Maria Hirvonen

JULKISHALLINNON ORGANISAATION PILVIPALVELUJEN TIETOTURVAN ARVIOINTI

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Hirvonen, Maria
Julkishallinnon organisaation pilvipalvelujen tietoturvan arviointi
Jyväskylä: Jyväskylän yliopisto, 2020, 43 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Seppänen, Ville

Pilvipalvelujen yleistyminen ja niiden käyttöönotto on edelleen kasvava trendi. Julkishallinnossa on vasta viime vuosina tehty koko julkishallintoa koskeva pilvipalvelulinjaus sekä pilvipalvelujen turvallisuuden auditointikriteeristö, jonka avulla julkishallinnon organisaatio voi arvioida omien pilvipalvelujensa turvallisuutta. Tässä kirjallisuuskatsauksena toteutetussa tutkielmassa selvitettiin pilvipalvelujen turvallisuuden arviointikriteeristöön sekä tieteelliseen kirjallisuuteen pohjautuen, millaisia tekijöitä julkishallinnon organisaation tulee ottaa huomioon pilvipalvelujen turvallisuutta arvioitaessa. Tutkielman tuloksena todettiin, että pilvipalvelujen turvallisuutta arvioitaessa tulee kiinnittää huomiota turvallisuusjohtamiseen, henkilöstöturvallisuuteen, fyysisen ympäristön turvallisuuteen, tietoliikenneturvallisuuteen, identiteetin ja pääsyn hallintaan, tietojärjestelmäturvallisuuteen, salaukseen, käyttöturvallisuuteen, siirrettävyyteen ja yhteensopivuuteen sekä muutostenhallintaan ja järjestelmäkehitykseen. Lisäksi tutkielmassa havaittiin, että pilvipalvelujen turvallisuuden arviointikriteeristössä on kattavasti otettu huomioon kirjallisuudessa esiintyviä pilvipalvelujen turvallisuuteen liittyviä tekijöitä.

Asiasanat: pilvipalvelut, tietoturva, tietoturvan arviointi, julkishallinto

ABSTRACT

Hirvonen, Maria
Assessment of a public administration organisation's cloud services security
Jyväskylä: University of Jyväskylä, 2020, 43 pp.
Information Systems science, Bachelor's thesis
Supervisor: Seppänen, Ville

The spread of cloud services and their deployment continues to be a growing trend. The public administration has recently published the cloud service policy for the entire public administration, as well as the Finnish audit criteria for the security of cloud services, which enables a public administration organization to assess their own security with the matter at hand. In this literature review, the aim is to investigate the factors that a public administration organization should take into account when assessing cloud services from the security perspective. As a result of this study, it is stated that attention should be paid to security management, personnel security, physical environment security, telecommunication security, identity and access management, information system security, encryption, operational security, portability and compatibility, as well as change management and system management. In addition, the study shows that regarding the factors related to the security of cloud services, the audit criteria are comprehensively considered.

Keywords: cloud services, information security, security assessment, public administration

KUVIOT

SISÄLLYS

1 JOHDANTO

Pilvipalveluita ja pilvipalveluteknologioita hyödynnetään julkishallinnossa koko ajan entistä enemmän uusien tietojärjestelmien sekä prosessien kehittämisessä (Valtiovarainministeriö, 2018). Pilvipalveluiden etuna on skaalautuvuus, joustavuus sekä mahdollisuus päästä tietoon käsiksi koska ja mistä tahansa hyödyntäen myös kevyitä mobiililaitteita. (Ryan, 2013; Valtiovarainministeriö, 2018). Ramgovindin, Eloffin ja Smithin (2010) mukaan pilvipalvelut tarjoavat markkinoille joustavaa ja skaalautuvaa tietojen varastointia sekä kapasiteettia, joka pystyy joustavasti vastamaan kysyntään ja toisaalta vähentämään fyysisiä investointeja. Erilaisten palvelu- ja toteutusmallien avulla voidaan rakentaa organisaatioille erilaisia toteutuksia (Valtiovarainministeriö, 2018).

Edellä mainittujen syiden vuoksi pilvipalvelujen käyttö yrityksissä on kasvanut 23 prosenttiyksikköä verrattuna viiden vuoden takaiseen käyttöön. Pilvipalvelujen käytön kasvu tarkoittaa, että jopa 74 prosenttia yrityksistä käyttää tällä hetkellä maksullisia pilvipalveluja. (Tilastokeskus, 2019). Vaikka pilvipalveluiden käyttö voi parantaa organisaation tietoturvaa (Valtiovarainministeriö, 2018), ei niiden käyttöönotto tietoturvan näkökulmasta ole täysin ongelmatonta. Cloud Security Alliancen (2017) mukaan 12 suurimman tietoturvauhan joukossa ovat esimerkiksi tietovuodot, palvelun estyminen, järjestelmähaavoittuvuudet sekä kohdistetut hyökkäykset. Kasvava pilvipalvelujen käyttö ja edellä mainitut uhkaesimerkit eivät koske pelkästään yrityksiä. Julkisen sektorin hyödyntäessä entistä enemmän sähköisiä palveluja, on palvelujen saavutettavuus ja tietoturva jokaisen kansalaisen etu. Julkishallinnon datan luonteen vuoksi tietoturvaa voidaan pitää erityisen tärkeänä (Ryoo, Rizvi, Aiken & Kissel, 2014). Datan suojelemisen lisäksi julkishallinnon haasteita ovat esimerkiksi yhteensopivuus, lainsäädäntö sekä hankintaan liittyvä säätely (Alonso, Escalante & Orue-Echevarria, 2016).

Pilvipalvelujen käyttö sekä tietoturva julkishallinnon organisaatioissa on ajankohtainen aihe. Suomi ei ole tässä yksin, sillä pilvipalveluiden käyttö tulevaisuudessa on monelle maalle strateginen valinta (Paquette, Jaeger & Wilson, 2010). Laajemmin tarkasteltuna pilvipalveluiden

käyttöönotolla on paitsi teknisiä seurauksia myös vaikutuksia organisaatioon ja ympäristöön, kuten kansalaisiin ja kansalaisten palveluihin (Alonso ym., 2016). ”Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi” -raportissa todetaan, että verkkoasioinnin kasvu sekä pilvipalveluiden käyttöönotto edellyttää tietoturvavaatimuksien uudelleenarviointia (Lehto, Limnell, Innola, Pöyhönen, Rusi & Salminen, 2017). Raportin julkaisun jälkeen Valtiovarainministeriön julkisen hallinnon pilvipalvelulinjaukset valmistuivat vuonna 2018 ja Liikenne- ja viestintäministeriön alaisen Kyberturvallisuuskeskuksen pilvipalvelujen turvallisuuskriteeristö (PiTuKri) vuonna 2019. Toistaiseksi pilvipalvelujen turvallisuuden auditointikriteeristöön on viitattu hyvin vähän tieteellisissä julkaisuissa ja suomalaisen julkishallinnon pilvipalveluturvallisuudesta ei ole tämän tutkielman kirjoitushetkellä tehty määrällisesti kovinkaan montaa tutkimusta tai aikaisempaa opinnäytetyötä.

Tässä kandidaatintutkielman tarkastellaan *Pilvipalveluiden turvallisuuden arviointikriteeristöä* (Kyberturvallisuuskeskus, 2020) ja sitä, mitä osa-alueita julkishallinnon tulee ottaa huomioon pilvipalveluiden turvallisuutta arvioidessa. Arviointikriteeristön osa-alueita täydennetään tieteellisellä kirjallisuudella. Tutkielman tavoitteena on saada vastaus kysymykseen ”Mitä tekijöitä julkishallinnon organisaation tulee ottaa huomioon käyttämiensä pilvipalveluiden turvallisuutta arvioidessa?”

Tämä tutkielma on toteutettu kirjallisuuskatsauksena. Tutkielman lähdeaineisto on kerätty pääasiassa Jyväskylän yliopiston kirjastosta, Google Scholar- sekä JYKDOK-hakupalvelujen kautta. Julkaisujen ajantasaisuus on pyritty varmistamaan käyttämällä pääosin vuoden 2009 jälkeen julkaistuja tutkimuksia. Sitä aikaisempaa kirjallisuutta on hyödynnetty ainoastaan tapauksissa, joissa julkaistu kirjallisuus on katsottu työn kannalta tarkoituksenmukaiseksi. Artikkelien ja kirjallisuuden valintakriteereinä ovat julkaisuvuoden lisäksi olleet julkaisun taso, vertaisarviointi sekä aiempien viittausten määrä. Julkaisujen tasoa on arvioitu hyödyntäen Julkaisufoorumin hakupalvelua. Julkaisufoorumin tasoluokituksen mukaan on valittu julkaisuja, joiden taso on minimissään yksi (1). Tässä työssä käytössä oleva arviointikriteeristö on haettu Kyberturvallisuuskeskuksen internet-sivuilta (Kyberturvallisuuskeskus, 2020). Kirjallisuuden hakusanoina on käytetty *cloud security*, *cloud computing security*, *cloud security auditing*, *cloud computing*, *information security*, *pilvipalvelut tietoturva*, *tietoturvan osa-alueet*, *cloud security + government*, *cloud security public administration* ja edellä mainittujen hakusanojen yhdistelmiä. Suomen lakiin liittyvissä viittauksissa on hyödynnetty oikeusministeriön oikeudellisen aineiston palvelua Finlexiä. Suomalaiseen julkishallintoon liittyvät artikkelit ja linjaukset on haettu vastuuviraston internet-sivuilta, ja niiden löytämiseen on käytetty Google-hakupalvelua hakusanoilla *julkishallinto pilvipalvelut* ja *pilvipalvelulinjaukset* rajaten hakutulokset suomen kielelle.

Tutkielma koostuu yhteensä viidestä luvusta sisältäen johdannon ja yhteenvedon. Seuraavassa luvussa, joka on tutkielman ensimmäinen

sisältökappale, käsitellään pilvipalveluja yleisesti. Kolmannessa luvussa käydään läpi tietoturvaa yleisesti sekä siihen liittyviä julkishallinnon erityispiirteitä. Viimeisessä sisältöluvussa käsitellään pilvipalvelujen turvallisuutta ja julkishallinnon pilvipalveluturvallisuuden arviointia.

2 PILVIPALVELUT

Tässä luvussa määritellään pilvipalvelut sekä käydään lyhyesti läpi pilvipalvelujen hyötyjä ja palvelu- ja toteutusmalleja. Luvussa tarkastellaan myös julkisen hallinnon pilvipalvelulinjauksia, jotka esittelevät haasteita ja pilvipalvelujen toteutusta julkisen sektorin näkökulmasta.

Tutkimuksissa ja kirjallisuudessa on pilvipalveluille useita eri määritelmiä kontekstista riippuen. Yhden määritelmän mukaan pilvipalvelut tarjoavat ajasta ja paikasta riippumattomat palvelut, jotka mahdollistavat pääsyn kaikkialla internetin kautta käytettävissä oleviin resursseihin, ja niiden tarkoitus on käyttää hajautetut resurssit tehokkaammin ja ratkaista suurempia ongelmia tietotekniikassa (Mell & Grance, 2011; Jadeja & Modi, 2012).

Vaikka pilvipalveluista on tullut trendi vasta 2010-luvulla, on niistä puhuttu jo pidempään. Konseptina pilvipalvelut on esitelty jo useampi vuosikymmen sitten 1960-luvulla. (Jadeja & Modi, 2012). Pilvipalvelu terminä on peräisin 1990-luvulta, jolloin alettiin käyttämään virtuaalista yksityistä verkkoa (VPN). (Kaufman, 2009).

2.1 Pilvipalveluille tyypilliset ominaisuudet

Mell ja Grance (2011) ovat määritelleet pilvipalveluille tyypillisiä ominaisuuksia, joihin on viitattu laajasti pilvipalveluihin liittyvissä tutkimuksissa. Ensimmäinen tyypillinen ominaisuus Mellin ja Grancen (2011) mukaan on itsepalvelumahdollisuus. Sillä tarkoitetaan palvelua, jossa asiakas pystyy itse tilaamaan ja muokkaamaan pilvipalvelun ominaisuuksia, kuten tallennustilaa, ilman minkäänlaista ihmiskontaktia palveluntarjoajaan. Toisena ominaisuutena Mell ja Grance (2011) esittelevät laajan pääsyn tietoverkkojen kautta. Tällä tarkoitetaan sitä, että palvelut ovat saatavilla internetissä verkon yli hyödyntäen erilaisia laitteita, kuten älypuhelimia.

Kolmas ominaisuus on resurssien jako, joka puolestaan tarkoittaa jaetun alustan politiikkaa. Jaettu alusta toimii siten, että useat palveluntarjoajan asiakkaat hyödyntävät samaa fyysistä alustaa, jossa resursseja jaetaan ja

uudelleen jaetaan asiakkaiden tarpeen mukaisesti. (Mell & Grance, 2011). Jaettu alusta tarkoittaa myös sitä, että palvelua ostavalla asiakkaalla ei tyypillisesti ole mahdollisuutta tietää tai kontrolloida datan tarkkaa fyysistä sijaintia. Asiakas voi kuitenkin tietää suuntaa-antavan sijainnin, kuten maan, kaupungin tai kaupunginosan, jossa data säilytetään. (Mell & Grance, 2011).

Joustavuus on yksi Mellin ja Grancen (2011) pilvipalveluille määrittelevä ominaisuus. Asiakas voi tarpeensa mukaan ostaa nopeasti ja jopa automaattisen prosessin kautta itselleen lisää tarvittavia resursseja, joita on tarjolla lähes rajattomasti. Viimeisenä tyypillisenä ominaisuutena on mitattavat palvelut. Sillä Mell ja Grance (2011) tarkoittavat automaattista kontrollia ja palvelujen optimointia perustuen mitattaviin arvoihin, kuten tallennustilaan, kaistanleveyteen tai aktiiviseen käyttäjämäärään. Resurssien käyttöä voidaan valvoa, kontrolloida ja raportoida, mikä tuo läpinäkyvyyttä asiakkaalle että palveluntarjoajalle. (Mell & Grance, 2011).

2.2 Palvelumallit

Kirjallisuudessa pilvipalvelumalleja esiintyy säännönmukaisesti yleensä vähintään kolme. Näiden lisäksi kirjallisuudessa esitetään myös muita malleja, jotka eivät esiinny yhtä usein ja säännönmukaisesti. (Elsenpeter, Velte & Velte, 2010, 69-76; Mell & Grance, 2011; Xun, 2011). Tsain, Sunin ja Balasooriyan (2010) mukaan palvelumalleista voidaan muodostaa hierarkkinen näkemys, jossa ylempi palvelumalli sisältää myös alemman ominaisuudet.

Tsain ym. (2010) mukaan kolme palvelumallia hierarkkisesti järjestettynä ovat seuraavat:

- Infrastruktuurialusta (Infrastructure as a Service, IaaS)
- Sovellusalusta (Platform as a Service, PaaS)
- Ohjelmistoalusta (Sofware as a Service, SaaS)

Alimmalla kerroksella eli infrastruktuurialustalla tarkoitetaan sitä, että asiakas käyttää IT-infrastruktuurin palveluita, kuten tallennustilaa, verkkoja ja muita tärkeitä tietoteknisiä resursseja pilvipalveluna ja pystyy ottamaan käyttöön sekä hallitsemaan niitä. (Dillon, Wu & Chang, 2010; Zissis & Lekkas, 2010; Tsai ym., 2010). Mell ja Grance (2011) nostavat palomuurin esimerkiksi IaaS-palvelusta.

