LAUREA AMMATTIKORKEAKOULU Uuden edellä

Pilvipalveluiden arvioinnin kehittäminen Kesko-konsernissa

Kaipio, Anssi

2012 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Pilvipalveluiden arvioinnin kehittäminen Kesko-konsernissa

Kaipio Anssi
Turvallisuusalan ko.
Opinnäytetyö
Toukokuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Anssi Kaipio

Pilvipalveluiden arvioinnin kehittäminen Kesko-konsernissa

Vuosi 2012 Sivumäärä 61

Pilvipalvelu on voimakkaasti kasvava malli, jossa tietojenkäsittelyresursseja tarjotaan joustavasti Internetin välityksellä. Pilvipalveluista ja niiden tietoturvallisuudesta on viimeaikoina ollut paljon uutisointia ja keskustelua. Usein ongelmalliseksi koetaan hallinnollisen vastuun siirtyminen pilvipalveluntarjoajalle. Tämä tarkoittaa sitä, että palveluntarjoajalla on merkittävä vastuu tietoturvallisuudesta. Palvelun asiakkaan on voitava luottaa siihen, että palveluntarjoaja toimii turvallisuusasioissa asiakkaan edun mukaisesti.

Työni tarkoitus oli kehittää pilvipalveluiden arviointiprosessia Kesko-konsernissa. Pilvipalvelut koettiin toimeksiantajaorganisaatiossa tietoturvallisuuden kannalta haasteelliseksi. Julkisen pilven toteutusmalli ja Software as a Service palvelumalli olivat toimeksiantajan näkökulmasta kiinnostavimmat selvityskohteet. Keskossa ei ollut aiemmin tehty selvityksiä pilvipalveluiden turvallisuudesta.

Selvitin mitä riskejä julkisen pilven Software as a Service -palveluihin liittyy ja tein selvitykseen perustuvan pilvipalvelun arviointityökalun. Riskien merkittävyydet arvioitiin Keskossa. Työkalua käyttämällä palveluntarjoajalle esitetään kysymyksiä haastattelutilanteessa. Vastaukset arvioidaan ja työkalu mahdollistaa palveluntarjoajien vertailun.

Lähestymistapana työssäni oli konstruktiivinen tutkimus. Menetelmänä riskiselvityksessä käytin kirjallisuuskatsausta. Keskeisiä lähteitä olivat Euroopan verkko- ja tietoturvavirasto ENISA:n ja Yhdysvaltalaisen National Institute of Standards and Technologyn julkaisut. Pilvipalvelun arviointityökalun toteutin Microsoftin Excel-taulukkolaskentaohjelmalla.

Työtäni hyödyntämällä Keskon liiketoimintayhtiöt voivat itsenäisesti arvioida pilvipalvelun toimittajien soveltuvuutta ja palveluiden tietoturvallisuutta. Arviointityökalua käyttämällä palveluntarjoajien järjestelmällinen arviointi on mahdollista. Työni perusteella toimeksiantaja voi yhtenäistää omia toimintatapojaan pilvipalveluiden arvioinnissa.

Asiasanat: Pilvipalvelu, julkinen pilvi, Software as a Service, riski

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Anssi Kaipio

Developing the cloud service evaluation process in Kesko Corporation

Year 2012 Pages 61

Cloud service is a rapidly growing model where computing resources are elastically provided over the Internet. Information security in cloud computing has been a popular topic recently in the news and discussions. A commonly experienced problem concerns governing the service, which is typically a responsibility of the cloud service provider. The cloud service provider has a remarkable responsibility for the information security. A cloud customer must rely on the service provider acting according to the customer's best interest when security is concerned.

The purpose of this thesis was to develop the evaluation process of cloud services in Kesko Corporation. Cloud services were considered challenging from an information security perspective. The deployment model of public cloud and the Software as a Service model were regarded as the most interesting targets for research. Investigations about the security of cloud services were not previously made at Kesko.

Research was conducted on the risks that are involved in the public cloud deployment model and the Software as a Service model and an evaluation tool for cloud services was created. Risk assessment was performed in Kesko. When using the evaluation tool, questions about the risks are presented to the cloud service provider in an interview. The replies are evaluated and the tool provides the possibility of comparing the service providers.

Constructive research was the approach in this thesis project. Literature review was used as a method. Important sources of information were publications of the European Network and Information Security Agency and the National Institute of Standards and Technology. The cloud service evaluation tool was created by using Microsoft Excel.

By using the results of this thesis, Kesko's business units are capable of independently evaluating the cloud service providers and information security of the services. With the evaluation tool, it is possible to evaluate cloud services in a more systematic way. Based on this thesis, Kesko Corporation can unify their procedures in the evaluation of cloud services.

Keywords: Cloud service, public cloud, Software as a Service, risk

Sisällys

1 Johdanto

Pilvipalvelu on kehittyvä ja tällä hetkellä voimakkaasti suosiotaan kasvattava malli, jossa tietojenkäsittelyresursseja tarjotaan joustavasti palveluna Internetin välityksellä. Pilvipalveluista ja niiden tietoturvallisuudesta on ollut viime vuosina paljon uutisointia ja keskustelua. Turvallisuusasiat ovat useasti merkittävä syy sille, miksi organisaatiot suhtautuvat varovaisesti pilvipalveluihin.

Tietoviikon ylläpitämässä tietohallintojohtajien uutispalvelu CIO.fi:ssä uutisoitiin 14.8.2011 tutkimusyhtiö IDC:n tekemästä arviosta, jonka mukaan vuonna 2015 jopa puolet IT-palveluista tulee pilvestä. Kyseisessä uutisessa todettiin, että pilvipalveluita käyttää jo 27 prosenttia suomalaisyrityksistä. Toisaalta samassa palvelussa uutisoitiin 2.8.2011 KPMG:n tutkimuksesta, jossa IT-palveluntarjoajien ja ulkoistuspalveluihin erikoistuneiden asiantuntijoiden mukaan yritysten IT-osastot eivät ymmärrä pilvipalveluita. Suomen asunto- ja viestintäministeri Krista Kiuru otti kantaa pilvipalveluihin 15.2.2012 järjestetyssä Viestintäfoorumissa. Kiuru totesi, että Suomesta tulee rakentaa uusi pilviteollisuuden keskittymä. (Korpimies 2011; Ranta 2011; Liikenne- ja viestintäministeriö 2012.)

Pilvipalveluiden turvallisuudesta on tehty selvityksiä. Ponemon-instituutin vuonna 2011 tekemässä tutkimuksessa haastateltiin yhteensä 127 pilvipalveluntarjoajaa, joista 103 olivat Yhdysvaltalaisia ja 24 kuudesta eri Euroopan maasta. Tutkimuksen mukaan suuri osa ei pidä turvallisuutta kilpailuetuna ja palveluntarjoajan tärkeänä vastuuna, eivätkä usko heidän palvelun merkittävästi suojaavan asiakkaiden luottamuksellista tietoa. Monet palveluntarjoajat näkivät, että pilvipalvelun turvallisuus on asiakkaiden vastuulla eikä järjestelmien turvallisuutta aina arvioida ennen kuin palvelu annetaan asiakkaan käyttöön. Palveluntarjoajat ilmoittivat käyttäneensä turvallisuuteen keskimäärin kymmenen prosenttia tai vähemmän heidän operatiivisista resursseista ja useimmat eivät uskoneet täyttävänsä asiakkaiden vaatimuksia turvallisuudelle. Suuri osa palveluntarjoajista myönsi, että heillä ei ole palvelun turvallisuudesta vastaavaa ja pelkästään sille omistautunutta henkilöstöä. Yksityisen pilven toteutusmallia käyttävät pilvipalveluntarjoajat olivat julkista ja hybridimallia käyttäviä palveluntarjoajia luottavaisempia siihen, että pystyvät täyttämään turvallisuusvaatimukset. Palveluntarjoajien mukaan asiakkaiden tyypillisimmät syyt pilvipalveluiden hankinnalle olivat kustannussäästöt ja nopeampi palveluiden käyttöönotto. (Ponemon Institute 2011, 1 - 2.)

Valitsin työni aihealueeksi julkisen pilven Software as a Service -palveluiden turvallisuuden, koska pilvipalvelut ovat ajankohtainen teema IT-alalla ja julkisen pilven palveluiden tietoturvallisuuteen liittyy paljon epätietoisuutta. Julkinen pilvi on suosituin pilvipalvelun toteutusmalli ja Software as a Service on yleisin palvelumalli. Tavoitteena on selvittää, mitä riskejä kyseisiin palveluihin liittyy asiakkaan näkökulmasta. Työssä riskiselvityksen pohjalta syntyvä

produkti, eli turvallisuudenarviointityökalu auttaa opinnäytetyön toimeksiantajaa tulevissa hankintaprosesseissa.

Opinnäytetyöni on osa laajempaa pilvipalveluselvitystä, jonka tein työn toimeksiantajan hyväksi. Toimeksiantaja on suomalainen kaupan alalla toimiva konserni Kesko Oyj. Taustalla oli työharjoitteluni, jossa kehittämistehtävänä selvitin pilvipalveluita ja niiden hyötyjä kaupan toimialan näkökulmasta. Tässä työssä keskityin turvallisuusnäkökulmaan. Aiheen rajasin tarkemmin koskemaan Keskon kannalta kiinnostavinta pilvipalveluiden toteutusmallia ja palvelumallia. Yhdessä nämä hankkeet ovat kokonaisuus, jonka perusteella toimeksiantajan on mahdollista arvioida pilvipalveluiden potentiaalia heidän omalla toimialallaan, palveluihin liittyviä riskejä sekä hankittavien pilvipalveluiden turvallisuutta. Otin aluksi yhteyttä Keskoon ja tarjosin pilvipalveluihin liittyviä aiheita työharjoitteluun sekä opinnäytetyöhön. Hyvin nopeasti selvisi, että kysyntää oli ja sovimme etenemisestä.

Kesko-konserni on johtava kaupan alan palveluyritys ja pörssiyhtiö. Konsernin toimialoja ovat ruokakauppa, käyttötavarakauppa, rautakauppa sekä auto- ja konekauppa. Keskon ketjutoimintaan kuuluu noin 2000 kauppaa Suomessa, Ruotsissa, Norjassa, Virossa, Latviassa, Liettuassa, Venäjällä sekä Valko-Venäjällä. Keskon pääjohtaja on Matti Halmesmäki. Kesko-konsernin liikevaihto vuonna 2011 oli 9 460 miljoonaa euroa ja henkilömäärä Joulukuussa 2011 oli 23 375, joista Suomessa työskenteli 13 124 henkilöä. Kesko perustettiin vuonna 1940, kun neljä kauppiaiden perustamaa alueellista tukkukauppaa, Savo-Karjalan Tukkuliike, Keski-Suomen Tukkukauppa Oy, Kauppiaitten Oy ja Maakauppiaitten Oy sulautuivat yhteen. (Kesko lyhyesti 2011; Keskon tilinpäätöstiedote 1.1.-31.12.2011 2012; Keskon historia 2010; Keskon hallinto ja johto 2011.)

Työn ohjaajan Jari Törmälän mukaan odotuksena olivat objektiiviset tuotokset, jotka lisäävät organisaation ymmärtämystä pilvikonseptista. Keskon ICT-infrastruktuuripalveluissa ei ollut käytettävissä omia henkilöresursseja pilvipalveluiden soveltuvuuden ja turvallisuuden selvittämiseen. Selvitys koettiin tarpeelliseksi tehdä. Työhön kuuluvan riskiselvityksen odotettiin tuottavan tietoa, joka tukee päätöksentekoa. Riskiselvityksen pohjalta syntyvän produktin tuli olla hyödyntämiskelpoinen käytännön toiminnassa. Tarkoituksena oli, että konsernin eri liiketoiminnot voivat tulevaisuudessa itsenäisesti arvioida pilvipalveluiden soveltuvuutta omaan käyttöön ja samalla yhtenäistää Keskon toimintatapoja pilvipalveluiden arvioinnissa ja käyttöönotossa.

Keskossa tiedostettiin, että esimerkiksi Euroopan verkko- ja tietoturvavirasto ENISA on listannut pilvipalveluntarjoajille esitettäviä kysymyksiä ja Cloud Security Alliance on tehnyt matriisin, jossa on riskienhallintamenettelyitä. Olemassa olevien kysymyslistojen, suositusten, matriisien ja tarkistuslistojen koettiin usein menevän liialliseen tarkkuuteen. Vastauksia palvelun-

tarjoajalta ei välttämättä ole odotettavissa ja käyttäjään kohdistuu liikaa paineita osaamisen suhteen. Vastaukset saattavat jäädä liian yksinkertaiseksi, jolloin niiden avulla ei saa riittävää arviointia tehtyä. Työni ratkaisi asian siten, että toteutin sen täysin Keskon toiveiden mukaisesti ja huomioiden tulevat loppukäyttäjät. Riskiselvityksen pyrin tekemään informatiiviseksi, mutta helposti ymmärrettäväksi ja produktin helppokäyttöiseksi. Lopputuloksena oli Keskon toimintaan soveltuva ratkaisu.

Tämä raportti jakautuu neljään osaan, jotka ovat kehittämistyö, tietoperusta, toteutus ja arviointi. Kehittämistyössä kuvaan kehittämiskohteen ja tehtävän, aiheen rajaukset sekä työn lähestymistavan ja menetelmän, jonka mukaan tein riskiselvityksen. Tietoperusta sisältää työssä oleellisten käsitteiden määrittelyn ja riskiselvityksen. Toteutuksessa esitän varsinaisen produktin tuottamisen. Arvioinnissa käsittelen työn onnistumista ja hyödynnettävyyttä Keskokonsernissa.

2 Kehittämistyö

Kehittämiskohde työssäni oli julkisen pilven Software as a Service -palveluiden hankintaprosessiin kuuluva palvelun turvallisuuden arviointi. Julkisen pilven Software as a Service -palvelut koettiin hankeorganisaatiossa tietoturvallisuuden kannalta ongelmalliseksi, koska kyseisissä palveluissa asiakkaalla ei ole kontrollia turvallisuusmenettelyihin, paitsi palvelun käytön osalta. Turvallisuuden arviointiin haasteellisuutta lisäsi myös se, että hankeorganisaatio ei ollut tehnyt aiempia selvityksiä pilvipalveluihin liittyvistä riskeistä.

Palvelunhankkijan näkökulmasta julkisen pilven palveluiden tietoturvallisuusasiat ovat haasteellisia. Turvallisuuteen voi lähtökohtaisesti vaikuttaa ainoastaan palveluun liittyvien sopimusten avulla ja valitsemalla mahdollisimman luotettavan palveluntarjoajan. Palveluntarjoajan ja palvelun luotettavuutta voi arvioida tiedustelemalla tarkemmin, miten palvelun turvallisuutta ylläpidetään ja miten siihen liittyviin turvallisuusriskeihin on varauduttu. Näin saa läpinäkyvyyttä palveluntarjoajan turvallisuusmenettelyihin, mikä lisää luottamusta ja vähentää mahdollisia tietoturvahuolia joita asiakas kokee. Palveluntarjoajan tulee pystyä osoittamaan asiakkaalle, että turvallisuuden ylläpitämiseen panostetaan ja palveluun liittyviin riskeihin on asianmukaisesti varauduttu. Mikäli asiakkaalle ei anneta riittävästi tietoa turvallisuutta koskevista asioista, on syytä kyseenalaistaa tarjotun palvelun luotettavuus. Asiakkaan on myös vaikeaa tehdä omaa riskienarviointia, mikäli palvelun taustalla olevat turvallisuusasiat ovat epäselviä.

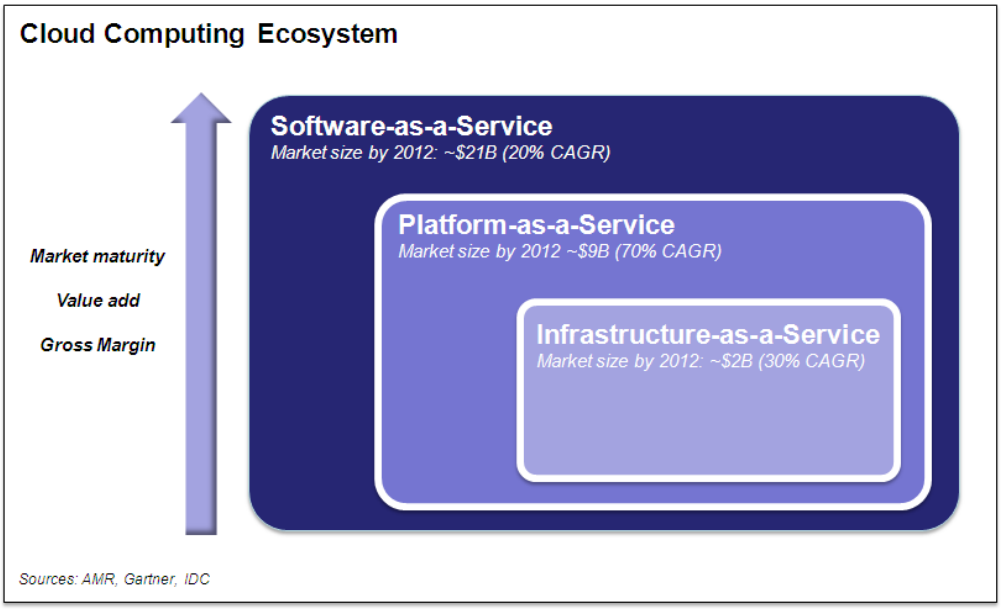
Kehittämistehtävänä oli selvittää julkisen pilven Software as a Service -palveluiden riskit ja tuottaa niiden perusteella työkalu palvelun turvallisuuden arviointiin. Lopputuloksena syntyi Excel-pohjainen arviointityökalu, jota voi hyödyntää palvelun hankintaprosessissa kun palve-

lun turvallisuutta arvioidaan. Työkaluun sijoitin julkisen pilven Software as a Service -palveluiden riskien perusteella laatimani kysymykset, jotka palveluntarjoajalle esitetään. Palveluntarjoajan niihin antamia vastauksia voi arvioida arvoasteikolla ja useita palveluntarjoajia on mahdollista vertailla keskenään. Työkalua käyttämällä voi saada tietoa palveluntarjoajan varautumisesta riskeihin, turvallisuuden ylläpidosta sekä halukkuudesta läpinäkyvyyteen. Työni avulla on mahdollista tunnistaa palveluntarjoajat, jotka eivät ole panostaneet riittävästi turvallisuuteen. Kehittämistehtävällä pyrin siihen, että tulevaisuudessa Kesko Oyj:n hankkimat julkisen pilven Software as a Service -palvelut ovat mahdollisimman turvallisia. Keskon tietoturvapäällikkö Jari Törmälä arvioi työn hyödynnettävyyttä ja onnistumista.

2.1 Rajaukset

Tehtävän aiheen rajasin koskemaan julkisen pilven toteutusmallia ja Software as a Service -palvelumallia. Syy rajaukselle oli työn toimeksiantajan intressi, koska julkinen pilvi koettiin Keskossa tietoturvallisuuden kannalta haasteelliseksi ja Software as a Service palvelumalliksi, jossa on tällä hetkellä eniten hyödyntämispotentiaalia. Käyttämäni rajaus oli Keskon kannalta mielenkiintoisin. Mikäli työ sisältäisi kaikki pilvipalveluiden palvelumallit ja toteutusmallit, niin selkeää fokusta ei olisi ja käsiteltävät aiheet saattaisivat jäädä liian yleiselle tasolle.

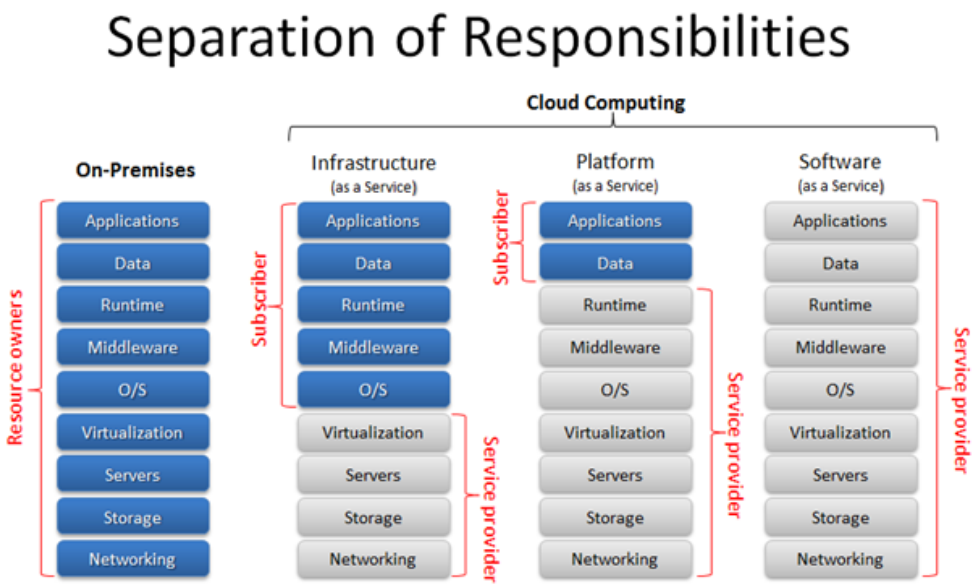
Aiheen rajaaminen Software as a Service palveluihin oli perusteltua niiden suosion vuoksi. Software as a Service on kypsin pilvipalveluiden segmentti ja suosituin pilvipalveluiden palvelumalli. Markkinaosuus pilvipalveluista Software as a Service -palvelumallilla on Bessemer Venture Partnersin vuonna 2010 tekemässä selvityksessä ennustettu olevan noin 21 miljardia dollaria vuonna 2012. Muiden yleisesti tunnettujen pilvipalvelumallien yhteenlaskettu osuus olisi noin 11 miljardia dollaria. Turun yliopiston SaaS-tutkimusprojektin tuottamassa SaaS-käsikirjassa on kuvattu markkinoilla olevan vahvaa kysyntää Software as a Service palveluille. Vuonna 2011 Software as a Service -yrityssovellusten markkinoiden uskottiin kasvavan 10.7 miljardiin dollariin, joka olisi 16.2 prosenttia kasvua vuodesta 2010. Osuuden ohjelmistoalan kokonaisliikevaihdosta on ennustettu nousevan vuoteen 2013 mennessä seitsemästä prosentista 17 prosenttiin ja saavuttavan merkittävän osuuden ohjelmistotuotemarkkinoilla, joka on noin neljännes koko ohjelmistomarkkinoista. (Botteri ym. 2010, 2; Järvi, Karttunen, Mäkilä & Ipatti 2011, 10.)



