kuo, Y. & Li, C. (2016). A resiliency framework for an enterprise cloud. *International Journal of Information Management, 36*(1), 155-166.

Chiba, Z., Abghour, N., Moussaid, K., El Omri, A. & Rida, M. (2016). A survey of intrusion detection systems for cloud computing environment. 2016 International Conference on Engineering & MIS (ICEMIS). 22-24 Sept. 2016. Agadir, Morocco (1-13). IEEE.

Cloud Security Alliance. (2020). Top threats to cloud computing - the egregious 11. Haettu 24.6.2020 osoitteesta https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society, 1*(1), 104-126.

Coppolino, L., D'Antonio, S., Mazzeo, G. & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers and Electrical Engineering, 59*, 126-140.

Defense Acquisition University. (2019). DoD cloud computing acquisition guidebook. Haettu 1.7.2020 osoitteesta https://www.dau.edu/guidebooks/Shared%20Documents%20HTML/DoD%20Cloud%20Acquisition%20Guidebook.aspx

Dincă, V. M., Dima, A. M. & Rozsa, Z. (2019). Determinants of cloud computing adoption by romanian smes in the digital economy. *Journal of Business Economics and Management, 20*(4), 798-820.

El-Gazzar, R., Hustad, E. & Olsen, D. H. (2016). Understanding cloud computing adoption issues: A delphi study approach. *Journal of Systems and Software, 118*, 64-84.

Esposito, C., Castiglione, A., Martini, B. & Choo, K. R. (2016). Cloud manufacturing: Security, privacy, and forensic concerns. *IEEE Cloud Computing, 3*(4), 16-22.

European Parliament and Council of European Union. (2016). *General data protection regulations (GDPR). Regulation, (EU) 2016/679.*

Fink, A. (2005). *Conducting research literature reviews : From the internet to paper* (2nd ed). Thousand Oaks, Calif: Sage Publications.

Finlex. (2015). Laki julkisen hallinnon turvallisuusverkkotoiminnasta 10/2015. Haettu 5.5.2020 osoitteesta https://www.finlex.fi/fi/laki/alkup/2015/20150010

Gangwar, H., Date, H. & Ramaswamy, R. (2016). Understanding cloud computing adoption: A model comparison approach. *Human Systems Management, 35*(2), 93-114.

Garg, R., Stiller, B., Butt, S. A., Tariq, M. I., Jamal, J., Ali, A., De-La-Hoz-Franco, E. (2014). Design and evaluation of an impact analysis methodology for the adoption of cloud-based services (IAMCIS); predictive variables for agile development merging cloud computing services. 10th International Conference on Network and Service Management (CNSM) and Workshop. 17-21 Nov. 2014. Rio de Janeiro, Brazil (260-263). IEEE.

Garrison, G. (2012). Success factors for deploying cloud computing. *Communications of the ACM, 55*(9), 62-68.

Gartner. (2018). Designing a public cloud exit strategy. Haettu 15.7.2020 osoitteesta https://www.gartner.com/document/code/311602?ref=authbody&refval=3891718.

Gartner. (2020). How to Build a Cloud Center of Excellence. Haettu 1.8.2020 osoitteesta https://www.gartner.com/document/3987428?ref=solrAll&refval=268164787.

Ghorbel, A., Ghorbel, M. & Jmaiel, M. (2017). Privacy in cloud computing environments: A survey and research challenges. *Journal of Supercomputing, 73*(6), 2763-2800.

Guarro, S. B. (1987). Principles and procedures of the LRAM approach to information systems risk analysis and management. *Computers & Security, 6*(6), 493-504.

Gutierrez, A. (2015). Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management, 28*(6), 788-807.

Hiran, K. K. & Henten, A. (2020). An integrated TOE–DoI framework for cloud computing adoption in the higher education sector: Case study of sub-saharan africa, ethiopia. *International Journal of Systems Assurance Engineering and Management, 11*(2), 441-449.

Hiran, K. K., Henten, A., Shrivas, M. K. & Doshi, R. (2018). Hybrid EduCloud model in higher education: The case of Sub-Saharan Africa, Ethiopia. 2018 IEEE 7th International Conference on Adaptive Science & Technology (ICAST). 22-24 Aug. 2018. Accra, Ghana (1-9). IEEE.

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Helsinki: Tammi.

Hsu, P., Ray, S. & Li-Hsieh, Y. (2014). Examining cloud computing adoption intention, pricing mechanism, and deployment model. *International Journal of Information Management, 34*(4), 474-488.

Järvinen, P. H. (2000). Research questions guiding selection of an appropriate research method. ECIS 2000, 3-5 July. Vienna: Vienna University of Economics and Business Administration, 2000. 124-131.

Kananen, J. (2015). *Opinnäytetyön kirjoittajan opas : Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun*. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Khan, N. & Al-Yasiri, A. (2016). Identifying cloud security threats to strengthen cloud computing adoption framework. *Procedia Computer Science, Volume 94, 2016.* 485-490.

Kuiper, E., Van Dam, F., Reiter, A. & Janssen, M. (2014). Factors influencing the adoption of and business case for cloud computing in the public sector. eChallenges e-2014 Conference Proceedings. 29-30 Oct. 2014. Belfast, UK (1-10). IEEE.

Kumar, D., Samalia, H. V. & Verma, P. (2017). Exploring suitability of cloud computing for small and medium-sized enterprises in india. *Journal of Small Business and Enterprise Development, 24*(4), 814-832.

Kuo, C. & Kang, Y. (2018). A study of continuance intention to adopt cloud services: The moderating effect of users' motivation. 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). 16-19 Dec. 2018. Bangkok, Thailand (477-481). IEEE.

Kyriakou, N. & Loukis, E. N. (2019). Do strategy, processes, personnel and technology affect firm's propensity to adopt cloud computing?: An empirical investigation. *Journal of Enterprise Information Management, 32*(3), 517-534.

Lansing, J., Siegfried, N., Sunyaev, A. & Benlian, A. (2019). Strategic signaling through cloud service certifications: Comparing the relative importance of certifications' assurances to companies and consumers. *Journal of Strategic Information Systems, 28*(4).