Infrastruktuurikerroksen päälle rakennetaan puolestaan sovellusalusta. Mell & Grance (2011) määrittelevät sovellusalustan siten, että pilvipalvelun asiakas voi lisätä ohjelmistoalustalle joko itse tehtyjä ja tai ostettuja ohjelmistoja hyödyntäen ohjelmointikieliä, -kirjastoja ja -palveluja. Asiakas ei itse pääse vaikuttamaan tai kontrolloimaan alustan infrastruktuuria, kuten palvelimia, käyttöjärjestelmää tai tallennustilaa (Mell & Grance, 2011).

Sovellusalustan päällä on kaikkein ylimmäinen taso, ohjelmistoalusta. Ohjelmistoalustan erityispiirteenä on, että yleensä alusta ja

ohjelmisto jaetaan muiden käyttäjien kanssa, päivitykset tulevat automaattisesti pilvipalvelun kautta ja erillisiä lisenssejä ei tarvitse ostaa. Ohjelmistoalustan palveluja käytetään yleensä selaimen kautta ja ne voidaan integroida osaksi muuta organisaation ympäristöä. (Tsai ym., 2010). Esimerkkejä ohjelmistoalustapalveluista ovat esimerkiksi Google Docs ja Google Mail (Mell & Grance, 2011).

2.3 Toteutusmallit

Jadejan ja Modin (2012) mukaan pilvipalvelua suunnitellessa on tärkeää määritellä myös sen toteutustapa. Palvelumallista riippumatta toteutusmallit voidaan jakaa neljään yleisesti kirjallisuudessa tunnistettuun osaan (Dillon ym., 2010; Mell & Grance, 2011). Neljä osaa ovat:

- julkinen
- yksityinen
- yhteisöllinen
- hybridipilvi

Julkinen pilvipalvelu antaa käyttäjälle mahdollisuuden saavuttaa pilvipalvelun käyttöliittymä esimerkiksi selaimen yli (Jadeja & Modin, 2012). Julkisen pilvipalvelun omistaa ja sitä hallinnoi yleensä jokin yritys, yhteisö tai julkinen organisaatio. Julkinen pilvipalvelu sijaitsee yleensä fyysisesti pilvipalvelun tarjoajan tiloissa. (Mell & Grance, 2011).

Mellin ja Grancen (2011) mukaan yksityisellä pilvipalvelulla tarkoitetaan ainoastaan yhden organisaation käytössä olevaa palvelua, jonka omistaa ja jota hallinnoi joko organisaatio itse, jokin kolmas osapuoli tai yhdistelmä molempia. Yksityisen pilvipalvelun käyttöönottoon voi olla useampia syitä, kuten esimerkiksi tietoturvan varmistaminen sekä mahdollisuus kontrolloida itse organisaatiolle kriittisiä palveluja (Dillon ym., 2010).

Organisaatioiden jakaessa pilvipalveluiden infrastruktuurin, vaatimukset sekä politiikan, puhutaan yhteisöllisestä pilvipalvelusta (Jadeja & Modin, 2012). Pilvipalvelua voi hallita joko jokin yhteisöllisen pilvipalvelun käyttäjäorganisaatio, jokin kolmas osapuoli tai jonkinlainen yhdistelmä molemmista vaihtoehdoista (Jadeja & Modin, 2012; Mell & Grance, 2011).

Hybridipilvi on puolestaan yhdistelmä yksityisestä sekä julkisesta pilvipalvelusta. Ramgovind ym., (2010) määritelmän mukaan hybridipilvi on yksityinen pilvipalvelu yhdistettynä yhteen tai useampaan ulkoiseen pilvipalveluun. Ulkoisella pilvipalvelulla voidaan tarkoittaa yhtä tai useampaa minkä tahansa tyyppistä pilvipavelua, kuten yhteisöllistä tai julkista (Dillon ym., 2010). Hybridipilven hyödyt organisaatiolle ovat esimerkiksi resurssien tehokkaampi hyödyntäminen sekä julkista pilvipalvelua parempi tietoturva,

säilyttäen mahdollisuuden päästä tiettyihin osiin myös internetin yli selaimella (Ramgovind ym., 2010; Dillon ym., 2010).

2.4 Julkisen hallinnon pilvipalvelulinjaukset

Valtiovarainministeriö julkaisi vuonna 2018 julkishallinnon organisaatioita koskevan pilvipalvelulinjauksen, jonka tarkoituksena on tukea julkisten organisaatioiden päätöksentekoa uusia palveluja hankittaessa. Linjauksen keskeisimpiä tavoitteita on palvelujen tuottamisen riskienhallinta ja riskiarvioiden tukeminen, käyttöönoton mahdollistaminen ja reunaehtojen määrittäminen, joita noudattamalla organisaatiot voivat turvallisesti hyödyntää pilvipalveluja (Valtiovarainministeriö, 2018).

Linjauksen (Valtiovarainministeriö, 2018) taustalla olevia keskeisimpiä teemoja on myös pilvipalveluiden haasteet. Taustaksi ja varsinaisen linjauksen haasteiksi määriteltiin ei-julkisten tietojen käsittely, toiminnan jatkuvuuteen liittyvät riskit, tietoturvan ja tietosuojan toteutuminen tiedon sijainnista ja hallinnasta riippuen, riskienhallinnan moniulotteisuus sekä yksipuoliset sopimusehdot (Valtiovarainministeriö, 2018).

Linjaus (Valtiovarainministeriö, 2018) koostuu seuraavasta seitsemästä kohdasta, joissa kannustetaan julkisia organisaatioita pilvipalvelujen käyttöön edellyttäen asianmukaista tietoturvaa ja -suojaa.

1. Pilvipalveluita tulee käsitellä kuin mitä tahansa muutakin ICT-palvelun hankintaa tai muutosta

2. Pilvipalveluissa on kiinnitettävä erityistä huomiota sopimuksiin, palvelun jatkuvuuden turvaamiseen ja tiedon saatavuuteen

3. Pilvipalvelun tulee täyttää hankkivan osapuolen palveluhyöty ja -takuuvaatimukset

4. Mikäli pilvipalvelu tai pilvipalveluteknologia tarjoavat parhaan palveluhyödyn ja-takuun, eikä muita esteitä ole, tulisi se ensisijaisesti valita

5. Pilvipalveluiden palveluhyötyä ja -takuuta tulee arvioida säännöllisesti sekä oleellisten sopimusehtojen muuttuessa.

6. Julkisen tiedon käsittelyä ei rajoiteta

7. Ei-julkista tietoa voi käsitellä julkisessa pilvipalvelussa, kun tietoturva ja -suoja on asianmukaisesti toteutettu ja todennettu

(Valtiovarainministeriö, 2018).

3 TIETOTURVA

Tässä kappaleessa käsitellään tietoturvaa yleisesti sekä tietoturvan osa-alueita. Lisäksi käsitellään tietoturvaan ja tiedonkäsittelyyn liittyen julkishallinnon erityispiirteet, kuten salassa pidettävä tieto ja tiedon julkisuus.

Vaikka tietoturva ja tietoturvariskit ovat viime vuosikymmenenä tulleet esille, ei tietoturva ja sen tärkeys ole uusi keksintö. Blakleyn, McDermottin ja Geerin (2001) mukaan tietoturvan merkitys kasvaa suhteessa organisaation riippuvuuteen käytettävästä tietotekniikasta. CIA-mallia (confidentiality, integrity, availability) pidetään tietoturvaan liittyvien elementtien standardina (Whitman ja Mattord, 2009). Se tuo tietoturvalle kolme yhteistä elementtiä: luottamuksellisuuden, eheyden ja saatavuuden, jotka esiintyvät yleisesti alan kirjallisuudessa (Zissis & Lekkas, 2010; Ramgovind ym., 2010).

Kolmen edellä mainitun elementin lisäksi Anderson (2003) tuo esille, että pelkästään CIA-malli ei riitä kattamaan tietoturvan määritelmää, vaikka sitä yleisesti kattavana määritelänä pidetäänkin. Anderson (2003) ehdottaa, että tietoturva määriteltäisiin varmuutena siitä, että riskit ja valvonta ovat tasapainossa. Tasapainon saavuttamisen lisäksi tietoturvaa voi lähestyä ja määritellä tietoturvapolitiikan kautta. Tietoturvapolitiikka määrittelee, kenellä on oikeus tehdä ja mitä (Blakley ym., 2001).

Von Solmsin ja Van Niekerkin (2013) mukaan luottamuksellisuudessa on kyse ennen kaikkea siitä, että määritellään, kenellä on oikeus päästä tietoon käsiksi. Luottamuksellisuus voi toteutua ainoastaan silloin, kun suojeltua tietoa voivat tarkastella vain sellaiset henkilöt, joilla on siihen oikeus (Zissis & Lekkas, 2010). Pääsyoikeuksien lisäksi luottamuksellisuuteen voidaan ottaa myös toinen näkökulma, eli tiedon salaaminen, silloin kun se on tarkoituksenmukaista (Posthumus & Von Solms, 2004).

Eheydellä tarkoitetaan tiedon suojelemista kaikkea asiatonta muokkaamista tai tuhoamista vastaan (Liu ym., 2011, 20). Eheys sisältää myös tiedon kiistämättömyyden, eli mahdollisuuden varmistaa myös jälkikäteen tiedon lähettäjään, vastaanottajaan tai itse tietoon liittyvät tapahtumat (Liu ym., 2011, s. 20; Sanastokeskus, 2004). Posthumusin ja Von Solmsin (2004) mukaan

eheydellä on erityisen tärkeä rooli tietoturvassa päätöksenteon vuoksi. Informaatio on päätöksenteossa myös tärkeää: mikäli data ei ole tarkkaa tai täydellistä, voi se johtaa väärin perustein tehtyihin päätöksiin (Posthumus & Von Solms, 2003).

Puhuttaessa minkä tahansa palvelun tietoturvasta, on saatavuuden merkitys suuri. Ramgovind ym. (2010) määrittelevät saatavuuden yhdeksi kaikkein kriittisimmäksi tietoturvan osaksi, joka tulisi varmistaa aina palvelutasosopimuksella. Saatavuus merkitsee sitä, että tarvittavat resurssit ovat oleellisten osapuolten saavutettavissa ja käytettävissä silloin, kun niitä tarvitaan (Posthumus & Von Solms, 2004).

Lähestymistavasta riippumatta, tietoturvasta ei voi koskaan lakata huolehtimasta. Blakley ym. (2001) esittävät, että tietoturvasta huolehtiminen on kuin ympyrä. Jokaisen kierroksen jälkeen on aika tehdä parannuksia edellisen kierroksen perusteella (Blakley ym., 2001).

3.1 Tietoturvan osa-alueet

Tietoturva voidaan jakaa yhteensä kahdeksaan osa-alueeseen: hallinnollinen tietoturva, fyysinen tietoturva, henkilöstöturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus, tietoliikenneturvallisuus ja käyttöturvallisuus (Hakala, Vainio & Vuorinen, 2006, 10; Andreasson & Koivisto, 2013, 52).

Hakalan ym. (2006, 10) mukaan hallinnollisen tietoturvan tarkoitus on varmistua tietoturvan kehittämisestä ja johtamisesta. Hallinnollisen tietoturvan ylläpito on yleensä organisaation tietohallinnon tehtävä ja siinä on erityisen tärkeässä asemassa organisaation tekemät sopimukset ja lainsäädäntö (Hakala ym., 2006, 11).

Fyysisen turvallisuuden tarkoituksena on estää fyysisesti tapahtuva tietojen luvaton käyttö ja varastaminen sekä huolehtia fyysisiin ongelmatilanteisiin liittyvistä toimenpiteistä, kuten sähkökatkoihin varautumisesta (Watkins, 2013). Fyysisen turvallisuuden tarkoitus voidaan tiivistää tarkoitukseen suojella organisaatiota fyysisiltä uhilta (Stewart, Chapple & Gibson, 2012). Se kattaa laajasti kaikki kiinteistöihin ja niissä kulkemiseen liittyvät osa-alueet, kuten vartioinnin, paloturvallisuuden ja jopa tietoaineistoja sisältävien lähetysten turvallisuuden (Andreasson & Koivisto, 2013, 53).

Henkilöstöturvallisuudella tarkoitetaan henkilöstön mahdollisuutta käyttää tietojärjestelmiä ja toisaalta myös rajata tarpeellisin osin oikeuksia organisaation järjestelmiin ja tietoihin (Hakala ym., 2006, 11). Oikeuksien jakamista voidaan kutsua myös identiteetin ja käyttövaltuuksien hallinnaksi. Sillä tarkoitetaan toimintatapoja, sääntöjä ja välineitä, joita hyödyntäen hallinnoidaan tietojärjestelmien käyttöä (Andreasson & Koivisto, 2013, 106).

Tietoaineiston turvallisuuteen kuuluu tiedon elinkaareen liittyvät toimenpiteet: säilyttäminen, varmistaminen, palauttaminen ja tuhoaminen

(Hakala ym., 2006, 11). Siihen kuuluvat sekä digitaaliset asiakirjat että muut, kuten paperiset asiakirjat (Hakala ym., 2006, 11).

Tietoliikenneturvallisuuden osa-alue huolehtii tietoliikennekomponenttien ja -protokollien turvallisuudesta (Stewart ym., 2012). Protokollilla tarkoitetaan standardoituja sääntöjä ja rajoituksia, joiden mukaan dataa siirretään tietoverkossa (Stewart ym., 2012). Tietoverkkoturvallisuus sisältää myös tietoverkkoliikenteen hallintaan ja kontrollointiin tarkoitetut palomuurit (Stewart ym., 2012).

Ohjelmistoturvallisuudella tarkoitetaan ohjelmiston elinkaareen liittyviä asioita, kuten sovellusten yhteensopivuus, testaus, toiminnan luotettavuus ja virheettömyys sekä ohjelmistoversioiden ja lisenssien hallintaan (Hakala ym., 2006, 11-12).

Laitteistoturvallisuus tarkoittaa fyysisten laitteiden elinkaaresta huolehtimista sekä laitteiden käytöstä johtuvien riskien minimoimista (Hakala ym., 2006). Elinkaaresta huolehtimiseen kuuluvat esimerkiksi asennukseen, takuuseen, huoltoon ja ylläpitoon sekä mahdolliseen tukipalveluun ja elinkaaren päättymiseen liittyvät asiat (Andreasson & Koivisto, 2013, 64).

Käyttöturvallisuuden tarkoituksena on varmistua tietojärjestelmiä käytettävän turvallisesti (Ruohonen, 2002, 5). Järjestelmän käyttäminen huolimattomasti, välinpitämättömästi tai vilpillisesti voi vaarantaa tietojärjestelmän käyttöturvallisuuden (Ruohonen, 2002, 5).

3.2 Tietoturva julkishallinnossa

Tietoturvan ja tiedonhallinnan erityispiirre julkishallinnossa on erillinen säädetty julkisuuslaki eli laki viranomaisen toiminnan julkisuudesta. Jotta julkisuusperiaate ja tietoturvallinen käsittely toteutuisi, ja jotta viranomaisten tietoaineistot pysyisivät yhdenmukaisena, vuoden 2020 alusta astui voimaan laki julkisen hallinnon tiedonhallinnasta (Laki julkisen hallinnon tiedonhallinnasta, 906/2019). Julkisuuslain ensimmäinen pykälä määrittelee, että kaikki viranomaisasiakirjat ovat julkisia, jollei julkisuuslaissa tai jossakin muussa laissa määritellä toisin (Laki viranomaisen toiminnan julkisuudesta, 621/1999, 1 §). Viranomaisella laissa tarkoitetaan esimerkiksi valtion hallintoviranomaisia, virastoja, laitoksia ja lainkäyttöelimiä (Laki viranomaisen toiminnan julkisuudesta, 621/1999, 4 §). Yksityisen organisaation omistamaan tietoon ei kohdistu julkisuuteen liittyviä lakeja, eli organisaatio voi itse päättää tiedon julkaisusta tai julkaisematta jättämisestä.

Julkisuuslain tarkoitus määritellään lain kolmannessa pykälässä seuraavasti: « Tässä laissa säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. « (Laki viranomaisen toiminnan julkisuudesta, 621/1999, 3 §).