Kuva 1: Pilvipalveluiden ekosysteemi (Botteri ym. 2010, 2)

Kuva yksi on Bessemer Venture Partnersin vuonna 2010 tekemästä selvityksestä. Software as a Service on kypsin palvelumalli. Myyntikatteet Software as a Service -palveluissa ovat parhaita ja palvelut tuottavat eniten lisäarvoa. Muiden yleisesti tunnettujen pilvipalvelumallien yhteenlaskettu osuus pilvipalveluiden markkinoista on pienempi kuin Software as a Service –palvelumallilla.

Otin julkisen pilven toteutusmallin tarkastelun alle, koska se on tietoturvallisuuden kannalta haasteellisin. Julkisessa pilvessä on useita tekijöitä, jotka aiheuttavat huolia tietoturvallisuuden näkökulmasta. Julkisen pilven ympäristöt ovat taustalla olevalta tekniikaltaan monimutkaisempia kuin perinteiset konesaliratkaisut. Yleiseen tietojenkäsittelyyn tarvittavien osien lisäksi julkisessa pilvessä tarvitaan useita pilviympäristön hallinnointiin liittyviä komponentteja. Palveluiden toteutus saattaa olla vielä riippuvaista useiden pilvijärjestelmien kerroksista, joita hallinnoivat useat palveluntarjoajat. Monimutkaisuus tyypillisesti vaikuttaa käänteisesti turvallisuuteen, koska monimutkaisissa järjestelmissä voi olla enemmän mahdollisuuksia haavoittuvuuksille. Toteutusmalli perustuu usean vuokralaisen periaatteeseen ja se voidaan organisaatioissa kokea tietoturvan kannalta ongelmallisena, koska käytetty palvelu on samassa järjestelmässä muiden tuntemattomien tahojen kanssa. Palvelut toimitetaan Internetin välityksellä, mikä altistaa Internetiin päin näkyvät rajapinnat verkkohyökkäyksille, kuten esimerkiksi asiakkaan itsepalveluun käyttämän hallinnointirajapinnan tai rajapinnan, jonka kautta palvelua käytetään. Hallinnon tai kontrollin menettäminen vielä korostaa koettuja tietoturvahaasteita, koska julkiseen pilveen siirtyminen edellyttää hallinnollisen vastuun siirtämistä palveluntarjoajalle. Tämä tarkoittaa sitä, että palvelun asiakkaan tieto-omaisuuden turvallisuudesta vastaa ulkopuolinen taho. Asiakkaan on luotettava siihen, että tämä ulkopuolinen taho toimii asiakkaan etujen mukaisesti. (Jansen & Grance 2011, 10 - 12.)



Kuva 2: Vastuut pilvipalveluissa (Chou 2010)

Kuvassa kaksi on vastuiden jakautuminen pilvipalveluissa. Resurssien omistaja on vastuussa kaikesta, mikäli palvelu on toteutettu omissa tiloissa ja omilla resursseilla. Julkisen pilven Software as a Service -palveluissa asiakas vastaa vain palvelun käytöstä. Palveluntarjoaja omistaa pilvi-infrastruktuurin resurssit ja ne sijaitsevat palveluntarjoajan tiloissa. Tämä tarkoittaa sitä, että julkisen pilven Software as a Service -palveluissa palveluntarjoajalla on merkittävä vastuu turvallisuudesta.

2.2 Lähestymistapa

Lähestymistapana työssä oli konstruktiivinen tutkimus. Kehittämistehtäväni täytti useat konstruktiiviselle tutkimukselle tyypilliset ominaispiirteet, sillä työssäni oli ratkaistavana toimeksiantajaorganisaation kohtaama käytännön ongelma. Työn tuloksena syntyi konkreettinen tuotos, jonka ominaisuudet perustuivat aiempien tutkimusten avulla tekemääni riskiselvitykseen.

Konstruktiivinen tutkimus on sopiva lähestymistapa, mikäli kehittämistyön tarkoituksena on tehdä jokin konkreettinen tuotos. Konstruktiivisessa tutkimuksessa käytännön ongelma ratkaistaan luomalla uusi rakenne tutkimustiedon pohjalta. Näiden uusien rakenteiden luomiseen tarvitaan jo olemassa olevaa teoreettista tietoa sekä käytännöstä kerättävää uutta tietoa. Lähestymistapa on soveltuva kehittämistehtäviin joissa kehittämistyön tuloksena syntyy uusi tuotos, kuten esimerkiksi www-sivut, koulutusmateriaali, prosessimalli tai muu tuote jota arvioidaan käytännön hyödyn perusteella. Tavoitteena konstruktiivisessa tutkimuksessa on saada käytännön ongelmaan uusi ja teoreettisesti perusteltu toimiva ratkaisu, joka tuo uutta tietoa liiketoimintaan ja tiedeyhteisöön. Konstruktiivinen tutkimus on hyvä tapa, mikäli käytännön

ongelman ratkaisemiseksi tarvitaan teoreettista tietoa. Tämän kaltaisen tutkimuksen perusteella kehittämisen kohdeorganisaatio saa puolueettoman ja teoreettiseen tietoon perustuvan ratkaisun. Kyse on siis käytännönläheisestä ongelmanratkaisusta, jossa luodaan uusi rakenne. Kohdeorganisaation sekä tutkimuksen toteuttajan välillä tapahtuva kommunikaatio korostuu ja oleellista on, että toimeksiantajaorganisaatio sitoutuu kehittämiseen. (Ojasalo, Moilanen & Ritalahti 2009, 65 - 66.)

Tutkimustyön prosessiin kuuluu kuusi vaihetta, jotka ovat mielekkään ongelman etsiminen, syvällisen teoreettisen ja käytännöllisen tiedon hankinta kehittämisen kohteesta, ratkaisujen laatiminen, ratkaisun toimivuuden testaus ja konstruktion oikeellisuuden osoittaminen, käytettyjen teoriakytkentöjen näyttäminen ja ratkaisun uutuusarvon osoittaminen sekä ratkaisun soveltamisalueen laajuuden tarkastelu. Prosessissa ratkaisun laatiminen vaatii teoreettisia perusteluita ja eri vaiheiden dokumentointi on tärkeää. Käytetyt menetelmät tulee perustella ja kehittämishaaste sekä tavoitteet tulee kirjata selkeästi. Ratkaisuvaihtoehdot tulee esitellä, perustella ja arvioida. (Ojasalo ym. 2009, 67.)

Konstruktiivinen tutkimus ei rajaa pois mitään menetelmiä, mutta aineisto kannattaa kerätä monin tavoin. Kehittämistyössä tulee painottaa yhteistyötä ja oleellista on tuntea lopullisen tuotoksen käyttäjien tarpeet sekä ottaa käyttäjiä mukaan kehittämistyöhön jo varhaisessa vaiheessa. Kehittäjä itse on aina muutosagentti, joka vaikuttaa kohdeympäristössä. Oppimisen edistäjän rooli on myös mahdollinen. (Ojasalo ym. 2009, 68.)

Valitsin kuvailevan kirjallisuuskatsauksen menetelmäksi tarvittavan tietoperustan hankkimiseen, koska tarkoituksena oli tehdä kattava kuvaus julkisen pilven SaaS-palveluihin liittyvistä riskeistä. Toteutustapa oli narratiivinen yleiskatsaus. Kuvailevalla kirjallisuuskatsauksella voi saavuttaa tarkoituksenmukaisen tuloksen, koska hyvin tunnetut tahot kuten esimerkiksi National Institute of Standards and Technology (NIST), European Network and Information Security Agency (ENISA), Gartner sekä Cloud Security Alliance (CSA) ovat jo tehneet aiheesta julkaisuja, jotka ovat tuoreita. Näissä tutkimuksissa pilvipalveluita on käsitelty kaikkien pilvipalvelumallien ja toteutusmallien osalta, joten seuloin sieltä vain ne riskit jotka koskevat julkisen pilven SaaS-palveluita. Keskustelin työn toimeksiantajan kanssa Keskossa tehtävistä haastatteluista mahdollisena menetelmänä, mutta sen osalta todettiin tietämyksen pilvipalveluiden osalta olevan vähäistä ja tästä syystä sillä ei saavutettaisi työn kannalta merkittävää tietoa.

2.3 Menetelmä

Kirjallisuuskatsaus on menetelmä, jossa tavoitteena on kehittää olemassa olevaa teoriaa sekä rakentaa uutta teoriaa. Sen avulla voi myös arvioida teoriaa. Kirjallisuuskatsauksessa raken-

netaan kokonaiskuva tietyistä asiakokonaisuuksista ja sillä pyritään tunnistamaan ongelmia. Katsauksen avulla on myös mahdollista kuvata tietyn teorian historiallista kehitystä. Kyseessä on metodi, jossa tutkitaan tehtyä tutkimusta, eli kootaan tutkimuksien tuloksia jotka toimivat perustana uusille tutkimuksille. Kirjallisuuskatsaukset perustuvat alkuperäisestä laadukkaasta tutkimuksesta tehtyihin johtopäätöksiin. Menetelmänä se on systemaattinen, täsmällinen ja toistettavissa oleva, jonka perusteella voidaan arvioida ja tiivistää valmiina olevaa ja julkaistua tutkimusaineistoa. Se ei ole lähdeluettelo jossa on selitykset mukana tai kirja-arvostelu. (Salminen 2011, 3 - 5.)

Kuvaileva kirjallisuuskatsaus on yleinen kirjallisuuskatsauksen tyyppi, jota voidaan luonnehtia yleiskatsaukseksi jossa ei ole tarkkoja sääntöjä. Aineistot voivat olla laajoja eikä niiden valintaa rajaa metodiset säännöt. Tutkimuskysymykset ovat väljiä kuvailevassa kirjallisuuskatsauksessa. Tutkittava asia tai ilmiö voidaan kuitenkin kuvata laajalti ja tarvittaessa luokittelemaan sen ominaisuuksia. Kuvailevassa kirjallisuuskatsauksessa on kaksi eri orientaatiota, jotka ovat narratiivinen ja integroiva. (Salminen 2011, 6 - 7.)

Narratiivinen kirjallisuuskatsaus on metodisesti kevein ja sen avulla pystytään antamaan laaja kuva käsiteltävästä aiheesta ja pyrkimyksenä on lopputulos joka on helppolukuinen. Narratiivinen yleiskatsaus on laajin tapa toteuttaa, jonka tarkoituksena on tiivistää aiemmin tehtyjä tutkimuksia. Narratiivisessa katsauksessa tutkimustietoa ei kovin systemaattisesti seulota, mutta silti sillä on mahdollista päätyä johtopäätöksiin joiden luonne on yhdistävä tai yhteen vetävä. (Salminen 2011, 7.)

3 Tietoperusta

Keskeisiä käsitteitä ovat pilvipalvelu, Software as a Service, julkinen pilvi sekä riski. Software as a Service -käsitteestä käytän myöhemmin lyhennettä SaaS. Riskiä käsittelen työssä ainoastaan mahdollisena vahingollisena tapahtumana. Käsitteiden kuvauksissa esitän lyhyesti työn aiheen rajauksen ulkopuolella olevat palvelumallit ja toteutusmallit, koska ne ovat tärkeitä ymmärtää osana pilvipalveluiden kokonaisuutta. Käsitteiden kuvauksen jälkeen on toteutusmallit, palvelumallit ja pilvipalveluiden erityispiirteet yhteen vetävä kuva.

Seuraavaksi ovat kuvattu mainitsemani keskeiset käsitteet sekä julkisen pilven Software as a Service -palveluiden riskit. Nämä tekijät ovat tietoperusta, johon työn tuotoksena syntynyt työkalu perustui. Riskiselvityksessä jokainen yksittäinen kappale on yksi riski. Tietoperustasta on yhteenveto, jossa käsittelen tarkemmin riskiselvityksen hyödyntämistä työkalussa. Raportin loppuarvioinnissa otan kantaa siihen, että oliko tietoperustan muodostamisessa käyttämäni menetelmä toimiva.

3.1 Käsitteet

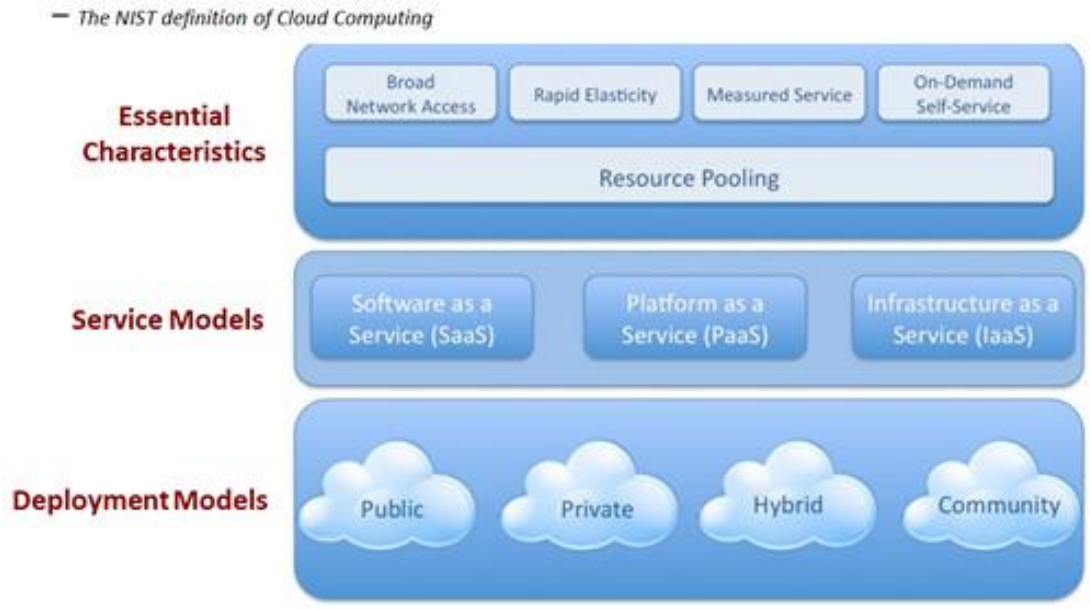
Pilvipalvelu on malli, jonka avulla mahdollistetaan pääsy tietojenkäsittelyresurssien jaettuun varantoon kaikkialta Internetin välityksellä ja helppokäyttöisesti. Esimerkkeinä näistä resursseista ovat palvelimet, tallennustila, tietoverkot, ohjelmat ja palvelut. Tietojenkäsittelyresursseja voidaan varata tai vapauttaa hyvin pienillä hallinnollisilla toimilla tai kanssakäymisellä pilvipalveluntarjoajan kanssa. (Mell & Grance 2011, 6.)

Pilvipalveluilla on viisi oleellista erityispiirrettä, jotka ovat itsepalvelu tarpeen vaatiessa, pääsy verkkoon laajalti, resurssien yhdistäminen, nopea joustavuus ja mitattavissa olevat palvelut. Itsepalvelu tarpeen vaatiessa tarkoittaa sitä, että asiakas voi halutessaan yksipuolisesti ottaa käyttöön lisää tietojenkäsittelyresursseja ilman ihmisten välistä kanssakäymistä asiakkaan ja pilvipalveluntarjoajan kanssa. Pilvipalveluihin pääsy tapahtuu verkon välityksellä käyttämällä standardeiksi muodostuneita mekanismeja jotka toimivat erilaisilla alustoilla, kuten esimerkiksi matkapuhelimilla, tableteilla, työasemilla tai kannettavilla tietokoneilla. Resurssien yhdistämistä tapahtuu siten, että palveluntarjoajan tietojenkäsittelyresurssit palvelevat asiakkaita usean vuokralaisen periaatteen mukaan, jossa erilaisia fyysisiä sekä virtuaalisia resursseja jaetaan dynaamisesti kysynnän mukaan. Usein asiakkaalla ei ole tarkkaa tietoa eikä kontrollia siihen, missä tarjotut resurssit sijaitsevat vaikkakin voi olla mahdollista määrittää sijainti esimerkiksi tiettyyn maahan tai konesaliin. Nopea joustavuus tarkoittaa sitä, että resursseja voidaan joustavasti varata ja vapauttaa. Tämä voi tapahtua joissain tapauksissa jopa automaattisesti. Kyse on siitä, että kysyntään voi vastata nopeasti skaalaamalla resursseja ulos- tai sisäänpäin. Pilvipalveluissa resurssien käyttöä voidaan usein mitata, hallita, raportoida ja näin ollen tarjota läpinäkyvyyttä sekä asiakkaalle että palveluntarjoajalle. (Mell & Grance 2011, 6.)

Software as a Service eli SaaS on yksi yleisistä pilvipalvelumalleista. Kyseessä on malli, jossa asiakkaalle tarjotaan mahdollisuus käyttää palveluntarjoajan pilvi-infrastruktuurissa suoritettavia ohjelmia. Näitä ohjelmia käytetään usein hyvin ohuen asiakasrajapinnan kautta, joka voi olla esimerkiksi Internet-selain. Asiakkaat eivät hallinnoi taustalla olevaa pilvi-infrastruktuuria johon kuuluu verkot, palvelimet, tallennustilat, käyttöjärjestelmät ja ohjelmien ominaisuudet. Joissain tapauksissa käyttäjäkohtaisia ohjelmistojen asetuksia voi olla mahdollista muuttaa. Muita tunnettuja pilvipalvelumalleja ovat Platform as a Service eli PaaS ja Infrastructure as a Service eli IaaS. Platform as a Service palvelut ovat ohjelmistokehitysalustoja ja Infrastructure as a Service palveluissa asiakkaan käyttöön tarjotaan IT-infrastruktuuria, kuten esimerkiksi laskentakapasiteettia tai tallennustilaa. (Mell & Grance 2011, 6 - 7.)

Julkinen pilvi (engl. public cloud) on pilvipalvelun toteutusmalli, jossa pilvi-infrastruktuurin resursseja tarjotaan avoimesti kaikkien käyttöön. Itse infrastruktuuri voi olla yrityksen, akateemisen- tai valtion organisaation omistamaa, ylläpitämää ja operoimaa. Edellä mainittujen tahojen yhdistelmä voi myös olla mahdollinen. Julkisen pilven infrastruktuuri sijaitsee palveluntarjoajan tiloissa. Muita toteutusmalleja ovat yhden organisaation käyttöön varattu yksityinen pilvi (engl. private cloud), yhteisöpilvi (engl. community cloud) jota käyttää ainoastaan tahot joilla on samoja intressejä ja hybridipilvi (engl. hybrid cloud) joka on eri toteutusmallien yhdistelmä. (Mell & Grance 2011, 7.)

Riski -sanan vastineita suomen kielessä perinteisesti ovat muun muassa vahingonvaara, vahingonuhka ja tappionuhka, jotka kuvaavat vahingollisen, haitallisen, vaarallisen tai epäedullisen tapahtuman mahdollisuutta. Tapahtuman epävarmuus, siihen liittyvät odotukset ja laajuus sekä vakavuus vaikuttavat siihen miten riski koetaan. Kogan ja Wallach ovat vuonna 1964 teoksessaan määritelleet riskin kaksitahoiseksi, koska se sisältää mahdollisuuden ja toisaalta vaaran aspektin. (Juvonen, Korhonen, Ojala, Salonen & Vuori 2008, 7 - 8.)



Kuva 3: Pilvipalveluiden visuaalinen malli (Coalfire 2012)

Kuvassa kolme on visuaalinen esitys pilvipalveluista. Alimpana ovat toteutusmallit, keskellä palvelumallit ja ylhäällä pilvipalveluiden erityispiirteet. Käsitteiden kuvauksessa keskityttiin julkisen pilven toteutusmalliin ja Software as a Service -palvelumalliin työssä olevan aiheenrajauksen mukaisesti.

3.2 Riskit

Käytin julkisen pilven SaaS-palveluiden riskien kuvauksessa viittä eri julkaisua, joiden taustalla on hyvin tunnettuja organisaatioita, kuten Cloud Security Alliance (CSA), Gartner, National Institute of Standards and Technology (NIST) ja European Network and Information Security Agency (ENISA). Gartnerin tutkimus on Jay Heiserin ja Mark Nicolettin tekemä. NIST:n julkaisut ovat tehneet Wayne Jansen, Timothy Grance sekä Lee Badger, Robert Patt-Corner ja Jeff Voas. ENISA:n tutkijat ovat Daniele Catteddu ja Giles Hogben. Hyödynsin myös Pittsburghin yliopiston tutkijoiden Hassan Takabin, James B.D. Joshin ja Arizonan yliopiston tutkijan Gail-Joon Ahnin kirjoittamaa artikkelia pilvipalveluiden turvallisuuteen ja yksityisyyteen liittyvistä haasteista. Riskit jaoin hallinnollisten riskien, teknisten riskien sekä juridisten riskien kategorioihin.