Lian, J. (2015). Critical factors for cloud based e-invoice service adoption in Taiwan: An empirical study. *International Journal of Information Management, 35*(1), 98-109.

Lian, J. (2014). An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. *International Journal of Information Management, 34*(1), 28-36.

Liikenne- ja viestintävirasto Traficom. (2019). Luottamuksen lähteillä Traficomin julkaisuja, 31/2019. Haettu 15.7.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf

Liikenne- ja viestintävirasto Traficom. (2020). Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Traficomin julkaisuja, 13/2020. Haettu 20.5.2020 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Lim, N., Grönlund, Å & Andersson, A. (2015). Cloud computing: The beliefs and perceptions of Swedish school principals. *Computers and Education, 84*, 90-100.

Liu, Y., Sun, Y., Ryoo, J., Rizvi, S. & Vasilakos, A. V. (2015). A survey of security and privacy challenges in cloud computing: Solutions and future directions. *Journal of Computing Science and Engineering, 9*(3), 119-133.

Loukis, E., Arvanitis, S. & Kyriakou, N. (2017). An empirical investigation of the effects of firm characteristics on the propensity to adopt cloud computing. *Information Systems and E-Business Management, 15*(4), 963-988.

Loukis, E. & Kyriakou, N. (2015). Organizational factors affecting propensity to adopt cloud computing. 2015 48th Hawaii International Conference on System Sciences. 5-8 Jan. 2015. Kauai, HI, USA (4230-4239). IEEE.

Low, C. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems, 111*(7), 1006-1023.

Luna, J., Suri, N., Iorga, M. & Karmel, A. (2015). Leveraging the potential of cloud security service-level agreements through standards. *IEEE Cloud Computing, 2*(3), 32-40.

Manuel, P. (2015). A trust model of cloud computing based on quality of service. *Annals of Operations Research, 233*(1), 281-292.

Masana, N. & Muriithi, G. M. (2019). Adoption of an integrated cloud-based electronic medical record system at public healthcare facilities in free-state, South Africa. 2019 Conference on Information Communications Technology and Society (ICTAS). 6-8 March 2019. Durban, South Africa, South Africa (1-6). IEEE.

McKnight, D. H. (2005). Trust in information technology. *The Blackwell Encyclopedia of Management. Vol. 7 Management Information Systems*. 329-331.

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing. *Cloud computing and government: Background, benefits, risks*. Nova Science Publishers, Inc. (171-173).

Metsämuuronen, J. (2005). Näyttöön perustuva päätöksenteko ja systemoitu kirjallisuuskatsaus. *Psykologia : Tiedepoliittinen Aikakauslehti, 40*(5), 581.

Minhaj, N. & Islam, M. H. (2016). Cloud adoption in industrial setup of Pakistan. 2016 13th International Bhurban Conference on Applied Sciences and Technology (IBCAST). 12-16 Jan. 2016. Islamabad, Pakistan (421-427). IEEE.

Miorandi, D., Rizzardi, A., Sicari, S. & Coen-Porisini, A. (2019). Sticky policies: A survey. *IEEE Transactions on Knowledge and Data Engineering 32(7),* 2481-2499.

Mishra, B. & Jena, D. (2019). Security of cloud storage: A survey. 2019 International Conference on Information Technology (ICIT). 19-21 Dec. 2019. Bhubaneswar, India, India (109-114). IEEE.

Okoli, C. & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Systems,* 10(26).

Oliveira, T., Thomas, M. & Espadanal, M. (2014). Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors. *Information & Management, 51*(5), 497-510.

Opara-Martins, J., Sahandi, R. & Tian, F. (2015). A business analysis of cloud computing: Data security and contract lock-in issues. 2015 10th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC). 4-6 Nov. 2015. Krakow, Poland (665-670). IEEE.

Oredo, J., Njihia, J. & Iraki, X. (2019). Institutional pressures and cloud computing adoption: The moderating effect of organizational mindfulness. 2019 IST-Africa Week Conference (IST-Africa). 8-10 May 2019. Nairobi, Kenya, Kenya (1-9). IEEE.

Oredo, J., Njihia, J. & Iraki, X. N. (2017). Cloud computing adoption in the Kenya's financial sector: An institutional perspective. 2017 IST-Africa Week Conference (IST-Africa). 30 May-2 June 2017. Windhoek, Namibia (1-9). IEEE.

Pahnila, S., Siponen, M. & Zheng, X. (2011). Integrating habit into UTAUT: The chinese eBay case. *Pacific Asia Journal of the Association for Information Systems*, 1-30.

Palos-Sanchez, P. R., Robina-Ramirez, R. & Velicia-Martin, F. (2019). What role does corporate governance play in the intention to use cloud computing technology? *Symmetry, 11*(10).

Papadopoulos, A. V., Versluis, L., Bauer, A., Herbst, N., Von Kistowski, J., Alieldin, A., Iosup, A. (2019). Methodological principles for reproducible performance evaluation in cloud computing. *IEEE Transactions on Software Engineering*.

Paquette, S., Jaeger, P. T. & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly, 27*(3), 245-253.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Petter, S. (2013). Information systems success: The quest for the independent variables. *Journal of Management Information Systems, 29*(4), 7-62.

Porrawatpreyakorn, N., Nuchitprasitchai, S., Viriyapant, K., Tangprasert, S. & Chaipunyathat, A. (2019). Understanding key enablers of cloud computing adoption and acceptance over time. (1-6).

Prieto-González, L., Tamm, G. & Stantchev, V. (2015). Governance of cloud computing: Semantic aspects and cloud service brokers. *International Journal of Web and Grid Services, 11*(4), 377-389.

Priyadarshinee, P., Raut, R. D., Jha, M. K. & Gardas, B. B. (2017). Understanding and predicting the determinants of cloud computing adoption: A two staged hybrid SEM - neural networks approach. *Computers in Human Behavior, 76*, 341-362.