Salassa pidettävän asiakirjan julkistaminen on kielletty, mikäli salassapidosta on säädetty joko julkisuuslain tai muun lain perusteella tai se on lakiin perustuen määrätty salassa pidettäväksi tai se sisältää vaitiolovelvollisuuden alaisia tietoja (Laki viranomaisen toiminnan julkisuudesta, 621/1999, 22 §). Salassa pidettävä asiakirja on aina merkittävä salassa pidettäväksi (Laki viranomaisen toiminnan julkisuudesta, 621/1999, 25 §). Mikäli asiakirjaa pidetään salassa pidettävänä viranomaisen toiminnan julkisuudesta annetun lain 24§:n perusteella, tulee sille tehdä turvallisuusluokan määrittely (Laki julkisen hallinnon tiedonhallinnasta, 906/2019, 18§).

Turvallisuusluokkia on yhteensä neljä: I, II, III ja IV (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 3§). Turvallisuusluokka määritellään sen perusteella, millaista vahinkoa tiedon oikeudeton paljastuminen tai käyttö voi aiheuttaa (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 3§). Turvallisuusluokka IV (TL IV) on kaikkein lievin ja asiakirja määritellään luokkaan IV silloin, kun sen paljastuminen tai käyttö aiheuttaa vain lievää vahinkoa. Luokka neljä merkitään asiakirjaan merkinnällä ”KÄYTTÖ RAJOITETTU.” (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 3§). Asiakirja luokitellaan luokkaan III siinä tapauksessa, että sen paljastuminen tai käyttö aiheuttaa vahinkoa suojattavalle edulle. Turvallisuusluokka III (TL III) merkittään asiakirjaan ”LUOTTAMUKSELLINEN.” (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 3§). Turvallisuusluokalle II (TL II, SALAINEN) on ominaista, että salassa pidettävän asiakirjan paljastuminen tai käyttö aiheuttaa merkittävää vahinkoa suojattavalle edulle (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 3§). Korkein luokitus, turvallisuusluokka I (TL I, ERITTÄIN SALAINEN), lisätään asiakirjaan silloin, kun tiedon paljastuminen tai käyttö voi aiheuttaa erityisen suurta vahinkoa (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 3§).

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, 7§-15§) asettaa myös vaatimuksia asiakirjojen luovuttamiselle, monitasoiselle suojaamiselle, asiakirjojen käsittelyoikeuksille, turvallisuusalueille sekä asiakirjan lukemiselle ja siirtämiselle.

3.2.1 Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (VAHTI)

Valtion julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, eli VAHTI on asetettu vastaamaan digitaalisen turvallisuuden strategisesta ohjauksesta sekä digitaalisen turvallisuuden ja digitalisaation edistämisestä (Valtiovarainministeriö, 2020).

Digi- ja väestötietovirasto (2020) nimeää VAHTI:lle yhteensä neljä päätavoitetta:

- ICT-palvelujen turvaaminen julkisessa hallinnossa
- Turvallinen mahdollistaminen uusien teknologioiden käyttöönotolle
- Julkiseen hallintoon luottamuksen säilyttämisen ylläpitäminen kansalaisten ja sidosryhmien keskuudessa
- Kansallinen ja kansainvälinen yhteistyö elinkeinoelämän kanssa

(Digi- ja väestötietovirasto, 2020).

Valtiovarainministeriö (2020) esittää VAHTI-ryhmän keskeisiksi tehtäviksi seuraavat asiat:

- Julkisen hallinnon digitaalisen turvallisuuden strateginen riskiarvio
- Kansallisen strategisen tason digitaalisen turvallisuuden yhteistoimintamallin luominen ja koordinoiminen
- Julkisen hallinnon digitaalisen turvallisuuden tilannearvio
- Digitaalisen turvallisuuden palvelujen arviointi, ohjaaminen, koordinointi ja valvonta

(Valtiovarainministeriö, 2020).

Digi- ja väestötietovirasto (2020) kuvaa VAHTI:n keskeiseksi tekemiseksi digitaalisen turvallisuuden edistämisen ja palvelutuotannosta vastaavien organisaatioiden koordinoinnin. Digitaaliseen turvallisuuteen liittyvät periaatepäätökset, kehittämisohjelmat ja hankkeiden toimeenpano on VAHTI:n vastuulla (Digi- ja väestötietovirasto, 2020). Lisäksi VAHTI:n keskeinen tehtävä on edistää tietoturvallista kulttuuria, digitaalisen turvallisuuden osaamista sekä asennetta digitaalista turvallisuutta kohtaan (Digi- ja väestötietovirasto, 2020).

3.2.2 Tietoturvallisuuden auditointikriteeristö viranomaisille (Katakri)

Salassapidettävän tiedon suojaamista varten on kehitetty tietoturvallisuuden auditointikriteeristö viranomaisille, eli Katakri (Puolustusministeriö, 2015). Katakri on kansallisista säädöksistä ja kansainvälisistä velvoitteista koostuva vähimmäisvaatimusten listaus, joka ei itsessään aseta tietoturvallisuudelle ehdottomia vaatimuksia (Puolustusministeriö, 2015). Katakria voidaan hyödyntää auditointityökaluna esimerkiksi turvallisuusjärjestelyjen toteutumisessa tai tietojärjestelmien turvallisuuden arvioimisessa. Lisäksi sen tavoitteena on varmistaa, että salassa pidettävän tiedon paljastuminen voidaan ehkäistä riittävillä turvallisuusjärjestelyillä (Puolustusministeriö, 2015).

Katakri (Puolustusministeriö, 2015) koostuu kolmesta osa-alueesta, joita kaikkia voidaan käyttää myös erikseen. Kolme osa-aluetta ovat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus (Puolustusministeriö, 2015). Katakrin (Puolustusministeriö, 2015) mukaan se on turvallisuuden minimivaatimus, eli sitä ei ole tarkoitus käyttää julkisessa hankinnassa sellaisenaan. Katakrin minimivaatimusten lisäksi tarvittavan turvallisuustason määrittely on julkisissa hankinnoissa tehtävä erikseen perustuen hankinnan riskeihin sekä erityistarpeisiin. Katakrin lisäksi

yksittäiseen hankkeeseen tai hankintaan voi sisältyä myös muita vaatimuksia tietojen käsittelystä tai suojaamisesta. (Puolustusministeriö, 2015)

4 PILVIPALVELUJEN TIETOTURVAN ARVIOINTI

Tässä luvussa käydään läpi pilvipalvelujen yleisimmät riskit ja tietoturvauhat sekä selvitetään, mitä tekijöitä julkishallinnon organisaation tulee ottaa huomioon pilvipalveluiden turvallisuutta arvioidessa. Näitä tekijöitä käsittelevässä alaluvussa hyödynnetään ensisijaisesti *Pilvipalveluiden turvallisuuden arviointikriteeristöä* (Kyberturvallisuuskeskus, 2020), jota täydennetään ja täsmennetään tarvittaessa tieteellisellä kirjallisuudella. Viimeisessä alaluvussa Pilvipalvelujen turvallisuuden arviointikriteeristöä verrataan tutkimuskirjallisuuteen.

4.1 Riskit ja tietoturvauhat pilvipalveluissa

Jotta ymmärtäisi pilvipalvelujen turvallisuusaspekteja, on hyvä hahmottaa pilvipalveluiden yleisiä turvallisuusuhkia ja -riskejä. Grobauer, Walloscheck ja Stöcker (2011) toteavat, että jotkin pilvipalveluiden uhat ovat tosiasiassa teknologioihin eikä varsinaisesti pilvipalveluihin liittyviä uhkia. Koska pilvipalvelut hyödyntävät jo olemassa olevia teknologioita, ovat niiden ongelmat siirtyneet mukana myös pilvipalveluihin (Anjana & Singh, 2018). Yleisten teknologiaan liittyvien uhkien lisäksi voidaan kuitenkin tunnistaa nimenomaisesti pilvipalveluille tyypillisiä uhkia, joita Grobauer ym. (2011) lähestyvät jo mainittujen Mellin ja Grancen (2011) määrittelemien pilvipalveluominaisuuksien kautta. Subashini ja Kavitha (2010) ovat puolestaan tarkastelleet pilvipalveluiden turvallisuusuhkia palvelumalleihin liittyen. Lähestymistavasta riippumatta turvallisuusuhat ovat pääasiassa samanlaisia.

Koska pilvipalveluita hallinnoidaan tyypillisesti itsepalveluportaalin kautta (Mell & Grance, 2011), on luvaton pääsy pilvipalvelun hallintapaneeliin nimenomaan pilvipalveluille mahdollinen ongelma (Grobauer ym., 2011). Laaja ja helppo pääsy pilvipalveluihin eri laitteilla altistaa pilvipalvelut haavoittuvien internet-protokollien ja ohjelmointirajapintojen kautta tehtäville hyökkäyksille (Grobauer ym., 2011;

Ryan, 2013; Mell & Grance, 2011). Anjanan ja Singhin (2018) mukaan etenkin ohjelmistoalustat ovat käyttötapansa vuoksi haavoittuvia luonnostaan, koska internet on ensisijainen tapa hyökätä ja varastaa sensitiivistä dataa. Vaikka palvelun hallinnoinnin yhteydessä käytettäisiin suojattua yhteyttä, tunnistavat Subashini ja Kavitha (2010) useita tapoja hyödyntää mahdollisia palveluntarjoajan haavoittuvuuksia internetin protokollissa. Subashinin ja Kavithan (2010) mukaan käyttäjänhallinta on myös haavoittuvuustekijä. Pilvipalveluiden ominaispiirteisiin kuuluu helppo pääsy monilta eri laitteilta (Mell & Grance, 2011). Koska käyttäjänhallinta toteutetaan usein pilvipalvelualustalta yrityksen oman infrastruktuurin sijaan, tarkoittaa käyttäjänhallinnassa epäonnistuminen sitä, että yrityksestä jo poistuneille henkilöille voi jäädä pääsyoikeus pilvipalveluiden sisältöön (Subashini & Kavitha, 2011).

Resurssien uudelleenkäyttö voi antaa nykyiselle resurssien käyttäjälle mahdollisuuden palauttaa edellisen käyttäjän data (Grobauer ym., 2013). Toisaalta pilvipalveluntarjoaja voi myös vahingossa poistaa asiakkaan datan tai muokata sitä (Ryan, 2013). Estääkseen mahdolliset ongelmat datan katoamiseen liittyen, on pilvipalveluntarjoajalle kriittistä ottaa kaikesta säilytetystä datasta varmuuskopiot (Anjana & Singh, 2018). Lisäksi pilvipalveluntarjoajan työntekijöillä sekä alihankkijoilla voi olla pääsy asiakkaan dataan, minkä Ryan (2013) sekä Anjana ja Singh (2018) näkevät tietoturvaongelmana. Mellin ja Grancen (2011) mukaan pilvipalveluille on tyypillistä saatavuuden ja käytön tarkka mittaaminen. Se mahdollistaa käytön optimoinnin, mutta voi avata mahdollisuuden mittausdatan manipuloinnille, jolla voi olla vaikutusta esimerkiksi laskutukseen (Grobauer ym., 2013).

Useamman asiakkaan kesken jaettu alusta on pilvipalveluille tyypillinen ominaisuus. Jaetun alustan hyödyntämisessä voivat muodostua uhaksi muut samalla alustalla olevat asiakkaat. (Ryan, 2013; Subashini & Kavitha, 2010). Jaettu alusta voi mahdollistaa muille saman alustan asiakkaille pääsyn toistensa dataa. Pilvipalvelutarjoajan on mahdollista estää muodostunut uhka varmistamalla, että etenkin ohjelmistoalustassa toisen dataan pääsy on estetty joko fyysisellä tai ohjelmistokerroksella. (Subashini & Kavitha, 2010). Mikäli näin ei ole tehty, tunnistivat Subashini ja Kavitha (2010) useita keinoja, joilla samalla alustalla olevien tietoihin voidaan päästä käsiksi. Anjana ja Singh (2018) käyttävät esimerkkinä suuria tunnettuja pilvipalveluntarjoajia, jotka ovat toteuttaneet estämisen vain yhdellä kerroksella, toisin kuin Subashini ja Kavitha (2010) suosittelevat.

Ryanin (2013) mukaan esimerkiksi jaetun alustan ongelmille, protokollahaavoittuvuuksille sekä datan katoamiselle on jo olemassa teknisiä ratkaisuja. Ryan (2013) korostaa, että suurin ongelma tällä hetkellä on datan mahdollinen näkyminen palveluntarjoajan työntekijöille sekä alihankkijoille. Subashinin ja Kavithan (2010) mukaan suurimmat pilvipalveluntarjoajat kuitenkin sallivat datan näkyvyyden ainoastaan liiketoimintasyistä ja silloinkin salatun yhteyden kautta. Salattujen yhteyksien käyttöä tarkastellaan rutiininomaisesti. On todennäköistä, että luvatta dataa tarkastelemaan pyrkivä

henkilö hyödyntää erilaisia hyökkäysmenetelmiä, kuten SQL-injektioita, päästäkseen käsiksi talletettuun dataan. (Subashini & Kavitha, 2010).

Mikäli palveluntarjoajan tarkoitus on ainoastaan säilyttää data, voidaan uhka datan tarkasteluun liittyen poistaa salaamalla säilytettävä data (Ryan, 2013; Subashini & Kavitha, 2010). Datan salaaminen ei aina ole mahdollista. Mikäli pilvipalveluntarjoajan tulee pystyä tekemään datalle toimenpiteitä tai data on esimerkiksi liiketoimintaprosesseihin liittyvää, ei salaaminen välttämättä onnistu. (Ryan, 2013).

Yhtenä ohjelmistoalustan ongelmana Subashini ja Kavitha (2010) esittävät datan sijainnin. Asiakas ei välttämättä ole tietoinen datan fyysisestä säilytyspaikasta tai data on jaettu useampaan eri paikkaan (Zissis & Lekkas, 2012), mikä joissain tapauksissa on välttämätön tietää lainsäädännöllisistä tai turvallisuuteen liittyvistä syistä (Subashini & Kavitha, 2010; Kyberturvallisuuskeskus, 2020). Myös palveluun liittyvät vaatimukset voivat asettaa rajoituksia palvelun sijainnille (Subashini & Kavitha, 2010; Kyberturvallisuuskeskus, 2020). Suomessa on rajoitteita esimerkiksi viranomaisen salassa pidettävän tiedon tai kansalliseen turvallisuuteen liittyvän tiedon fyysiseen sijaintiin (Kyberturvallisuuskeskus, 2010). Sijainnit jaotellaan kolmeen kategoriaan: Suomi, tietosuojasääntelyn mahdollistamat alueet (EU/ETA) sekä muut maat (Kyberturvallisuuskeskus, 2020).

4.2 Pilvipalvelujen tietoturvan arviointi julkishallinnossa

Tässä alaluvussa käsitellään pilvipalvelujen tietoturvan arviointia julkishallinnossa hyödyntäen Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKria. Pilvipalveluiden auditoinnin tarkoituksena on ensisijaisesti osoittaa pilvipalvelusta niille tyypillisiä ongelmia, joita perinteiset auditointikriteeristöt eivät pysty selvittämään (Ryoo ym., 2014).

PiTuKri on Liikenne- ja viestintäministeriön Kyberturvallisuuskeskuksen ensimmäisen kerran vuonna 2019 julkaisema arviointikriteeristö (Kyberturvallisuuskeskus, 2020). Kyberturvallisuuskeskus (2019) on määritellyt kriteeristön tavoitteeksi viranomaisen salassa pidettävän tiedon suojaamisen pilvipalveluissa. Kriteeristö on rakennettu suomen kansallisten tarpeiden näkökulmasta ja se on tarkoitettu käytettäväksi työkaluna turvallisuuden arviointiin. Lisäksi kriteeristön on tarkoitus tukea Valtiovarainministeriön julkishallinnon pilvipalveluiden linjausta sekä sen käyttöönottoa. (Kyberturvallisuuskeskus, 2020).