Riskien kuvauksessa pyrin tiivistykseen ja helppolukuisuuteen. Jokaisessa tekstin kappaleessa on käsitelty riski sekä sen aiheuttama ongelma tai seuraus. Riskit jotka koskevat vain muita toteutusmalleja ja palvelumalleja ovat työn aihealueen ulkopuolella. Jokaisen riskikategorian jälkeen on taulukko, johon sijoitin selvityksessä kuvatut riskit. Riskeille tein omat koodit sen perusteella, että mihin kategoriaan riski kuuluu, monesko riski on omassa kategoriassaan ja koko selvityksessä. Esimerkiksi riski T1-R13 on ensimmäinen tekninen riski ja kokonaisuudessaan 13 riski. Riskien koodeja on hyödynnetty myöhemmin arviointityökalussa. Riskikategorioiden yhteenvedossa käsittelen selvityksen tuloksia ja niiden tulevaa käyttöä produktin tuottamisessa.

3.2.1 Hallinnollisia riskejä

Tiedon sisään lukkiutuminen palveluntarjoajalle on hallinnollinen SaaS-palvelun riski. Tällä hetkellä ei ole monia työkaluja, eikä standardeja tiedostomuotoja tai menettelyitä joilla voidaan taata tiedon ja palveluiden siirrettävyys. Tästä syystä asiakkaan on vaikeaa siirtyä pilvipalveluntarjoajasta toiseen tai siirtää tietoa ja palveluita omasta IT-ympäristöstään. Pilvipalveluntarjoajilla saattaa myös olla kannustetta pyrkiä estämään tiedon siirrettävyys. Riippuvuuksia palveluntarjoajiin voi syntyä. Ongelmia voi aiheutua tilanteissa joissa palveluntarjoaja menee vararikkoon ja tiedon siirtäminen toiselle palveluntarjoajalle olisi liian kallista tai varoitusta taloudellisista ongelmista ei anneta riittävän ajoissa. Mikäli palveluntarjoaja ostetaan, voi se aiheuttaa samankaltaisen tilanteen koska politiikat ja ei-sitovat sopimukset saattavat muuttua nopeasti. SaaS:n osalta on mahdollista, että palveluntarjoajan järjestelmässä asiakkaan tiedot ovat palveluntarjoajan räätälöimässä tietokantamallissa joka ei tue tiedon viemistä muihin järjestelmiin. Asiakas joutuu itse rakentamaan tarvittavat rutiinit ja tekniikan tiedon siirtämiseksi uuteen järjestelmään. Ohjelmien osalta voi myös syntyä riippuvuuksia, mikäli palveluntarjoaja on rakentanut oman räätälöidyn SaaS-palvelun heidän kohde-

markkinoitaan varten. Asiakkaille joilla on paljon käyttäjiä, saattaa aiheutua merkittäviä kustannuksia, koska toiseen palveluntarjoajaan siirtyminen muuttaa käyttäjäkokemusta. Käyttäjäkokemuksen muuttumisen vuoksi on järjestettävä koulutuksia. (Catteddu & Hogben 2009, 25 - 26.)

Pilvipalveluissa asiakas antaa palveluntarjoajalle hallinnollisen vastuun useisiin asioihin jotka liittyvät turvallisuuteen. Voidaan puhua hallinnon menettämisen riskistä. Esimerkiksi käyttöehdoissa saattaa olla kielto verkkotiedusteluille, haavoittuvuuksien arvioinnille tai läpäisykykytesteille. Ristiriitoja voi esiintyä asiakkaan turvallisuuden koventamismenettelyiden ja pilviympäristön välillä. Palvelutasosopimuksissa ei välttämättä ole kuvattuna sitoumusta edellä mainittujen palveluiden hoitamiseen, mikä jättää aukon turvajärjestelyihin. Palveluntarjoaja voi myös ulkoistaa palveluitaan kolmannelle osapuolelle joka ei tarjoa samoja takuita, kuin mitä palveluntarjoaja ilmoittaa. Hallinnon menetys voi vaikuttaa organisaation strategiaan sekä johtaa tilanteeseen jossa ei pystytä täyttämään turvallisuusvaatimuksia. Tiedon luottamuksellisuus, eheys ja saatavuus voivat vaarantua sekä suorituskyky ja palvelun laatu heiketä. Ongelmia voi ilmetä myös palvelulle asetettujen vaatimustenmukaisuuksien noudattamisessa. (Catteddu & Hogben 2009, 28 - 27.)

Pilvipalveluissa asiakkaalle voi olla haasteellista noudattaa vaatimustenmukaisuuksia. Palvelun käyttäjään kohdistuu useita säännöksiä joiden perusteella käyttäjä on vastuussa tiedon turvallisuudesta ja eheydestä, vaikka se sijaitsee palveluntarjoajan infrastruktuurissa. Perinteiset palveluntarjoajat suostuvat ulkopuolisten tahojen tekemiin auditointeihin ja sertifiointeihin, joissa palveluntarjoajat antavat asiakkaalle tietoa turvakontrolleista. Pilvipalveluntarjoaja saattaa olla haluton ryhtymään auditointeihin tai auditointi ei ole mahdollista. (Heiser & Nicolett 2008, 3.)

Maineen menetys muiden vuokralaisten toiminnan vuoksi on myös mahdollista. Resurssien jakamisen vuoksi haitalliset tai pahantahtoiset toimet pilvipalvelua käyttävän toisen asiakkaan, eli vuokralaisen toimesta voivat vaikuttaa muidenkin maineeseen. Mikäli joku toinen asiakas esimerkiksi lähettää roskapostia tai jakaa haitallista sisältöä pilvipalvelun kautta, voi se johtaa IP-osoitteiden estämiseen johon kuuluvat myös muut asiakkaat hyökkääjän lisäksi. Resursseja voidaan myös takavarikoida muiden, usein naapurina olevien vuokralaisten aktiviteettien vuoksi. Seurauksena muiden vuokralaisten toiminnasta voi olla ongelmat palvelun toimittamisessa, tiedon menetykset ja maineen huonontuminen. (Catteddu & Hogben 2009, 30 - 31.)

Pilvipalvelun lopettaminen tai toimintahäiriö on mahdollista, mikäli palveluntarjoaja kohtaa esimerkiksi liiketoiminnallisia haasteita ja menee vararikkoon. Asiakkaan on arvioitava palveluntarjoajan pidemmän aikavälin jatkuvuutta. Palveluntarjoajan tulee pystyä vakuuttamaan asiakas siitä, että palvelun jatkuvuus on turvattu. Palvelun käyttäjän tulee saada tietoa siitä,

että onko tieto enää saatavilla ja helposti siirrettävissä korvaavaan palveluun, mikäli palveluntarjoaja joutuu lopettamaan toiminnan. (Heiser & Nicolett 2008, 4.)

Pilvipalveluntarjoajan hankkiminen eli yrityskauppa todennäköisesti johtaa strategisiin muutoksiin ja voi riskeerata ei-sitovat sopimukset, joita ovat esimerkiksi ohjelmistorajapinnat, investoinnit turvallisuuteen tai turvallisuusjärjestelyt. Näiden muutokset voivat aiheuttaa mahdottomuuden noudattaa turvallisuusvaatimuksia. Lopulta vaikutukset voivat ulottua organisaation maineeseen, työntekijöiden uskollisuuteen ja asiakkaiden luottamukseen. (Catteddu & Hogben 2009, 31 - 32.)

Pilvipalveluissa voi myös ilmetä toimitusketjun häiriöitä. Pilvipalveluntarjoaja voi ulkoistaa joitain osia tai tiettyjä tehtäviä pilvipalvelun tuottamisessa. Tästä syystä palveluntarjoajan turvallisuus voi riippua jokaisen alihankkijan tai mukana olevan tahon turvallisuudesta. Keskeytykset palvelun tuotannossa tai epäselvyydet kaikkien osapuolten vastuiden osalta voi johtaa palvelun saatavuuden sekä tiedon luottamuksellisuuden, eheyden ja saatavuuden menettämiseen. Taloudelliset menetykset ja kolhut maineelle ovat mahdollisia, koska ei pystytä täyttämään omia velvollisuuksia asiakkaille eikä vastaamaan kysyntään. Mikäli palveluntarjoaja ei kuvaa mitkä tärkeimmät osat palvelusta ovat ulkoistettuja, niin ei myöskään ole realistista odottaa että he kertoisivat mitä alihankkijoita käyttävät. Tästä syystä asiakas ei pysty kunnolla arvioimaan riskejä ja läpinäkyvyyden puute voi vähentää luottamusta palveluntarjoajan ja asiakkaan välillä. (Catteddu & Hogben 2009, 33.)

Tuntematon riskiprofiili on mahdollinen, mikäli palveluntarjoaja ei anna tarkempia tietoja omista sisäisistä turvallisuusmenettelyistään, auditoinneistaan, ohjelmistopäivityksistä tai tapahtumalokitiedostoista. Asiakkaalle on usein tärkeää oman riskien arvioinnin kannalta tietää tarkasti palvelun ohjelmistojen versiot, päivitykset, turvallisuusmenettelyt, haavoittuvuusprofiilit, hyökkäysyritykset, lokitiedot ja taustalla oleva turvallisuussuunnittelu. On mahdollista, että asiakkaan kannalta oleellisia riskejä jää tunnistamatta mikäli pilvipalveluntarjoaja ei jaa tietoa siitä, mitä lokitietoja kerätään, miten niitä tallennetaan, kenellä on pääsy niihin ja mitä tietoa on saatavilla, jos turvallisuustapahtuma havaitaan. (Cloud Security Alliance 2010, 14.)

Tärkeää on selvittää, miten palveluntarjoaja auttaa riskien vähentämisessä koska siitä voi muodostua lisää riskejä, jos tukea riskienhallintaan ei palveluntarjoajalta saa. Ongelmia voi ilmetä, mikäli palveluntarjoaja ei anna riittävästi tietoa asiakkaan käyttäjille siitä, kuinka heidän palveluaan käytetään turvallisesti ja luotettavasti. Asiakkaan ylläpidosta vastaavan henkilökunnan tulee saada riittäviä ohjeita, joiden perusteella he voivat luoda pilvipalveluun liittyviä politiikkoja ja seurata niiden toteutumista. (Heiser & Nicolett 2008, 4.)

Pilvipalveluissa kuten missä tahansa muussa käyttöasteeseen perustuvassa palvelussa tehdään palvelutasosopimus. Palvelutasosopimukseen laatimiseen liittyy riskejä, koska niiden huolimaton toteuttaminen voi johtaa epäselvyyksiin palveluiden, prioriteettien, vastuiden ja takuiden osalta. Pilvipalveluissa palvelutasosopimuksella hallitaan resurssien käyttöä. Turvallisuus, luottamus ja yksityisyyden suoja ovat palvelutasosopimuksen kannalta haastavia, koska ne eivät sellaisenaan ole mitattavissa. Palveluntarjoajan on pystyttävä vakuuttamaan asiakas siitä, että palvelu toimii siten kuin on sovittu ja turvallisesti. Mikäli asiakas ei luota palveluntarjoajan itse tekemiin mittauksiin, on syytä ottaa kolmas osapuoli valvomaan palvelutasosopimuksen kriittisimpien kohtien toteutumista ja ilmoittamaan rikkomuksista. (Takabi, Joshi & Ahn 2010, 25 - 26.)

Palveluntarjoajan reagoimisesta turvallisuustapahtumiin on asiakkaan kannalta tärkeää saada tarkempaa tietoa. Pilvipalveluntarjoajan rooli on kriittinen siinä, miten hyökkäyksiin reagoidaan, miten niitä todennetaan, kuinka hyökkäyksiä analysoidaan, miten hyökkäyksiä eristetään ja kuinka palveluita palautetaan takaisin toimintaan ongelmien jäljiltä. Palveluntarjoajan tulee käsitellä turvallisuustapahtumia siten, että mahdolliset vahingot rajoittuvat ja aiheutuneista häiriöistä palaudutaan mahdollisimman nopeasti. Turvallisuustapahtumien hallinta- ja käsittelyprosessi tulee olla läpinäkyvä. (Jansen & Grance 2011, 33.)

Politiikkojen ja käytäntöjen yhteensopimattomuus asiakkaan ja palveluntarjoajan välillä on hallinnollinen riski. Palveluntarjoajan omat turvallisuuspolitiikat ja käytännöt eivät välttämättä ole riittäviä tai yhteensopivia asiakkaan vastaavien kanssa, mikä voi johtaa tietoturvariskien toteutumiseen, rikkomuksiin, epäselvyyksiin vastuiden suhteen ja valvonnan heikkenemiseen. Pilvipalveluntarjoaja saattaa esimerkiksi käsitellä arkaluontoista tietoa eri tavalla kuin miten asiakkaan politiikka edellyttää. (Jansen & Grance 2011, 39.)

H1-R1	Tiedon sisään lukkiutuminen
H2-R2	Hallinnon menettäminen
H3-R3	Vaatimustenmukaisuuksien noudattaminen
H4-R4	Muiden vuokralaisten toiminta
H5-R5	Palvelun lopettaminen
H6-R6	Yrityskauppa
H7-R7	Toimitusketjun häiriöt
H8-R8	Tuntematon riskiprofiili
H9-R9	Puutteellinen riskienhallinnan tukeminen
H10-R10	Palvelutasosopimuksen huolimaton toteutus
H11-R11	Puutteellinen reagoiminen turvallisuustapahtumiin
H12-R12	Politiikkojen- ja käytäntöjen yhteensopimattomuus

Taulukko 1: Hallinnolliset riskit

Taulukossa yksi on yhteenveto aiemmin kuvatuista hallinnollisista riskeistä. Hallinnollisia riskejä on 12. Riskeille annettuja koodeja hyödynnetään varsinaisessa produktissa. Koodin ensimmäinen osa tarkoittaa riskin sijoitusta omassa kategoriassaan ja toinen osa sijoitusta koko riskiselvityksessä.

3.2.2 Teknisiä riskejä

Resurssien ehtyminen tilanteissa joissa yli- tai alivarataan, on tekninen riski. Pilvipalveluita käytetään tarpeen mukaan ja siihen sisältyy riski, koska pilven resurssien varaaminen perustuu tilastollisiin ennusteisiin. Mikäli resurssien käytön mallinnus on epätarkkaa, on mahdollista että resurssien varaamiseen liittyvä oikeudenmukaisuus vääristyy, jolloin resursseja varataan riittämättömästi tai infrastruktuuriin tehdään riittämättömiä investointeja. Asiakkaan näkökulmasta ongelmat laskentakapasiteetin mitoituksessa voi johtaa palvelun toimittamisen häiriöihin ja suorituskyvyn laskemiseen. Luottamuksellisuus ja eheys voi vaarantua jos hallitsematon resurssien käyttö johtaa pääsynvalvontajärjestelmän vaarantumiseen. Näiden lisäksi taloudelliset ja maineeseen liittyvät menetykset ovat mahdollisia, koska palveluntarjoaja ei pysty täyttämään asiakkaiden vaatimuksia. (Catteddu & Hogben 2009, 33 - 34.)

Pilvipalvelut toimivat useamman vuokralaisen periaatteella ja resurssit ovat jaettuja, joten riskinä on myös eristämisen epäonnistuminen tai pettäminen. Software as a Service -palveluissa asiakkaat saattavat jakaa saman ohjelman tai tietokannan. Resurssien jakamiseen liittyvät mekanismit palveluntarjoajan puolella ovat riippuvaisia monimutkaisista menettelyistä, joilla asiakkaat pidetään erillään toisistaan. Riski eristämisen pettämisestä on olemassa ja vikoja eristämisessä on dokumentoitu ennenkin. (Badger, Grance, Patt-Corner & Voas 2011, 64.)

Palveluntarjoajan pahantahtoiset työntekijät ovat riski joka yleisesti tunnetaan hyvin. Tämä riski korostuu pilvipalveluissa, joissa usein on muutenkin läpinäkyvyyden puutetta. Palveluntarjoaja ei välttämättä kuvaa tarkemmin omaa rekrytointiprosessiaan tai kuinka he valvovat omia työntekijöitään. Tietoa ei välttämättä ole saatavilla siitä, miten työntekijöiden pääsy sallitaan fyysisiin ja virtuaalisiin resursseihin tai kuinka palveluntarjoaja analysoi ja raportoi tietoa politiikkojen noudattamisesta. (Cloud Security Alliance 2010, 10.)

Hallinnointirajapinnan vaarantuminen on riski. Pilvipalveluissa palveluntarjoajat antavat asiakkaille ohjelmistorajapinnat tai ohjelmointirajapinnat, joiden kautta palvelua hallinnoidaan ja käytetään. Resurssien varaaminen, hallinta, seuranta ja järjestely tapahtuvat näiden rajapintojen kautta. Pilvipalveluissa palvelun turvallisuuteen vaikuttaa merkittävästi näiden rajapintojen turvallisuus. Käyttäjien todentaminen, pääsynhallinta, salausmenetelmät ja tapahtumien seuranta ovat esimerkkejä tavoista, joilla torjutaan pahantahtoisia yrityksiä ohittaa

politiikka. Palveluntarjoajat käyttävät näitä rajapintoja myös tarjotakseen lisäominaisuuksia ja siten lisäarvoa asiakkailleen. Tämä lisää rajapinnan monimutkaisuutta ja riskit kasvavat. (Cloud Security Alliance 2010, 9.)

Pilvipalveluissa tiedonsiirron kaappaaminen ja sen seurauksena syntyvä tietovuoto on riski, mitä ei ainakaan helpota pilven jaettu arkkitehtuuri. Pilvipalveluissa tietoa siirretään paljon enemmän kuin perinteisissä arkkitehtuureissa. Tietoa siirretään esimerkiksi useiden jaettujen levykuvien synkronoimiseksi tai siirtämiseksi useille fyysisille koneille, pilvi-infrastruktuurien välillä tai web-asiakkaille. Usein konesalien tietoa käsitellään VPN-tyyppisen yhteysympäristön kautta, mutta tätä ei aina noudateta pilvipalveluissa. Joissain tapauksissa pilvipalveluntarjoajat eivät anna sopimukseen kohtaa tai ne kohdat ovat riittämättömiä, joissa luottamuksellisuuden menettämiseen puututaan ja kunnioitetaan asiakkaan salaista tietoa. Tiedonsiirron kaappaamiseen liittyvät ongelmat koskevat myös asiakkaan ja pilvipalveluntarjoajan välistä liikennettä. (Catteddu & Hogben 2009, 38.)

Turvaton tai tehoton tiedon hävitys on ongelma, koska aina kun palveluntarjoajaa vaihdetaan, resursseja skaalataan alaspäin tai fyysisiä laitteita kohdennetaan uudelleen, voi tietoa jäädä yli turvapolitiikassa määritetyn elinkaaren. Turvapolitiikan edellyttämiä menettelyitä voi olla mahdotonta toteuttaa, koska täydellinen tiedon hävittäminen on ainoastaan mahdollista jos tuhotaan fyysinen laite jota käyttää muutkin pilven asiakkaat. Mikäli palveluntarjoajaa pyydetään poistamaan tietoa, niin se ei välttämättä johda todelliseen tiedon hävittämiseen. (Catteddu & Hogben 2009, 39 - 40.)

Palvelunestohyökkäykset joilla häiritään pilvipalvelun toimivuutta, pätevät riskinä myös pilvipalveluissa. Palvelunestohyökkäyksessä palveluun tehdään tekaistuja kyselyitä, jotta palvelu ei vastaisi riittävän nopeasti oikeisiin kyselyihin. Nämä hyökkäykset tapahtuvat tyypillisesti käyttämällä hyväksi useita tietokoneita tai tietokoneiden verkostoa. Vaikkakin palvelunestohyökkäys ei onnistuisi, se saattaa silti kuluttaa paljon pilvi-infrastruktuurin resursseja ja haitata pilvipalveluille tyypillistä dynaamista resurssien varaamista. (Jansen & Grance 2011, 33.)

Salausavaimien menettäminen voi johtaa tiedon menetyksiin. Tähän riskiin kuuluu SSL-avaimien, tiedostojen salaamiseen käytettyjen avaimien, asiakkaiden yksityisten avaimien ja salasanojen päätyminen vääriin käsiin, niiden häviäminen tai korruptoituminen sekä niiden luvaton käyttö. Digitaalisten varmenteiden kiistämättömyyden menetys kuuluu salausavaimien menettämisen riskiin. (Catteddu & Hogben 2009, 41 - 42.)

Epäsuoria riskejä pilvipalveluille ovat pahantahtoiset skannaukset, joita käytetään tiedon keräämiseen mahdollista hyökkäystä varten. Lopputuloksena voi olla palvelun ja tiedon luotta-

muksellisuuden, eheyden ja saatavuuden menetys. Esimerkkejä skannauksista ovat port scannit eli verkkotiedustelut ja verkon kartoitusyritykset. (Catteddu & Hogben 2009, 42.) Palvelumoottorin vaarantuminen on tekninen riski. Pilviarkkitehtuurissa luotetaan erittäin erikoistuneeseen palvelumoottoriin, joka on fyysisten resurssien yläpuolella ja hallinnoi asiakkaiden resursseja infrastruktuurin eri tasoilla. Kuten missä tahansa ohjelmistossa, palvelumoottorin koodi voi sisältää haavoittuvuuksia ja on altis hyökkäyksille tai toimintahäiriöille. Hyökkäys palvelumoottoriin voi mahdollistaa asiakkaiden eristämisen ohittamisen jotta hyökkääjä pääsee käsiksi eri asiakasympäristöihin ja niiden sisältämiin tietoihin. Tietoa voi seurata ja muokata tai resursseja vähentää, mikä aiheuttaa palveluneston. (Catteddu & Hogben 2009, 42 - 43.)