Priyadarshinee, P., Raut, R. D., Jha, M. K. & Kamble, S. S. (2017). A cloud computing adoption in indian SMEs: Scale development and validation approach. *Journal of High Technology Management Research, 28*(2), 221-245.

Puolustusministeriö. (2015). Katakri tietoturvallisuuden auditointikriteeristö viranomaisille. Haettu 1.3.2020 osoitteesta https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Puthal, D., Sahoo, B. P. S., Mishra, S. & Swain, S. (2015). Cloud computing features, issues, and challenges: A big picture. 2015 International Conference on Computational Intelligence and Networks. 12-13 Jan. 2015. Bhubaneshwar, India (116-123). IEEE.

Raggad, B. G. (2010). *Information security management : Concepts and practice*. Boca Raton, Florida ; London, England ; New York: CRC Press.

Rahi, S. B., Bisui, S. & Misra, S. C. (2017). Identifying the moderating effect of trust on the adoption of cloud-based services. *International Journal of Communication Systems, 30*(11).

Rao, R. V. & Selvamani, K. (2015). Data security challenges and its solutions in cloud computing. *Procedia Computer Science, 48*(C), 204-209.

Ratten, V. (2015). Factors influencing consumer purchase intention of cloud computing in the united states and turkey: The role of performance expectancy, ethical awareness and consumer innovation. *EuroMed Journal of Business, 10*(1), 80-97.

Rebollo, O. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*(C), 44-57.

Rogers, E. M. (2003). *Diffusion of innovations* (5th ed). New York: Free Press.

Sabi, H. M., Uzoka, F. -. E., Langmia, K. & Njeh, F. N. (2016). Conceptualizing a model for adoption of cloud computing in education. *International Journal of Information Management, 36*(2), 183-191.

Sabi, H. M., Uzoka, F. -. E., Langmia, K., Njeh, F. N. & Tsuma, C. K. (2018). A cross-country model of contextual factors impacting cloud computing adoption at universities in sub-saharan africa. *Information Systems Frontiers, 20*(6), 1381-1404.

Salminen, A. (2011). *Mikä kirjallisuuskatsaus? : Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasa: Vaasan yliopisto.

Sanastokeskus, T. (2018). Kyberturvallisuuden sanasto. Haettu 25.6.2020 osoitteesta https://turvallisuuskomitea.fi/wp-content/uploads/2018/06/Kyberturvallisuuden-sanasto.pdf

Senarathna, I., Wilkin, C., Warren, M., Yeoh, W. & Salzman, S. (2018). Factors that influence adoption of cloud computing: An empirical study of australian SMEs. *Australasian Journal of Information Systems, 22*.

Senyo, P. K., Effah, J. & Addae, E. (2016). Preliminary insight into cloud computing adoption in a developing country. *Journal of Enterprise Information Management, 29*(4), 505-524.

Sfondrini, N., Motta, G. & Longo, A. (2018). Public cloud adoption in multinational companies: A survey. 2018 IEEE International Conference on Services Computing (SCC). 2-7 July 2018. San Francisco, CA, USA (177-184). IEEE.

Sfondrini, N., Motta, G. & You, L. (2015). Service level agreement (SLA) in public cloud environments: A survey on the current enterprises adoption. 2015 5th International Conference on Information Science and Technology (ICIST). 24-26 April 2015. Changsha, China (181-185). IEEE.

Sharma, V. & Srivastava, G. M. S. (2016). Evolution and present status of cloud computing: A comprehensive analysis. *International Journal of Business Information Systems, 22*(2), 123-142.

Shee, H., Miah, S. J., Fairfield, L. & Pujawan, N. (2018). The impact of cloud-enabled process integration on supply chain performance and firm sustainability: The moderating role of top management. *Supply Chain Management: An International Journal, 23*(6), 500-517.

Shin, J., Jo, M., Lee, J. & Lee, D. (2014). Strategic management of cloud computing services: Focusing on consumer adoption behavior. *IEEE Transactions on Engineering Management, 61*(3), 419-427.

Singh, A., Sharma, S., Kumar, S. R. & Yadav, S. A. (2016). Overview of PaaS and SaaS and its application in cloud computing. 2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH). 3-5 Feb. 2016. Noida, India (172-176). IEEE.

Siponen, M. (2002). *Designing secure information systems and software: Critical evaluation of the existing approaches and a new paradigm.* University of Oulu, Finland.

Siponen, M. (2005). An analysis of the traditional IS security approaches: Implications for research and practice. *European Journal of Information Systems, 14*(3), 303-315.

Siponen, M. (2006). Secure-system design methods: Evolution and future directions. *IT Professional, 8*(3), 40-44.

Siponen, M. & Baskerville, R. (2018). Intervention effect rates as a path to research relevance : Information systems security example. *Journal of the Association for Information Systems,* 19 (4), 247-265.

Siponen, M. & Klaavuniemi, T. (2020). Demystifying beliefs about the natural sciences in information system. *Journal of Information Technology.* 1-13.

Sirohi, P. & Agarwal, A. (2015). Cloud computing data storage security framework relating to data integrity, privacy and trust. 2015 1st International Conference on Next Generation Computing Technologies (NGCT). 4-5 Sept. 2015. Dehradun, India (115-118). IEEE.

Soh, C. & Markus, M. L. (1995). How IT creates business value: A process theory synthesis. *ICIS 1995 Proceedings.* 4. 29-41.

Stieninger, M., Nedbal, D., Wetzlinger, W., Wagner, G. & Erskine, M. A. (2018). Factors influencing the organizational adoption of cloud computing: A survey among cloud workers. *International Journal of Information Systems and Project Management, 6*(1), 5-23.

Straub, E. T. (2009). Understanding technology adoption: Theory and future directions for informal learning. *Review of Educational Research, 79*(2), 625-649.

Sun, X. (2018). Critical security issues in cloud computing: A survey. 2018 IEEE 4th International Conference on Big Data Security on Cloud (BigDataSecurity). 3-5 May 2018. Omaha, NE, USA (216-221). IEEE.