Kyberturvallisuuskeskuksen (2020) kriteeristö koostuu yhdestätoista osa-alueesta, joista ensimmäisen eli esiehtojen, ilmoitetaan olevan erityisasemassa. Esiehdot määrittävät tiedon tyyppien perusteella mahdolliset rajoitukset toteutusmallin, palvelun fyysisen sijainnin sekä pilvipalvelutarjoajan suhteen. (Kyberturvallisuuskeskus, 2020). Muut yhdeksän osaa koostuvat kattavasti turvallisuusjohtamisesta, henkilöstöturvallisuudesta, fyysisestä turvallisuudesta, tietoliikenneturvallisuudesta, tietojärjestelmäturvallisuudesta,

tietoaineistoturvallisuudesta, käyttöturvallisuudesta, siirrettävyydestä ja yhteensopivuudesta sekä muutoksenhallinnasta ja järjestelmäkehityksestä. Jokaisessa osa-alueessa on tarkempi sisältö jaettu vaatimuskortteihin. Jokaisessa vaatimuskortissa on kuvattu vaatimus, soveltamiskohteet, suojaustavoite sekä mahdolliset lisätiedot tulkinnan ja toteuttamisen tueksi. PiTuKri ei sulje pois vaatimusten täyttymisen osoittamisen osalta kokonaan muita viitekehyksiä tai sertifiointeja, vaan niitä voi hyödyntää tietyin rajoituksin. (Kyberturvallisuuskeskus, 2020).

Pilvipalveluiden turvallisuuden arviointikriteerit eri osa-alueille kattavat ensisijaisesti erilaisen salassa pidettävän tiedon, henkilötiedon sekä turvallisuusluokiteltujen tietojen ja kasaumien turvallisuudesta huolehtimisen. Kasaumalla tarkoitetaan merkittävää määrää turvallisuusluokiteltua aineistoa (Valtiovarainministeriö, 2019). Julkisen tiedon säilyttämiseen ei liity samanlaisia turva- ja suojausvaatimuksia. (Kyberturvallisuuskeskus, 2020). Arviointikriteeristö on sovellettavissa kaikille pilvipalvelujen palvelumalleille. Palvelumallin valinta kuitenkin vaikuttaa palvelun toimittajan ja asiakkaan vastuunjakoon. (Kyberturvallisuuskeskus, 2020).

4.2.1 Esiehdot

Pilvipalveluiden turvallisuuden auditointikriteeristön (Kyberturvallisuuskeskus, 2020) esiehdoissa ensimmäinen kategoria on järjestelmäkuvaus. Järjestelmäkuvauksen perusteella arvioidaan pilvipalvelun soveltuvuutta asiakkaan käyttötapaukseen (Kyberturvallisuuskeskus, 2020). Kyberturvallisuuskeskuksen (2020) mukaan järjestelmäkuvauksessa tulee olla

- Palvelu- ja toteutusmallit sekä niihin liittyvä palvelutasosopimus
- Elinkaaren periaatteet, menettelyt ja turvatoimet sekä valvontatoimet
- Pilvipalvelun infrastruktuurin, verkon ja järjestelmäkomponenttien kuvaus
- Muutostenhallinnan periaatteet ja käytännöt
- Käsittelyprosessit poikkeaville tapahtumille
- Roolit ja vastuunjako asiakkaan ja toimittajan välillä
- Alihankkijoille siirretyt tai ulkoistetut toiminnot

(Kyberturvallisuuskeskus, 2020).

Palvelun arviointi voidaan tehdä ainoastaan infrastruktuurin, verkon ja järjestelmäkomponenttien tarkan kuvauksen perusteella (Popović & Hocenski, 2010; Kyberturvallisuuskeskus, 2020). Osana järjestelmäkuvausta ja sopimusta tehtävä palvelutasosopimus on kriittinen osa sekä soveltuvuuden arvioinnissa että valmiin palvelun aikana (Kandukuri, Paturi & Rakshit, 2009; Kyberturvallisuuskeskus, 2020). Palvelutasosopimuksella sovitaan toteutettavat palvelut, niiden käytettävyys, ongelmanhallinta, lainsäädäntöön liittyvät asiat, asiakkaalle kuuluvat vastuut, tietoturva sekä palvelun irtisanomiseen kuuluvat asiat (Kandukuri ym., 2009). Kriteeristön esiehdossa otetaan kantaa myös

kokonaan uusiin ja testausvaiheessa oleviin palveluihin. Niissä asiakkaan tulee ottaa huomioon myös vastuut käyttöönotossa, etenkin salassa pidettävän tiedon osalta (Kyberturvallisuuskeskus, 2020).

Toisena osana esiehtoja on lainsäädäntöjohdannaiset riskit. Kyberturvallisuuskeskus (2020) määrittelee lainsäädäntöjohdannaisen riskin seuraavasti: "Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa pilvipalveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy pilvipalvelun asiakkaiden salassa pidettäviin tietoihin." Lainsäädäntöjohdannaisen riskit voivat olla joko fyysiseen sijaintiin tai tietojen luovuttamiseen hallintayhteyden kautta toiseen valtioon liittyviä riskejä (Kyberturvallisuuskeskus, 2020). Myös lainsäädäntöjohdannaiset riskit tulee olla kuvattu palvelukuvauksessa ja asiakkaan on kyettävä tekemään riskiarvio kuvauksen perusteella (Kyberturvallisuuskeskus, 2020). Kyberturvallisuuskeskuksen (2020) mukaan palvelukuvauksessa on oltava seuraavat tiedot:

- Tiedon fyysinen sijainti sen koko elinkaaren ajalta mahdolliset alihankinta- tai ulkoistusketjut mukaan lukien
- Palvelun eri toimintojen ja komponenttien fyysinen sijainti koko elinkaaren ajalta
- Palvelun tuottamiseen osallistuvat tahot
- Käyttöön ja tiedonkäsittelyyn sovellettava lainsäädäntö ja oikeuspaikka
- Tahot, joilla on pääsy palvelussa käsiteltäviin tietoihin, lainsäädännöstä johtuen

(Kyberturvallisuuskeskus, 2020).

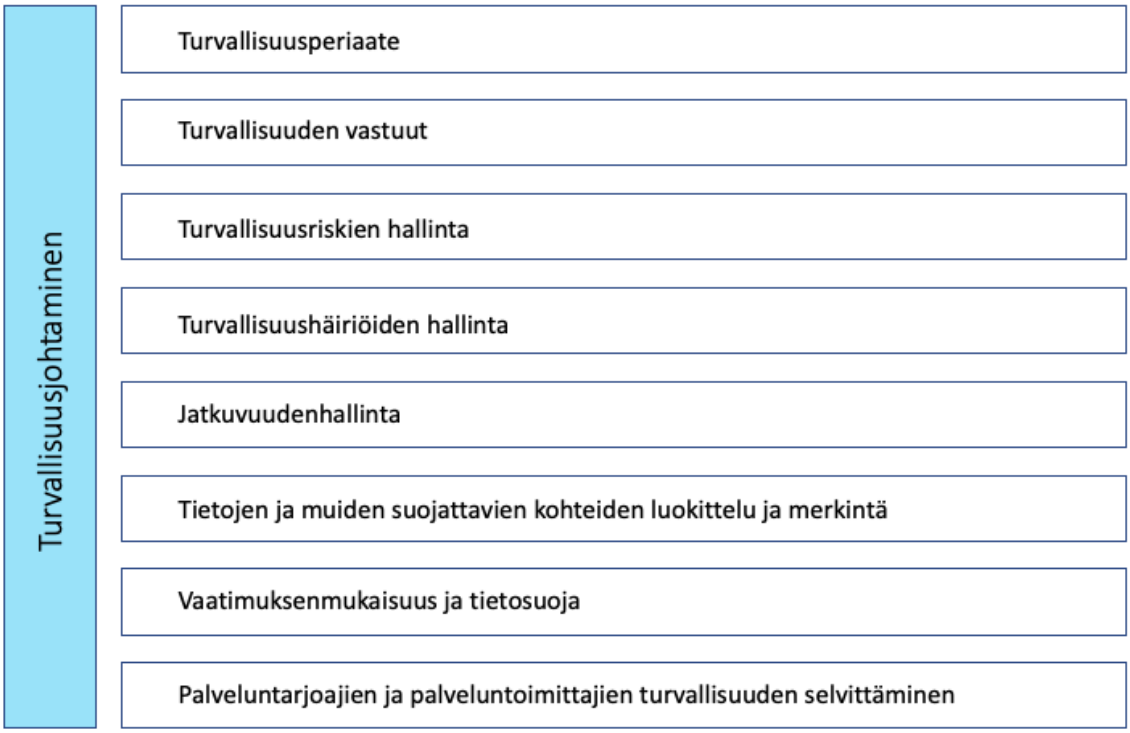
Lainsäädäntöjohdannaiset eivät saa rajoittaa palvelun soveltuvuutta käyttötapaukseen (Kyberturvallisuuskeskus, 2020). Lisäksi ehtona on, että asiakkaan tiedot sijaitsevat palvelun elinkaaren ajan sopimuksessa sovitussa paikassa, ellei asiakas ole erikseen kirjallisesti hyväksynyt tietojen siirtämistä toiseen sijaintipaikkaan (Kyberturvallisuuskeskus, 2020). On myös otettava huomioon se, etteivät sopimusehdot rajoita palvelun soveltuvuutta käyttötapaukseen (Kyberturvallisuuskeskus, 2020). Lainsäädäntöjohdannaiset rajoittavat myös pilvipalvelujen toteutusmalleja tietyissä tilanteissa (Kyberturvallisuuskeskus, 2020). Käytettävään toteutusmalliin tulee rajoitteita tapauksessa, jossa suojattavan tiedon turvallisuusluokka on korkeampi, kuin TL IV. Mikäli turvallisuusluokan IV tietoja on merkittävä määrä ja ne muodostavat kasauman, koskevat rajoitukset silloin myös luokan IV tietoja (Kyberturvallisuuskeskus, 2020). Mainittuja tietoja ei voida säilyttää julkisessa pilvessä tai hybridipilvessä. Soveltuvia ratkaisuja ovat joko yksityinen tai yhteisöllinen pilvipalvelu. (Kyberturvallisuuskeskus, 2020).

Toimittajan ja palvelun sopivuuden arvioinnista Kandukuri ym. (2009) nostavat esille riskin palveluntarjoajan konkurssiin menosta tai

siirtymisestä osaksi toista yritystä. Heidän mukaansa tulee varmistua siitä, että data on tallella edelleen kummankin mahdollisen tapahtuman jälkeen (Kandukuri ym., 2009).

4.2.2 Turvallisuusjohtaminen

Turvallisuusjohtaminen koostuu yhteensä yhdeksästä alla esitetystä osa-alueesta.



KUVIO 1 Turvallisuusjohtamisen osa-alueet

Ensimmäinen turvallisuusjohtamisen osa-alue on turvallisuusperiaate. Turvallisuusperiaatteella tarkoitetaan ennen kaikkea sitä, että turvallisuustyö tukee organisaation toimintaa ja johto sitoutuu turvallisuustyöhön (Kyberturvallisuuskeskus, 2020). Kyberturvallisuuskeskuksen (2020) mukaan se tarkoittaa kolmea asiaa: ylin johto on hyväksynyt organisaation turvallisuusperiaatteet, periaatteet ovat suojattavien kohteiden ja organisaation kannalta kattavia ja tarkoituksenmukaisia sekä ohjaavat turvallisuustoimintaa. Organisaatio voi osoittaa turvallisuusperiaatteen täyttymisen esimerkiksi ISO27001-sertifikaatilla edellyttäen, että sertifiointi kattaa myös pilvipalveluihin liittyvät prosessit (Kyberturvallisuuskeskus, 2020).

Toisena tuvallisuusjohtamisen vaatimuksena on turvallisuuden vastuut. Vaatimuksella tavoitellaan sitä, että keskeisimmät osa-alueet ovat vastuutettu henkilöille, joilla on tiedossa omat vastuualueensa sekä valtuutensa (Kyberturvallisuuskeskus, 2020). Turvallisuuteen liittyvän johtoryhmän tulee

selkeästi määritellä turvallisuuteen liittyvät roolit ja vastuualueet sekä sidosryhmät (Popović & Hocenski, 2010). Vastuualueiden määrittely on tärkeää, jotta henkilöt voivat toteuttaa omalla vastuualueellaan olevat tehtävät. Pilvipalveluiden turvallisuuden arvioinnin kannalta tämä tarkoittaa sitä, että hoidettavat tehtävät ja vastuut on määrittelyn lisäksi myös dokumentoitu. Lisäksi vastuunjako asiakkaan ja toimittajan välillä on selvä, ja tiedossa on myös turvallisuudesta vastaava nimetty henkilö. (Kyberturvallisuuskeskus, 2020).

Turvallisuusjohtamisen kolmas vaatimus, turvallisuusriskien hallinta, pyrkii tunnistamaan ja hallitsemaan vaarantavia tekijöitä sekä hallitsemaan riskejä siten, etteivät toiminta ja tavoitteet kärsi (Kyberturvallisuuskeskus, 2020). Riskienhallinnalla pyritään huomioimaan erilaiset lainsäädännön ja viranomaisen vaatimukset turvallisuustason suunnittelussa (Kyberturvallisuuskeskus, 2020), mutta myös datan ja datan käyttötarkoitukset liiketoiminnassa (Popović & Hocenski, 2010). Riskienhallinta vaatii organisaatiolta erilaisten vaatimusten, kuten viranomaisvaatimusten, tunnistamista ja niistä huolehtimista, vaikka organisaation omat turvavaatimukset olisivat lievempiä (Kyberturvallisuuskeskus, 2020). Riskienhallinta on syytä kohdentaa ensisijaisesti salassa pidettävän tiedon monitasoiseen suojaamiseen (Kyberturvallisuuskeskus, 2020). Monitasoisessa suojauksessa yksittäisen suojauksen pettäessä tiedot pysyvät edelleen salassa, koska muut suojaukset ja turvatoimet huolehtivat edelleen riittävästä suojaustasosta (Kyberturvallisuuskeskus, 2020). Kybeturvallisuuskeskuksen (2020) mukaan riittävästä turvallisuusriskien hallinnasta pilvipalveluissa huolehditaan seuraavin keinoin

- Organisaatiolla tulee olla erillinen riskienhallintaprosessi, joka on dokumentoitu, säännöllinen ja jatkuva
- Riskien analysointi on oltava järjestelmällistä ja ymmärrettävää
- Tilaturvallisuuden, turvallisuusjohtamisen sekä tietoturvallisuuden osa-alueet tulee kattaa riskien analysoinnissa
- Sidosryhmäriskit tulee huomioida
- Organisaation turvallisuustavoitteiden luomisessa hyödynnetään riskienhallintaprosessin tuloksia
- Oikein mitoitetut turvatoimet
- Valvonta- ja turvatoimet dokumentoidaan

(Kyberturvallisuuskeskus, 2020).

Lista turvallisuusriskien hallinnan keinoista on linjassa myös Popovićin ja Hocenskin (2010) arvion kanssa, minkä mukaan organisaatiolla tulee olla aina erillinen riskienhallintaprosessi, jonka tehtävänä on etukäteen tunnistaa turvallisuusriskejä ja suunnitella riskien hallintaa. Lisäksi riskienhallintaprosessin tulisi ottaa kantaa sovellus- ja infrastruktuuritason riskeihin (Popović & Hocenski, 2010).

