Vesa Lehtinen

TIETOTURVAN JA TIETOSUOJAN KEHITTÄMINEN PILVITEKNOLOGIASSA – STANDARDIT JA KEHYSMALLIT SEKÄ RISKIENHALLINNAN NÄKÖKULMA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2010

TIIVISTELMÄ

Lehtinen, Vesa
Tietoturvan ja tietosuojan kehittäminen pilviteknologiassa — standardit ja kehysmallit sekä riskienhallinnan näkökulma
Jyväskylä: Jyväskylän yliopisto, 2010, 94 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Tyrväinen, Pasi

Informaatioteknologian kehityksen myötä on syntynyt idea tietojenkäsittelyn myymisestä palveluna minkä tahansa hyödykkeen tavoin. Kustannustehokas, skaalautuva ja helppokäyttöinen pilviteknologia herättää mielenkiintoa eri puolilla maailmaa. Internetin yli tarjottavien pilvipalveluiden tietoturva ja tietosuoja vaativat kuitenkin erityishuomiota yritysten ulkoistaessa tietojenkäsittelynsä kolmannen osapuolen hoidettavaksi. Tietoturvan tai tietosuojan pettäminen on merkittävä riski eri osapuolille. Tästä syystä yritysten liikesalaisuudet tai yksilöiden arkaluontoiset tiedot tulee riskien realisoitumisen välttämiseksi suojata asianmukaisin keinoin. Erilaisten tietojenkäsittelystandardien ja -kehysmallien avulla on mahdollista kiinnittää erityishuomiota pilviteknologian turvallisuuteen sekä minimoida siihen kohdistuvia riskejä.

Pilviteknologian ajankohtaisuus ja henkilökohtainen mielenkiinto standardeja kohtaan vaikuttivat tutkielman aiheen valintaan. Tutkielmassa käsiteltiin kirjallisuuden ja haastattelujen avulla, kuinka tietoturva ja tietosuoja voidaan ottaa huomioon kehitettäessä pilviteknologiaa tai pilvipalveluita erilaisten standardien ja kehysmallien avulla. Laadullisen tutkimuksen tarkoituksena oli käsitellä aihetta mahdollisimman monipuolisesti. Tutkielmassa selvitettiin myös palvelutasosopimusten, teknisesti toimivien ja laadukkaiden tietojenkäsittelyratkaisujen sekä kypsyysmallien potentiaalia riskejä pienentävinä tekijöinä. Tästä syystä tutkielmassa on lisäksi riskienhallinnallinen näkökulma.

Saatujen tulosten perusteella havaittiin, että tietoturva ja tietosuoja huomioidaan yrityksissä erilaisten määriteltyjen käytäntöjen, prosessien ja vaatimusten avulla. Tämän lisäksi havaittiin, että tietoturvaan ja tietosuojaan liittyviä riskejä voidaan minimoida monipuolisesti tutkielmassa käsitellyillä tavoilla. Tutkimustulokset vahvistavat kirjallisuudessa esiintyviä ilmiöitä sekä tarjoavat uutta pohdittavaa pilviteknologian kehittämiseen.

Asiasanat: Pilviteknologia, pilvipalvelu, tietoturva, tietosuoja, riskienhallinta, standardit

ABSTRACT

Lehtinen, Vesa
Development of Information Security and Privacy Protection in Cloud Computing — Standards, frameworks and risk management point of view
Jyväskylä: University of Jyväskylä, 2010, 94 p.
Information Systems, Master's Thesis
Supervisor: Tyrväinen, Pasi

The evolution of information technology has generated an idea of selling information and communication technology as a service similar to any utility. Cloud computing which is cost effective, scalable and easily usable has caught attention globally. The information security and privacy protection of cloud services, which are delivered over the network, require special consideration when companies outsource computing for third party. Failure in information security or privacy protection is a significant risk for every interest group. That is why the protection of commercial secrets or sensitive information of individuals needs decent protection in order to avoid the risk realization. By using different ICT-standards and frameworks, it is possible to take account and emphasize security issues in cloud computing.

Novelty of cloud computing and personal interest in standards had influence on topic discovery. In this thesis by reviewing literature and analyzing the interview answers it was examined how information security and privacy protection is taken account when developing cloud computing and cloud services with help of ICT-standards and frameworks. The purpose of this qualitative research was to cover the whole issue extensively. Furthermore, the potential of service level agreements, technically working ICT-solutions of good quality and capability maturity models as a way to mitigate risks was found out. Due this the thesis includes risk management viewpoint.