Tariq, M. I., Tayyaba, S., Rasheed, H. & Ashraf, M. W. (2017). Factors influencing the cloud computing adoption in higher education institutions of Punjab, Pakistan. 2017 International Conference on Communication, Computing and Digital Systems (C-CODE). 8-9 March 2017. Islamabad, Pakistan (179-184). IEEE.

Tilastokeskus. (2019). Suomen virallinen tilasto (SVT): Tietotekniikan käyttö yrityksissä [verkkojulkaisu]. Haettu 10.8.2020 osoitteesta http://www.stat.fi/til/icte/2019/icte_2019_2019-12-03_kat_003_fi.html

Tornatzky, L. G. & Fleischer, M. (1990). *The processes of technological innovation* Lexington, (Mass.) : Lexington Books 1990.

Valtiovarainministeriö. (2018). Julkisen hallinnon pilvipalvelulinjaukset Valtiovarainministeriön julkaisuja, 35/2018. Haettu osoitteesta https://vm.fi/documents/10623/1107406/VM_35_2018_Julk_hallinnon_pilvipalvelulinjaukset.pdf/a7ef16b7-025f-7d17-f906-d556e3455ef3/VM_35_2018_Julk_hallinnon_pilvipalvelulinjaukset.pdf?version=1.0

Vance, A. (2008). Examining trust in information technology artifacts : The effects of system quality and culture. *Journal of Management Information Systems,* 24:4, 73-100.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Wade, M. & Hulland, J. (2004). Review: The resource-based view and information systems research: Review, extension, and suggestions for future research. *Mis Quarterly, 28*(1), 107-142.

Wang, C., Wood, L. C., Abdul-Rahman, H. & Lee, Y. T. (2016). When traditional information technology project managers encounter the cloud: Opportunities and dilemmas in the transition to cloud services. *International Journal of Project Management, 34*(3), 371-388.

Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly, 26*(2), 13-23.

Yigitbasioglu, O. M. (2015). The role of institutional pressures and top management support in the intention to adopt cloud computing solutions. *Journal of Enterprise Information Management, 28*(4), 579-594.

Zissis, D. & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems, 28*(3), 583-592.

LIITE 1 LUVUSSA 5 KÄYTETYT ARTIKKELIT

Yksilöivä tunnus	Kirjoittajat ja julkaisuvuosi	Otsikko	Tutkimus	Lyhyt kuvaus
1	Aissaoui K.; Aitidar H.; Belhadaoui H.; Rifi M. (2017)	Survey on data remanence in Cloud Computing environment	Tutkimus	Remanenssi-ilmiö: Poistuuko poistettu data lopullisesti palveluntarjoajan levyjärjestelmästä vai voidaanko se palauttaa?
2	Al-Jabri I.M., Alabdulhadi M.H. (2016)	Factors affecting cloud computing adoption: Perspectives of IT professionals	Tutkimus online-kysely 106 IT-ammattilaista, Saudi-Arabia	Ylimmän johdon tuki merkittävin vaikuttaja pilviadoptiopäätökseen.
3	Alassafi M.O., Alharthi A., Walters R.J., Wills G.B. (2017)	A framework for critical security factors that influence the decision of cloud adoption by Saudi government agencies	Tutkimus Verkkokysely 32 kokenutta IT-ammattilaista, Saudi-Arabia; Triangulaatio	Valtaosa viitekehyksen kategorioista olivat tilastollisesti merkittäviä pilviadoptiolle.
4	Alemeye F.; Getahun F. (2015)	Cloud readiness assessment framework and recommendation system	Kyselytutkimus, 29 IT-manageria, Etiopia	Syntyi arviointikehys pilvipalveluiden käyttöönottopäätöstä varten.
5	Ali O., Soar J., Yong J., Tao X. (2016)	Factors to be considered in cloud computing adoption	Kyselytutkimus 480 kunnallishallinnon IT-henkilöä, Australia	Internet-yhteyden sekä käytettävyyden ja luotettavuuden haasteet.

6	AlKharusi M. H.; Al-Badi A. H. (2016)	IT personnel perspective of the slow adoption of cloud computing in public sector: Case study in Oman	Online-kyselytutkimus, 74 vastaajaa, Oman	IT-ammattilaiset eivät pelkää työpaikkojensa menetystä pilvipalveluita käyttöönotettaessa. Tietoturva arveluttaa.
7	Alkhater N.; Wills G.; Walters R. (2015)	Factors Affecting an Organisation's Decision to Adopt Cloud Services in Saudi Arabia	Online-kyselytutkimus, 30 IT-henkilöä, Saudi-Arabia	Kaikki muut kehyksen teemat vaikuttivat, paitsi monimutkaisuus ja kilpailullinen paine.
8	Alkhwaldi A.; Kamala M.; Qahwaji R. (2017)	From e-govemment to cloud-government: Challenges of Jordanian citizens' acceptance for public services	Kyselytutkimus, 108 vastaajaa, Jordania	Teknologiset, inhimilliset, taloudelliset ja esim. turvallisuuskäsitys sähköisen hallinnon esteinä.
9	Almanea M. I. M. (2014)	A Survey and Evaluation of the Existing Tools that Support Adoption of CC and Selection of Trustworthy and Transparent Cloud Providers	Kyselypohjainen tutkimus, jossa vastaajat arvioivat työkalujen hyödyllisyyttä	Cloud Trust protocol ja C.A.R.E valittiin parhaiksi työkaluiksi, osa ei ollut käyttänyt kaikkia valikoimassa olleita työkaluja.
10	Almazroi A. A.; Shen H.; Teoh K.; Babar M. A. (2016)	Cloud for e-Learning: Determinants of Its Adoption by University Students in a Developing Country	Kokeellinen tapaustutkimus, 527 yliopisto-opiskelijaa, Saudi-Arabia	Yksilökäyttäjien SaaS-kokemuksia
11	Alsmadi D., Prybutok V. (2018)	Sharing and storage behavior via cloud computing: Security and	Kyselytutkimus, 129 IT-ammattilaista	Yksilökäyttäjille vertaiskokemus tärkeä vaikuttaja. Tekniikkaan luotetaan myös turvallisuuden osalta.