Riskin muodostavat myös ristiriidat asiakkaan turvallisuuden koventamismenettelyiden ja pilviympäristön välillä. Pilvipalveluntarjoajien tehtävänä on tarjota usean vuokralaisen periaatteella toimiva ympäristö. Useiden asiakkaiden sijoittaminen samaan paikkaan johtaa väistämättä ristiriitaan pilvipalveluntarjoajan osalta, koska eri asiakkaiden vaatimukset tiedonvälityksen turvallisuudelle ovat toisistaan poikkeavia. Esimerkiksi samassa jaetussa verkossa voi olla asiakkaat, joista toinen haluaa palomuurin estävän kaiken liikenteen paitsi jonkin tietyn palvelun, kun taas toinen asiakas tarvitsee sellaisia palveluita mitä toinen haluaisi kieltää. Samantyyppinen ristiriita ilmenee myös, kun asiakkailla on omia määräystenmukaisuusvaatimuksia. Mitä enemmän asiakkaita on, niin sitä haasteellisemmaksi tilanne käy ja palveluntarjoajan on kyettävä vastaamaan tähän ongelmaan tekniikalla, politiikoilla ja sopivalla läpinäkyvyydellä. Palveluntarjoajan on myös tehtävä asiakkaille selväksi, mitkä ovat asiakkaan vastuut ja velvollisuudet turvallisuuden osalta. Mikäli pilvipalvelussa olevat asiakkaat eivät hoida omaa osuuttaan turvallisuudesta, voi se aiheuttaa riskin koko pilviympäristölle jos asiakkaiden eristäminen toisistaan pettää. (Catteddu & Hogben 2009, 43 - 44.)

Tiedon palauttamiseen liittyvät asiat ovat tärkeitä selvittää pilvipalvelun osalta, jotta palvelun selviytymistä katastrofitilanteista voidaan arvioida. Vaikka palveluntarjoaja ei kertoisi, missä tiedot tarkalleen sijaitsevat ja minne tai miten varmuuskopiointi tehdään, on heidän kuitenkin kerrottava mitä asiakkaan tiedolle ja palvelulle tapahtuu katastrofitilanteissa. Palveluntarjoajan tulee voida kuvata, että onko täydellinen palautus mahdollista ja kauanko palauttaminen kestää. (Heiser & Nicolett 2008, 3.)

Pilvipalveluissa ongelmia saattaa ilmetä identiteettien ja pääsynhallinnan osalta. Asiakkaan omat tunnistamiseen ja todennukseen käytetyt rakenteet eivät välttämättä helposti ulotu pilvipalveluun. Näiden rakenteiden muuttaminen voi osoittautua vaikeaksi. Kahden eri todennusjärjestelmän ylläpito joista toinen on sisäisiä järjestelmiä ja toinen ulkoisia pilvijärjestelmiä varten, voi ajan saatossa osoittautua toimimattomaksi ratkaisuksi. Tärkeää on selvittää, että onko palveluntarjoajan kanssa mahdollista löytää yhteensopivuus heidän todennusjärjes-

telmän ja pilvipalvelun asiakkaan todennusjärjestelmän välille. (Jansen & Grance 2011, 25 - 27.)

Palveluihin kohdistuvat hyökkäykset saattavat olla todennäköisempiä ja niitä voi esiintyä useammin, jos pilvijärjestelmässä on paljon arvokasta tietoa. Pilvipalvelua voi myös käyttää jokin asiakas jolla on korkea riskiprofiili eli uhka joutua hyökkäyksen kohteeksi. Mikäli pilviympäristöön kohdistuu esimerkiksi palvelunestohyökkäyksiä, niin vaikutukset voivat olla laajoja ja kohdistua asiakkaisiin joita vastaan hyökkäys ei alun perin ole tarkoitettu. (Jansen & Grance 2011, 29.)

T1-R13	Resurssien ehtyminen
T2-R14	Eristämisen epäonnistuminen
T3-R15	Pahantahtoiset työntekijät
T4-R16	Hallinnointirajapinnan vaarantuminen
T5-R17	Tiedonsiirron kaappaaminen
T6-R18	Turvaton tai tehoton tiedon hävitys
T7-R19	Palvelunestohyökkäykset
T8-R20	Salausavaimien menettäminen
T9-R21	Pahantahtoiset skannaukset
T10-R22	Palvelumoottorin vaarantuminen
T11-R23	Ristiriidat turvallisuuden koventamismenettelyissä
T12-R24	Puutteelliset menettelyt tiedon palauttamisessa
T13-R25	Identiteettien ja pääsynhallinnan yhteensopimattomuus
T14-R26	Korkean riskiprofiilin asiakkaat

Taulukko 2: Tekniset riskit

Taulukossa kaksi on yhteenveto teknisistä riskeistä. Teknisiä riskejä on 14. Kaiken kaikkiaan riskejä on 26, mikäli hallinnolliset ja tekniset riskit lasketaan yhteen.

3.2.3 Juridisia riskejä

Fyysisten laitteiden takavarikointi sitä varten, että niitä tarvitaan todistusaineistoksi viranomais- ja siviilikanteissa, on juridinen riski pilvipalveluissa. Tiedon varastoinnin keskittyminen ja usean vuokralaisen periaate aiheuttaa sen, että useilla asiakkailla on vaarana tiedon päätyminen ei-toivottujen tahojen haltuun. Kyseessä on tilanne, jossa takavarikoidaan fyysinen laite ja siinä menee mukana muutakin tietoa kuin vain se, mikä on välttämätöntä oikeudenkäyntiä varten. (Catteddu & Hogben 2009, 44 - 45.)

Lainsäädännön muutokset aiheuttavat riskin pilvipalveluille. Asiakkaiden tietoa saatetaan säilyttää useiden toimivaltojen alaisuudessa, joista osa saattaa olla erittäin riskialttiita. Mikäli

konesalit sijaitsevat korkean riskin maissa, on mahdollista että paikalliset viranomaiset tekevät ratsioita ja tietojärjestelmät suljetaan tai takavarikoidaan. Riskialttiilla maalla tarkoitetaan maata, joka ei toimi oikeusvaltioperiaatteen mukaan tai siellä on ennalta arvaamattomat oikeudelliset puitteet sekä lain toimeenpano. Riskialttiit maat saattavat olla yksinvaltaisia poliisivaltioita ja ne eivät noudata kansainvälisiä sopimuksia. (Catteddu & Hogben 2009, 45 - 46.)

Tietosuojaan liittyviä riskejä on useita. Asiakkaalle saattaa olla vaikeaa tehokkaasti valvoa, että palveluntarjoaja käsittelee tietoa lainmukaisesti. On syytä tehdä selväksi, että asiakas on vastuussa henkilötietojen käsittelystä vaikkakin pilvipalveluntarjoaja ulkoisena toimijana niitä myös käsittelisi. Tietosuojaan liittyvän lainsäädännön rikkominen voi johtaa tiedon omistajan, eli asiakkaan osalta rikosoikeudellisiin sanktioihin. Asiaa vaikeuttaa vielä, mikäli tietoja siirretään useiden pilvijärjestelmien välillä. On mahdollista, että palveluntarjoaja ei informoi asiakasta eli tietojen omistajaa turvallisuusaukoista. Asiakas voi menettää hallinnan siihen, mitä tietoa palveluntarjoaja käsittelee. Palveluntarjoaja voi myös vastaanottaa tietoa, jota asiakas ei ole lainmukaisesti kerännyt. (Catteddu & Hogben 2009, 46 - 47.)

Lisensointiin liittyy myös riski, mikäli ohjelman käytöstä maksetaan joka kerta kun uusi kone ilmenee. Tässä tapauksessa asiakkaan lisenssimaksut kasvavat nopeasti vaikka he käyttäisivät kokoajan saman määrän koneita ja yhtä kauan aikaa. Lisensointiehdot yksittäisten käyttäjien määrän mukaan tai online-lisensointitarkastukset eivät välttämättä onnistu pilviympäristössä. (Catteddu & Hogben 2009, 47.)

Tiedon sijaintiin liittyvät lakiasiat ovat yksi huomioitava riski pilvipalveluita hankittaessa. Asiakas ei välttämättä tiedä tarkalleen, missä käsiteltävä tieto maantieteellisesti sijaitsee. Tämä voi olla ongelma, jos asiakkaan on täytettävä oman maansa lakien mukaiset vaatimukset tietosuojalle. Oleellinen kysymys on, että suostuuko palveluntarjoaja toimimaan tiedon tallentamisen ja käsittelyn suhteen jonkin tietyn lainsäädännön mukaisesti sekä suostuvatko sopimukseen jossa he sitoutuvat noudattamaan tiettyä lakia. (Heiser & Nicolett 2008, 3.)

Väärinkäyttö- ja rikostapauksissa voi ilmetä riskejä, mikäli palveluntarjoaja ei anna tukea selvitystyöhön, joka on tarpeellista tutkinnan suorittamiseksi. Sisäisten tutkintojen tekeminen sähköisestä aineistosta on muutenkin haastavaa jopa omassa IT-ympäristössä ja vielä vaikeampaa se on, kun kyseessä ovat pilvipalvelut. Pilvipalveluita on vaikeaa tutkia, koska useiden asiakkaiden tietoa ja lokitiedot saattavat sijaita fyysisesti samoissa paikoissa ja levinneenä useisiin konesaleihin. (Heiser & Nicolett 2008, 4.)

J1-R27	Viranomais- ja siviilikanteet
J2-R28	Lainsäädännön muutokset
J3-R29	Tietosuoja
J4-R30	Lisensointi
J5-R31	Tiedon sijainti
J6-R32	Sisäiset tutkinnat

Taulukko 3: Juridiset riskit

Taulukossa kolme on juridisten riskien yhteenveto. Juridisia riskejä on kuusi. Kaikki riskikategoriat yhteenlaskettuna riskejä on 32.

3.3 Tietoperustan yhteenveto

Narratiivinen kuvaileva kirjallisuuskatsaus oli toimiva menetelmä varsinaista produktin tuottamista varten tarvittavan tietoperustan laatimiseksi. Tutkimusten ja julkaisujen sisällön tiivistin siten, että käsiteltävästä aiheesta saa kokonaiskuvan. Aiheen rajauksen mukaisesti käsitteiden määrittelyssä keskityin julkisen pilven toteutusmalliin ja SaaS-palvelumalliin. Riskiselvityksessä ovat vain julkisen pilven SaaS-palveluihin vaikuttavat riskit.

Riskien kuvauksessa pyrin käyttämään hyvin tunnettujen tahojen tekemiä tutkimuksia, jotka eivät ole pilvipalveluntarjoajien tekemiä tai rahoittamia. Tarkoituksena oli saavuttaa mahdollisimman puolueeton kuvaus riskeistä. Cloud Security Alliance on voittoa tavoittelematon organisaatio, jonka tehtävänä on edistää yleisiä hyviä käytäntöjä pilvipalveluiden turvaamiseksi. Cloud Security Alliancea johtavat alan toimijoiden, yritysten, järjestöjen ja muiden merkittävien sidosryhmien edustajat. Gartner on vuonna 1979 perustettu Yhdysvaltalainen johtava informaatioteknologian tutkimusyhtiö, jolla on yhteensä noin 1280 analyytikkoa ja konsulttia 85 eri maassa. ENISA eli Euroopan verkko- ja tietoturvavirasto on osaamiskeskus, joka toimii Euroopan Unionin instituutioiden ja jäsenmaiden hyväksi tietoturva-asioissa. ENISA:n tavoitteena on jakaa tietoa ja hyviä käytänteitä tietoturvallisuuden alalla. National Institute of Standards and Technology eli NIST on vuonna 1901 perustettu Yhdysvaltojen kauppaministeriön alaisuudessa toimiva ei-säädelty virasto, jonka tarkoituksena on tutkimustyöllään parantaa yhdysvaltalaisten yritysten kilpailukykyä. Takabi, Joshi ja Ahn ovat tutkijoita tietoturvallisuuden kentällä, joiden työtä tukee Yhdysvaltojen kansallinen tiedesäätiö. (Cloud Security Alliance 2012; Gartner 2012; ENISA 2012; NIST 2012; Takabi, Joshi & Ahn 2010, 31.)

Riskiselvitys oli työn kannalta tarkoituksenmukainen. Tavoitteena oli löytää aineistosta kattavasti julkisen pilven SaaS-palveluiden riskejä ja sijoittaa ne sopiviin kategorioihin. Riskien kuvauksen tuli olla sen tasoista, että saatua tietoa voi hyödyntää varsinaisen produktin tuottamisessa. Kuvaukset ovat tiivistyksestä huolimatta riittävän informatiivisia ja riskejä on sijoitettu kategorioihin joihin ne kuuluvat. Riskikuvauksissa ei oteta kantaa riskien vakavuuteen, koska eri organisaatioille tietyt riskit voivat olla merkitykseltään erilaisia. Hankittavan palvelun tyyppi ja siellä käsiteltävä tieto vaikuttavat riskien merkittävyyteen. Riskienarviointi tapahtui Kesko Oyj:n tietoturvapäällikön kanssa. Arvioinnin tulokset näkyvät produktissa siten, että palveluntarjoajien vertailu on mahdollista eritasoisten riskien osalta. Riskiselvityksen perusteella laadin jokaista riskiä varten palveluntarjoajille esitettäviä kysymyksiä, jotka sijoitan riskikategorioittain työkaluun.

Lähdeaineistoa käyttäessäni saavutin hyvin nopeasti tilanteen jossa samat riskit alkoivat toistua. Tämän lisäksi lähteissä useasti käytiin läpi tiettyä riskiä tai ongelmaa hieman eri termein ja ilmaisuin, mutta käytännössä tarkoittaen samaa asiaa. Jouduin useasti pohtimaan, että olenko jo aiemmin kuvannut saman riskin. Monet riskit ovat kytköksissä toisiinsa siten, että yhden riskin toteutuminen saattaa aiheuttaa jonkin toisen riskin toteutumisen, kuten esimerkiksi hallinnollinen riski toteutuessaan voi johtaa teknisen riskin toteutumiseen. Riskien jaottelu oli ajoittain haasteellista, koska esimerkiksi tietyllä riskillä voi olla hallinnollisen riskin tunnuspiirteitä vaikka se on luokiteltu lähdeaineistossa tekniseksi riskiksi. Riskien määrä voi aiheuttaa produktin käytön kannalta haasteita, koska tietyn riskin läpikäymiseen palveluntarjoajan kanssa voi tarvita useita kysymyksiä ja lopulta produktin käytöstä voi tulla raskas ja aikaa vievä prosessi.

4 Toteutus

Tämän osion tarkoitus on käsitellä työn toteutusta ja käytännön toimintaa Keskossa sekä omaa opinnäytetyöprosessiani. Merkittävin osa toteutusta on arviointityökalun toiminnallisuuksien esittely. Keskon tietoturvapäällikön kanssa tehdyn riskienarvioinnin toteuttaminen ja laatimani kysymyslista ovat myös kuvattu, koska niiden perusteella varsinaiseen työkaluun sain tarvittavan sisällön. Produktin kuvauksessa kiinnitin huomiota siihen, että sen perusteella olisi mahdollista kenen tahansa tehdä samanlainen työkalu.

Käytännön toimintaa Keskossa arvioin hankeorganisaatiota koskevassa osuudessa. Kyseinen osuus sisältää myös organisaatiokuvauksen työyhteisöstä. Toimintaa hankeorganisaatiossa arvioin erityisesti yhteistyön sujuvuuden kannalta. Opinnäytetyöprosessin kuvauksessa hyödynsin prosessin aikana pitämääni työskentelypäiväkirjaa. Toteutuksen yhteenvedossa pohdin työkalun toteuttamista.

4.1 Arviointityökalu

Microsoftin Excel-taulukkolaskentaohjelmalla toteuttamani työkalu sisältää merkitykseltään, eli riskitasoltaan erilaisia riskejä sekä palveluntarjoajille esitettäviä kysymyksiä. Toiminnallisuuksien taustalla ovat ne riskit, jotka aiemmin kuvasin tietoperustaan kuuluvassa riskiselvityksessä. Selvityksessä esittämäni riskit arvioitiin, jotta sain luokiteltua ne eri riskitasoihin. Riskien kuvausten perusteella muodostin työkalussa olevat palveluntarjoajille esitettävät kysymykset. Tässä osiossa esitän arviointityökalun ja sen toiminnallisuudet sekä työkalun taustalla olevan riskienarvioinnin ja kysymyslistan.

Riskienarvioinnin osalta kuvasin, minkälaista riskin määritelmää työssä on käytetty, mihin käytetyt riskitasot perustuvat ja miten riskienarviointi tehtiin. Näiden lisäksi käsittelin riskienarvioinnin lähtökohdat, saavutetut tulokset ja tulosten hyödyntämisen arviointityökalussa. Esitin myös, mitä palveluntarjoajille esitettävillä kysymyksillä on tarkoitus saavuttaa. Produktin kuvauksessa arviointityökalun toiminnallisuudet ja asetukset esitin jokaisen välilehden osalta. Työkalu sisältää paljon samojen toimintaperiaatteiden toistoa, joten yksittäisiä esimerkkejä toiminnallisuuksista on käytetty tiivistämiseksi.

4.1.1 Riskienarviointi ja kysymyslista

Riskiselvityksessä kuvatut riskit arvioitiin käyttämällä kehittynyttä riskin määritelmää:

$$\text{todennäköisyys} * \text{vakavuus}^2$$

Todennäköisyys ja vakavuus ovat välillä 1-5. Merkityksetön riski on riskiarvoltaan pienempi kuin 10, kohtalainen riski on välillä 10 - 20 ja merkittävä riski on arvoltaan suurempi kuin 20. Näin arvioimalla saa korostettua riskin vakavuutta ja vältettyä tilanne, jossa todennäköisyydeltään pienin mutta seurauksiltaan vakavin riski saa vertailuun saman arvon kuin riski, jonka todennäköisyys on suurin mutta seuraukset vähäisimmät. Riskin perinteisessä määritelmässä on mahdollista, että kaksi vakavuudeltaan täysin erilaista riskiä saavat saman riskiarvon, koska perinteinen määritelmä on todennäköisyys * vakavuus. Riskienhallintatyössä seurausten vakavuudella tulee olla suurempi merkitys kuin todennäköisyydellä, jotta merkittävimmät uhat voi selkeästi osoittaa. (Juvonen ym. 2008, 9 - 11.)

Riskienarviointi tehtiin 1.3.2012 Kesko-konsernin tietoturvapäällikkö Jari Törmälän kanssa siten, että hän tutustui ensin tietoperustassa kuvaamiini riskeihin ja tämän jälkeen kävimme keskustellen läpi jokaisen riskin. Törmälä antoi arvionsa riskien todennäköisyyksistä ja vaka-

vuuksista asteikolla 1-5. Tämän jälkeen laskin lopulliset riskiarvot riskin kehittyneemmän määritelmän mukaan. Tärkeää on huomata, että Törmälän mukaan Kesko ei lähtökohtaisesti tule hankkimaan sellaisia pilvipalveluita, joiden toimintahäiriöt tai lopettaminen voisi aiheuttaa suuren uhkan Keskon liiketoimintojen jatkuvuudelle tai yrityksen olemassaololle. Riskiarvojen tarkoitus on kuvata, kuinka merkittävänä ongelmana jokin tietty riski nähdään julkisen pilven SaaS-palvelussa. Riskejä on kokonaisuudessaan 32, joista kolme arvioitiin merkityksettömiksi, 13 kohtalaisiksi ja 16 merkittäviksi. Hallinnollisissa riskeissä on yksi merkityksetön riski, neljä kohtalaista riskiä ja seitsemän merkittävää. Teknisissä riskeissä arvioitiin olevan kaksi merkityksetöntä riskiä, kahdeksan kohtalaista ja neljä merkittävää riskiä. Juridisten riskien osalta on viisi merkittävää ja yksi kohtalainen riski. Riskienarvioinnin tarkemmat tulokset ovat liitteessä kaksi.

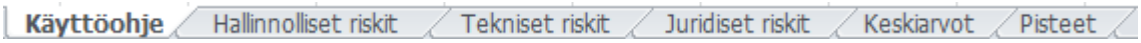
Tehdyn riskienarvioinnin perusteella arviointityökalussa voi vertailla palveluntarjoajien vastauksia merkittävyyksiltään erilaisissa riskeissä. Tarkoituksena on helpottaa päätöksentekoa. Esimerkiksi kahden palveluntarjoajan kokonaisarviot riskikategorioissa voivat olla samaa tasoa, mutta toinen on pärjännyt paremmin merkittävissä riskeissä. Näin palveluntarjoajan on mahdollista erottua edukseen vastaamalla hyvin kaikista tärkeimmiksi koettuihin riskeihin.

Arviointityökaluun sijoitin riskikategorioihin yksittäisiä riskejä koskevia kysymyksiä, jotka laadin tietoperustassa esitettyjen riskikuvausten perusteella. Kysymykset esitetään palveluntarjoajalle ja vastauksia kysymyksiin arvioidaan. Arvioidut kysymykset muodostavat kokonaisarvion tietystä riskistä. Tarkoituksena on, että jokaisesta riskistä syntyy avoin keskustelu jossa palveluntarjoaja kuvaa miten he ovat kyseiseen riskiin varautuneet. Vastauksilta odotetaan läpinäkyvyyttä ja niiden tulee olla hyvin perusteltuja. Esimerkiksi mahdolliset toimitusketjujen häiriöt on tunnistettu riski, mutta jos palveluntarjoaja ei keskustelussa kuvaa tarkemmin, mitä alihankkijoita palvelun tuottamisessa on käytetty tai mitkä ovat alihankkijoiden tehtävät, niin vastaukset eivät ole tyydyttäviä. Mikäli alihankkijoita ei käytetä ollenkaan, niin vastauksen voi arvioida olevan palvelunhankkijan näkökulmasta kiitettävä, koska silloin palvelun toimivuus ei ole riippuvainen useasta eri tahosta ja niiden turvallisuudesta. Keskustelun aikana on mahdollista esittää lisäkysymyksiä. Kysymyslista on liitteessä yksi.