By reviewing the research results, it was noticed that information security and privacy protection is taken account in different defined practices, processes and requirements in many companies. It was also noticed that it is possible to mitigate risks related to information security and privacy protection extensively with techniques discussed. Research results were comparable to issues in literature and offered new subjects to be considered in development of cloud computing.

Keywords: Cloud computing, cloud service, information security, privacy protection, risk management, standards

ESIPUHE

Haluan kiittää saamistani neuvoista ohjaajaani professori Pasi Tyrväistä ja vaimoani Annaa kaikesta saamastani tuesta tutkielmaa tehdessäni.

”Onnellinen se, joka on löytänyt viisauden, se, joka on tavoittanut tiedon, sillä parempi on viisaus kuin hopea, tuottoisampi on tieto kuin kulta.” Sananl. 3:13-14

KUVIOT

TAULUKOT

KÄSITEHAKEMISTO

ACM = Association for Computing Machinery
CMM = Capability Maturity Model
CMMI = Capability Maturity Model-Integrated
IaaS = Infrastructure as a service, Palveluinfrastruktuuri
IEC = International Electrotechnical Commission
IEEE = Institute of Electrical and Electronics Engineers
ISMS = Information Security Management System, Tietoturvallisuuden hallintajärjestelmä
ISO = International Organization for Standardization
ITIL = Information Technology Infrastructure Library
OASIS = The Organization for the Advancement of Structured Information Standards
OECD = Organization for Economic Cooperation and Development
PaaS = Platform as a service, Pilvialusta
PIA = Privacy Impact Assessment, Yksityisyyden merkityksen arviointi
SaaS = Software as a service, Palveluohjelmisto
SEI = Software Engineering Institute
SOA = Service oriented architecture, Palvelukeskeinen arkkitehtuuri
SW-CMM = Capability Maturity Model for Software
VM = Virtual Machine, Virtuaalikone
W3C = Word Wide Web Consortium

SISÄLLYS

1 JOHDATUS AIHEALUEESEEN

Informaatioteknologian yleistymisen seurauksena muutamien viime vuosikymmenten aikana henkilökohtaisten tietojen käsittely erilaisissa tietojärjestelmissä on lisääntynyt radikaalisti (Croft & Signorile, 2009). Tämänkaltaisen kehityksen myötä yritykset ja kuluttajat ovat aiempaa enemmän huolissaan tietojensa joutumisesta vääriin käsiin (Gadzheva, 2008). Tietojen suojaamiseen on alettu kiinnittää paremmin huomiota yhä useampien yritysten hyödyntäessä hajautettuja teknologiapalveluita (Gadzheva, 2008). Tietoturvaan ja tietosuojaan liittyvät osa-alueet ovat erityisen ajankohtaisia pilviteknologian yleistyessä nopeasti.

Pilviteknologia on yksi tuoreimmista, laajasti kiinnostusta herättäneistä tietojenkäsittelyparadigmoista. Palvelusuuntautunutta rakennetta, hilalaskentaa, hajautettuja järjestelmiä ja virtualisointia yhdistelevä teknologia tarjoaa mahdollisuuden myydä ja ostaa tietojenkäsittelypalveluita hyödykkeenä sähkön tai veden tapaan. (Youseff, Butrico & Da Silva, 2008) Pilviteknologian kenties suurin etu on sen kustannustehokkuudessa. Palvelun kustannukset muodostuvat suoraan käytettyjen resurssien perusteella (Vaquero, Rodero-Merino, Caceres ja Lindner, 2009).

Pilviteknologian innovatiivisuudesta huolimatta uuteen tietojenkäsittelymenetelmään liittyy ongelmia. Youseffin ym. (2008) mukaan pilviteknologian yleistymistä hidastavat eniten turvallisuuteen ja yksityisyyteen liittyvät tekijät. Henkilökohtaisten tietojen altistuessa erilaisille väärinkäytöksille tietosuoja on vakavalla tavalla uhattuna.

1.1 Tutkielman fokus

Tässä tutkielmassa on tarkoitus selvittää standardien ja kehysmallien hyödyntämistä erityisesti tietoturvan ja tietosuojan kehittämiseksi — pilviteknologian kontekstissa. Tietoturva koostuu Hakalan, Vainion & Vuorisen (2006, s. 4) mukaan luottamuksellisuudesta, käytettävyydestä ja eheydestä. Tietosuoja on sen

sijaan Järvisen (2010, s. 15) mukaan ”henkilöön tai hänen toimintaansa liittyvien tietojen suojaamista luvatonta keräämistä ja käyttöä vastaan”.