		privacy in research and practice		
12	Andriole S. J. (2017)	The Adoption of Emerging Technology Technology Before Requirements	Haastattelututkimus	Teknologia edellä palveluiden käyttäjäksi, määrittelyt vasta myöhemmin. Hallintakysymykset ja varjo-IT aiheuttavat pohdintaa.
13	Arpaci I. (2017)	Antecedents and consequences of cloud computing adoption in education to achieve knowledge management	Tutkimus, 221 opiskelijaa, Turkki	Havaittu hyödyllisyys tukee tietämyksen luomista, tallentamista ja jakamista.
14	Arvanitis S., Kyriakou N., Loukis E.N. (2017)	Why do firms adopt cloud computing? A comparative analysis based on South and North Europe firm data	Tutkimus, aineisto 556 teollisuusyritystä, Eurooppa	Etelä-Euroopassa kustannukset merkittävin tekijä, mutta Keski-Euroopassa pilvisiirtymään liittyvät hyödyt.
15	Attasena, V., Darmont, J., Harbi, N. (2017)	Secret sharing for cloud data security: a survey	Tutkimus	Secret sharing -tekniikan käyttö ja sen soveltuvuuden arvioinnin tärkeys.
16	Balaaooriya L. N. P.; Wibowo S.; Wells M. (2017)	Factors influencing cloud technology adoption in Australian organisations	Kyselytutkimus, 220 IT-ammattilaista, Australia	Kyberhyökkäyksiä tai pilven luotettavuuskysymyksiä ei pidetä esteenä adoptiolle.
17	Bhajantri L. B. ; Mujawar T. (2019)	A Survey of Cloud Computing Security Challenges, Issues and their Countermeasures	Tutkimus, Piviturvallisuuskysymysten arviointia	Pilviturvallisuudelle tärkeitä: asianmukainen autentikointi, vahva salaustekniikka ja tietojen menetyksen estäminen.

18	Boillat T.; Legner C. (2014)	Why Do Companies Migrate Towards Cloud Enterprise Systems? A Post-Implementation Perspective	Tapaustutkimus, kaksi sveitsiläistä yritystä vertailussa, migraatiostrategian vertailua	Yritykset valitsevat ensin SaaS:n (esim. sähköposti). Yrityssovellukset haastavampia viedä pilveen.
19	Bouaynaya W. (2020)	Cloud computing in SMEs: towards delegation of the CIO role	Kyselytutkimus, 800 eurooppalaista pilvessä operoivaa yritystä 16 maasta	CIO:n rooli delegoidaan siirtymävaiheessa ulkoiselle toimijalle. Tukee varmistaen tehdyt ratkaisut.
20	Butt S. A.; Tariq M. I.; Jamal T.; Ali A. ; D √ ≠az Martinez J. L.; De-La-Hoz-Franco E. (2019)	Predictive Variables for Agile Development Merging Cloud Computing Services	Kyselytutkimus, 200 ohjelmistoalan osallistujaa, Pakistan	Pilven käyttöönotto ohjelmistoteollisuudessa nähtiin vähentävän kustannuksia
21	Caldarelli A., Ferri L., Maffei M. (2017)	Expected benefits and perceived risks of cloud computing: an investigation within an Italian setting	Kyselytutkimus, 65 yritystä, 130 yritysjohtajaa tai ICT-manageria, Italia	Riskialttiudesta huolimatta PK-yritykset valmiita pilven käyttöönottoon odotettujen hyötyjen vuoksi
22	Candel Haug K., Kretschmer T., Strobel T. (2016)	Cloud adaptiveness within industry sectors - Measurement and observations	Analyysi, kaksi datasettiä tietokannoista CITDB ja ORBIS	Palvelusektori (business, rahoitus ja tukkukauppa) päätöksenteossa valmistavaa teollisuutta edellä.
23	Chang V., Ramachandran M., Yao Y., Kuo Y.-H., Li C.-S. (2016)	A resiliency framework for an enterprise cloud	Kyselytutkimus, 400 vastaajaa, Englanti	Organisaatiot investoineet tietoturvallisuuteen varautuen siten uhkiin

24	Chang V.; Ramachandran M. (2016)	Towards Achieving Data Security with the Cloud Computing Adoption Framework	Tutkimus	Laadittu viitekehys turvallisuussuunniteluun: cloud adoption framework
25	Chiba Z.;Abghour N.; Moussaid K.; Omri A. El; Rida M. (2016)	A survey of intrusion detection systems for cloud computing environment	Analyysi pilven tietoturvatekniikoista	IDS tärkeä tietoturvallisuuden komponentti erilaisia uhkia ja hyökkäyksiä vastaan
26	Dincă V.M., Dima A.M., Rozsa Z. (2019)	Determinants of cloud computing adoption by romanian smes in the digital economy	Online-kyselytutkimus, 198 PK-yritysten johtajaa, Romania.	Johdon IT-tietotaito ja kustannushyödyt tärkeimmät tekijät pilviadoptiossa
27	Esposito C.; Castiglione A.; Martini B.; Choo K. R. (2016)	Cloud Manufacturing: Security, Privacy, and Forensic Concerns	Tutkimus käsittelee pilvipalveluiden tietoturvahaasteita, Italia	Esittelee muun muassa keinoja vähentämään sisäpiiriläisten tuottamia riskejä.
28	Garg R.; Stiller B. (2014)	Design and evaluation of an Impact Analysis Methodology for the adoption of Cloud-based Services (IAMCIS)	Menetelmän kehittäminen	Pilvipalveluiden käyttöönottoa koskevan vaikutusanalyysimenetelmän suunnittelu ja arvio
29	Ghorbel A., Ghorbel M., Jmaiel M. (2017)	Privacy in cloud computing environments: a survey and research challenges	Tutkimus	Kryptausmenetelmiä ja -tekniikkaa
30	Hiran K. K.; Henten A.;	Hybrid EduCloud Model in Higher	Kyselytutkimus, 30 vastaajaa, Etiopia	Laadittu 5-vaiheinen malli pilvipalveluiden käyttöönotosta korkeakouluissa