4.1.2 Excel-toteutus

Työkalussa on yhteensä kuusi välilehteä. Ensimmäinen välilehti on käyttöohje. Kolme seuraavaa välilehteä ovat riskiselvityksessä käytetyt riskikategoriat, eli hallinnolliset riskit, tekniset riskit ja juridiset riskit. Riskikategoriat sisältävät kaikki yksittäiset riskit sekä niistä esitettävät kysymykset. Riskikategorioissa arvioidaan vastauksia ja työkalu laskee vastauksista keskiarvoja ja pisteitä. Kaksi viimeistä välilehteä ovat palveluntarjoajien vastausten vertailua varten. Vertailussa käytetään vastausten keskiarvoja ja yhteenlaskettuja pisteitä jokaisesta

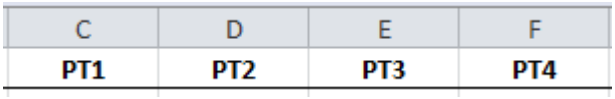
riskikategoriasta ja ne on sijoitettu pylväsdiagrammeihin. Keskiarvoja ja pisteitä varten ovat omat välilehdet. Työkalu mahdollistaa useamman palveluntarjoajan arvioimisen ja vertailun eri riskikategorioissa ja merkitykseltään eritasoisissa riskeissä. Yhden palveluntarjoajan arvioiminen on myös mahdollista. Koko laskentataulukossa käytetty fontti on oletusfontti Calibri 11.



Kuva 4: Välilehdet

Käyttäjälle toimitettavat dokumentit ovat Word-tiedosto joka sisältää taustalla olevan tietoperustan, eli keskeiset käsitteet ja riskiselvityksen sekä varsinainen arviointityökalu. Tarkoituksena on, että käyttäjä perehtyy tietoperustan avulla pilvipalveluihin ja tietää työkalussa olevien riskien taustat, jotka ovat kuvattu riskiselvityksessä. Työkalua käytetään neuvottelutilanteessa, jossa palvelunhankkijan ja palveluntarjoajan edustajat ovat paikalla ja sovittuna teemana on palvelun tietoturvallisuus. Aikaa keskusteluun tulee varata runsaasti, koska riskejä sekä kysymyksiä on paljon ja ne edellyttävät monesti laajoja vastauksia.

Arviointityökalun käyttö tapahtuu siten, että työkalua käyttävä henkilö perehtyy ensimmäiseen välilehteen, joka on käyttöohje. Tämän jälkeen jokaisesta riskikategoriavälilehdestä tulee korvata C1, D1, E1 tai F1-soluissa olevat palveluntarjoajaa tarkoittavat kohdat palveluntarjoajien oikeilla nimillä. Esimerkiksi PT1 tarkoittaa ensimmäistä arvioitavaa palveluntarjoajaa.



Kuva 5: Palveluntarjoajat

Kun käyttäjä on perehtynyt käyttöohjeeseen ja palveluntarjoajan oikea nimi on syötetty, on kaikki valmista kysymysten läpikäymiseen. Palveluntarjoajalle esitetään jokaisen riskikategoriavälilehden riskeihin liittyvät kysymykset. Vastaukset arvioidaan asteikolla 1-5, jossa 1 on huono, 2 tyydyttävä, 3 hyvä, 4 erinomainen ja 5 kiitettävä. Oletuksena työkalussa on 0 jokaisen kysymyksen kohdalla, joka tulee korvata arvolla 1-5. Työkalu laskee automaattisesti keskiarvot ja pisteet sekä syöttää ne vertailua varten diagrammeihin. Tämän jälkeen raportin voi tarvittaessa tulostaa. Tulostuksessa tulee skaalata tiedot mahtumaan yhdelle sivulle valitsemalla asetukseksi ”sovita taulukko yhteen sivuun.”

Käyttöohje -välilehdessä on kuvattu työkalun käyttökohde, käyttötarkoitus ja työkalulla saavutettavien tulosten tavoitteet. Välilehdessä on esitetty miten työkalua tulee käyttää, minkälaisessa tilanteessa sitä tulee käyttää sekä on asetettu rajoitukset työkalun muokkaamisen

suhteen. Työkalun eri välilehtien sisältö ja toiminnallisuudet on käyty läpi yleisellä tasolla. Käyttöohje -välilehti on ensimmäinen, joka työkalun käyttäjälle avautuu kun Excel-tiedoston avaa ensimmäistä kertaa. Käyttöohje on kirjoitettu ensin Word-tiedostoon, josta se on kopioitu välilehteen. Käyttöohje -välilehdestä on otettu ruudukkoviiva, kaavarivi ja otsikot pois näkyvistä. Työkalussa käytetty käyttöohje on liitteessä kolme.

Kaikki riskikategoriat sisältävät kahdeksan saraketta, jotka ovat otsikoiltaan Riski, Kysymys, PT1, PT2, PT3, PT4, Status ja Kommentti. Riski -sarakkeessa on jokaisen riskin koodi, jonka perusteella kunkin riskin kuvaus löytyy helposti tietoperustan riskiselvityksestä. Riskienarvioinnin mukainen merkittävyys on sijoitettu samaan sarakkeeseen. Kysymys -sarakkeeseen on sijoitettu palveluntarjoajalle esitettävät kysymykset. PT -sarakkeisiin sijoitetaan arviot palveluntarjoajien vastauksista. Status-kenttään tulee automaattisesti huutomerkki, mikäli arvioitu vastaus on 1 tai 2. Tämä helpottaa analysointia työkalun käytön jälkeen, koska puutteellisiksi arvioidut vastaukset korostuvat. Kommentti -sarake on työkalun käyttäjän muistiinpanoja varten. Sarakkeiden leveydet ovat järjestyksessä 13, 70, 10, 10, 10, 10, 10 ja 10. Sarakkeiden otsikot on lihavoitu ja tekstit keskitetty.

A	B	C	D	E	F	G	H
Riski	**Kysymys**	**PT1**	**PT2**	**PT3**	**PT4**	**Status**	**Kommentti**

Kuva 6: Riskikategorian sarakkeet

Riskit ovat sijoitettuna allekkain riskikategorioissa ja erotettu toisistaan käyttämällä reunaviiva-toimintoa. Jokaisesta riskistä lasketaan yhteen palveluntarjoajien pisteet sekä arvioitujen vastausten keskiarvo. Kaikki keskiarvot ovat yhden desimaalin tarkkuudella. Oletuksena arviointikentissä on nollat, jotka korvataan 1-5 arviolla. Piste- ja keskiarvokentissä olevat arvot on lihavoitu. Kysymykset on tasattu vasemmalle ja samassa sarakkeessa viimeisillä riveillä olevat Pisteet: ja Keskiarvo: -tekstit on tasattu oikealle. Kaikki muu on keskitetty.

T12-R24	Miten tiedon varmuuskopiointi on järjestetty?	3	4	0	0		
Kohtalainen	Minne tiedot varmuuskopioidaan?	3	4	0	0		
	Onnistuuko tiedon täydellinen palautus, mikäli jokin katastrofi tapahtuu?	4	5	0	0		
	Kuinka kauan tiedon palauttaminen kestää?	2	5	0	0	!	
	Pisteet:	**12**	**18**	**0**	**0**		
	Keskiarvo:	**3,0**	**4,5**	**0,0**	**0,0**		

Kuva 7: Tekninen riski

Kuvassa seitsemän on arvioitu kahden palveluntarjoajan vastaukset tiedon palauttamista koskevaan tekniseen riskiin. Riskin koodi on T12-R24, mikä tarkoittaa riskin olevan tekninen riski numero 12 ja riski numero 24 selvityksessä. Koodin perusteella kyseisen riskin kuvaus on löydettävissä riskiselvityksestä. Koodien avulla on helpompi esimerkiksi taulukoida riskejä tai sijoittaa niitä erilaisiin kuvaajiin, mikäli työkalun käyttäjällä on tarvetta niin tehdä. Riskin

merkitys on arvioitu kohtalaiseksi. Kysymyksiä on neljä ja niissä PT2 eli palveluntarjoaja 2 on pärjännyt paremmin. Status-kenttään on tullut viimeisen kysymyksen kohdalla merkintä, koska PT1 on vastannut siihen vain tyydyttävästi.

Pisteet on laskettu jokaisen palveluntarjoajan kohdalta käyttämällä =SUMMA() -funktiota ja valitsemalla alueeksi kysymysten vastauskentät. Keskiarvon laskeminen on tehty käyttämällä samoihin alueisiin =KESKIARVO() -funktiota. Status -sarakkeen huutomerkki on toteutettu =JOS() ja =TAI() -funktioilla. Esimerkiksi kuvassa neljä oleva Status -merkintä on toteutettu seuraavasti: =JOS(TAI(C67=1; D67=1; E67=1; F67=1;C67=2; D67=2; E67=2; F67=2);"!";""). Funktio palauttaa huutomerkin, mikäli arvo on tosi, eli palveluntarjoajien sarakkeissa on kysymyksen rivillä arvo 1 tai 2. Mikäli arvo on epätosi, niin mitään ei palauteta. Samalla periaatteella toimiva funktio on sijoitettu Status -sarakkeessa jokaisen kysymyksen riville.

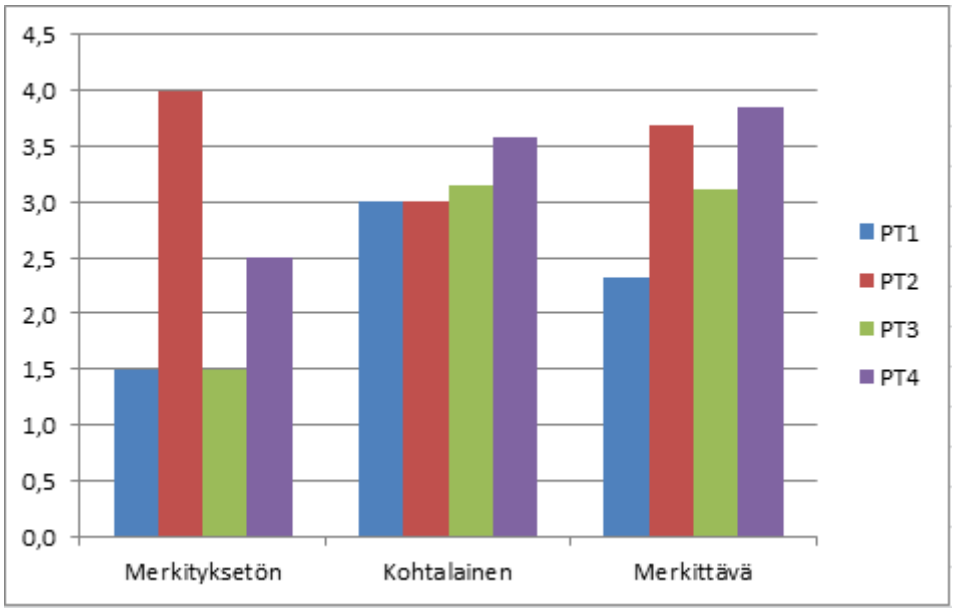
Riskikategorioissa on kaikkien riskien jälkeen yhteenvedot jokaisen palveluntarjoajan osalta. Yhteenvetoja hyödynnetään palveluntarjoajien vertailussa Keskiarvot ja Pisteet -välilehdissä. Palveluntarjoajien kokonaispisteet, pisteet merkittävyyksiltään erilaisissa riskeissä, kaikkien vastausten kokonaiskeskiarvot sekä vastausten keskiarvot merkittävyyksiltään erilaisissa riskeissä kuuluvat yhteenvetoon. Juridisissa riskeissä ei ole arvioituna merkityksettömiä riskejä, joten kyseisen kategorian yhteenvedossa ei ole kaavoja merkityksettömien riskien kohdalla.

Kokonaispisteet	**68**	**102**	**0**	**0**
Merkityksetön	**3**	**8**	**0**	**0**
Kohtalainen	**17**	**19**	**0**	**0**
Merkittävä	**48**	**75**	**0**	**0**
Kokonaiskeskiarvo	**2,4**	**3,6**	**0,0**	**0,0**
Merkityksetön	**1,5**	**4,0**	**0,0**	**0,0**
Kohtalainen	**2,4**	**2,7**	**0,0**	**0,0**
Merkittävä	**2,5**	**3,9**	**0,0**	**0,0**

Kuva 8: Riskikategorian yhteenveto

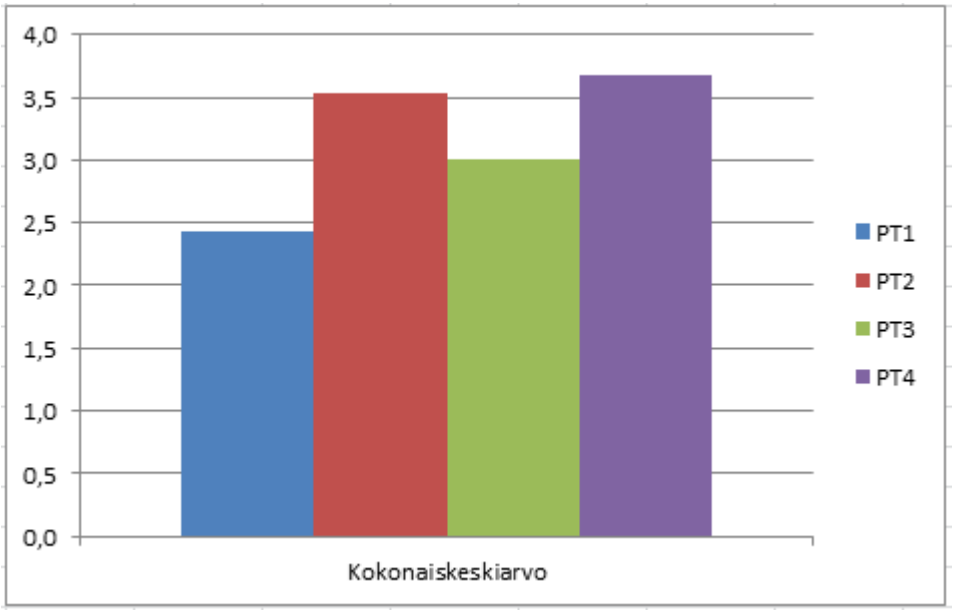
Kuvassa kahdeksan on yhteenveto yhdestä riskikategoriasta, jossa on arvioitu kaksi palveluntarjoajaa. Pisteiden laskuun on käytetty =SUMMA() -funktiota ja keskiarvojen laskuun =KESKIARVO() -funktiota. Kokonaispisteissä funktion alueena ovat aiemmin jokaisen riskin kohdalla yhteenlasketut pisteet. Pisteet merkitykseltään eritasoisista riskeistä on laskettu yhteen käyttämällä alueena kunkin riskitason riskien yhteenlaskettuja pisteitä. Keskiarvojen osalta periaate on sama, mutta alueeksi ovat valittuna yksittäisten kysymysten arviot. Kokonaiskeskiarvoa tai eri riskitasojen keskiarvoja ei voi laskea aiemmin riskien kohdilla lasketuista keskiarvoista, koska se ei tuota tarkkaa lopputulosta.

Keskiarvot -välilehti sisältää jokaisesta riskikategoriasta kaksi pylväsdiagrammia. Riskikategorian ensimmäisessä diagrammissa on palveluntarjoajien keskiarvojen vertailu merkitykseltään erilaisissa riskeissä. Toinen diagrammi vertailee palveluntarjoajien kokonaiskeskiarvoja. Diagrammeissa selitteen osat eli sarjat ovat solut joissa palveluntarjoajien nimet ovat. Vaaka-akselin luokkina on vertailuun tarvittava alue. Vertailussa käytetyt alueet on otettu riskikategorioiden yhteenvedoista. Pystyakselin arvot vaihtuvat automaattisesti vertailuun otettujen lukujen suuruuden mukaan. Kaikkien diagrammien korkeus on 7,9 ja leveys 12,4.



Kuva 9: Hallinnollisten riskien keskiarvojen vertailu riskitasoittain

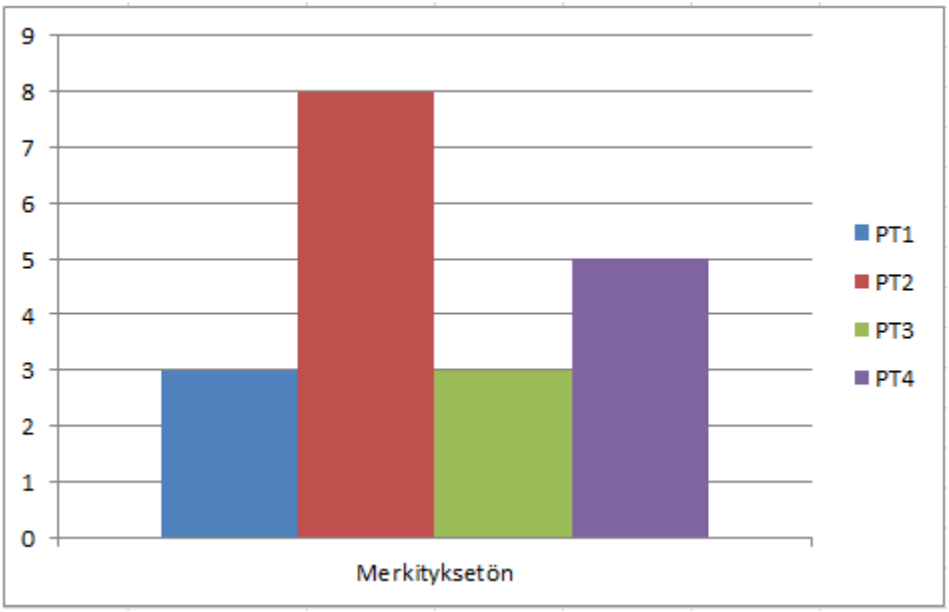
Kuvan yhdeksän vertailun perusteella PT4 eli palveluntarjoaja 4:n vastaukset on arvioitu keskimäärin parhaiksi hallinnollisten riskien kategorian kohtalaisissa ja merkittävissä riskeissä, mikä on päätöksenteon kannalta tärkeä tieto. Diagrammin tietoalue on ='Hallinnolliset riskit'!$B$1:$F$1;'Hallinnolliset riskit'!$B$81:$F$83. Näin vertailuun saadaan hallinnollisten riskien välilehdestä palveluntarjoajien nimet ja kyseisen riskikategorian yhteenvedossa lasketut keskiarvot eri riskitasoista. Muiden riskikategorioiden vastaava diagrammi on toteutettu samalla periaatteella, mutta tiedot on haettu kunkin kategorian omasta välilehdestä.



Kuva 10: Hallinnollisten riskien kokonaiskeskiarvojen vertailu

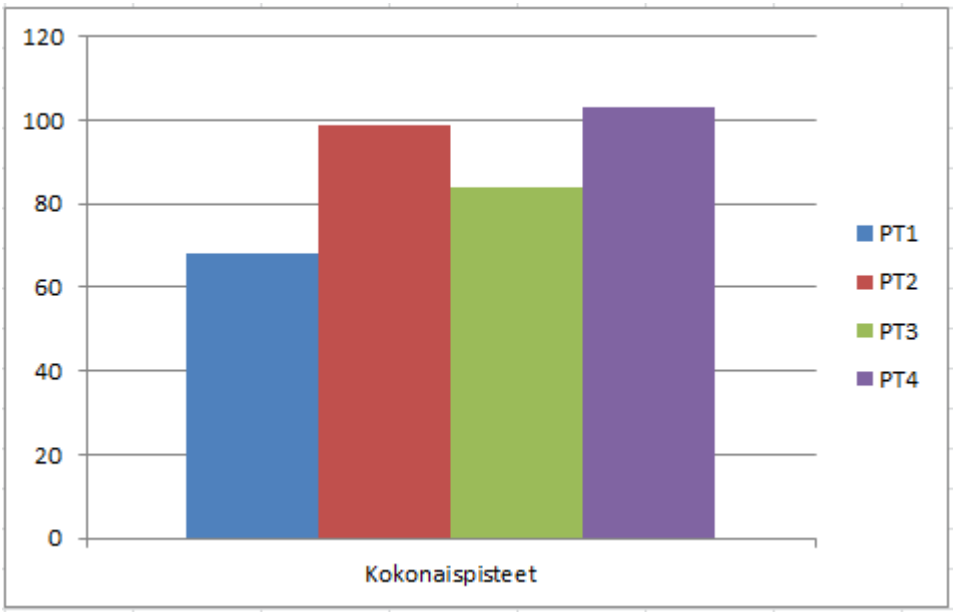
Kuvassa 10 on vertailtu hallinnollisten riskien kategorian kokonaiskeskiarvoja. Palveluntarjoaja 4 on vastannut keskimäärin parhaiten, kun kaikki kategoriat otetaan huomioon. Tietoalue on ='Hallinnolliset riskit'!$B$1:$F$1;'Hallinnolliset riskit'!$B$79:$F$79. Käyttämällä edellä mainittua tietoaluetta, on hallinnollisten riskien välilehdestä otettu vertailuun yhteenvedossa lasketut kokonaiskeskiarvot ja selitteeksi palveluntarjoajien nimet. Kaikkien riskikategorioiden kokonaiskeskiarvoja vertailevat diagrammit noudattavat samaa periaatetta ja tiedot on haettu oikeista välilehdistä.