Pilviteknologia erilaisine tietoteknisine ratkaisuineen on lähtökohtana verkon yli tarjottaville pilvipalveluille. Näin ollen merkittävä seikka tutkielman kannalta on tietojenkäsittelyn ulkoistaminen ja siihen liittyvät riskit, kuten tietojen suojaamisen epäonnistuminen ja tietojen kontrolloinnin hämärtyminen. Näihin teemoihin liittyen voidaan pohtia erilaisten standardien ja kehysmallien merkitystä niin pilviteknologian kuin pilvipalveluidenkin tietoturvan ja tietosuojan kehittämiseksi. Tutkielmassa käsitellään korkeamman abstraktiotason standardeja ja kehysmalleja: tietoturva-, prosessi-, laatu- ja riskienhallintastandardeja sekä kehysmalleja. Teknisiin ratkaisuihin perustuvat standardit rajautuvat pois tutkimusalueesta. Tutkielman teoriaosuuden ja empirian avulla pyritään vastaamaan kysymykseen:

> Kuinka tietoturva ja tietosuoja huomioidaan erilaisten standardien ja kehysmallien avulla pilvipalveluita kehitettäessä?

Henkilökohtaisten ja arkaluontoisten tietojen suojaaminen on tärkeää niin pilvipalveluita kehittävän kuin hankkivan tahon kannalta (Dey, 2007). Tietoturvan ja tietosuojan rikkoontuminen on myös merkittävä riski liiketoiminnalle ja yksilöiden yksityisyydelle (Tafti, 2005). Näin ollen tietoturvan ja tietosuojan takaaminen ovat siis oleellisia riskienhallinnan osa-alueita.

Tutkielmassa käsitellään myös riskienhallintaa osana tietojenkäsittelyyn liittyvien standardien ja kehysmallien hyödyntämistä. Tämän lisäksi tutkielmassa selvitetään palvelutasosopimusten, teknisesti toimivien ja laadukkaiden ratkaisujen sekä kypsyysmallien potentiaalia riskienhallinnan näkökulmasta tietoturvaa ja tietosuojaa edistävinä tekijöinä.

Pilvipalveluihin liittyviä riskejä ja niiden minimoimista tutkitaan varsinaista tutkimusongelmaa tukevana alakysymyksenä. Varsinaisen tutkimusongelman lisäksi tutkielman avulla pyritään vastaamaan alakysymykseen:

> Kuinka palvelutasosopimusten, teknisesti toimivien ja laadukkaiden ratkaisujen sekä kypsyysmallien avulla voidaan pienentää pilvipalveluihin liittyviä riskejä?

1.2 Aikaisempi tutkimus

Aikaisempaa tutkimusta tietojenkäsittelystandardeihin ja -kehysmalleihin sekä riskienhallintaan liittyen on olemassa jonkin verran, mutta ei merkittävästi. Lyytisen & Kingin (2006) mukaan ICT-alan standardien tärkeydestä huolimatta niitä ei ole tutkittu juuri ollenkaan. Kauffmanin & Tsain (2010) mukaan erityisesti prosessistandardeihin liittyvä tutkimus on erityisen vähäistä, vaikkakin kasvussa. Useat tutkimukset ovat laadultaan standardeja vertailevia, eikä niin-

kään niiden vaikutuksia tutkivia (Baldassarre, Piattini, Pino & Visaggio, 2009), (Mazlan, Rahim, Shazi & Mazlan, 2009) ja (Khosgoftar & Osman, 2009).

Prosessistandardien vaikutuksia yritykseen ovat tutkineet mm. Münstermann & Weitzel (2008). Barlette & Fomin (2008) ovat tutkineet turvallisuusstandardien sopivuutta pienyrityksille. Tietoturvan ja tietosuojan huomioimista standardien ja kehysmallien avulla, ei liene tutkittu aikaisemmin.