	Shrivas M. K.; Doshi R. (2018)	Education: The case of Sub-Saharan Africa, Ethiopia		
31	Hiran K.K., Henten A. (2020)	An integrated TOE–DoI framework for cloud computing adoption in the higher education sector	Tapaustutkimus, 500 vastaajaa, Etiopia	Organisaation valmius ja ylimmän johdon tuki tärkeimmät edistäjät
32	Kuiper E.; Van Dam F.; Reiter A.; Janssen M. (2014)	Factors influencing the adoption of and business case for Cloud computing in the public sector	Soveltava tutkimus	Suhteellinen hyöty ja kustannussäästöt tärkeimmät pilvikäyttöönoton edistäjät
33	Kumar D., Samalia H.V., Verma P. (2017)	Exploring suitability of cloud computing for small and medium-sized enterprises in India	Tutkimus	PK-yritysten pilvikäyttöönottoihin vaikuttavat eniten ylimmän johdon tuki, kilpailupaineet ja turvallisuusseikat
34	Kuo C.; Kang Y. (2018)	A Study of Continuance Intention to Adopt Cloud Services	Online-kysely, 313 vastaajaa, Taiwan	Yksilökäyttäjien kokemuksia (IS success model)
35	Kyriakou N., Loukis E.N. (2019)	Do strategy, processes, personnel and technology affect firm's propensity to adopt cloud computing?	Empiirinen tutkimus	Organisaation strategiset valinnat edistävät käyttöönottoja. (esim. ICT-kustannusten vähentämisstrategia).
36	Lansing J., Siegfried N., Sunyaev A.,	Strategic signaling through cloud service certifications	Tutkimus	Arvioita erilaisten sertifiointien hyödyistä palveluntuottajille ja päätöksentekijöille.

	Benlian A. (2019)			
37	Lian J.-W. (2015)	Critical factors for cloud-based e-invoice service adoption in Taiwan	Online-kyselytutkimus, 80 vastaajaa, Taiwan	Käytön helppous, sosiaalinen vaikutus ja luottamuskysymykset vaikuttavat merkittävästi sähköisten palveluiden käyttöhalukkuuteen
38	Lim N., Grönlund Å., Andersson A. (2015)	Cloud computing: The beliefs and perceptions of Swedish school principals	Tutkimus, 342 rehtoria, Ruotsi	Internetin välityksellä laaja käyttömahdollisuus tukee tietovarantojen sujuvaa käyttöä, mutta tietoturvallisuus askarruttaa
39	Liu Y., Sun Y., Ryoo J., Rizvi S., Vasilakos A.V. (2015)	A survey of security and privacy challenges in cloud computing: Solutions and future directions	Tutkimus	Tietoturvallinen käyttö merkittävin haaste. Teknisten tietoturvaratkaisuiden kehitys viivästyttää käyttöönottoa
40	Loukis E. ; Kyriakou N. (2015)	Organizational Factors Affecting Propensity to Adopt Cloud Computing	Tutkimus, jossa aineisto 676 eurooppalaisesta yrityksestä	Yrityksen strategia, koko ja resurssit vaikuttavat
41	Loukis E., Arvanitis S., Kyriakou N. (2017)	An empirical investigation of the effects of firm characteristics on the propensity to adopt cloud computing	Tutkimus 2, jossa aineistona 676 eurooppalaista lasi-, keramiikka- ja sementtialan yritystä	Erikoistuneen ICT-henkilöstön palkkaaminen ja viestintätekniikan ulkoistaminen tuottavat myönteisiä vaikutuksia yrityksen aikomukseen ottaa käyttöön pilvipalveluita
42	Luna J.; Suri N.; Iorga M.; Karmel A. (2015)	Leveraging the Potential of Cloud Security Service-Level Agreements through Standards	Tutkimus ja analyysi pilviturvallisuussovellusten määrittelystä ja käytöstä	Riskienhallintaprosessin täytyy tunnistaa ongelmat, lieventää niitä ja seurata aktiivisesti. Vastuun ulkoistus myös pilvipalveluntarjoajalle

43	Masana N.; Muriithi G. M. (2019)	Adoption of an Integrated Cloud-Based Electronic Medical Record System	Tutkimus, terveydenhuoltoalan toimijat, Etelä-Afrikka	Suhteellinen etu, tietoturvaongelmat, ylimmän johdon tuki ja organisaation valmius vaikuttivat eniten sähköisen potilastietojärjestelmän käyttöönottoon
44	Minhaj N.; Islam M. H. (2016)	Cloud adoption in industrial setup of Pakistan	Tutkimus pilvimallien soveltuvuudesta	Tarve on yksityiselle, sekä julkiselle ja edelleen hybridipilviratkaisulle
45	Miorandi D.; Rizzardi A. ; Sicari S.; Coen-Porisini A. (2019)	Sticky Policies: A Survey	Tutkimus sensitiivisen datan tietoturvakäytännöistä	Pilvipalveluiden turvallisuutta ja yksityisyyttä parantavat turvallisuuskäytännöt (Sticky policies) sensitiiviselle datalle.
46	Mishra B.; Jena D. (2019)	Security of Cloud Storage	Tutkimus, Pilven tietoturvallisuusongelmat ja keinoja tavoitteiden saavuttamiseen	Tuloksina muun muassa luottamuksen parantamista tukevaa pohdintaa.
47	Opara-Martins J., Sahandi R., Tian F. (2016)	Critical analysis of vendor lock-in and its impact on cloud computing migration	Kyselytutkimus, 114 IT-ammattilaista, Englanti	Kun tietojenkäsittely viedään pilveen ”lukitusongelma” pahenee. Hyvin laaditut sopimukset sekä standardeihin perustuvat rakenteet ja rajapinnat välttämättömiä.
48	Opara-Martins J.; Sahandi R.; Tian F. (2015)	A Business Analysis of Cloud Computing: Data Security and Contract Lock-In Issues	Tutkimus, 114 IT-ammattilaista, Englanti	Tuottaa vastauksia siihen, miten pilvipalveluiden käyttöönottoon liittyen strategioilla voidaan lieventää riskejä.
49	Oredo J.; Njihia J.; Iraki X. N. (2019)	Institutional Pressures and Cloud Computing Adoption: The Moderating Effect of Organizational Mindfulness	Tutkimus, 60 rahoituslaitosta Etelä-Afrikassa	Toimintaympäristö vaikuttaa pilvipalveluiden käyttöönoton leviämiseen. Bandwagon-ilmiö.