Pisteet -välilehti sisältää jokaisesta riskikategoriasta neljä pylväsdiagrammia. Eritasoisista riskeistä on kaikissa riskikategorioissa omat diagrammit vertailua varten sekä kokonaispisteiden vertailut. Riskitasojen pisteiden vertailua varten ovat omat diagrammit, koska esimerkiksi merkityksettömiä riskejä on huomattavasti vähemmän kuin kohtalaiseksi arvioituja, joten niissä maksimipistemäärät ovat paljon alhaisempia. Yhdessä diagrammissa kaikkien riskitasojen pisteiden vertailu ei näytä hyvältä, mikäli merkityksettömistä riskeistä maksimimäärä on esimerkiksi 10, mutta kohtalaisista voi parhaimmillaan saada 60. Tämä johtaisi siihen, että merkityksettömien riskien pylväistä tulisi vertailussa kovin pieniä, vaikka palveluntarjoaja olisi saavuttanut täydet pisteet kyseisessä riskitasossa. Toimintaperiaatteet diagrammeissa ovat samat kuin keskiarvojen vertailussa käytetyissä diagrammeissa. Tietoalueina käytetään riskikategorioiden yhteenvedoissa laskettuja pistemääriä sekä palveluntarjoajien nimiä. Kooltaan diagrammit ovat samoja kuin keskiarvovertailussa ja pystyakselin arvot muuttuvat automaattisesti pisteiden määrän mukaan.



Kuva 11: Merkityksettömien hallinnollisten riskien pisteiden vertailu

Kuvassa 11 palveluntarjoaja 2 on saanut parhaat pisteet merkityksettömiksi arvioitujen hallinnollisten riskien osalta. Diagrammin tietoalue on ='Hallinnolliset riskit'!$B$1:$F$1;'Hallinnolliset riskit'!$B$76:$F$76. Tietoalueeseen kuuluu hallinnollisten riskien välilehdestä yhteenvedossa yhteenlasketut merkityksettömien riskien pisteet sekä palveluntarjoajien nimet. Vertailu riskitasoltaan erilaisissa riskeissä tapahtuu omissa diagrammeissaan samalla periaatteella, mutta tietoalueena ovat kohtalaisten tai merkittävien riskien yhteenlasketut pisteet. Eri riskikategorioissa olevat vastaavat diagrammit toimivat samoin, mutta tiedot on haettu niille kuuluvista välilehdistä.

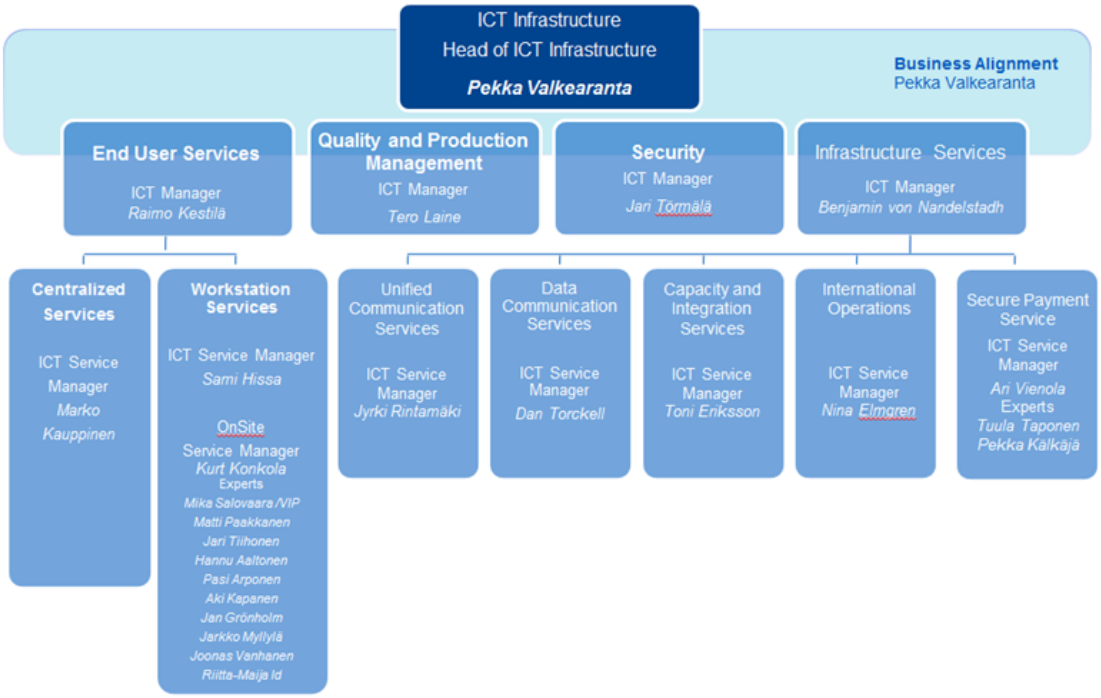


Kuva 12: Hallinnollisten riskien kokonaispisteiden vertailu

Kuvassa 12 on vertailtu palveluntarjoajien kokonaispisteet hallinnollisissa riskeissä. Diagrammissa käytetty tietoalue on ='Hallinnolliset riskit'!$B$1:$F$1;'Hallinnolliset riskit'!$B$74:$F$74. Tietoalue ottaa selitteeksi hallinnollisten riskien välilehdestä palveluntarjoajien nimet ja vertailuun yhteenvedossa yhteenlasketut kokonaispisteet. Kaikkien riskikategorioiden vastaavat diagrammit toimivat samalla tavalla, mutta tietoalueena ovat eri kategorioiden omista välilehdistä.

4.2 Toiminta hankeorganisaatiossa

Työyhteisönä ja hankeorganisaationa oli Keskon tietohallintoon kuuluva ICT-infrastructure services -yksikkö. Yksikön palveluihin kuuluvat tieto- ja puheliikennepalvelut, loppukäyttäjäpalvelut, kapasiteetti- ja integraatiopalvelu, turvallinen maksaminen sekä konsernin tietoturva. Opinnäytetyön ohjaaja hankeorganisaatiosta on konsernin tietoturvapäällikkö Jari Törmälä. ICT-infrastructure services -yksikköä johtaa Pekka Valkearanta ja työntekijöitä on 25.



Kuva 13: ICT-infrastruktuuripalvelut

Kuvassa 13 on Keskon ICT-infrastruktuuripalvelut -yksikön organisaatio ja sen toiminnot. Yksikkö sijaitsee Vantaan Hakkilassa Keskon keskusvarastojen läheisyydessä. Opinnäytetyöni ohjaaja on Security -toiminnossa.

Työskentely ja opinnäytetyön tekeminen hankeorganisaatiossa tapahtui pääosin työharjoitteluni ohessa ja pystyin käyttämään opinnäytetyön tekemiseen riittävästi aikaa päivittäin. Usein

oli kokonaisia työpäiviä, jotka pystyin käyttämään pelkästään opinnäytetyön tekemiseen. Tämä oli merkittävä tekijä sen suhteen, että työ valmistui alun perin suunnittelemaani aikataulua edellä. Työstäminen tapahtui käytännössä samalla tavalla kuin olisin tehnyt sitä varsinaisesti työkseni arkisin kahdeksan tunnin työpäivinä. Keskolta järjestettiin kaikki tarvittavat puitteet opinnäytetyön tekemistä varten. Minulle annettiin käyttöön työhuone, tietokone ja kaikki tarvittavat pääsyoikeudet. Ensimmäisenä päivänä mainittiin, että mikäli tarvitsen jotain materiaaleja opinnäytetyön tekemistä varten, niin ne hankitaan kyllä. Kaikki puitteet olivat valmiina heti tullessani paikalle ensimmäisenä päivänä 9.1.2012 ja pystyin aloittamaan opinnäytetyön suunnittelun varsin pikaisesti. Työharjoittelujaksoni loppui 23.3.2012 ja tämän jälkeen jäin tekemään opinnäytetyötä sillä periaatteella, että tulin paikalle mikäli työn edistämisen kannalta tarvetta oli. Kulkuoikeuteni säilytettiin, jotta pääsin paikalle. Tästä sovittiin, jotta kommunikaatio pysyi mahdollisimman mutkattomana ja nopeana.

Yhteistyö Keskon tietoturvapäällikön kanssa oli erittäin hyvin toimivaa. Keskusteluja opinnäytetyöstä on käyty lähes päivittäin ja kaikkiin kysymyksiin tai tarpeisiin vastattiin nopeasti. Mikäli oli jotain epäselvää, tarvitsin mielipidettä tai arviota johonkin opinnäytetyöhön liittyvään asiaan, niin käytännössä ei tarvinnut muuta kuin kävellä Törmälän työhuoneeseen kysymään. Sähköpostien ja puhelimen välityksellä asioita ei tarvinnut hoitaa. Työn edetessä lähetin säännöllisesti työkalun uusia versioita sekä Keskoa koskevia tekstin osuuksia kommentoitavaksi. Tietoperustassa olevat riskien kuvaukset olivat myös kommentoitavana. Työkalun toiminnallisuuksista ja ulkoasusta on sovittu yhdessä ja siten varmistin, että työkalu on varmasti sellainen kuin toimeksiantaja haluaa. Riskienarviointi tehtiin yhdessä ja työkaluun laatimani kysymykset lähetin arvioitavaksi.

4.3 Työskentelyprosessi

Opinnäytetyöprosessista pitämäni työskentelypäiväkirjan perusteella on selkeästi havaittavissa jaot orientaatio- ja suunnitteluvaiheisiin sekä toteutus- ja julkaisuvaiheisiin. Prosessin voi katsoa alkaneen 6.10.2011 Laureassa pidetyssä opinnäytetöiden orientaatioseminaarissa. Seuraavaksi on kuvattu jokaisen vaiheen ajallinen sijoittuminen sekä yleisesti merkittäviä tapahtumia. Tarkempi työskentelypäiväkirja on liitteessä neljä.

Orientaatiovaihe sijoittui ajanjaksolle 6.10.2011 – 16.1.2012. Opinnäytetyöprosessi alkoi osallistumisella lokakuussa 2011 järjestettyyn opinnäytetyöseminaariin. Noin kaksi viikkoa tämän jälkeen otin yhteyden Keskoon ja kysyin työharjoittelu sekä opinnäytetyömahdollisuudesta. Tarjosin heille opinnäytetyön aihetta, jonka teema rakentuisi pilvipalveluiden turvallisuuden ympärille. Marraskuussa sovimme työharjoittelun ja opinnäytetyön aloittamisesta. Tammikuussa 2012 aloitin työskentelyn Keskossa. Pari viikkoa töiden aloittamisen jälkeen palautin opinnäytetyön aiheanalyysin, joka sisälsi muun muassa ehdotuksen varsinaisesta aiheesta sekä

alustavan työsuunnitelman. Tässä vaiheessa minulla oli kartoitettuna jo tärkeimmät lähteet opinnäytetyön tekemistä varten sekä hyvä käsitys siitä, mikä työn tarkoitus on ja miten Kesko siitä hyötyy. Aiheanalyysin palauttaminen päätti orientaatiovaiheen.

Aiheanalyysini hyväksyttiin 31.1.2012 ja tästä alkoi suunnitteluvaihe. Aiheanalyysin perusteella opinnäytetyön ohjaajaksi ilmoitettiin Seija Tiainen, jonka kanssa ensimmäinen ohjaustapaaminen oli helmikuun ensimmäisinä päivinä. Olin alun perin suunnitellut tekeväni tutkimuksellisen opinnäytetyön ja sen toteuttamista kävimme läpi ensimmäisessä keskustelussa. Tiaisen suosituksen perusteella kävin myös tapaamassa Anssi Mattilaa, joka on Laureassa tietojenkäsittelyn koulutusohjelman lehtori. Mattilan kanssa käyty keskustelu oli merkittävä opinnäytetyön kannalta, koska sen perusteella suunnittelemani toteutus vaihtui tutkimuksellisesta opinnäytetyöstä toiminnalliseksi. Kävin aiheesta keskustelun Keskossa ohjaajani Jari Törmälän kanssa sekä lähetin asiasta sähköpostia Tiaiselle. Minä sekä Tiainen olimme sitä mieltä, että toiminnallinen opinnäytetyö oli tarkoituksenmukaisempi ja Keskon edustaja mainitsi jonkin käytännön toiminnassa hyödynnettävän produktin olevan heidän kannalta hyödyllisempi, kuin empiirinen tutkielma. Tältä pohjalta tein varsinaisen opinnäytetyön työsuunnitelman, jossa esitin tarkemmin miten toteutan työn. Työsuunnitelman palauttamisen jälkeen minulla oli tarvittava aineisto valmiina. Tiesin toteuttavani varsinaisen produktin Excelillä ja olimme sopineet Törmälän kanssa työkalun toiminnallisuuksista. Suunnitteluvaihe päättyi 15.2.2012, kun aloitin opinnäytetyöraportin kirjoittamisen. Työsuunnitelman esitin 28.2.2012, koska se ei ollut vielä valmis 8.2.2012 järjestettyä opinnäytetyöseminaaria varten.

Työn toteutusvaihe sisälsi opinnäytetyöraportin kirjoittamista ja arviointityökalun tekemisen. Vaiheen voi katsoa alkaneen 15.2.2012 ja päättyneen opinnäytetyön esitystilaisuuteen 19.4.2012. Ensimmäiset kolme viikkoa käytin opinnäytetyöraportin toteutuksen kuvausta edeltävien osioiden kirjoittamiseen. Ensimmäisenä lähdin työstämään raportin tietoperustaa, kehitystyön kuvausta sekä lähestymistapaa ja menetelmää. Näiden jälkeen kirjoitin työlle alustavan johdanto-osuuden. Riskienarviointi tehtiin Keskossa tietoturvapäällikkö Jari Törmälän kanssa 27.2.2012 ja sen perusteella laadin riskeistä palveluntarjoajille esitettävät kysymykset työkalua varten. Kysymykset ja riskienarvioinnin tulokset lähetin Törmälälle arvioitavaksi vielä ennen työkalun tekemisen aloittamista. 2.3.2012 aloitin arviointityökalun laatimisen. Työkalun saamiseksi lähes valmiiksi kului viikko tekemällä töitä pelkästään sen parissa. Toteutuksen aikana lähetin sen Törmälälle ja Tiaiselle kommentoitavaksi. Työkalun valmistuttua riskienarvioinnin, kysymyslistan ja arviointityökalun toiminnallisuuksien kuvaamiseen kului noin viikko. Ohjauskeskustelu Tiaisen kanssa oli 20.3.2012 ja Mattilan kanssa 26.3.2012. Toteutusvaiheen lopussa kirjoitin opinnäytetyön loppuarviointia ja tein pieniä korjauksia. 3.4.2012 lähetin työni ohjaajille luettavaksi ja sen perusteella sain luvan esittää työni opinnäytetyöseminaarissa 19.4.2012.

Opinnäytetyön julkaisuvaiheeseen kuului valmiin työn esittäminen opinnäytetyöseminaarissa. Tämän jälkeen viimeistelin työtä vielä seminaarin yhteydessä tulleiden kommenttien ja työn ohjaajan kommenttien perusteella. Työn esittämisen lisäksi julkaisuun liittyi valmistumiseen kuuluvat toimet, kuten valmiin työn tallentaminen Theseukseen ja lähettäminen Keskon tietoturvapäällikölle. Julkaisuvaihe ajoittui välille 19.4.2012 – 8.5.2012.

4.4 Toteutuksen yhteenveto

Työskentelyä Kesko-konsernin ICT-infrastruktuuripalvelut -yksikössä voi parhaiten kuvata mutkattomaksi. Olen erityisen tyytyväinen siihen, että pystyin tekemään opinnäytetyötäni työharjoittelujaksoni ohessa ilman haasteita esimerkiksi ajankäytön osalta. Pystyin suunnittelemaan omaa työskentelyäni molempien osalta, eikä opinnäytetyön edistämiselle ilmennyt mitään rajoitteita. Hankeorganisaatio järjesti kaikki tarvittavat työvälineet ja puitteet opinnäytetyön tekemistä varten. Sain joka kerta luvan poistua opinnäytetyöseminaaria tai ohjauskertoja varten, vaikka ne tapahtuivat suurimmalta osin työharjoittelujaksoni aikana. Dialogi minun ja Keskon tietoturvapäällikön välillä oli lähes jokapäiväistä. Ohjausta sain tarvittaessa ilman viiveitä. Ainoa kritisoitava asia hankeorganisaatiossa toimimisessa liittyy omaan toimintaani. Olisin voinut hyödyntää enemmän ICT-infrapalvelut -yksikössä olevia muita asiantuntijoita työn toteuttamisessa. En pysty arvioimaan, että olisiko se vaikuttanut toteutukseen millään tavalla, mutta se mahdollisuus minun olisi pitänyt käyttää tehokkaammin hyväksi.

Työprosessin eteneminen oli johdonmukaista ja työskentely oli järjestelmällistä. Koko opinnäytetyöprosessi kesti ajallisesti yli puoli vuotta ensimmäisestä orientaatioseminaarista valmiin työn palautukseen. Suunnittelu, toteutus ja julkaisuvaihe kestivät yhteensä arviolta neljä kuukautta. Asetin itselleni selkeitä aikatauluja ja tavoitteita, joiden täyttymisen kanssa ei ilmennyt ongelmia. Työ valmistui tavoiteaikataulua etuajassa. Suurin käännekohta työn kannalta oli opinnäytetyön vaihtaminen tutkimuksellisesta toiminnalliseksi. Tämä tarkoitti työn siirtymistä enemmän käytännönläheiseksi jossa tavoitteena oli auttaa ratkaisemaan hankeorganisaation eli Keskon käytännön toiminnassa kokema haaste. Prosessin aikana oli useita tapaamisia ja sähköpostinvaihtoja opinnäytetyön ohjaajan Seija Tiaisen sekä lehtori Anssi Mattilan kanssa. Mikäli minun pitäisi tehdä työ uudestaan, niin se todennäköisesti tapahtuisi samanlaisen prosessin mukaan.

Riskienarviointia pidän onnistuneena, koska sen perusteella tietoperustassa kuvatuille riskeille saatiin arvioitujen todennäköisyyksien ja vakavuuksien perusteella riskiarvot toimeksiantaja-organisaation näkökulmasta. Arviointi toteutettiin konsernin tietoturvapäällikön kanssa keskustelemalla ja yhteistyö oli mutkatonta. Mielestäni on tärkeää, että jokainen pilvipalvelua arvioiva organisaatio tekee itse oman riskienarvioinnin, koska riskinkantokyvyt eri yrityksillä ja hankittavat palvelut ovat erilaisia, mitkä vaikuttavat siihen kuinka vakavaksi riskit koetaan.

Tehdyssä riskienarvioinnissa oli taustalla Keskon tietoturvapäällikön Jari Törmälän antama tieto, että Kesko ei ainakaan tällä hetkellä aio siirtää kriittisiä toimintoja pilvipalveluna toteutettavaksi. Tästä syystä merkittäväksikin arvioitu riski toteutuessaan ei tule uhkaamaan organisaation olemassaoloa ja toimintojen jatkuvuutta, mutta palvelun jatkuvuuteen vaikutus voi olla suuri. Riskiarvojen avulla riskit luokittelin tasoiltaan merkityksettömiksi, kohtalaisiksi tai merkittäviksi. Nämä luokittelut ovat työkalun vertailutoiminnallisuuksien kannalta oleellisia. Riskitasojen avulla työkalun käyttäjä näkee, mitkä riskit ovat tärkeimpiä ja voi ottaa sen huomioon palveluntarjoajien arvioinnissa. Riskienarvioinnin haasteena on, että Keskon sisälläkin voi olla eri toimintoja jotka saattavat kokea riskit merkityksiltään erilaisiksi, kuin miten tehdyssä arvioinnissa on määritelty. Arvioinnin tulokset lähetin Törmälälle tarkistettavaksi, mutta muutoksia tehtyihin arvioihin hän ei halunnut vielä tehdä. Riskienarvioinnissa syntyneet riskiarvot ovat tarvittaessa muutettavissa ja mikäli merkitykset muuttuvat, niin muutokset voi tehdä työkaluun.

Tietoperustassa kuvattujen riskien perusteella muodostin jokaisesta riskistä palveluntarjoajille esitettäviä kysymyksiä, jotka ovat työkalun tärkeintä sisältöä. Laatimani kysymykset lähetin Törmälän arvioitavaksi, eikä niihin tullut sen jälkeen suuria muutoksia. Kysymyksissä pyrin siihen, että ne johtaisivat laajempaan keskusteluun eikä lisäkysymysten esittäminen ole poissuljettua. Haasteena kysymyslistassa on kysymysten määrä ja odotettujen vastausten laajuus. Kysymysten läpikäyminen palveluntarjoajan kanssa voi viedä paljon aikaa, mikä työkalun käyttäjän tulee ottaa huomioon. Palveluntarjoaja saattaa myös vastata useampaan kysymykseen samalla kerralla, joten työkalun käyttäjän on noteerattava se keskustelussa. On myös mahdollista, että tietoturvakeskusteluun osallistuva SaaS-palveluntarjoaja ei itse hallinnoi taustalla olevaa pilvi-infrastruktuuria vaan on sijoittanut oman ohjelmistonsa jonkin toisen palveluntarjoajan pilvipalveluun. Tässä tapauksessa SaaS-palveluntarjoaja ei välttämättä pysty vastaamaan tyydyttävästi esitettyihin kysymyksiin.