1.3 Tutkimusmenetelmä ja tulokset

Tässä tutkielmassa pyritään käsittelemään valittua aihealuetta eri näkökulmista, loogisena kokonaisuutena. Sisällöllisesti teoreettinen osa on jäsennetty Hirsjärven ym. (1997, s. 35) luokittelujen mukaan temaattiseksi. Tutkimus on luonteeltaan laadullinen, ja tutkimusstrategia mukailee Survey-tutkimusta. Tätä ajatellen valittiin teoriaosuutta parhaiten tukeva tiedonkeruutapa: teemahaastattelu.

Saatujen vastausten avulla voidaan todeta, että tietoturva ja tietosuoja on mahdollista huomioida hyvin monella tavalla erilaisia standardeja ja kehysmalleja hyödynnettäessä. Useissa yrityksissä huomioidaan tietoturva ja tietosuoja ennalta määriteltyjen prosessien, käytäntöjen ja yritysten sisäisten sääntöjen avulla. Näissä on usein jonkinlainen standardinomainen yrityksen itse määrittelemä sisältö. Tämän lisäksi palvelutasosopimuksilla, teknisesti toimivilla ja laadukkailla ratkaisuilla sekä kypsyysmalleilla nähtiin olevan riskienhallinnallista merkitystä, ja niiden vaikutus riskejä pienentävinä tekijöinä koettiin olevan olemassa. Tarkempi analyysi tuloksista on luvussa 8.

1.4 Tutkielman rakenne

Tutkielman teoreettisessa osassa käsitellään pilviteknologiaa ja siihen liittyviä osa-alueita kuten pilvipalveluita. Tyypillinen pilven ontologia selkeyttää, mistä pilviteknologiassa on kyse. Pilviteknologiaan liittyy oleellisesti tiettyjä hyötyjä ja haittoja, jotka käydään läpi ensimmäisen luvun lopussa. Pilviteknologian lisäksi käsitellään tietoturvaa ja tietosuojaa. Tietoturvan ja tietosuojan toteutuminen edellyttää monien eri asioiden huomioimista; tietoturvauhkien, -haavoittuvuuksien ja lainsäädännön merkitys on oleellinen. Tietoturva ja tietosuoja -luvussa käsitellään myös erityisesti pilviteknologiaan liittyviä haasteita tietoturvan ja tietosuojan kannalta.

Edellisten lisäksi käsitellään riskienhallintaa ja sen eri osa-alueita. Riskit ja niiden hallinta -luvussa käsitellään riskienhallintaa yleisesti, ulkoistamiseen liittyviä riskejä, perinteisiä riskienhallinnan menetelmiä sekä toisen tutkimusongelman eri osa-alueita: palvelutasosopimuksia, teknisesti toimivia ja laadukkaita ratkaisuja sekä kypsyysmalleja Tietoturvaa ja tietosuojaa sekä riskienhallintaa käsittelevissä luvuissa esitellään aiheeseen liittyviä standardeja ja kehysmalleja, joita organisaatioissa hyödynnetään – tai kenties voitaisiin hyödyntää.

Ennen tutkielman empiiristä osaa on teoriaosuuden analyysi, jossa käsitellään mm. edellytyksiä pilviteknologian yleistymiselle sekä standardeihin liittyviä ongelmallisuuksia. Empiirisen osan aloittaa luku, jossa käsitellään suoritettavaa tutkimusta, siihen liittyviä motiiveja sekä tutkimusmenetelmää. Tämän luvun tarkoituksena on antaa lukijalle selkeä kuva siitä, miten varsinainen tutkimus toteutettiin. Haastatteluvastaukset-luvussa esitellään haastatellut henkilöt ja käsitellään tutkielman kannalta merkitykselliset haastatteluvastaukset. Vastaukset käsitellään teema kerrallaan: pilviteknologia ja pilvipalvelut, tietoturva ja tietosuoja, riskienhallinta ja tietojenkäsittelystandardit.

Tulokset ja päätelmät -luvussa analysoidaan, miten kerätty haastatteluaineisto vastaa tutkimusongelmaan ja tukeeko haastatteluista saatu aineisto aihealueesta julkaistua aikaisempaa kirjallisuutta. Tämän lisäksi arvioidaan tutkimuksen onnistumista. Luvun päättää kontribuutio aihealueesta. Tutkielman viimeisenä lukuna on lyhyt pohdinta kokonaisuudesta.