Neljäntenä turvallisuusjohtamisen vaatimuksena on turvallisuushäiriöiden hallinta, jolla varmistetaan organisaation toimiminen tehokkaasti kaikissa ei-toivotuissa tilanteissa samalla minimoiden vahingot ja palauttaen tilanteen normaaliksi. Vaatimuksen mukaan turvallisuushäiriöiden hallinta tulee suunnitella ja luoda menettelytavat turvallisuushäiriöitä varten. (Kyberturvallisuuskeskus, 2020). Menettelytavoissa tulee ottaa huomioon mahdollinen ilmoitusvelvollisuus tietosuojaa koskevissa loukkauksissa, kuten myös ilmoituksen teko joko poliisille tai Kyberturvallisuuskeskukselle turvallisuushäiriön niin vaatiessa (Kyberturvallisuuskeskus, 2020). Luodut prosessit tulee dokumentoida, ohjeistaa ja kouluttaa henkilöstölle. Organisaatiolla tulee myös selkeästi olla henkilö tai taho, jolle häiriöistä ilmoitetaan. Turvallisuushäiriötilanteita tulee harjoitella ja toteutuneiden turvallisuushäiriöiden tyyppejä ja määriä seurata. (Kyberturvallisuuskeskus, 2020). Lisäksi asiakkaita koskevista häiriöistä tulee ilmoittaa asiakkaalle. Organisaatiossa tulee myös olla viestintäkäytänteet ja -vastuut sovittuna (Kyberturvallisuuskeskus, 2020).

Turvallisuusjohtamisen viides vaatimus, jatkuvuudenhallinta, tarkoittaa palvelun jatkuvuuden varmistamista siten, että saatavuus-, eheys- ja luottamuksellisuusvaatimukset täyttyvät (Kyberturvallisuuskeskus, 2020). Jatkuvuudenhallinnan prosesseissa tulee huomioida toimintavaatimuksiin nähden tarpeeksi nopea toipuminen, ennaltaehkäisevät ja korjaavat toimenpiteet, havaittujen poikkeamien vieminen osaksi riskiarviointia sekä tietojen suojaaminen hätätilanteissa (Kyberturvallisuuskeskus, 2020). Jatkuvuudenhallinnan prosessit tulee suunnittelun lisäksi myös toteuttaa, testata sekä kuvata (Kyberturvallisuuskeskus, 2020; Herbane, Elliott & Swartz, 2004). Lisäksi tulee varmistaa sekä lainsäädännön että palvelutasosopimuksen velvoiteisiin vastaaminen (Kyberturvallisuuskeskus, 2020).

Kuudes turvallisuusjohtamisen vaatimus on tietojen ja muiden suojattavien kohteiden luokittelu ja merkintä (Kyberturvallisuuskeskus, 2020). Tietojen osalta turvallisuusluokkaa koskeva merkintä tulee tehdä niissä tapauksissa, kun tieto on salassa pidettävää (Laki julkisen hallinnon tiedonhallinnasta, 906/2019, 18§). Sillä pyritään mittaamaan ja tunnistamaan suojattavien kohteiden suojaustarpeita. Vaatimuksen mukaisesti luokittelun kannalta oleelliset tiedot tulee merkitä yhdenmukaisesti ja luokitteluun on oltava yhdenmukainen menetelmä. (Kyberturvallisuuskeskus, 2020). Kaikille laitteille ja ohjelmille tulee olla omistaja tai vastuutaho, ja lisäksi ne tulee luokitella kriittisyyden mukaisesti. Kaikista laitteistoista ja ohjelmista tulee olla myös ajantasainen kirjanpito, ja muutokset voidaan havaita vertaamalla suunniteltua toteutusta dokumentaatioon. Kyberturvallisuuskeskus, 2020).

Seitsemäs turvallisuusjohtamisen vaatimus, vaatimustenmukaisuus ja tietosuoja, tähtää sekä lainsäädäntöön että sopimusvelvoitteisiin liittyvien vaatimusten täyttämiseen (Kyberturvallisuuskeskus, 2020). Kaikkien sovellettavien lakien ja säädösten määräykset sekä menettelyt on tunnistettu ja dokumentoitu. Dokumentaatio tulee myös päivittää säännöllisesti. (Kyberturvallisuuskeskus, 2020). Organisaation tulee varmistaa tarvittava

tietosuojaosaaminen, jotta voidaan olla varmoja edellä mainittujen toimenpiteiden täyttämisestä (Popović & Hocenski, 2010). Lisäksi palveluille tulee olla arviointisuunnitelma, jonka mukaisesti riippumaton kolmas osapuoli tekee arvion pilvipalveluun liittyvästä toiminnasta, prosesseista sekä järjestelmistä. Ulkopuolisen ja riippumattoman tarkastajan lisäksi vuosittain tulee tehdä sisäinen tarkastus, joka selvittää palvelun vastuiden täyttämisen liittyen tietoturvakäytänteisiin sekä sopimuksellisiin ja lainsäädännöllisiin vaatimuksiin. (Kyberturvallisuuskeskus, 2020). Havaittujen poikkeamien priorisointi, korjaukset ja korvaavien suojausten käyttöönotto ovat ylimmän johdon vastuulla (Kyberturvallisuuskeskus, 2020).

Viimeinen turvallisuusjohtamisen vaatimus on palveluntarjoajien ja toimittajien turvallisuuden selvittäminen. Ennen kuin voidaan sallia toimittajan pääsy suojattavaan kohteeseen, tulee huolehtia samanlaisista suojaustoimenpiteistä, kuin organisaation omalla henkilöstöllä. Tällä tarkoitetaan esimerkiksi salassapitositoumuksia, turvaselvityksiä ja koulutuksia. (Kyberturvallisuuskeskus, 2020). Lisäksi palveluntarjoajan tulee noudattaa vastaavia suojauksia kuin organisaatio itse. Suojauksista sovitaan ja ohjeisestaan kirjallisesti sekä sopimusvelvoitteiden että ohjeiden muodossa. Sopimusvelvollisuuksien noudattamista valvotaan myös sopivin menettelytavoin. (Kyberturvallisuuskeskus, 2020). Lisäksi toimittajien tulee olla viranomaishyväksynnän tai vastaavan menettelyn piirissä. Lisäksi EU:n yleinen tietosuoja-asetus asettaa vaatimuksen, jossa mahdollisista henkilötietojen käsittelyssä tulee tehdä vielä erikseen kirjallinen sopimus. (Kyberturvallisuuskeskus, 2020).

4.2.3 Henkilöstöturvallisuus

Henkilöstöturvallisuuden suhteen pilvipalveluiden turvallisuuden arviointikriteeristössä on viisi vaatimusta. Ensimmäinen on työsuhteen elinkaaren huomioiminen, minkä tarkoituksena on pienentää henkilöstöön liittyviä riskejä (Kyberturvallisuuskeskus, 2020). Toisena kriteerinä on henkilöstön luotettavuuden arviointi (Kyberturvallisuuskeskus, 2020). Luotettavuuden arvioinnilla tarkoitetaan taustojen tarkistamista lainsäädännön sallimien rajojen puitteissa. Taustatarkistuksella tarkoitetaan henkilöllisyyden, työhistorian sekä koulutuksen todentamista, ja tarvittaessa keskustelemista esimerkiksi suosittelijoiden kanssa (Stewart, Chapple & Gibson, 2012; Kyberturvallisuuskeskus, 2020). Lisäksi tarvittaessa henkilön luotettavuutta voidaan arvioida myös turvaselvityksellä, mikäli tehtävä sisältää turvaluokiteltujen aineistojen käsittelemistä (Kyberturvallisuuskeskus, 2020). Kahden ensimmäisen vaatimuksen tarkoituksena on pystyä todentamaan, että henkilö on tehtävään sopiva ja pätevä sekä luotettava (Stewart ym., 2012). Kolmantena vaatimuksena on salassapito- ja vaitiolositoumukset (Kyberturvallisuuskeskus, 2020), joissa työntekijä sitoutuu olemaan kertomatta organisaation salassa pidettäviä asioita ulkopuolelle ja joiden rikkomisesta

työntekijällä on sopimuksen mukainen korvausvastuu (Stewart ym., 2012). Vaatimuksen mukaisesti mahdolliset salassapitosopimukset allekirjoitetaan ennen sopimussuhteen alkua tai pääsyä asiakkaan tietoihin (Kyberturvallisuuskeskus, 2020). Salassapitosopimuksessa yksilöidään salassa pidettävät tiedot, sopimuksen ehdot, sopimuksen päättymiseen liittyvät toimenpiteet, tietojen omistaja, salassapitosopimusta koskevat säännöt ja säädökset sekä seuraamukset salassapitosopimusten ehtojen rikkomisesta (Kyberturvallisuuskeskus, 2020).

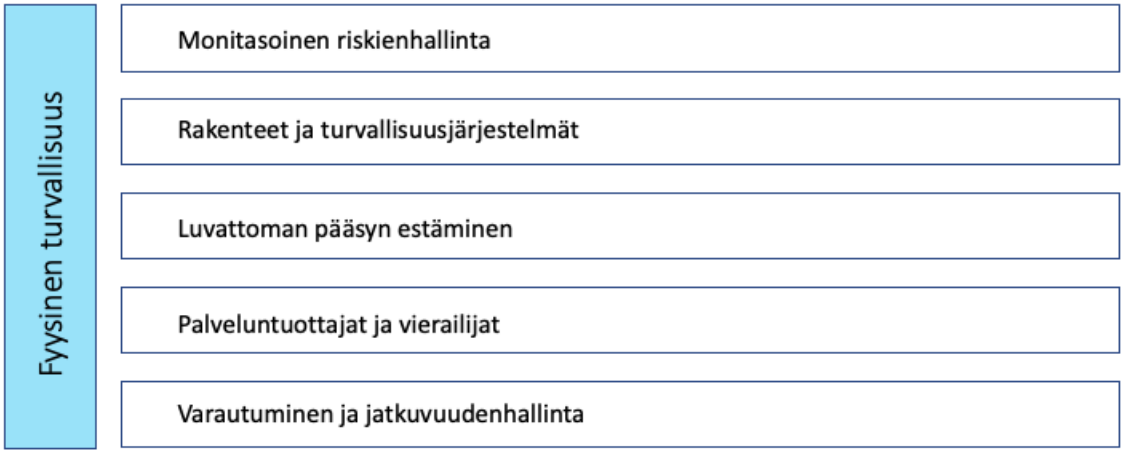
Neljäs henkilöstöön liittyvä vaatimus on turvallisuustietoisuus, jonka mukaan turvalliset toimintatavat suunnitellaan ja henkilöstö voi toimia turvallisesti, myös erikoistilanteissa (Kyberturvallisuuskeskus, 2020). Myös toimintamallit turvallisuustietoisuuden lisäämiseksi, kuten koulutukset, tulee selkeästi kirjata ylös (Stewart ym., 2012).

Viimeinen henkilöstöä koskeva vaatimus on tiedonsaantitarpeet ja tehtävien erottelu. Vaatimuksen tavoite on varmistaa, ettei salassa pidettävä tieto ole saatavilla kuin valtuutetuille henkilöille tiedonsaantitarpeen mukaisesti. (Kyberturvallisuuskeskus, 2020). Tehtävistä, joissa edellytetään salassa pidettävän tiedon käsittelyä, tulee pitää kirjaa ja pääsy salassa pidettävään tietoon myönnetään vasta, kun henkilön tiedonsaantitarve on selvitetty. Turvaluokiteltujen tietojen käsittelyoikeuksista tulee pitää luetteloa ja tehtävät sekä vastuualueet tulee eriyttää mahdollisuuksien mukaan. (Kyberturvallisuuskeskus, 2020).

Ensimmäiseen vaatimukseen, työsuhteen elinkaareen, liittyy kiinteästi myös työsuhteen päättyminen (Stewart ym., 2012). Stewart ym. (2012) korostavat, että työsuhteen päättyessä tulee huolehtia esimerkiksi kaikkien organisaatioille kuuluvien välineiden, kuten kulkukorttien, palautuksesta sekä sen jälkeen tapahtuvasta pääsyoikeuksien ja vastaavien päättämisestä.

4.2.4 Fyysinen turvallisuus

Fyysisen turvallisuuden vaatimukset koostuvat yhteensä viidestä alla esitetystä osa-alueesta.



KUVIO 2 Fyysisen turvallisuuden osa-alueet

Ensimmäinen fyysisen turvallisuuden kriteeri on monitasoinen riskienhallinta, jonka tavoitteena on estää luvaton pääsy konesaleihin ja salassa pidettävään tietoon (Kyberturvallisuuskeskus, 2020). Lisäksi vaatimuksen tarkoitus on estää varkaudet, vahingot, menetykset, taloudelliset tappiot ja häiriöt (Kyberturvallisuuskeskus, 2020). Vaatimus täytetään toteuttamalla fyysiset turvatoimet monitasoisella suojamisella, luokittelemalla tilat turvallisuusalueiksi, henkilökohtaisella kulunvalvonnalla sekä riittävillä turvatoimien mitoituksella (Kyberturvallisuuskeskus, 2020). Turvallisuusalueella tarkoitetaan fyysisesti suojattua hallinnollista tai turva-aluetta (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 9§). Hallinnollisella alueella tulee olla selkeät rajat ja alueelle voidaan päästää ainoastaan sellainen henkilö, joka on valtionhallinnon viranomaisen valtuuttama (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 9§). Turva-alue on myös selkeästi rajattu ja siellä tapahtuvaa kulkua tulee valvoa. Tilaan saa päästää ilman saattajaa sellaisia henkilöitä, joiden luotettavuus on varmistettu (Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 9§). Tiloja suunnitellessa tulee ottaa huomioon, ettei kaikkien henkilöiden pääsy kaikkiin tiloihin yleensä ole välttämätöntä (Stewart ym., 2012). Lisäksi tilojen luokittelu toteutetaan kuten minkä tahansa IT-omaisuuden luokittelu (Stewart ym., 2012). Riittävillä turvatoimilla tarkoitetaan esimerkiksi ympärivuorokautista valvontaa, biometristä tunnistusta, kameravalvontaa sekä lämmön ja muiden fyysisten elementtien pitämistä optimaalisena tietokoneille (Popović & Hocenski, 2010).

Toinen fyysisen turvallisuuden vaatimus on rakenteet ja turvallisuusjärjestelmät. Vaatimuksen tavoitteena on estää luvaton pääsy tiloihin huolehtimalla, että rakenteet ja turvallisuusjärjestelmät ovat vaatimuksenmukaisia (Kyberturvallisuuskeskus, 2020). Rakenteilla ja turvallisuusjärjestelmillä tarkoitetaan esimerkiksi aitoja, ovia ja lukkoja, joiden tulee olla riittävän varmat luvattoman pääsyn estämiseksi (Stewart ym., 2012).

Kolmas vaatimus, luvattoman pääsyn estäminen, tähtää siihen, että vain valtuutetuilla henkilöillä on pääsy salassa pidettävään tietoon, laitteisiin tai järjestelmiin (Kyberturvallisuuskeskus, 2020). Pääsyoikeuksia voidaan edellä mainittujen keinojen lisäksi varmistaa esimerkiksi kulkutunnisteilla (Stewart ym., 2012).

Fyysisen turvallisuuden neljäs vaatimus ottaa kantaa palveluntuottajiin ja vieraisiin. Vaatimuksen tavoite on sama kuin kolmannessa vaatimuksessa: luvattoman pääsyn estäminen kaikkeen salassa pidettävään tietoon, laitteistoihin ja järjestelmiin. (Kyberturvallisuuskeskus, 2020). Vierailijoiden osalta tämä tarkoittaa vierailijoiden tunnistamista, niiden kirjaamista ja vierailijakortin antamista. Vierailijoiden kulku tiloissa tulee järjestää ohjatuksi ja vierailijoita tulee valvoa (Stewart ym., 2012). Vaatimukset koskevat myös muuta henkilökuntaa, kuten siivoojia, huoltohenkilöitä sekä muuta henkilöstöä. Mikäli henkilöllä on työn puolesta tarve liikkua valvomatta alueella, tulee henkilölle tehdä turvallisuusselvitys. Lisäksi kaikki ylläpitoon,

päivityksiin ja huoltoihin liittyvät asiat tulee dokumentoida. (Kyberturvallisuuskeskus, 2020).