Arviointityökalu sisältää kaikki toiminnallisuudet mitä siihen alun perin olin suunnitellut ja tein sen toimeksiantajan toiveiden mukaisesti. Työkalun rakenteessa pyrin selkeään asetteluun. Palveluntarjoajien vertaileminen on mahdollista, työkalun käyttö on yksinkertaista ja sen muokkaaminen tarpeiden mukaan onnistuu vähällä vaivalla. Haasteet työkalussa liittyvät käyttäjään. Käyttäjä voi vahingossa käyttää työkalua väärin, esimerkiksi syöttämällä virheellisiä arvoja tai poistamalla vahingossa sisältöä. Soluja ei ole lukittu eikä syötettäville arvoille ole asetettu rajoituksia, koska se hankaloittaa sisällön muokkaamista. Mikäli on esimerkiksi tarpeellista käyttää erilaista arviointiasteikkoa, niin kaikista soluista täytyisi poistaa rajoitukset. Käyttäjän osaaminen on myös merkittävässä osassa, koska työkalu yksinkertaisuudestaan huolimatta edellyttää jonkinlaisia Excelin perustaitoja. Isoimmat haasteet käyttäjän taitojen osalta ovat osaaminen tietotekniikassa ja siihen liittyvässä turvallisuudessa. Pilvipalveluiden riskeistä keskusteleminen palveluntarjoajien kanssa ja vastausten arviointi ei todennäköisesti

onnistu tarkoituksenmukaisesti, mikäli osaamista käsiteltävistä aihealueista ei ole riittävästi. Tätä helpotetaan siten, että työkalun käyttäjälle toimitetaan tietoperustassa olevat kuvaukset keskeisistä käsitteistä ja riskeistä.

5 Arviointi

Opinnäytetyöprosessin eteneminen oli tasaista ja työn tekeminen johdonmukaista. Työskentelyn voi katsoa kestäneen yli puoli vuotta alkaen ensimmäisestä orientaatioseminaarista syksyllä 2011 ja päättyen työn arvioitavaksi jättämiseen keväällä 2012. Työ valmistui etuajassa alkuperäiseen suunniteltuun aikatauluun nähden ja uskon sen johtuneen pääosin siitä, että asetin prosessin aikana pienempiä lyhyen aikavälin tavoitteita joista pidin kiinni. Aikatauluun vaikutti myös hankeorganisaation toiminta, koska työharjoittelujaksoni aikana pystyin tekemään myös opinnäytetyötä.

Työprosessin aikana ei ilmennyt varsinaisia ongelmia. Ainoa minkä voi mainita, on ajan tuhlaaminen opinnäytetyön alkuvaiheessa tutkimuksellisen opinnäytetyön suunnitteluun. Onneksi kuitenkin kävin varhaisessa vaiheessa ohjauskeskustelun Anssi Mattilan kanssa, joka suositteli hyvää kirjallisuuslähdettä käytännöllisemmän työn tekemiseksi. Tämän jälkeen työ vaihtui toiminnalliseksi ja eteneminen oli huomattavasti helpompaa ja tarkoituksenmukaisempaa. Asiat selkeytyivät ja Keskossakin oltiin tyytyväisiä käytännön toiminnassa hyödynnettävään ratkaisuun. Uskon tämän muutoksen nopeuttaneen työskentelyä huomattavasti.

Työn tavoitteisiin ja tarkoitukseen vaikuttivat merkittävästi työn toimeksiantajan odotukset. Työltä odotettiin puolueetonta selvitystä julkisen pilven SaaS-palveluihin liittyvistä riskeistä ja käytännön toiminnassa hyödynnettävää tuotosta. Tarkoituksena oli saavuttaa tulokset, jotka tukevat pilvipalveluihin liittyvää päätöksentekoa Kesko-konsernissa. Opinnäytetyön perusteella Keskossa on tarkoituksena yhtenäistää toimintatapoja ja mahdollistaa eri liiketoimintojen omatoiminen pilvipalveluiden soveltuvuuden arviointi. Uskon, että työni täyttää toimeksiantajan sille asettamat odotukset. Keskossa ei ole aiemmin tehty selvityksiä pilvipalveluiden turvallisuudesta, eikä käytössä ole ollut järjestelmällistä tapaa arvioida pilvipalveluiden turvallisuutta. Nyt toimeksiantajalla on saatavilla kattava selvitys potentiaalisimmaksi koetun pilvipalveluiden palvelumallin ja tietoturvallisuuden kannalta ongelmallisimmaksi havaitun toteutusmallin riskeistä, sekä tapa jonka mukaan toimia tulevissa hankintaprosesseissa. Tulevaisuudessa Keskossa on mahdollista käsitellä hankittavan pilvipalvelun tietoturvallisuutta perusteellisemmin ja hyvällä todennäköisyydellä onnistua mahdollisimman turvallisen palvelun valinnassa.

Työssäni toimin valitsemani lähestymistavan ja menetelmän mukaan. Konstruktiivisessa tutkimuksessa ratkaistaan jokin käytännössä havaittu ongelma rakentamalla konstruktio eli pro-

dukti tai tuote, joka pohjautuu aiempaan laadukkaaseen tutkimustietoon. Riskiselvitys perustuu aiempaan tutkimustietoon ja sen perusteella tein varsinaisen tuotoksen, eli arviointityökalun. Lähestymistapaa pidän parhaana mahdollisena tämänkaltaisen työn toteuttamiseksi. Menetelmänä selvityksen tekemisessä käytin narratiivista kuvailevaa kirjallisuuskatsausta. Kirjallisuuskatsaukset ovat menetelmiä joissa tiivistetään aiempaa tutkimustietoa johtopäätösten tekemistä varten. Riskien kuvauksessa pyrin tiivistykseen ja helppolukuisuuteen, jotta käsiteltävästä aihealueesta saa laajan kokonaiskuvan. Selvitys oli kuitenkin riittävän tarkka, jotta yksittäisiä riskejä voitiin arvioida produktia varten. Mielestäni onnistuin valitsemani menetelmän toteutuksessa. Alun perin suunnittelin myös haastattelun tekemistä Keskossa, mutta keskusteltuani Keskon tietoturvapäällikön kanssa tulimme siihen tulokseen, että haastattelulla ei saavutettaisi riittävän hyviä tuloksia.

Kehittämistyön osuudessa kuvatut konstruktiivisen tutkimuksen prosessiin kuuluvat vaiheet ovat havaittavissa työskentelyprosessin kuvauksen perusteella. Alussa eli orientaatio- ja suunnitteluvaiheissa etsin mielekkään ongelman ja hankin teoreettista tietoa aiheesta sekä käytännön tietoa toimeksiantajasta. Toteutusvaiheessa laadin ratkaisut, eli arviointityökalun ja opinnäytetyöraportin jossa on riskiselvitys. Toteutuksen aikana piti testata ratkaisun toimivuus, mikä jäi puutteelliseksi, sillä todellinen toimivuus selviää vasta kun työkalua käytetään Keskossa. Tarkoituksena oli testata työkalua todellisessa tilanteessa, mutta sopivaa pilvipalvelun hankintaprosessia ei ollut meneillään tai alkamassa. Toimivuutta Keskon tietoturvapäällikkö on arvioinut liitteen viisi lausunnossa. Teoriakytkentöjä, eli aikaisempien tutkimusten perusteella tehdyn riskiselvityksen hyödyntämistä toteutuksessa käsittelin useaan otteeseen koko prosessin aikana eri osioiden pienoisjohdannoissa ja yhteenvedoissa. Julkaisuvaiheeseen kuului ratkaisun uutuusarvon osoittaminen ja soveltamisalueen laajuuden tarkastelu, jotka ovat osa loppuarviointia.

Lähteitä pyrin käyttämään työni kannalta tarkoituksenmukaisesti. Tarkoituksena oli lähteiden avulla saada aikaisempien tutkimusten tai julkaisujen perusteella kuvattua julkisen pilven SaaS-palveluihin liittyviä riskejä, jotta ne voitiin Keskossa arvioida ja siirtää osaksi turvallisuudenarviointityökalua. Valitsin ainoastaan lähteitä, jotka ovat ajantasaisia ja joiden taustalla on jokin uskottavaksi ja luotettavaksi kokemani taho. Pyrin myös siihen, että lähteinä käytetyt tutkimukset ja julkaisut ovat mahdollisimman puolueettomia, eivätkä esimerkiksi pilvipalveluntarjoajien itse julkaisemia tai rahoittamia. Vanhin tässä työssä käytetyistä lähteistä on vuodelta 2008. Pilvipalveluiden osalta lähteiden ajantasaisuus on tärkeää, koska pilvikonsepti ja siihen liittyvät palvelut kehittyvät huimaa vauhtia.

Opinnäytetyötä suunnitellessani käytin Googlen Scholar -hakua pilvipalveluihin ja niiden tietoturvallisuuteen liittyvien suomalaisten lopputöiden ja tutkimusten löytämiseksi. Vesa Lehtinen on tehnyt vuonna 2010 pro gradun aiheesta ”Tietoturvan ja tietosuojan kehittäminen pil-

viteknologiassa — standardit ja kehysmallit sekä riskienhallinnan näkökulma.” Jussi-Pekka Erkkilä on tehnyt kandintyön vuonna 2011 aiheena ”Tietoturva julkisissa pilvipalveluissa” ja Jouni Lehto ylemmän AMK-tutkinnon lopputyön aiheesta ”Pelastustoiminnan parantaminen katvealueella sekä pilvipalveluiden hyödyntäminen pelastustoiminnassa: suunnittelututkimus.” Kaikkia näitä töitä yhdistää se, että pilvipalveluihin liittyvät riskit ovat kuvattu suppeammin ja näkökulmat ovat eriäviä. Mainituissa töissä ei ole tehty riskienarviointia eikä lopputuotetta, kuten opinnäytetyössäni on. Lehtinen ja Lehto käsittelevät työssään pilvipalveluita yleisemmin, kun omassa työssäni on rajaus pelkästään julkiseen pilveen ja SaaS-palveluihin. Erkkilän kandintyössä on keskitytty erityisesti IaaS-palveluihin ja tietoturvaratkaisuihin. Scholar-haun perusteella pilvipalveluiden tietoturvaan liittyviä töitä on todella vähän. Pilvipalveluista yleisesti, niiden hyödyistä ja käyttöönotosta on tehty enemmän lopputöitä. Näissä useasti tietoturvan osuus on vain sivuosassa. Omaa opinnäyteyötäni vastaavaa työtä en löytänyt.

Työssäni oli riskin osalta pelkästään uhkanäkökulma, eli riskejä käsittelin vain potentiaalisina haitallisina tapahtumina. Ehdotan jatkoselvitysten osalta, että pilvipalveluiden avulla saavutettavia mahdollisia turvallisuushyötyjä selvitettäisi. Uskon pilvipalveluista olevan hyötyä varsinkin pienille yrityksille, joilla ei välttämättä ole riittävästi resursseja omien IT-järjestelmien turvallisuuden varmistamiseen. Voi olla hyvinkin mahdollista, että siirtyminen pilveen jopa parantaa turvallisuuden tasoa. Aiheeni olin rajannut julkisen pilven toteutusmalliin ja Software as a Service -palveluihin, joten jatkoselvityksissä kannattaa myös paneutua muihin toteutusmalleihin ja palvelumalleihin. Mielenkiintoinen selvittämisen aihe on myös pilvipalveluna toteutetut turvallisuuspalvelut, joissa pilvipalveluiden avulla suojataan muita tietoteknisiä palveluita.

Ensisijaisesti työkalu on tarkoitettu hyödynnettäväksi Keskon toiminnassa, kun pilvipalveluiden hankintaprosessi on meneillään. Riskiselvityksen perusteella Keskossa on mahdollista ymmärtää paremmin pilvipalveluita ja niihin liittyviä potentiaalisia ongelmia. Arviointityökalun avulla konsernin liiketoiminnot voivat itsenäisesti arvioida pilvipalveluiden soveltuvuutta ja Keskon toimintatapoja pilvipalveluiden arvioinnin osalta voi yhtenäistää. Vaikkakin opinnäytetyöni on tarkoitettu Keskon käyttöön, niin tekemääni työkalua ja riskiselvitystä voi rajoituksetta käyttää mitkä tahansa yritykset ja henkilöt. Työni on hyödyllinen organisaatioille, joilla on tarvetta arvioida pilvipalveluiden ja erityisesti julkisen pilven SaaS-palveluiden tietoturvallisuutta. Arviointityökalua on myös mahdollista muokata sen käyttäjien omaan toimintaan soveltuvaksi. Kysymyksiä ja riskejä voi lisätä ja poistaa sekä kokonaisia riskikategorioita voi tehdä. Vertailua varten on mahdollista lisätä uusia toiminnallisuuksia. Todennäköisesti työkalu saa lopullisen muotonsa vasta pidemmällä aikavälillä käyttäjien palautteen perusteella. Opinnäytetyön toimeksiantaja arvioi työn selkeästi hyödylliseksi heidän toiminnassaan. Keskokonsernin tietoturvapäällikön ja opinnäytetyön ohjaajan Jari Törmälän lausunto työn hyödynnettävyydestä ja onnistumisesta on liitteessä viisi.

Jatkotoimenpiteet Keskossa liittyvät työkalun käyttöönottoon. Suosittelen toimimaan siten, että työkalun käyttöä varten laaditaan lyhyt saateviesti joka sisältää käyttöohjeen sekä kuvauksen työkalun käyttötarkoituksesta. Saateviestiä käytettäisiin, kun sähköpostin välityksellä lähettää työkalun ja siihen liittyvät dokumentit sen käyttäjälle. Sama lyhyt kuvaus voi olla sijoitettuna ohessa, mikäli työkalu tallennetaan työtiloihin tai Intranettiin. Saateviestin lisäksi kannattaa varautua pitämään pienimuotoisia koulutushetkiä. Opinnäytetyöni raportista on suositeltavaa ottaa tietoperusta erilliseksi dokumentiksi, joka toimitetaan arviointityökalun käyttäjälle varsinaisen Excel-laskentataulukon lisäksi. Lukemalla tietoperustassa olevat keskeiset käsitteet sekä riskiselvityksen, saa työkalun käyttäjä paremman kokonaiskuvan pilvipalveluista ja voi ymmärtää paremmin työkaluun sijoitettujen riskien kontekstin. Tämä on ensiarvoisen tärkeää, kun arviointityökalua käytetään todellisessa tilanteessa.

Oman oppimisen kannalta opinnäytetyö oli merkittävä. Työn toteuttamisen jälkeen voin todeta, että minulla on nyt parempaa asiantuntemusta pilvipalveluihin liittyen. Ymmärrän paremmin pilvikonseptin kokonaisuutena ja siihen liittyviä turvallisuushaasteita. Tärkeää oppimiseni kannalta oli myös toimiminen hankeorganisaatiossa eli Keskossa. Toiminnan perusteella hahmotan paremmin pilvipalveluihin liittyviä haasteita ja mahdollisuuksia suuryrityksen näkökulmasta. Tarkoituksena on tulevaisuudessa jatkaa työskentelemistä tietoturvallisuuden parissa

Lähteet

Badger, L., Grance, T., Patt-Corner R. & Voas, J. 2011. DRAFT Cloud Computing Synopsis and Recommendations. Viitattu 24.4.2012
http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

Botteri, P., Cowan, D., Deeter, B., Fisher, A., Garg, D.,
Goodman, B., Levine, J., Messiana, G., Sarin, A. & Tavel, S. 2010. Bessemer's Top 10 Laws of Cloud Computing and SaaS. Viitattu 23.2.2012
http://www.bvp.com/downloads/saas/BVPs_10_Laws_of_Cloud_SaaS_Winter_2010_Release.pdf

Catteddu, D. & Hogben, G. 2009. Cloud Computing: benefits, risks and recommendations for information security. Viitattu 20.2.2012
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Chou, Y. 2010. Cloud Computing Primer for IT Pros. Viitattu 15.3.2012
http://blogs.technet.com/b/yungchou/archive/2010/11/15/cloud-computing-primer-for-it-pros.aspx

Cloud Security Alliance. 2010. Top Threats to Cloud Computing V1.0. Viitattu 21.2.2012
https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

Cloud Security Alliance. 2012. About: Cloud Security Alliance. Viitattu 24.4.2012
https://cloudsecurityalliance.org/about/

Coalfire. 2012. Spotlight on Cloud Computing: An Overview. Viitattu 15.3.2012
http://www.coalfire.com/Resources/Spotlight-Compliance

ENISA. 2012. About ENISA. Viitattu 23.4.2012
http://www.enisa.europa.eu/about-enisa

Gartner. 2012. About Gartner. Viitattu 23.4.2012
http://www.gartner.com/technology/about.jsp

Heiser, J. & Nicolett, M. 2008. Assessing the Security Risks of Cloud Computing. Viitattu 21.2.2012
http://cloud.ctrls.in/files/assessing-the-security-risks.pdf

Jansen, W. & Grance, T. 2011. Guidelines on Security and Privacy in Public Cloud. Viitattu 22.2.2012
http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

Juvonen, M., Korhonen, H., Ojala, VM., Salonen, T. & Vuori, H. 2008. Yrityksen riskienhallinta. Helsinki: Yliopistopaino

Järvi, A., Karttunen, J., Mäkilä, T. & Ipatti, J. 2011. SaaS-Käsikirja. Viitattu 23.2.2012
http://dl.dropbox.com/u/3753443/SaaS%20kirja%202011%20iPad.pdf

Keskon hallinto ja johto. 2011. Viitattu 23.2.2012
http://www.kesko.fi/fi/Kesko-yrityksena/Hallinto-ja-johto/

Keskon historia. 2010. Viitattu 23.2.2012
http://www.kesko.fi/fi/Kesko-yrityksena/Keskon-historia/

Kesko lyhyesti. 2011. Viitattu 23.2.2012
http://www.kesko.fi/fi/Kesko-yrityksena/Kesko-lyhyesti/

Keskon tilinpäätöstiedote 1.1 -31.12.2011. 2012. viitattu 23.2.2012
http://www.kesko.fi/fi/Media/Tiedotteet/Porssitiedotteet/2011/Keskon-tilinpaatostiedote-11-31122011/

Korpimies, A. 2011. Jopa puolet IT-palveluista tulee pilvestä vuonna 2015. Viitattu 24.2.2012
http://www.tietoviikko.fi/cio/jopa+puolet+itpalveluista+tulee+pilvesta+vuonna+2015/a667170

Liikenne- ja viestintäministeriö. 2012. Kiuru Viestintäfoorumissa: Suomen tuleva kasvu digitaalisissa palveluissa. Viitattu 24.12.2012
http://www.lvm.fi/web/fi/tiedote/-/view/2973795

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. Viitattu 15.2.2012
http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

NIST. 2012. NIST General Information. Viitattu 24.3.2012
http://www.nist.gov/public_affairs/general_information.cfm

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOYpro Oy

Ponemon Institute. 2011. Security of Cloud Computing Providers Study. Viitattu 24.2.2012
http://www.ca.com/~/media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf

Ranta, N. 2011. Tutkimus: IT-osasto ei ymmärrä pilvipalveluja. Viitattu 24.2.2012
http://www.tietoviikko.fi/cio/tutkimus+itosasto+ei+ymmarra+pilvipalveluja/a661793

Salminen, A. 2011. Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Viitattu 20.2.2012
http://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf

Takabi, H., Joshi, B.D. J. & Ahn, G-J. 2010. Security and Privacy Challenges in Cloud Computing. Viitattu 22.2.2012
http://www.sis.pitt.edu/~jjoshi/courses/IS2620/Spring11/cloud.pdf

Kuvat

Taulukot

Liitteet

Liite 1: Kysymyslista

Hallinnolliset riskit

H1-R1 – Tiedon sisään lukkiutuminen

1.1 Miten tiedon siirtäminen onnistuu palvelusta pois tai toiseen palveluun?

1.2 Onko käytössä standardeja tiedostomuotoja, tekniikkaa ja menettelyitä joilla tiedon siirrettävyys on varmistettu?

H2-R2 – Hallinnon menettäminen

2.1 Miten turvallisuuspalvelut, kuten haavoittuvuuksien arvioinnit ja läpäisykyky-testit ovat järjestetty?

2.2 Onko palvelun toteutuksessa käytetty kolmansia osapuolia?

2.3 Mikäli kolmansia osapuolia (alihankkijoita) käytetään, niin takaavatko he turvallisuuden osalta saman tason?

2.4 Miten varmistetaan, että ristiriitoja ei ilmene asiakkaan omien turvallisuuden koventamismenettelyiden ja pilviympäristön välillä?

H3-R3 – Vaatimustenmukaisuuksien noudattaminen

3.1 Minkä sertifikaattien ja standardien osalta pilviympäristö on yhteensopiva?

3.2 Onko palvelun auditointi mahdollista?

H4-R4 – Muiden vuokralaisten toiminta

4.1 Miten asiakkaiden mahdollista haitallista toimintaa valvotaan?

4.2 Takavarikoidaanko muiden käytössä olevia resursseja, mikäli haitallista toimintaa havaitaan?

H5-R5 – Palvelun lopettaminen

5.1 Miten palvelun jatkuvuus on turvattu?

H6-R6 – Yrityskauppa

6.2 Miten ei-sitovien sopimusten käy jos esimerkiksi yrityskauppa toteutuu?

H7-R7 – Toimitusketjun häiriöt

7.1 Miten palvelun toimitusketjujen häiriöihin on varauduttu?

7.2 Miten alihankkijoiden tai muiden mukana olevien tahojen turvallisuus on varmistettu?

7.3 Mitä osia palvelusta on ulkoistettu?

H8-R8 – Tuntematon riskiprofiili

8.1 Mitä tietoa käytetyistä turvallisuusmenettelyistä, auditoinneista, päivityksistä, ohjelmistoversioista, haavoittuvuusprofiileista, hyökkäyksistä ja tapahtumalokeista on saatavilla?