50	Oredo J.; Njihia J.; Iraki X. N. (2017)	Cloud computing adoption in the Kenya's financial sector: An institutional perspective	Tutkimus, 60 rahoituslaitosta Keniassa	Muiden jäljittely ja normatiiviset paineet johtavat pilvipalveluiden käyttöönottoon.
51	Palos-Sanchez P.R., Robina-Ramirez R., Velicia-Martin F. (2019)	What role does corporate governance play in the intention to use cloud computing technology?	Kyselytutkimus, 164 teknologia-alan yritystä, Espanja	Yritysjohtamisella, organisaation menettelytavoilla sekä käytännöillä on vaikutus pilvipalvelun ja siihen liittyvän liiketoimintamallin omaksumiseen.
52	Papadopoulos A. V.; Versluis L.; Bauer A.; Herbst N., ym. (2019)	Methodological Principles for Reproducible Performance Evaluation in Cloud Computing	Menetelmäkehitys	Ehdottavat periaatteita, joita voisi käyttää tutkimuksessa pilvipalveluiden suorituskyvyn mittaamiseen.
53	Porrawatpreyakorn N.; Nuchitprasitchai S.; Viriyapant K.; ym. (2019)	Understanding Key Enablers of Cloud Computing Adoption and Acceptance Over Time	Kyselytutkimus, 490 vastaajaa Thaimaan hallinnosta	Pilven käyttöpolitiikalla, suunnitelmalla ja kustannustehokkuudella oli selkeä vaikutus palvelun hyväksymisen ja omaksumisen suhteen.
54	Prieto-González L., Tamm G., Stantchev V. (2015)	Governance of cloud computing: Semantic aspects and cloud service brokers	Tutkimus	Pilvipalveluiden hallintomalli nähtiin välttämättömänä käyttäjäorganisaation ja pilvipalveluvälittäjän välisissä suhteissa.
55	Priyadarshinee P., Raut R.D., Jha M.K., Kamble S.S. (2017)	A cloud computing adoption in Indian SMEs: Scale development and validation approach	Kyselytutkimus, 110 PK-yritystä, Intia	Muodostivat yhdeksän keskeistä aihealuetta sisältävän mallin, jota yritys voi hyödyntää arvioidessaan pilvikäyttöönottopäätöstä suunnitellessaan.

56	Rahi S.B., Bisui S., Misra S.C. (2017)	Identifying the moderating effect of trust on the adoption of cloud-based services	Kyselytutkimus, 188 vastaajaa, Intia	Luottamukseen ja turvallisuuteen liittyvät tekijät hillitsevät, vaikkakaan eivät estä pilvikäyttöönottopäätöstä, sillä hyödyt nähdään niin merkittäviksi.
57	Ratten V. (2015)	Factors influencing consumer purchase intention of cloud computing in the United States and Turkey	Kyselytutkimus, opiskelijat Turkki ja USA	Koettu helppokäyttöisyys ja käytännöllisyys sekä innovaation ja suorituskyvyn odotus keskeisimmät vaikuttajat molemmissa maissa.
58	Sabi H.M., Uzoka F.-M.E., Langmia K., Njeh F.N. (2016)	Conceptualizing a model for adoption of cloud computing in education	Online-tutkimus, pilottivaihe, 19 yliopiston työntekijää, Saharan eteläpuolinen Afrikka	Turvallisuusnäkökulmat olivat keskeisimpiä seikkoja.
59	Sabi H.M., Uzoka F.-M.E., Langmia K., Njeh F.N., Tsuma C.K. (2018)	A cross-country model of contextual factors impacting cloud computing adoption at universities in sub-Saharan Africa	Kyselytutkimus, 355 ICT-asiantuntijaa ja päätöksentekijää.	Sosiokulttuuriset tekijät, demonstroinnin tarve ja tietoturvallisuus olivat tärkeimmät seikat vaikuttamassa käyttöönottopäätöksiin
60	Senarathna I., Wilkin C., Warren M., Yeoh W., Salzman S. (2018)	Factors that influence adoption of cloud computing: An empirical study of Australian SMEs	Onkine-kyselytutkimus, 149 PK-yritystä, Australia	Organisaatioiden kyvykkyyden parantamiseen johtavat tekijät vaikuttivat käyttöönottopäätöksiin merkittävämmin, kuin riskeihin liittyvät hillitsevät tekijät.
61	Senyo P.K., Effah J., Addae E. (2016)	Preliminary insight into cloud computing adoption in a developing country	Kyselytutkimus, 305 organisaatiota, Ghana	Päätöksessä merkittävää: suhteellinen etu, turvallisuusasiat, ylimmän johdin tuki. Vähäpätöisiä: yrityksen koko, yhteensopivuus ja sääntelyn tuki.