2 PILVITEKNOLOGIA

Tässä luvussa käsitellään pilviteknologian yleisiä piirteitä ja tämän tutkimuksen kannalta merkittäviä osa-alueita. Luvun alussa käydään läpi yleisiä asioita pilviteknologiaan liittyen; mistä pilviteknologia on saanut alkunsa ja kehittynyt, mitä pilvistä yleisesti ajatellaan ja miten pilviteknologiaa voidaan määritellä. Tämän jälkeen käsitellään tyypillinen pilviontologia ja määritellään pilvelle tyypillisiä ominaisuuksia. Luvun lopussa käsitellään vielä pilviteknologiaan liittyviä hyötyjä ja ongelmia. Kohdan 2.7 Yhteenveto-kappale kokoaa yhteen luvun oleellisimmat osa-alueet.

2.1 Yleistä pilviteknologiasta

Informaatioteknologian kehittyessä valtavaa vauhtia tietoliikenneyhteyksien nopeuden, tallennuskapasiteetin suuruuden ja prosessointitehon määrän kasvu on saanut aikaan idean tietojenkäsittelystä myytävänä hyödykkeenä sähkön ja veden tapaan (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009). Näin ollen tietojenkäsittelypalveluita voitaisiin ostaa tarvittava määrä tilannekohtaisesti. Kustannustehokkuus ja joustavuus ovat äärimmäisen tärkeitä tekijöitä pohdittaessa informaatioteknologisia ratkaisuja osana toimivaa ja tehokasta liiketoimintaa – pilviteknologia voi olla yksi ratkaisuvaihtoehto (Chow ym., 2009).

Pilviteknologian voidaan ajatella periytyvän hilalaskennasta, joka alkoi yleistyä 1980-luvun lopulla ja 1990-luvun alussa. Hilalaskennassa jokainen tietokone on oma solmunsa ja tietokoneiden kokonaisuutta voidaan kuvata ”ritilänä”. Ajatellen pilviteknologian kehittymistä 1990-luvun tietoteknistä kehitystä leimasi virtualisoinnin käyttöönotto ja kehittyminen. Hiljalleen alettiin pohtia tietojenkäsittelyn ulkoistamista sekä sen myyntiä palveluna. (Zhang, Zhang, Chen, & Wu, 2010.) Pilviteknologian kehittymistä voidaan ajatella toisaalta myös seurauksena internetissä tapahtuvasta kehityksestä (Armbrust ym., 2009).

Pilviteknologia haastaa aikaisemman olemassa olevan tietojenkäsittelykäytännön, jossa tieto on keskitetty suuriin palvelinsaleihin ja monitoroitua

ympäri vuorokauden. Pilviteknologia mahdollistaa ulkoistetut pilvipalvelut. Tiedon käsittely pilvessä tarjoaa asiakasyrityksille monipuolisia mahdollisuuksia mukauttaa ulkoistettu tietojenkäsittely vastaamaan yrityksen tarpeita ja todellista käyttöastetta. Tietojenkäsittelyn integroituessa entistä enemmän osaksi asiakasyritysten liiketoimintaa pilvipalveluita tarjoavien organisaatioiden tulee ottaa huomioon palvelujen kokonaisvaltainen toimivuus. Tyypillisesti palvelujen sisällöstä ja ehdoista voidaan sopia palvelutasosopimusten (Service Level Agreement, SLA) avulla. (Buyya ym., 2009.)

Pilviteknologiaa voidaan hyödyntää erityisellä tavalla internetiä silmällä pitäen. Youseffin ym. (2008) mukaan tiedon saatavuus internetpalveluja tarjottaessa on merkittävää pilviteknologiassa; jos yksi pilvi pettää, toinen pilvi pystyy edelleen tarjoamaan pääsyn sovelluksiin ja tietoon. Pilviteknologian avulla esimerkiksi internetpalveluja tarjoavien yritysten on aidosti mahdollista toteuttaa muuntautuvia, kaikkialla läsnä olevia sekä ajasta ja paikasta riippumattomia palveluja. (Buyya ym., 2009). Useat informaatioteknologian jättiyritykset kuten IBM, Google, Amazon ja Microsoft tarjoavat asiakkailleen pilvipalveluita, joiden hyödyntämismahdollisuudet ovat lähes rajattomat (Weiss, 2007).