8.2 Mitä tietoa on saatavilla, mikäli turvallisuuspoikkeama havaitaan?

8.3 Mitä lokitietoja kerätään, miten ne tallennetaan ja kenellä on pääsy niihin?

H9-R9 – Puutteellinen riskienhallinnan tukeminen

9.1 Onko palvelun turvalliseen käyttöön saatavilla ohjeita ja koulutusta?

9.2 Onko ylläpidosta vastaaville henkilöille saatavilla ohjeita ja koulutusta?

H10-R10 – Palvelutasosopimuksen huolimaton toteutus

10.1 Miten turvallisuus huomioidaan palvelutasosopimuksessa?

10.2 Miten turvallisuutta mitataan?

10.3 Onko tarvittaessa mahdollisuus ottaa kolmas osapuoli valvomaan palvelutasosopimuksen toteutumista?

H11-R11 – Puutteellinen reagoiminen turvallisuustapahtumiin

11.1 Miten havaittuihin turvallisuustapahtumiin reagoidaan?

11.2 Miten hyökkäyksiä todennetaan ja analysoidaan?

11.3 Miten hyökkäysten eristäminen tapahtuu?

11.4 Miten mahdollisen keskeytymisen jälkeinen palautuminen tapahtuu?

H12-R12 – Politiikkojen ja käytäntöjen yhteensopimattomuus

12.1 Miten varmistetaan, että tietoturvapolitiikat ja käytännöt ovat yhteensopivia?

Tekniset riskit

T1-R13 – Resurssien ehtyminen

13.1 Miten pilvijärjestelmän resurssien riittävyys on varmistettu?

13.2 Miten resurssien riittävyyttä valvotaan ja tulevaisuuden käyttöastetta mallinnetaan?

T2-R14 – Eristämisen epäonnistuminen

14.1 Miten pilvipalvelun asiakkaat ja niiden tiedot eristetään toisistaan?

14.2 Miten eristämisen toimivuutta valvotaan?

T3-R15 – Pahantahtoiset työntekijät

15.1 Miten on varauduttu mahdollisiin pahantahtoisiin työntekijöihin?

T4-R16 – Hallinnointirajapinnan vaarantuminen

16.1 Miten palvelun käyttörajapintojen turvallisuus on varmistettu?

T5-R17 – Tiedonsiirron kaappaukset

17.1 Miten pilvijärjestelmässä tapahtuvaan tiedonsiirtoon kohdistuviin hyökkäyksiin on varauduttu?

17.2 Miten asiakkaan ja pilvijärjestelmän välillä tapahtuvaan tiedonsiirtoon kohdistuviin hyökkäyksiin on varauduttu?

17.3 Miten palvelutasosopimuksessa huomioidaan mahdollisen tiedonsiirron kaappaamisen aiheuttamat tietovuodot?

T6-R18 – Turvaton tai tehoton tiedon hävittäminen

18.1 Miten tietoja hävitetään, kun fyysisiä laitteita kohdennetaan uudelleen tai resursseja vapautetaan?

18.2 Miten varmistetaan, että tietoa ei jää yli asiakkaan toivoman elinkaaren?

18.3 Mikäli tietoa pyydetään hävittämään, niin johtaako se todelliseen tiedon hävittämiseen?

T7-R19 – Palvelunestohyökkäykset

19.1 Miten palvelunestohyökkäyksiin on varauduttu?

T8-R20 – Salausavaimien menettäminen

20.1 Kuinka on varmistettu, että pilvijärjestelmässä käytettyjä salausavaimia ei menetetä?

20.2 Miten digitaalisten varmenteiden kiistämättömyys on varmistettu?

T9-R21 – Pahantahtoiset skannaukset

21.1 Miten havaittuihin verkkotiedusteluihin ja kartoitusyrityksiin reagoidaan?

T10-R22 – Palvelumoottorin vaarantuminen

22.1 Miten palvelua hallinnoivan palvelumoottorin ja siihen liittyvän tekniikan turvallisuus on varmistettu?

T11-R23 – Ristiriidat turvallisuuden koventamismenettelyissä

23.1 Miten on ratkaistu ristiriidat eri asiakkaiden toivomien turvallisuuden koventamismenettelyiden välillä?

T12-R24 – Puutteelliset menettelyt tiedon palauttamisessa

24.1 Miten tiedon varmuuskopiointi on järjestetty?

24.2 Minne tiedot varmuuskopioidaan?

24.3 Onnistuuko tiedon täydellinen palautus, mikäli jokin katastrofi tapahtuu?

24.4 Kuinka kauan tiedon palauttaminen kestää?

T13-R25 – Identiteettien ja pääsynhallinnan yhteensopimattomuus

25.1 Onko asiakkaan tunnistamiseen ja todentamiseen käytetty järjestelmä sovitettavissa yhteen jo olemassa olevien todennusjärjestelmien kanssa?

T14-R26 – Korkean riskiprofiilin asiakkaat

26.1 Otetaanko pilvijärjestelmään korkeamman riskiprofiilin omaavia asiakkaita?

26.2 Miten on varauduttu korkeamman riskiprofiilin asiakkaista aiheutuvaan hyökkäysten todennäköisyyden kasvuun?

Juridiset riskit

J1-R27 – Viranomais- ja siviilikanteet

27.1 Onko mahdollista, että muidenkin kuin asianosaisten tietoja päätyy ulkopuolisten haltuun, mikäli fyysisiä laitteita tarvitaan todistusaineistoksi viranomais- ja siviilikanteissa?

J2-R28 – Lainsäädännön muutokset

28.1 Säilytetäänkö tietoja maissa, joissa palvelun toimintaan vaikuttavaan lainsäädäntöön saattaa tulla yhtäkkisiä ennalta arvaamattomia muutoksia?

28.2 Säilytetäänkö tietoja riskialttiissa maissa, kuten esimerkiksi maissa jotka eivät toimi oikeusvaltioperiaatteen mukaan ja joissa oikeusjärjestelmä on puutteellinen?

J3-R29 – Tietosuoja

29.1 Miten on varmistettu, että tietoja käsitellään lainmukaisesti?

29.2 Miten tietosuojaan liittyvä lainsäädäntö on huomioitu palvelussa?

29.3 Mitä asiakkaiden tietoja palvelussa käsitellään?

J4-R30 – Lisensointi

30.1 Mistä tekijöistä palvelun hinta muodostuu?

J5-R31 – Tiedon sijainti

31.1 Missä palveluun tallennettu tieto sijaitsee maantieteellisesti?

31.2 Minkä maan lainsäädännön mukaan tietoja käsitellään?

31.3 Onko tietyn lain noudattamisesta mahdollista tehdä sopimus?

J6-R32 – Sisäiset tutkinnat

32.1 Onko mahdollista saada tukea sisäisen tutkintatyön tekemiseksi, mikäli havaitaan väärinkäytöksiä tai epäillään rikosta?

Liite 2: Riskienarviointi

Todennäköisyys x **V**akavuus^2 = **R**iski**a**rvo
[1-5] [1-5]

Merkityksetön riski: < 10
Kohtalainen riski: 10 – 20
Merkittävä riski: 20 <

Riski		**T**	**V**	**RA**
H1-R1	Tiedon sisään lukkiutuminen	4	2	16
H2-R2	Hallinnon menettäminen	4	4	64
H3-R3	Vaatimustenmukaisuuksien noudattaminen	1	2	4
H4-R4	Muiden vuokralaisten toiminta	2	3	18
H5-R5	Palvelun lopettaminen	3	4	48
H6-R6	Yrityskauppa	2	3	18
H7-R7	Toimitusketjun häiriöt	3	4	48
H8-R8	Tuntematon riskiprofiili	4	4	64
H9-R9	Puutteellinen riskienhallinnan tukeminen	3	2	12
H10-R10	Palvelutasosopimuksen huolimaton toteutus	4	4	64
H11-R11	Puutteellinen reagoiminen turvallisuustapahtumiin	4	4	64
H12-R12	Politiikkojen- ja käytäntöjen yhteensopimattomuus	3	3	27
T1-R13	Resurssien ehtyminen	3	2	12
T2-R14	Eristämisen epäonnistuminen	2	4	32
T3-R15	Pahantahtoiset työntekijät	2	3	18
T4-R16	Hallinnointirajapinnan vaarantuminen	2	3	18
T5-R17	Tiedonsiirron kaappaaminen	2	4	32
T6-R18	Turvaton tai tehoton tiedon hävitys	2	4	32
T7-R19	Palvelunestohyökkäykset	2	3	18
T8-R20	Salausavaimien menettäminen	2	3	18
T9-R21	Pahantahtoiset skannaukset	2	3	18
T10-R22	Palvelumoottorin vaarantuminen	2	3	18
T11-R23	Ristiriidat turvallisuuden koventamismenettelyissä	2	2	8
T12-R24	Puutteelliset menettelyt tiedon palauttamisessa	3	2	12
T13-R25	Identiteettien ja pääsynhallinnan yhteensopimattomuus	3	3	27
T14-R26	Korkean riskiprofiilin asiakkaat	2	2	8
J1-R27	Viranomais- ja siviilikanteet	3	3	27
J2-R28	Lainsäädännön muutokset	3	4	48
J3-R29	Tietosuoja	4	4	64
J4-R30	Lisensointi	2	3	18
J5-R31	Tiedon sijainti	3	4	48
J6-R32	Sisäiset tutkinnat	4	4	64

Liite 3: Arviointityökalun käyttöohje

Julkisen pilven Software as a Service – palveluiden arviointityökalu

- Tämä työkalu on tarkoitettu julkisen pilven Software as a Service – palveluiden tietoturvallisuuden arviointiin Kesko-konsernissa.
- Työkalun avulla esitetään pilvipalveluntarjoajille palvelun turvallisuuteen liittyviä kysymyksiä sekä arvioidaan vastauksia.
- Saavutettujen tulosten tarkoitus on tukea palvelun hankintaan liittyvää päätöksentekoa ja auttaa mahdollisimman turvallisen palveluntarjoajan valitsemisessa.
- Usean palveluntarjoajan vertailu on mahdollista.
- Työkalua tulee käyttää ainoastaan neuvottelutilanteissa, eikä sitä tule lähettää palveluntarjoajalle täytettäväksi.
- Työkalua ei tule omatoimisesti muokata, vaan yhteys tulee ottaa Kesko-konsernin tietoturvapäällikköön, mikäli muutoksille on tarvetta.

- Työkalu sisältää kolme riskikategoriaa, jotka ovat sijoitettu omiin välilehtiin.
- Riskikategoriat ovat hallinnolliset riskit, tekniset riskit ja juridiset riskit.
- Jokainen kategoria sisältää useita riskejä, joiden alle on sijoitettu palveluntarjoajalle esitettäviä kysymyksiä.
- Riskien merkittävyyden on arvioinut Kesko-konsernin tietoturvapäällikkö Jari Törmälä. Riskien kuvaukset ovat työkalun mukana lähetetyssä dokumentissa.
- Palveluntarjoajien vertailun helpottamiseksi työkalu sisältää välilehdet, joissa palveluntarjoajia vertaillaan pylväsdiagrammien avulla.

Käyttöohje:

1. Tutustu työkalun lisäksi annettuun dokumenttiin, joka sisältää riskien kuvaukset. Riskien kuvauksia on hyvä pitää saatavilla työkalun käyttötilanteessa.
2. Korvaa riskikategorioista PalvelunTarjoaja1 – 4 (PT1, PT2, PT3, PT4) – yritysten oikeilla nimillä.
3. Palveluntarjoajalle esitettyyn kysymykseen saatu vastaus arvioidaan asteikolla 1 – 5, jossa:
   1 = huono
   2 = tyydyttävä
   3 = hyvä
   4 = erinomainen
   5 = kiitettävä
4. Vastauksen arvio sijoitetaan kunkin palveluntarjoajan alle korvaamalla kysymyksen kohdalla oleva ”0” -merkintä.

5. Mikäli on tarvetta tulostaa raportti, valitse tulostusasetuksista tarvittavat laskentataulukot ja asetukseksi ”Sovita kaikki sarakkeet yhteen sivuun”

- Työkalu laskee automaattisesti keskiarvoja ja pisteitä sekä sijoittaa ne ”Keskiarvot” ja ”Pisteet” – välilehtien diagrammeihin vertailua varten.
- Työkalussa olevaan ”Status” – sarakkeeseen tulee automaattisesti merkintä, mikäli jonkin palveluntarjoajan vastaus on tasoa 1 – 2. Tämä helpottaa tulosten analysointia.
- ”Kommentti” – sarakkeeseen voi kirjata omia merkintöjä ja muistiinpanoja

Liite 4: Työskentelypäiväkirja

6.10.2011 – Opinnäytetyön orientaatioseminaari

18.10.2011 – Yhteydenotto Keskoon, työharjoittelun ja opinnäytetyöaiheen tarjoaminen

1.11.2011 – Sopiminen työharjoittelun tekemisestä ja opinnäytetyöstä

9.1 – Töiden aloittaminen Keskossa

16.1 – Aiheanalyysin palautus

31.1 – Aiheanalyysin hyväksyntä, ohjaajaksi Seija Tiainen

2.2 – Ensimmäinen tapaaminen Tiaisen kanssa, prosessin käynnistäminen

6.2 – Tapaamisen sopiminen tietojenkäsittelyn lehtorin Anssi Mattilan kanssa

9.2 – Tapaaminen Anssi Mattilan kanssa, keskustelun perusteella päätös opinnäytetyön toteuttamisen vaihtamisesta tutkimuksellisesta toiminnalliseksi

10.2 – Keskustelu Törmälän kanssa arviointityökalun sisällöstä ja toiminnallisuudesta

15.2 – Tietoperustan kirjoittamista, menetelmää ja lähestymistapaa sekä keskeisiä käsitteitä

16.2 – Keskeisten käsitteiden ja menetelmän kirjoittamista

17.2 – Käsitteiden ja menetelmän kirjoittamista

20.2 – Menetelmän ja riskien kuvaamista

21.2 – Riskien kuvaamista

22.2 – Riskien kuvaamista

23.2 – Johdannon, kehittämiskohteen ja menetelmän kirjoittamista

24.2 – Johdannon ja rajauksen kirjoittamista, tietoperustan korjaamista

27.2 – Johdannon kirjoittamista sekä pienien korjausten tekemistä, keskustelu Törmälän kanssa riskien arvioimisesta ja riskiarvojen laittamisesta työkaluun, keskustelu työyhteisön odotuksista opinnäytetyöhön liittyen

28.2 – Työyhteisön odotusten kirjoittamista, kysymysten muodostamista hallinnollisista riskeistä, työsuunnitelman esittäminen

29.2 – Kysymysten muodostamista teknisistä riskeistä ja juridisista riskeistä. Alustavien kysymysten lähettäminen Törmälälle arvioitavaksi

1.3 – Riskiarvojen läpikäyminen Törmälän kanssa, riskiarvoliitteen laatiminen

2.3 – Arviointityökalun tekemisen aloittaminen, prototyypin näyttäminen Törmälälle

5.3 – Keskustelua Törmälän kanssa riskien painoarvottamisesta työkalussa. Riskityökalun saattaminen vaiheeseen, jossa riskikategoriat ovat valmiina

6.3 – Vertailuvälilehtien tekeminen työkaluun, työkalun ulkoasun muuttaminen, Status - toiminnallisuuden lisääminen, työkalun käyttöohjeen laatiminen

7.3 – Työkalun prototyypin, kysymyslistan ja riskienarvioinnin lähettäminen Tiaiselle arviointiin, työkaluun lisätty keskiarvojen lisäksi pisteytys

8.3 – Työkalun hiomista, suunnitelman tekeminen työkalun toiminnallisuuksien kuvaamiseksi raporttiin

9.3 – Riskienarvioinnin kuvaaminen raporttiin, taulukoiden tekeminen riskeistä ja riskienarvioinnin tuloksista

12.3 – Kysymyslistan kuvaaminen raporttiin, Arviointityökalun toiminnallisuuksien kuvaamista

13.3 – Arviointityökalun toiminnallisuuksien kuvaamista, työkaluun liittyvän johdannon kirjoittaminen raporttiin

14.3 – Kysymyslistan, riskienarvioinnin ja työkalun yhteenvedon kirjoittaminen

15.3 – Raportin hiomista, havainnollistavien kuvien lisäämistä, tapaamisen sopiminen Tiaisen kanssa

20.3 – Ohjauskeskustelu Tiaisen kanssa

21.3 – Raportin rakenteen hiomista, johdannon kirjoittaminen toteutusosioon, hankeorganisaatiossa toimimisen kuvaaminen, tapaamisen sopiminen Mattilan kanssa

22.3 – Raportin rakenteen hiomista ja tekstin korjausta, opinnäytetyöprosessin kirjoittamista, tietoperustan yhteenvedon kirjoittamista

23.3 – Työharjoittelujakso Keskossa päättyi, hankeorganisaation toiminnan yhteenvedon kirjoittaminen

26.3 - Ohjauskeskustelu Mattilan kanssa

27.3 - Opinnäytetyöprosessin kirjoittamista

28.3 - Toteutuksen yhteenvedon kirjoittamista

29.3 – Tietoperustan yhteenvedon kirjoittamista, johdannon kirjoittamista

1.4 - Arvioinnin kirjoittamista

2.4 – Arvioinnin kirjoittamista, johdannon kirjoittamista

3.4 – Arvioinnin kirjoittamista, oikolukeminen ja lähettäminen ohjaajille luettavaksi

10.4 – Tiivistelmien kirjoittamista, korjailua

19.4 – Opinnäytetyön esittäminen seminaarissa

19.4 – 7.5.2012 – Työn viimeistelyä ja palauttaminen

Liite 5: Toimeksiantajan lausunto

KESKO

ARVIOINTI 1 (2)

03.04.2012

OPINNÄYTETYÖN ARVIOINTI

Tekijä	Anssi Kaipio
Aihe	Pilvipalveluiden arvioinnin kehittäminen Kesko -konsernissa
Kohde	Kesko Oyj, Tietohallinto, ICT infrapalvelut

1 Opinnäytetyön arviointi

1.1 Yhteistyö

Yhteistyö opinnäytetyön tekijän Anssi Kaipion kanssa sujui hyvin. Pohjatyöt oli tehty huolellisesti ja kun oli aika antaa Keskon kommentit työhön, oli selkeästi etukäteen mietitty, miten ja millä kysymyksillä saadaan asia käytyä mahdollisimman tehokkaasti läpi.

Toimintatapaan ja asian jäsentelyyn ei ollut tarvetta juurikaan puuttua, vaan opinnäytetyön tekeminen ja siihen liittyvän työvälineen kehitys ovat olleet johdonmukaisia. Asiat oli selkeästi mietitty valmiiksi ja kysyttäessä Kaipio pystyi hyvin perustelemaan valitsemansa näkökulman.

1.2 Toimintatapa

Ennen opinnäytetyön aloittamista keskustelimme mahdollisista aiheista, jotka hyödyttäisivät Keskoa organisaationa. Aluksi sovimme riskilähtöisestä selvityksestä pilvipalveluiden sovellettavuudesta Keskon liiketoimintaan, mutta Kaipion ehdotuksesta päädyimme toiminnalliseen vaihtoehtoon. Keskon näkökulmasta se tuo enemmän käytännön hyötyä sekä Kesko konsernille, että liiketoimintayhtiöille.

Kaipio valmisteli työkalua keskustelujemme pohjalta ja kysyi kommentteja sen etenemisen aikana. Kaipio oli valmistellut kysymykset, joilla määriteltiin eri osa-alueiden painoarvot Keskolle. Oli helppo antaa arvot pilvipalveluiden riskien mukaan ja mielestäni se oli hyvä toimintatapa toisistaan erilaisten asioiden arvottamiseksi.

Jari Törmälä

Kesko Oyj
Satamakatu 3
Helsinki
00016 KESKO

Puhelin 010 53 11
www.kesko.fi

Y-tunnus 0109862-8
Kotipaikka Helsinki

KESKO

ARVIOINTI 2 (2)

03.04.2012

1.3 Hyödynnettävyys

Keskon liiketoimintayhtiöillä on vapaus valita liiketoimintansa järjestelmät ja niihin palvelutoimittajat. Keskon tietohallinnon tehtävänä on tarjota välineet, jotta liiketoiminnot voivat arvioida järjestelmien soveltuvuutta myös tietoturvallisuuden näkökuomasta. On hyödyllistä, että liiketoiminnoille voidaan antaa käyttöön väline, jolla voidaan arvioida pilvipalvelun toimittajien soveltuvuutta ja tietoturvallisuutta liiketoiminnon henkilöiden toimesta. Välttämättä paikalla ei tarvitse olla tietohallinnon henkilöä tätä tekemässä. Lisäksi työkalulla saadaan puolueettomampi kuva siitä, mikä toimittaja tai palvelu soveltuu liiketoiminnan tarpeisiin parhaiten. Tietoturvallisuus paranee, kun toimittaja arvioidaan järjestelmällisesti, eivätkä toimittajat jatkossa edes tarjoa palvelujaan, ennen kuin osaavat vastata työvälineen kysymyksiin uskottavaksi.

Liiketoimintojen ymmärtämys pilvipalveluiden selvittämisestä lisääntyy työkalun avulla. Henkilöt pystyvät kiinnittämään paremmin huomiota tärkeisiin seikkoihin vertaillessaan eri pilvipalveluvaihtoehtoja.

Jari Törmälä
Tietoturvapäällikkö
Kesko konserni, ICT infrapalvelut