Viimeinen fyysisen turvallisuuden osa-alue, varautuminen ja jatkuvuudenhallinta, tarkoittaa tässä yhteydessä konesalien suojaamista yleisesti tunnettuja riskejä vastaan (Kyberturvallisuuskeskus, 2020). Osana suojautumista tulee päättää millä tavalla riskejä vastaan suojaudutaan: varmistamalla konesalin helppo korvattavuus vai kenties jatkuvuussuunnitelma samoissa tiloissa jatkamiseksi (Stewart ym., 2012). Tunnettuja riskejä ovat vaatimuksen mukaan esimerkiksi luonnon ja ihmisen aiheuttamat uhat, räjähdykset, tulipalo, vesivahinko ja levottomuudet (Kyberturvallisuuskeskus, 2020).

4.2.5 Tietoliikenneturvallisuus

Tietoliikenneturvallisuuden vaatimukset koostuvat kahdesta vaatimuksesta: tietoliikenneverkon rakenne ja yleisiä verkkohyökkäyksiä vastaan suojautuminen (Kyberturvallisuuskeskus, 2020). Tietoliikenneverkon rakennevaatimukset tähtäävät siihen, että palvelu tuotetaan ja liikenne rajataan vain välttämättömiin yhteyksiin, joissa on lisäksi sisäinen suodatus (Kyberturvallisuuskeskus, 2020). Pilvipalveluissa asiaan on kiinnitettävä erityisesti huomiota, koska konesaleissa tietoliikenneyhteyksiin liittyvät asiat on usein virtualisoitu, jolloin täydellinen fyysinen erottelu ei välttämättä enää ole mahdollista (Wailly, Lacoste & Debar, 2011). Vaatimus täytetään silloin, kun palvelu on erotettu muusta ympäristöstä, palvelu on jaettu vyöhykkeisiin ja liikennettä rajoitetaan sekä valvotaan (Kyberturvallisuuskeskus, 2020). Yleisiä verkkohyökkäyksiä vastaan suojautumisella tavoitellaan sitä, ettei palvelujen käyttö esty esimerkiksi palvelunestohyökkäyksen vuoksi, joka on yksi vakavimmista pilvipalveluiden turvallisuusuhista (Joshi, Vijaya & Joshi, 2012; Kyberturvallisuuskeskus, 2020). Palvelun käytön estymisen lisäksi Joshi ym. (2012) esittävät, että etenkin palveluestohyökkäyksille tyypillistä on, ettei hyökkääjää pystytä hyökkäykseen käytettävien tekniikoiden vuoksi selvittämään. On myös tärkeää suojella luottamuksellisuutta ja eheyttä vaarantumiselta (Kyberturvallisuuskeskus, 2020). Vaatimuksen mukaan kaikkia järjestelmiä tulee lähtökohtaisesti epäillä ja sen vuoksi varautua yleisiin hyökkäyksiin (Kyberturvallisuuskeskus, 2020).

4.2.6 Identiteetin ja pääsyn hallinta

Identiteetin- ja pääsynhallinnan vaatimukset koostuvat kolmesta osasta: käyttäjäoikeushallinnasta, käyttäjätunnistamisesta sekä hallintayhteyksistä (Kyberturvallisuuskeskus, 2020). Käyttäjäoikeuksien hallinnan keskeinen kysymys auditoinnissa on palveluntarjoajan tasapaino turvallisuuden ja

saavutettavuuden välillä; henkilöillä voi olla tarve päästä käsiksi tietoon myös toimiston ulkopuolelta (Ryoo ym., 2014).

Käyttöoikeushallinnan tavoite on vähimpien oikeuksien peruste, eli käyttöoikeuksien luovuttaminen henkilöille vain, jos heillä on siihen välttämätön tarve oman työroolinsa puolesta (Kyberturvallisuuskeskus, 2020). Vähimpien oikeuksien periaatteen lisäksi Popović ja Hocenski (2010) ehdottavat myös vähimmän ajan periaatetta, eli pääsyoikeus tulee myöntää niin vähäksi aikaa kuin on välttämätöntä. Käyttöoikeushallintaan on oltava oma ennalta määritelty prosessi, jota toteuttaen annetaan henkilöille välttämättömät oikeudet. Käyttöoikeuksien myöntämisen yhteydessä myös tarkastetaan henkilön oikeus saada tiedot. (Kyberturvallisuuskeskus, 2020). Organisaatiolla tulee olla oma ohjeistus käyttöoikeuksien käsittelyyn sekä myöntämiseen, kuten myös henkilöstössä tapahtuvien muutosten ilmoittamiseen. Lisäksi kaikki käyttö- ja pääsyoikeudet tulee tarkastaa säännöllisesti, vaatimuksen mukaan minimissään puolivuosittain. (Kyberturvallisuuskeskus, 2020). Myös Paquette, Jaeger ja Wilson (2010) toteavat että palveluntarjoajan tulee varmistaa, että olemassa olevat käyttöoikeudet voidaan varmistaa asiakkaan tai ulkopuolisen tahon auditoinnissa.

Auditoinnin kannalta tärkeä kysymys on, voiko palveluun päästä käsiksi sellainen henkilö, joka esittää oikeutettua käyttäjää (Ryoo ym., 2014). Jotta vain valtuutetut käyttäjät pääsevät käsiksi tietoihin ja palveluihin, on tärkeää huolehtia käyttäjätunnistuksesta. Käyttäjä tulee pystyä tunnistamaan luotettavasti, eli käytössä on oltava yksilölliset käyttäjätunnukset. Jokainen käyttäjä tulee tunnistaa ja tunnistamisessa tulee hyödyntää tunnettua ja turvalliseksi todettua kaksivaiheista tunnistustekniikkaa. (Kyberturvallisuuskeskus, 2020). Yhteiskäyttötunnuksia tulee välttää, ja mikäli sellaisia teknisten vaatimusten vuoksi tehdään, tulee luoda käyttäjän yksilöinnin mahdollistavat hallintakäytänteet (Kyberturvallisuuskeskus, 2020). Organisaation omaa käyttäjänhallintaa ei aina välttämättä ole mahdollista yhdistää pilvipalveluun ja niissä tapauksissa käyttäjänhallinnasta tulee huolehtia muulla tavalla, joten turvallisuusarvioinnissa tulee selvittää palveluntarjoajan läpinäkyvyys käyttäjänhallinnan menetelmistä (Ryoo ym., 2014; Wayne & Grance, 2011). Mikäli käyttäjätunnuksella tunnistautuminen epäonnistuu useamman kerran peräkkäin, tulee tunnusten lukittua automaattisesti (Kyberturvallisuuskeskus, 2020). Fyysisesti suojatun turvallisuusalueen ulkopuolella kulkeva tieto tulee salata virnaomaisen hyväksymällä salausratkaisulla, ja kaikki palveluntarjoajan sekä asiakkaan päätelaitteet ja järjestelmät tulee tunnistaa ennen kuin voidaan myöntää pääsy suojattavaan tietoon (Kyberturvallisuuskeskus, 2020).

Viimeinen identiteetin- ja pääsynhallinnan vaatimus liittyy hallintayhteyksiin. Vaatimuksen tavoitteena on varmistaa, että hallintayhteyksien suojaus on riittävä ja hallintayhteyttä voivat käyttää vain valtuutetut henkilöt (Kyberturvallisuuskeskus, 2020). Hallintayhteyksiä myöntäessä tulee varmistua siitä, että yhteys myönnetään vain sellaisille henkilöille, joiden työtehtävät ehdottomasti vaativat yhteyden muodostamisen

(Stewart ym., 2012). Hallintayhteyksien pääsynhallinnassa toteutetaan samaa periaatetta kuin muussa pääsynhallinnassa: kaksivaiheista tunnistautumista. Salattavaa tietoa sisältävät laitteet tulee suojata asianmukaisesti, mikäli ne viedään hyväksyttyjen turvallisuusalueiden ulkopuolelle. Lisäksi turvallisuusluokiteltua tietoa voi tarkastella ja hallita ainoastaan kyseisen turvallisuusluokan mukaiselta alueelta, ympäristöstä sekä päätelaitteelta. (Kyberturvallisuuskeskus, 2020).

4.2.7 Tietojärjestelmäturvallisuus

Ensimmäinen tietojärjestelmäturvallisuuden vaatimus, jäljitettävyys ja havainnointikyky, tähtää kaiken luvattoman käytön havaitsemiseen ja selvittämiseen (Kyberturvallisuuskeskus, 2020). Jäljitettävyys voidaan määritellä kaikkien tapahtumien kirjaamisena siten, että jälkikäteen voidaan selvittää, mitä toimenpiteitä kukin on järjestelmäympäristössä tehnyt ja tarvittaessa selvittää kaikki luvattoman käyttäjän tekemät tapahtumat (Kyberturvallisuuskeskus, 2020; Stewart ym., 2012, 11). Tapahtumatallenteiden tulee olla riittävän laajat, eli niitä tulee säilyttää vähintään kuusi kuukautta, ellei viranomaisvaatimus tai tiedon turvallisuusluokka vaadi pidempää tallennusaikaa. Vaatimuksen mukaan palveluntarjoajan tulee myös toimittaa kerätyt tiedot asiakkaan tarpeen mukaan siten, että ne ovat muodossa, jossa asiakas voi tulkita niitä. (Kyberturvallisuuskeskus, 2020).

Toisen tietojärjestelmäturvallisuuden vaatimuksen, järjestelmäkovennuksen, tavoite on poistaa tarpeettomat toiminallisuudet käytöstä, jolloin riski ohjelmisto- ja konfiguraatiovirheisiin pienenee (Kyberturvallisuuskeskus, 2020). Tarpeettomat ominaisuudet tai protokollat vaikuttavat myös järjestelmähaavoittuvuuksiin sekä tarjoavat yhden lisämahdollisuuden hyökätä järjestelmää vastaan (Stewart ym., 2012, 579). Järjestelmäkovennukseen vaaditaan kaksi asiaa: systemaattinen tapa järjestelmäasennuksiin siten, että järjestelmäkovennus toteutuu ja toisena, että kovennettu järjestelmä sisältää ainoastaan välttämättömät komponentit ja palvelut toimintavaatimusten täyttämiseksi (Kyberturvallisuuskeskus, 2020).

Kolmantena tietojärjestelmäturvallisuuden vaatimuksena on tiedon erottelu. Vaatimus tähtää siihen, että salassa pidettävä tieto on saatavilla ainoastaan kyseiselle asiakkaalle (Kyberturvallisuuskeskus, 2020). Se tarkoittaa, että asiakkaan salassa pidettävät tiedot tulee erotella sekä virtuaalisissa että fyysisissä järjestelmissä ja säilyttää toisistaan eroteltuna (Kyberturvallisuuskeskus, 2020). Tiedon erottelun tulee tapahtua jokaisen palvelumallin osalta sille soveltuvin keinoin (Wayne & Grance, 2011). Haittaohjelmasuojauksella puolestaan tarkoitetaan sitä, että järjestelmäympäristössä käytetään riittävää haittaohjelmasuojausta yleisiä haittaohjelmia vastaan, jotta voidaan turvata tiedon eheys, luottamuksellisuus ja saatavuus (Kyberturvallisuuskeskus, 2020). Haittaohjelmasuojaus tulee myös päivittää suojauksen ohjeiden mukaisesti, jotta suojaus toimii myös uusia haittaohjelmia vastaan (Stewart ym., 2012, 333).

Suojattavien kohteiden siirtäminen ja poistaminen on viimeinen tietojärjestelmäturvallisuuden kohta. Vaatimus pyrkii tietojen suojaamiseen myös silloin, kun tieto siirretään fyysisesti suojattujen alueiden ulkopuolelle. Suojattavaa tietoa ei voida siirtää fyysisesti suojattujen alueiden ulkopuolelle ilman erillisitä valtuutusta. (Kyberturvallisuuskeskus, 2020). Lisäksi tiedon siirtäminen fyysisesti suojatun alueen ulkopuolelle tulee tapahtua aina suojattavan tiedon turvaluokituksen mukaisesti. Salassa pidettävää tietoa siirtäessä tulee myös huomioida, että tiedon on oltava viranomaisen hyväksymän salauskäytänteen mukaisesti salattua ja jatkuvasti valvonnan alaisena. (Kyberturvallisuuskeskus, 2020). Ennen salassa pidettävän tiedon käsittelyä tulee tiedon vastaanottaja pystyä varmistamaan ja tunnistamaan riittävän luotettavalla tavalla (Laki julkisen hallinnon tiedonhallinnasta, 906/2019, 14§). Salattavan tiedon poistamisessa tulee huomioida, että data voi jäädä joihinkin laitteisiin luettavaksi myös sen jälkeen, kun se on poistettu, ja sen vuoksi datan poistamiseen tulee kiinnittää erityistä huomiota (Stewart ym., 2012, 497).

4.2.8 Salaus

Kahdeksas vaatimusten alakohta, salaus, koostuu kolmesta osa-alueesta: salauskäytännöt ja avainhallinta, salaus fyysisesti suojatun alueen ulkopuolella sekä salaus fyysisesti suojatun alueen sisäpuolella (Kyberturvallisuuskeskus, 2020). Yleisesti salaus voidaan tehdä joko ennen datan siirtämistä pilvipalveluun tai antaa palveluntarjoajan huolehtia salauksesta. Kumpikaan vaihtoehdoista ei ole täysin ongelmaton. (Ryoo ym., 2014). Salauskäytänteiden ja avainhallinnan keskeisin tavoite on tuottaa riittävä suojaus hyödyntäen salausmenetelmiä (Kyberturvallisuuskeskus, 2020). Salausratkaisut voivat olla ainoa tiedon eheyttä ja luottamuksellisuutta suojaava tekijä, mikäli osana pilvipalveluratkaisua on heikommin suojattu verkko-osuus (Kyberturvallisuuskeskus, 2020). Ryoon ym. (2014) mukaan datan salaamiseen liittyy kuitenkin aina saatavuuteen ja suorituskykyyn liittyviä ongelmia. PiTuKri ei kuitenkaan ota kantaa salaamisen vaiheeseen tai siihen, missä ja miten data tulee salata: vaatimuksina salauskäytänteille ja avainhallinnalle on, että siihen liittyvät prosessit ovat sekä suunniteltu, toteutettu että kuvattu (Kyberturvallisuuskeskus, 2020). Salausavaimet saavat olla ainoastaan valtuutettujen käyttäjien ja prosessien käytössä (Kyberturvallisuuskeskus, 2020).

Fyysisesti suojatun alueen ulkopuolella tulee vaatimuksen mukaan huolehtia, ettei luottamuksellisuus tai eheys vaarannu (Kyberturvallisuuskeskus, 2020). Alueen ulkopuolisuudella voidaan tarkoittaa esimerkiksi konesalien välistä liikennöintiä julkisen verkon, kuten operaattorien tarjoamien MPLS-verkkojen kautta. Vaatimuksen mukaan salassa pidettävä tieto tulee siirtää hyödyntäen validoituja sekä standardoituja salausratkaisuja sekä siten, että vastaanottaja voidaan tunnistaa riittävällä tavalla ennen tietoon käsiksi pääsyä. (Kyberturvallisuuskeskus, 2020). Fyysisesti suojatun alueen sisäpuolella voidaan siirtää dataa myös salaamattomana tai vaihtoehtoisesti

alemman tason salauksella, mikäli fyysinen suoja on tiedon turvatasolle riittävä. Tieto kuitenkin tulee tallentaa salattuna, pois lukien mahdollinen laskutukseen tai muuhun asiakkuudenhallintaan käytettävä metatieto. Salausavaimet tulee myös erotella asiakaskohtaisesti. (Kyberturvallisuuskeskus, 2020).