62	Sfondrini N. ; Motta G. ; You L. (2015)	Service level agreement (SLA) in Public Cloud environments: A Survey on the current enterprises adoption	Kyselytutkimus, 58 migraation tehnyttä eri toimialan yritystä, Kiina	Ydinliiketoiminnan sovelluksia ei ole viety pilveen. SLM:t vaativat selkeyttämistä ja jäsentämistä. Valvontakyky vain palveluntuottajalla itsellään. Yleisesti hyväksytyt standardit vielä puuttuvat
63	Sfondrini N.; Motta G. ; Longo A. (2018)	Public Cloud Adoption in Multinational Companies: A Survey	Haastattelututkimus, jossa yli 60:sta monikansallisesta yrityksestä IT-managereja ja pilviarkkitehtejä.	Monikansalliset yritykset kokevat, etteivät palveluntuottajat kykene vielä käsittelemään turvallisuuden, säännösten ja suorituskyvyn hallinnan kriittisiä seikkoja.
64	Sharma V., Srivastava G.M.S. (2016)	Evolution and present status of cloud computing: A comprehensive analysis	Kirjallisuuskatsaus, jonka tausta-aineistona mm. IT-ammattilaisille RightScalen (2014) suorittamia kyselyjä.	Turvallisuus on edelleen kriittinen kysymys jota on käsiteltävä lisää, jotta pilvipalvelut jatkaisivat menestyspolulla.
65	Shee H., Miah S.J., Fairfield L., Pujawan N. (2018)	The impact of cloud-enabled process integration on supply chain performance and firm sustainability	Kyselytutkimus, data kerätty 105 vähittäiskaupan yrityksen otoksesta. Australia	Pilvipohjaisella tekniikalla on positiivinen vaikutus toimitusketjujen integraatioihin. Suorituskyky paranee ja yritystoiminnan vakaus lisääntyy.
66	Shin J.; Jo M.; Lee J.; Lee D. (2014)	Strategic Management of Cloud Computing Services: Focusing on Consumer Adoption Behavior	Kyselytutkimus, 400 vastaajaa, Korea	Palvelumaksu ja vakaus ovat kriittisimmät käyttöönottoon vaikuttavat tekijät.

67	Singh A.; Sharma S.; Kumar S. R.; Yadav S. A. (2016)	Overview of PaaS and SaaS and its application in cloud computing	Online-kysely, vastaajien määrä puuttuu,	SaaS:a käytetään enemmin kuin PaaS:ia mutta Google Apps on käytetyin.
68	Sirohi P.; Agarwal A. (2015)	Cloud computing data storage security framework relating to data integrity, privacy and trust	Viitekehyksen kehitys	Ehdotettu malli perustuu 3-tasoiseen todennusmekanismiin datan suojauksen parantamiseksi vanhaan perinteiseen järjestelmään verrattuna. Lisää läpinäkyvyyttä vähentäen tietoturvauhkia pilviympäristössä.
69	Stieninger M., Nedbal D., Wetzlinger W., Wagner G., Erskine M.A. (2018)	Factors influencing the organizational adoption of cloud computing	Online-kyselytutkimus, 203 pilviosaajaa vastaajina	Yhteensopivuus, suhteellinen etu, turvallisuuden ja luottamuksen kysymykset sekä helppokäyttöisyys johtavat positiiviseen asenteeseen pilvipalveluiden omaksumisessa.
70	Sun X. (2018)	Critical Security Issues in Cloud Computing: A Survey	Kirjallisuuskatsaus	Pilviturvallisuuden kolmea tärkeintä: kyberturvallisuus, verkkoturvallisuus ja tietoturva.
71	Ahmed T, Alhadi N.; Seliaman M. E. (2015)	Acceptance of e-Government Services in Sudan: an Empirical Investigation	Tutkimus	Sähköisten verkkopalveluiden kätevä helppokäyttöisyys ja hyödyllisyys ovat eduksi. Luottamusta ei koettu ongelmaksi.
72	Tariq M. I.; Tayyaba S.; Rasheed H.; Ashraf M. W. (2017)	Factors influencing the Cloud Computing adoption in Higher Education Institutions of Punjab, Pakistan	Kyselytutkimus, 900 korkeakouluopiskelijaa, Pakistan	Pilvipalveluita halutaan käyttöön, ulkoinen paine vaikuttaa, mutta luottamuskysymykset askarruttavat.
73	Wang C., Wood L.C., Abdul-	When traditional information technology	Kyselytutkimus, 110 IT-projektipäällikköä	Muutoshallintasuunnitelmien ja yksityiskohtaisen riskienhallintasuunnitelman

	Rahman H., Lee Y.T. (2016)	project managers encounter the cloud	tärkeimmiltä toimittajayrityksiltä kuten Cisco ja SAP	sisällyttäminen pilvikäyttöönottoihin pidettiin edellytyksenä yksityisyys- ja tietoturvaongelmien huomioimiseen.
74	Yigitbasioglu O.M. (2015)	The role of institutional pressures and top management support in the intention to adopt cloud computing solutions	Kyselytutkimus, 120 IT-päättäjää, valmistavateollisuus ja palveluala, Australia	Ylimmän johdon jatkuvalla tuella on suuri merkitys. Innovaatioiden käyttöönotto voi saada alkunsa kuitenkin organisaatiossa myös alhaalta ylöspäin.
75	Yuvaraj M. (2016)	Determining factors for the adoption of cloud computing in developing countries	Tapaustutkimus, 28 kirjastoammattilaista, Intia	Koettu käytön helppous, hyödyllisyys ja laaja saatavuus ovat pilvikäyttöönoton vahvoja edistäjiä. Turvallisuusriski nähdään tärkeänä, mutta ei estä käyttöä.
76	Gangwar, ym. (2015)	Understanding determinants of cloud computing adoption using an integrated TAM-TOE model	Tutkimus, 280 yritystä (IT-, valmistava teollisuus ja rahoitusala) Intia	Suhteellinen etu, yhteensopivuus, organisaation halukkuus, ylimmän johdon sitoutuminen, harjoittelu ja koulutus ovat tärkeitä muuttujia vaikuttamaan pilvipalveluiden adoptiopäätökseen.
77	Gutierrez ym. (2015)	Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK	Kyselytutkimus, 257 yritys- ja IT-ammattilaista, Englanti	Avaintekijöitä pilvipalveluiden hyväksymispäätöksissä: kilpailullinen paine, monimutkaisuus, teknologiavalmius ja kauppakumppaneiden paine.
78	Hsu P-F., Ray S., Li-Hsieh Y-Y (2014)	Examining cloud computing adoption intention, pricing mechanism, and deployment model	Kyselytutkimus, 200 yritysjohtajia ja tietohallintojohtajia ICT-alalta, Taiwan	Pilviadoptio on vielä alkuvaiheessa. Koetut hyödyt, liiketoiminnan huolet ja IT-kyvykkyydet ovat merkittävin vaikuttaja käyttöönottopäätökselle. Ulkoinen paine ei vaikuta.