Pilviteknologia on herättänyt mielenkiintoa viimeaikaisissa tutkimuksissa, ja sitä voidaankin pitää edeltäjiensä palvelukeskeisen arkkitehtuurin (Service-oriented Architecture, SOA), hajautettujen järjestelmien ja hilalaskennan sekä virtualisoinnin perijänä. (Youseff ym., 2008) Youseffin ym. (2008) mukaan pilviteknologian merkittävänä etuna on aikaisemmista tietojenkäsittelyratkaisuista poikkeava kyky tarjota yrityksille mahdollisuus hyödyntää tietojenkäsittelyä palveluna verkon yli. Mitä tulee pilviteknologian tutkimukseen, käsitteiden selkeyttäminen ja yhtenäistäminen sekä käsitteiden keskinäisten suhteiden määrittely on ensisijaisen tärkeää, jotta pilviteknologia voisi entisestään kehittyä (Youseff ym., 2008). Pilviteknologian ontologioiden määrittely on tärkeää myös tietoturvallisuuden kannalta. Tiedon kontrolloinnin hämärtyessä pilvessä huoli tietojen vaarantumisesta kasvaa (Chow ym., 2009).

2.2 Määrittely

Terminologian määrittely on relevanttia, sillä pilviteknologiaan liittyy useita erilaisia tietojenkäsittelyratkaisuja, kuten hilalaskentaa ja virtualisointia sekä oleellisena osana palvelurakenteinen arkkitehtuuri. Ymmärrettäessä eri osa-alueiden väliset mahdollisuudet ja rajoitteet voidaan pilviteknologiaa kehittää kohti teknologian innovatiivista hyödyntämistä. Tuloksena tämänkaltaisen ymmärryksen omaksumisesta voi olla esimerkiksi pilvien välisen yhteentoimivuuden kehittyminen paremman saatavuuden aikaansaamiseksi. (Youseff ym., 2008.)

Pilven ja pilviteknologian käsitteen määrittely on haasteellista teknologian tuoreuden vuoksi. Vaquero ym. (2009) pitävät määrittelyä tärkeänä kokonaisvaltaisen ja tasapainoisen ymmärryksen takaamiseksi. Heidän määritelmänsä mukaan *”pilvet ovat suuria, helposti käytettäviä ja saatavilla olevia, virtualisoituja*

resursseja. Resurssit voidaan dynaamisesti konfiguroida vastaamaan vaihtelevaa kuormitusta mahdollistaen täten optimaalisen resurssien hyödyntämisen. Tällaista resurssia hyödynnetään maksa-kun-käytät -menetelmällä, jonka vaatimukset on sovittu yhdessä palveluntarjoajan kanssa palvelutasosopimuksessa."

Buyya ym. (2009) taas määrittelevät pilven "*rinnakkaisten ja hajautettujen järjestelmien joukoksi, jotka sisältävät toisiinsa yhteydessä olevia, virtualisoituja tietokoneita*" Tämän lisäksi oleellista on myös "*tietokoneiden dynaaminen sijoittuminen kuvattuna resurssikokonaisuutena asiakkaalle palvelutasosopimusten mukaisten vaatimusten mukaisesti*". Näin ollen pilvi on sekoitus klustereita ja hilalaskentaa. Edellisten lisäksi keskeistä pilviteknologialle on datakeskittymien virtualisointi virtuaalikoneiden (Virtual Machine, VM) avulla, jolloin dynaaminen sijoittaminen mahdollistaa tilannekohtaiset, asiakassopimusten vaatimukset täyttävät palvelut. (Buyya ym., 2009.)