4.2.9 Käyttöturvallisuus

Yhdeksäs kohta, käyttöturvallisuus, koostuu neljästä osa-alueesta. Ensimmäinen, järjestelmäkuvaus jatkuvuuden ja käyttöturvallisuuden tukemiseksi, pyrkii suojaamaan käytön aikaisilta virheiltä sekä varmistumaan, että häiriötilanteesta palautuminen tapahtuu sopimusvelvoitteiden mukaisesti (Kyberturvallisuuskeskus, 2020). Jatkuvuuden ja palautumisen kannalta on Kandukurin ym. (2009) mukaan tärkeää varmistaa, että data on varmuuskopioitu ja infrastruktuuri kahdennettu. Tavoitteen toteutuminen edellyttää, että pilvipalvelusta on olemassa sekä ohjeet palvelun käyttöön että tarpeeksi laaja järjestelmäkuvaus, joita kumpaakin ylläpidetään ja pidetään saatavilla kaikille niitä tarvitseville henkilöille (Kyberturvallisuuskeskus, 2020). Jatkuvuuden turvaamiseksi organisaation tulisi myös Waynen ja Grancen (2011) mukaan suoriutua kriittisistä tehtävistä ilman pilvipalveluissa olevaa dataa.

Toinen käyttöturvallisuuden osa-alue on suorituskyvyn hallinta, jonka toteutuessa pilvipalvelu toimii sopimuksen mukaisen palvelutason puitteissa (Kyberturvallisuuskeskus, 2020). Jotta pilvipalvelu voi toimia palvelutason puitteissa, tulee sen kapasiteetti mitoittaa sopimuksen edellyttämälle tasolle (Kyberturvallisuuskeskus, 2020). Kapasiteetti asettaa vaatimuksia myös toimittajalle, jonka tulee laskea tarvittavan kapasiteetin määrä välttääkseen mahdolliset koko palvelun ylikuormittumistilanteet (Paquette ym., 2019). Lisäksi kapasiteetin käyttöä tulee pystyä mittaamaan, ja molempien osapuolten on analysoitava mittaustulokset säännöllisesti yhdessä (Kandukuri ym. 2009). Analysoitujen mittaustulosten perusteella voidaan ennustaa tulevaisuuden suorituskykytarvetta (Kyberturvallisuuskeskus, 2020). Mittaus edellyttää, että palveluntarjoaja tarjoaa käytön seurannan (Kyberturvallisuuskeskus, 2020). Mikäli kapasiteetti on laskettu väärin ja sen tarve ylittää todellisen kapasiteetin, on vaarana, että palvelu kaatuu (Paquette ym., 2010).

Kolmas vaatimus, varmistus- ja palautusprosessit, tavoittelevat saatavuuden, eheyden että luottamuksellisuuden säilymistä (Kyberturvallisuuskeskus, 2020). Varmistus- ja palautusprosessit ovat myös kiinteä osa jatkuvuussuunnitelmaa, jotta voidaan toimia sekä palvelutasosopimusten että lainsäädännön mukaisesti unohtamatta liiketoimintavaatimuksia (Kyberturvallisuuskeskus, 2020). Toiminnan jatkuvuuden sisällytys palvelutasosopimukseen edellyttää, että varmistetaan edellä mainitut varmistus- ja palautusprosessit; lisäksi tarvitaan suunnitelma palvelun palauttamiseksi katastrofitilanteessa (Kandukuri ym., 2009). Katastrofitilanteella voidaan tarkoittaa esimerkiksi sitä, ettei pilvipalvelussa oleva data ole käytettävissä pitkittyneen katkon vuoksi, tai pahimmassa

tapauksessa data on lopullisesti tuhoutunut (Wayne & Grance, 2011). Otettujen varmuuskopioiden suojauksessa tulee noudattaa samoja käytänteitä kuin alkuperäisen tiedon suojaamisessa (Kyberturvallisuuskeskus, 2020). Mikäli tietoa on paljon ja se kasautumisvaikutuksen vuoksi vaatii korkeamman suojaustason kuin alkuperäinen tieto, tulee siinä tapauksessa toimia uuden turvaluokituksen mukaisesti (Kyberturvallisuuskeskus, 2020).

Haavoittuvuuksien hallinta on viimeinen käyttöturvallisuuteen liittyvä vaatimus. Sillä pyritään hallitsemaan ohjelmistohaavoittuvuuksia koskevia riskejä ja pitämään ne kestettävällä tasolla (Kyberturvallisuuskeskus, 2020). Haavoittuvuuksia voidaan estää esimerkiksi tunkeutumisenestojärjestelmällä, joka hälyttää mahdollisen hyökkäyksen sattuessa ja tarjoaa mahdollisuuden torjua hyökkäys (Stewart ym., 2012). Ohjelmistohaavoittuvuuksien hallitsemiseksi tulee myös seurata sekä viranomaisten että laite- ja ohjelmistovalmistajien tietoturvatiedotteita sekä tehdä hallitusti julkaistut tietoturvaan liittyvät päivitykset (Kyberturvallisuuskeskus, 2020; Stewart ym., 2012). Järjestelmille tulee myös tehdä kuukausittainen tunnettujen haavoittuvuuksien tarkastus, kuten myös säännöllinen riippumattoman tahon suorittama tunkeutumistestaus (Kyberturvallisuuskeskus, 2020). Tietoverkkoon liittyviä haavoittuvuuksia voi estää myös sisällyttämällä tietoverkkoinfrastruktuuriin palomuurin (Stewart ym., 2012). Toimittajan tulee tiedottaa asiakkaitaan merkittävistä haavoittuvuuksista ja haavoittuvuuden vaikutuksesta asiakkaan tietoihin (Kyberturvallisuuskeskus, 2020).

4.2.10 Siirrettävyys ja yhteensopivuus

Siirrettävyyden ja yhteensopivuuden keskeinen ajatus on, että asiakas voi tarvittaessa vaihtaa palveluntarjoajaa tai vaihtoehtoisesti hyödyntää useita palveluntarjoajia kerralla (Kyberturvallisuuskeskus, 2020). Tietojen siirto toiselle palveluntarjoajalle tai niiden hajauttaminen ei saa vaarantaa tietoturvan perusperiaatteita (Kyberturvallisuuskeskus, 2020). Tiedon hajauttaminen voi parantaa tiedon saatavuutta, mutta uhata etenkin tiedon eheyttä, sillä tiedon sijaitessa useassa paikassa, on mahdollisuus siihen, että data on kahdentunut. Lisäksi datan korruptoitumisen tutkiminen on vaikeaa. (AlZain, Pardede, Soh & Thom, 2012). Jotta siirrettävyys ja yhteensopivuus toteutuu, tulee pilvipalvelujen tukea yleisesti tunnettuja siirrettävyysohjelmistoja, ja ohjelmointirajapintojen tulee olla julkaistu yhteistoimivuuden varmistamiseksi (Kyberturvallisuuskeskus, 2020). Ohjelmointirajapinnan julkaiseminen on kriittistä, sillä sille ei ole olemassa varsinaisia standardeja, ja suurin osa ohjelmointirajapinnoista ei ole julkisia, joten yhteensopivuuden sekä yhteensopivien palvelujen suunnittelu on vaikeaa ilman kuvauksia (Paquette ym., 2010). Lisäksi palvelun hallinnointiin sekä kaikkeen tietojen tuontiin tai vientiin käytetään vakiintuneita ja tunnettuja verkkoprotokollia (Kyberturvallisuuskeskus, 2020).

Tietoaineistojen tuhoamisen vaatimuksen tavoitteena on, että pilvipalvelusta poistuessakaan salassa pidettävä tieto ei vaarannu (Kyberturvallisuuskeskus, 2020). Jotta salassa pidettävä tieto ei vaarannu, tulee tietojen tuhoaminen järjestää riittävän luotettavasti sen ollessa viimeinen osa tiedon ja laitteen elinkaarta (Kyberturvallisuuskeskus, 2020; Stewart ym., 2012, 544; Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 15§). Tiedot tulee tuhota aina asiakkaan pyytäessä, sopimuksen päättyessä ja laitteistoihin liittyvien toimenpiteiden, kuten laitevaihdon yhteydessä siten, että tuhoaminen kattaa koko palvelun elinkaaren (Kyberturvallisuuskeskus, 2020). Lisäksi tuhottavan tiedon edes osittainen uudelleenkokoaminen ja uudelleenkäyttäminen tulee pystyä estämään kaikissa tilanteissa, etenkin salassa pidettävään aineistoon liittyen (Kyberturvallisuuskeskus, 2020; Stewart ym., 2012, 544; Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, 1101/2019, 15§). Tuhoaminen voidaan tehdä esimerkiksi silppuamalla, ylikirjoittamalla tai yhdistelemällä eri menetelmiä (Kyberturvallisuuskeskus, 2020).

4.2.11 Muutostenhallinta ja järjestelmäkehitys

Muutostenhallinta on yksi julkisen hallinnon pilvipalveluturvallisuuden auditoinnin avainkohdista (Ryoo ym., 2014) ja sen tavoitteena on, että tietoturvallisuuden perusperiaatteet eivät vaarannu muutosten yhteydessä (Kyberturvallisuuskeskus, 2020). Tavoitteen saavuttamiseksi palvelun muutoksille on oltava erikseen määritelty muutoksenhallintamenettely, jossa huomioidaan sekä vaatimuksenmukaisuus että sopimukselliset velvoitteet (Kyberturvallisuuskeskus, 2020). Muutoksenhallintamenettelyn osana arvioidaan muutoksen riskit, testataan muutokset erillisessä testiympäristössä, sekä hyväksytetään muutos tarvittavilla tahoilla. Testauksen yhteydessä tulee muodostaa kuva muutoksen vaikutuksista ennen sen vientiä tuotantoon. (Kyberturvallisuuskeskus, 2020). Popović & Hocenski (2010) ehdottavat, että turvallisuusnäkökulmasta voidaan standardoida pienet muutokset, jolloin henkilötyöaika voidaan käyttää kompleksisempiin ja tärkeämpiin tuotannon muutoksiin.

Järjestelmäkehitysvaatimusten taustalla on tavoite siitä, ettei luottamuksellisuus, eheys tai saatavuus vaarannu tehdyn järjestelmäkehityksen seurauksena (Kyberturvallisuuskeskus, 2020). Järjestelmäkehitykseen liittyviä vaatimuksia on yhteensä viisi, joista ensimmäinen on sovelluksien ja ohjelmointirajapintojen toteuttaminen hyviä ja tunnettuja tietoturvakäytänteitä noudattaen (Kyberturvallisuuskeskus, 2020). Toisena vaatimuksena on, että tuotantoympäristö on täysin erotettu muista ympäristöistä ja kaikki muutokset testataan ennen tuotantoympäristöön vientiä (Kyberturvallisuuskeskus, 2020; Stewart ym., 2012, 314). Kolmas vaatimus liittyy versionhallintaan: valtuuttamattomien versioiden siirto tuotantoympäristöön ei saa onnistua (Kyberturvallisuuskeskus, 2020). Jokainen uusi versio tulee hyväksyttää erillisesti organisaation versionkontrollien mukaisesti (Stewart ym., 2012, 314).

Neljäntenä vaatimuksena on, että organisaatiossa jokaisella ohjelmiston kanssa työskentelevällä tulee olla riittävä osaaminen turvallisista ohjelmistokehitysprosesseista (Kyberturvallisuuskeskus, 2020). Viimeinen, ulkoistamiseen liittyvä vaatimus edellyttää, että ulkoistettaessa huomioidaan sopimuksellisesti turvallinen ohjelmistokehitys, riittävä testaus, hyväksymistestaus sekä oikeus kehitysprosessin testaamiseen ja valvontatoimiin (Kyberturvallisuuskeskus, 2020).

4.3 Vertailu tutkimuskirjallisuutta vasten

Pilvipalvelujen turvallisuuden arviointikriteeristö (Kyberturvallisuuskeskus, 2020) on rakentunut kirjallisuudessa yleisesti tunnettujen tietoturvan osa-alueiden (Hakala, Vainio & Vuorinen, 2006, 10; Andreasson & Koivisto, 2013, 52) sekä pilvipalvelujen palvelu- ja toteutusmallien mukaisesti (Tsai ym., 2010; Dillon ym., 2010; Mell & Grance, 2011.) Lisäksi PiTuKrissa (Kyberturvallisuuskeskus, 2020) korostetaan tietoturvan peruselementtejä, luotettavuutta, eheyttä ja saatavuutta (Whitman ja Mattord, 2009), useissa eri kohdissa. Vaikka yleisesti tunnetut palvelu- ja toteutusmallit vaikuttavatkin taustalla, keskittyy PiTuKri arvioimaan turvallisuutta laajemmin, eikä suoraan erittele eri palvelumalleille kohdistettuja kriteeristön osia.

Tietoturvan osa-alueet ovat puolestaan näkyvässä roolissa: PiTuKrin yhteensä yksitoista osa-aluetta ovat johdettu kirjallisuudessa tunnetuista tietoturvan osa-alueista. Tietoturvan osa-alueista yhteensä neljä toistuu sellaisenaan PiTuKrissa. Joitain kirjallisuudessa pienemmässä roolissa olevia alakohtia, kuten siirrettävyys ja yhteensopivuus sekä muutoksenhallinta ja järjestelmäkehitys on erotettu PiTuKrissa omiksi alakohdikseen. Se on tietoturvan osa-alueisiin liittyvä merkittävin ero kirjallisuuden ja PiTuKrin välillä.

Pilvipalvelujen turvallisuusuhkiin liittyen PiTuKri pyrkii vastaamaan kirjallisuudessa tunnistettuihin turvallisuusuhkiin vaatimuksilla. Esimerkki vaatimuksesta on datan sijainti, jonka Subashini ja Kavitha (2010) tunnistavat yhdeksi turvallisuusuhaksi. Siinä missä kirjallisuudessa todettiin datan mahdollisesti jakautuvan useampaan paikkaan ilman, että asiakas on tietoinen sen sijainnista (Subashini & Kavitha, 2010; Zissis & Lekkas, 2012), on PiTuKrin vaatimuksen mukaisesti datan sijainti tiedettävä myös tapauksissa, joissa sijainti vaihtelee (Kyberturvallisuuskeskus, 2020). Toinen keskeinen ero kirjallisuuden sekä PiTuKrin välillä liittyy datan salaamiseen. Sekä PiTuKrissa että kirjallisuudessa tunnistetaan salaamisen olevan ratkaisu näkyvyyden estämiseen tahoille, joilla ei ole oikeutta tarkastella dataa. Ryanin (2013) ja Subashinin ja Kavithan (2010) mukaan datan salaamista ei aina kuitenkaan tapahdu tai se ei ole teknisesti mahdollista. PiTuKri (Kyberturvallisuuskeskus, 2020) puolestaan lähtee olettamuksesta, että kaiken säilytettävän datan on oltava salattua. Ainoastaan datan siirtäminen samassa fyysisessä tilassa joko ilman suojausta tai alemman suojaustason mukaisesti voidaan sallia. Kolmas

esimerkki turvallisuusuhkaan vastaamisesta on jaetun alustan käyttö. Datan salaamisen lisäksi PiTuKrissa on vaatimuksia pilvipalvelutyypille, mikäli säilytettävä data on luokiteltu korkeaan turvallisuusluokkaan. Korkeamman turvallisuusluokan dataa ei ole sallittu säilyttää julkisessa pilvipalvelussa eikä jaetulla alustalla, ellei kyseessä ole valtionhallinnon tai viranomaisyhteistyön kautta rajoituksin toteutettu jaettu alusta. (Kyberturvallisuuskeskus, 2020). Niissä tapauksissa kirjallisuudessa esiintyneet jaetun alustan ongelmat (Ryan, 2013) eivät realisoidu.

Pilvipalvelujen turvallisuuden arviointikriteeristön esiehdot on nostettu erityisasemaan (Kyberturvallisuuskeskus, 2020). Esiehtojen erityisasema voidaan johtaa Valtiovarainministeriön (2018) pilvipalvelulinjauksista, joiden mukaisesti sopimuksiin, palvelun jatkuvuuteen ja tiedon saatavuuteen on kiinnitettävä erityishuomiota. Popović ja Hocenski (2010) sekä Kyberturvallisuuskeskus (2020) ovat samaa mieltä siitä, että palvelun turvallisuutta voidaan arvioida ainoastaan järjestelmän tarkan kuvauksen perusteella. Osana järjestelmäkuvausta tulee olla myös palvelutasosopimus (Kyberturvallisuuskeskus, 2020), joka on kriittinen osa palvelua sekä palvelun soveltuvuuden arvioinnissa että valmiin palvelun aikana (Kandukuri ym., 2009). Nämä eivät kuitenkaan toistu järjestelmällisesti yhdessä siten, että niistä muodostuisi vastaava erityisasemassa oleva kokonaisuus, kuin Pilvipalvelujen turvallisuuden arviointikriteeristössä.

Esiehtojen jälkeen tulevat muut osa-alueet eivät ole erityisasemassa, mutta sisältävät kirjallisuudesta tunnettuja ja turvallisuuden kannalta oleellisia tekijöitä, joita tässä työssä täsmennettiin ja tarkennettiin kirjallisuuden avulla. Täsmentämällä ja tarkentamalla varmistuttiin myös siitä, että PiTuKrin tekijät ovat yleisesti kirjallisuudessa tunnettuja ja sisällöltään samanlaisia. Tunnettuuden ja sisällön varmistaminen on tässä tutkielmassa tutkimuskysymykseen vastaamisen kannalta oleellista. Kaikkien osa-alueiden ollessa keskenään tasavertaisia, muodostuu niistä kattava kokonaisuus, jossa jokainen osa-alue tulee ottaa huomioon turvallisuutta arvioitaessa.

Tietoturvan osa-alueiden ja turvallisuusuhkien lisäksi sekä kirjallisuudessa että Pilvipalvelujen turvallisuuden arviointikriteeristössä toistuu elinkaariajattelu. Hakalan ym. (2006, 11) mukaan koko tietoaineiston elinkaaresta on huolehdittava. PiTuKri on samaa mieltä ja korostaa tiedon tallennukseen, siirtämiseen, palauttamiseen ja tuhoamiseen liittyviä asioita (Kyberturvallisuuskeskus, 2020). Hakalan ym. (2006, 11) näkemys koskee laajemmin sekä digitaalisia että paperisia asiakirjoja, mutta sen sisältäessä digitaaliset asiakirjat, on ajatus sovellettavissa myös pilvipalveluihin.

PiTuKrin ollessa arviointikriteeristö, se ei suoraan esitä kirjallisuudessa esiintyvää näkemystä siitä, että tietoturva olisi kuin ympyrä (Blakley ym., 2001). Siitä huolimatta PiTuKriin on kuvattu erillinen hyväksyntäprosessi, joka osittain noudattaa Blakleyn ym. (2001) ympyräajattelua. Hyväksyntäprosessissa ympyräajattelu toistuu niin kauan, kun hyväksynnän edellytykset täyttyvät. Mikäli hyväksynnän jälkeen hyväksynnän edellytykset eivät enää täyty, hyväksyntä raukeaa ja uusi

hyväksyntäprosessi alkaa alusta (Kyberturvallisuuskeskus, 2020). Blakleyn ym. (2001) ajattelussa on kuitenkin kuvattu myös jatkuvan parantamisen vaihe, jota PiTuKriin ei ole kuvattu (Kyberturvallisuuskeskus, 2020).

5 YHTEENVETO

Tämä kandidaatintutkielma on kirjallisuuskatsausmuodossa. Tutkielmassa käsitellään sitä, millä tavoin yksittäinen julkishallinnon organisaatio voi arvioida käyttämiensä pilvipalveluiden turvallisuutta. Tutkielman teon yhteydessä huomattiin, että pilvipalveluita ja niiden turvallisuutta on tutkittu runsaasti, mutta Suomessa vastaavaa tutkimusta on vain vähän. Lisäksi sekä pilvipalveluita että pilvipalveluiden turvallisuutta koskevat julkishallinnon linjaukset ovat verrattain uusia.

Tutkielman ensimmäinen osa käsittelee pilvipalveluja yleisesti tieteellisen kirjallisuuden pohjalta käyden läpi pilvipalvelujen ominaispiirteitä sekä yleiset toteutus- ja palvelumallit. Lisäksi luvussa käsitellään Valtiovarainministeriön vuonna 2018 julkaisemat pilvipalvelulinjaukset, jonka pohjalta julkishallinnon organisaatiot voivat suunnitella pilvipalvelujen käyttöönottoa. Toisessa osassa käsitellään tietoturvan osa-alueita ja yleisesti tietoturvaa julkishallinnossa. Erityisiä piirteitä tietoturvalle julkishallinnossa asettaa Julkisuuslaki sekä vuoden 2020 alusta voimaan tullut Tiedonhallintalaki. Lisäksi Suomessa on Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI, jonka tehtävänä on vastata digitaalisen turvallisuuden strategisesta ohjaamisesta.

Tutkielman kolmas sisältöluku käsittelee sekä yleisimpiä tietoturvauhkia pilvipalveluissa että julkishallinnon pilvipalvelutututurvallisuuden varmistamista. Tutkielman varsinainen tutkimuskysymys on: ”Mitä tekijöitä julkishallinnon organisaation tulee ottaa huomioon käyttämiensä pilvipalveluiden turvallisuutta arvioidessa?” Käsittelyn pohjana tutkielmassa käytettiin tieteellistä kirjallisuutta sekä *Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKria*, joka on julkaistu ensimmäisen kerran vuonna 2019. Koska PiTuKri ottaa huomioon sekä julkishallinnon tietoturvaan liittyviä asioita, kuten VAHTI-ohjeet sekä turvallisuutta koskevan lainsäädännön että muita yleisesti käytössä olevia kaupallisia malleja, päätettiin kaupalliset mallit jättää muilta osin tässä tutkielmassa huomiotta.

Kirjallisuuden ja PiTuKrin yhteinen näkemys tietoturvan osa-alueista ja jokaisen osa-alueen alla olevista tekijöistä tuottavat kattavan ja yhdenmukaisen listan huomioon otettavista tekijöistä. Tutkielman johtopäätöksenä voidaankin todeta, että julkishallinnon organisaation tulee ottaa huomioon Pilvipalvelujen turvallisuuden arviointikriteeristössä lueteltuja tekijöitä käyttämiensä pilvipalvelujen turvallisuuden tai uuden palvelun sopivuuden arvioinnissa. Huomioon otettavat tekijät jakautuvat esiehtojen, turvallisuusjohtamisen, henkilöstöturvallisuuden, fyysisen ympäristön turvallisuuden, tietoliikenneturvallisuuden, identiteetin ja pääsyn hallinnan, tietojärjestelmäturvallisuuden, salauksen, käyttöturvallisuuden, siirrettävyyden ja yhteensopivuuden sekä muutostenhallinnan ja järjestelmäkehityksen alle. Mainitut osa-alueet sisältävät laajasti erilaisia henkilöihin, tietoliikenneyhteyksiin, laitteistoihin, palvelun ylläpitoon, siirrettävyyteen ja kehittämiseen liittyviä tekijöitä. Tekijöiden selvittäminen ja niiden oikeellisuuden varmistaminen tutkimuskirjallisuuden avulla vastaa tämän tutkielman tutkimuskysymykseen. Lisäksi tutkielman sivuhuomiona voidaan todeta, että Pilvipalvelujen turvallisuuden arviointikriteeristö on kattava työväline pilvipalvelujen turvallisuuden arviointiin julkishallinnossa.

Tutkimuskirjallisuudesta ei selvinnyt, kuinka paljon julkishallinnon organisaatiot ovat käyttäneet pilvipalveluita ennen julkaistuja pilvipalvelulinjauksia ja pilvipalvelujen turvallisuuden arviointikriteeristöä. Sen lisäksi tutkielmaa tehdessä ei löytynyt tietoa siitä, ovatko linjaukset ja arviointikriteeristö helpottaneet tai lisänneet julkishallinnon halukkuutta ottaa pilvipalveluja käyttöön. Aiheelle sopivia jatkotutkimusaihe voisi olla, miten julkishallinnon pilvipalveluiden käyttö ja niiden turvallisuuden varmistaminen koettiin ennen ja jälkeen pilvipalvelulinjausten ja turvallisuuden arviointikriteeristön julkaisun. Toisena jatkotutkimusaiheena voisi pohtia, onko pilvipalvelujen käyttö ja/tai turvallisuus lisääntynyt vuosien 2018–2019 jälkeen.

LÄHTEET

Alonso, J., Escalante M., Orue-Echevarria, L. (2016) Transformational Cloud Government (TCG): Transforming Public Administrations with a Cloud of Public Services. *Procedia Computer Science* 97, 43-52.

AlZain M., Pardede E., Soh, B. & Thom J. (2012) Cloud Computing Security: From Single to Multi-Clouds. *Hawaii International Conference on System Sciences*. IEEE.

Anjana & Singh, A. (2018) Security concerns and countermeasures in cloud computing: a qualitative analysis. *International Journal of Information Technology*, 11(4), 683-690.

Anderson, J. (2003) Why we need a new definition of information security. *Computers & Security*, 22 (4), 308-313

Andreasson, A., Koivisto J. (2013) Tietoturvaa toteuttamassa. Tietosanoma.

Blakley, B., McDermott E., Geer, D. (2001) Information security is information risk management. *Proceedings of the 2001 workshop on New security paradigms*, 97-104. doi: 10.1145/508171.508187

Cloud Security Alliance (2017) Top Threats to Cloud Computing + Industry Insights. Haettu osoitteesta https://downloads.cloudsecurityalliance.org/assets/research/top-threats/treacherous-12-top-threats.pdf

Digi- ja väestötietovirasto (2020) Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. Haettu 07.06.2020 osoitteesta https://dvv.fi/vahti

Dillon, T., Wu, C. & Chang, E. (2010) Cloud Computing: Issues and Challenges. *IEEE International Conference on Advanced Information Networking and Applications,* 27-33

Elsenpeter, R., Velte, A. & Velte, T. (2010) Cloud Computing: A Practical Approach

Grobaurer, B., Walloscheck T. & Stöcker E. (2011) Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy*, 9(2), 50-57.

Hakala, M., Vainio M., Vuorinen O. (2006) Tietoturvallisuuden käsikirja. Talentum Pro.

Herbane, B., Elliott, D. & Swartz E. (2004) Business Continuity Management: time for a strategic role? *Long Range Planning*, 37(5), 435-457.

Jadeja Y. & Modi, K. (2012) Cloud computing - concepts, architecture and challenges. 2012 *International Conference on Computing, Electronics and Electrical Technologies* [ICCEET]

Joshi B., Vijayan A. & Joshi B. K. (2012) Securing cloud computing environment against DDoS attacks. *2012 International Conference on Computer Communication and Informatics*, 1-5

Julkisuuslaki 621/1999. Laki viranomaisen toiminnan julkisuudesta.

Kandukuri, B. & Paturi, R., Rakshit A., (2009). Cloud Security Issues. *2009 IEEE International Conference on Services Computing*, 517-520. Bangalore: IEEE.

Kaufman, L. (2009). Data Security in the World of Cloud Computing. *IEEE Security & Privacy*, 7(4), 61-64.

Kyberturvallisuuskeskus (2020) Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri). Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Lehto M., Limnéll, J., Innola E., Pöyhönen J., Rusi T., Salminen M. (2017). Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitteen saavuttamiseksi. Valtioneuvoston selvitys- ja tutkimustoiminta. Haettu 4.7.2020 osoitteesta http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160233/Suomen_kybertu rvallisuuden_nykytila%2c__tavoitetila_ja.pdf?sequence=1&isAllowed=y

Liu, F., Tong J., Mao J., Bohn, R., Messina J., Badger L, & Leaf D. (2011). NIST Cloud Computing Reference Architecture.

Mell, P. & Grance, T. (2011). The NIST definition of cloud computing.

Paquette S., Jaeger, P. T. & Wilson S. C. (2010) Identifying the security riss associated with governmental use of cloud computing. *Government Information Quarterly*, 27(2), 245-253

Popović, K. & Hocenski Ž. (2010). Cloud computing security issues and challenges. *The 33rd International Convention MIPRO*, 344-349

Posthumus, S. & Von Solms, R. (2004) A framework for the governance of information security. *Computers & Security*, 23(8), 638-646

Ramgovind, S., Eloff M., Smith, E. (2010) The management of security in Cloud computing. 2010 *Information Security for South Africa*, 1-7

Ruohonen, M. 2002. Tietoturva. Porvoo: WS Bookwell.

Ryan, M. (2013) Cloud computing security: The scientific challenge, and survey of solutions. *The Journal of Systems and Software*, 86(9), 2263-2268.

Ryoo, J., Rizvi, S., Aiken, W. & Kissel J. (2014) Cloud Security Auditing: Challenges and Emerging Approaches. *IEEE Security & Privacy*, 12(6), 68-74.

Sanastokeskus (2004). Tiivis tietoturvasanasto. Haettu 25.4.2020 osoitteesta https://www.tsk.fi/fi/info/TiivisTietoturvasanasto.pdf

Subashini, S. & Kavitha, V. (2011) A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(1), 1-11.

Stewart, J., Chapple M. & Gibson D. (2012) CISSP: Certified Information Systems Security Professional Study Guide.

Tiedonhallintalaki 906/2019. Laki julkisen hallinnon tiedonhallinnasta.

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

Tilastokeskus (2019) Tietotekniikan käyttö yrityksissä. Haettu osoitteesta http://tilastokeskus.fi/til/icte/2019/icte_2019_2019-12-03_fi.pdf

Tsai, W., Sun, X. & Balasooriya, J. (2010). Service-oriented cloud computing architecture. *Information Technology: New Generations (ITNG), 2010 Seventh International Conference* (684-689). IEEE.

Valtioneuvoston asetus turvallisuusluokittelusta valtionhallinnossta, 1101/2019.

Valtiovarainministeriö (2020) VAHTI-toiminnan organisointi. Haettu 06.06.2020 osoitteesta https://vm.fi/vahti-toiminnan-organisointi

Valtiovarainministeriö (2018) Julkisen hallinnon pilvipalvelulinjaukset. 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

Valtiovarainministeriö (2019) Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa, muistio. Haettu 07.06.2020 osoitteesta https://valtioneuvosto.fi/delegate/file/63446

Von Solms, R. & Van Niekerk, J. (2013) From information security to cyber security. *Computers & Security*, 38 (2013) 97-102

Wailly A., Lacoste M. & Debar H. (2011) *Towards Multi-Layer Autonomic Isolation of Cloud Computing and Networking Resources.* 2011 Conference on Network and Information Systems Security, 1-9.

Watkins, S. (2013) An Introduction to Information Security and ISO27001 : 2013.

Wayne, J. & Grance T. (2011) Guidelines on Security and Privacy in Public Cloud Computing. NIST.

Whitman, M. & Mattord, H. (2009) Principles of information security.

Xun, X. (2011) From cloud computing to cloud manufacturing. *Robotics and Computer-Integrated Manufacturing* 28 (2012) 75–86

Zissis D. & Lekkas D. (2010) Addressing cloud computing security issues. *Future Generation Computer Systems* 28 (2012) 583–592.