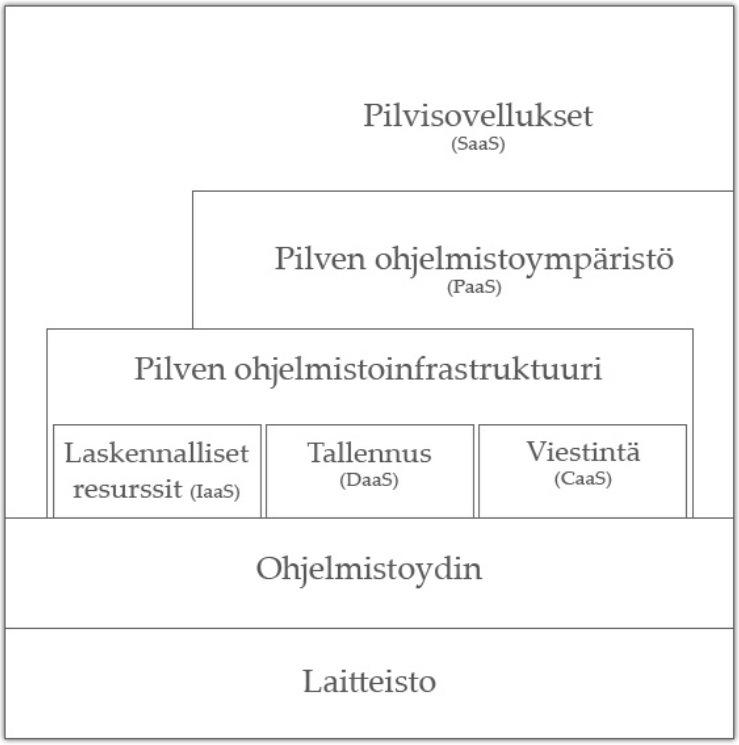
Rimalin, Choin & Lumbin (2009) mukaan pilvet voidaan jakaa kolmeen kategoriaan: yksityiset pilvet, julkiset pilvet ja hybridipilvet. Yksityisessä pilvessä tietojenkäsittely on organisaation sisäistä. Tällöin kaistanleveys, turvallisuus tai lakisääteiset vaatimukset eivät vaikuta toimintaan yhtä merkittävästi kuin muissa pilvimalleissa. Julkiset pilvet taas voidaan ajatella yleisinä resursseina, jotka ovat hienosäädettyjä, kolmansien osapuolien myymiä internetpohjaisia palveluja. Hybridipilvien ajatellaan olevan useista sisäisistä ja ulkoisista palveluntarjoajista koostuva pilvi. (Rimal ym., 2009.)

2.3 Tyypillinen ontologia

Konkreettinen tapa määritellä pilvi, on käyttää ontologiaa, jossa pilvi on esitetty eri tasoille jaettuna kerroksisena rakenteena. Rakennetta voidaan kuvata eri toimijoiden ja kerrosten välisenä kokonaisuutena (Vaquero ym., 2009). Youseff ym. (2008) jakavat pilviteknologian viiteen eri tasoon, joita ovat:

- sovelluskerros
- ohjelmistoympäristöt
- ohjelmistoinfrastruktuuri
- ohjelmistoydin
- laitteisto

Kerrokset ja niihin liittyvät palvelut havainnollistuvat graafisessa muodossa (kuvio 1). Tämäntyyppisessä ontologiassa korostuu pilviteknologian yksi tärkeimmistä osa-alueista: palvelurakenteinen arkkitehtuuri.



KUVIO 1 Youseffin ym. (2008) ontologia pilven eri kerroksista

Sovelluskerroksen ollessa loppukäyttäjälle jaottelun näkyvin osa-alue, se on myös hyvä esimerkki pilven hyödyistä prosessoinnin siirtyessä pois loppukäyttäjän työpisteeltä laitteistotason palvelimille (Youseff ym., 2008). Vaqueron ym. (2009) mukaan esimerkkinä sovelluskerroksen ohjelmistoista voidaan pitää mm. tekstinkäsittelysovelluksia. Sovellustason palvelu on nimeltään palveluohjelmisto (Software as a service, SaaS).

Toisena kerroksena mallissa on ohjelmistoympäristö. Ohjelmistoympäristöä hyödyntävät sovelluskehittäjät, joille kerros tarjoaa ohjelmointi- ja ympäristörajapinnan. Ohjelmistoympäristön avulla pilven ympäristöjen kanssakäymistä saadaan kehitettyä ja pilven skaalautuvuutta parannettua. (Youseff ym., 2008) Ohjelmistoympäristö tarjoaa ohjelmistoalustan, jossa tietojärjestelmiä voidaan ajaa. Palveluna tarjottavaa ohjelmistoympäristöä kutsutaan yleisesti pilvialustaksi (Platform as a service, PaaS). (Vaquero ym., 2009.)

Pilven ohjelmistoinfrastruktuurin kerros, joka on kolmantena käsiteltävässä mallissa, on perustavanlaatuinen kahdelle ylimmälle kerrokselle, mutta se voidaan myös ohittaa sovelluksia tai ohjelmistoympäristöä suunniteltaessa. Ohjelmistoinfrastruktuurikerros on jaettavissa vielä kolmeen alakategoriaan: laskennallisiin resursseihin, tiedon tallentamiseen ja tiedonvälitykseen. Laskennalliset resurssit pitävät pääosin sisällään virtualisoinnin, tiedon tallentamiseen taas liittyy tiedon replikointi sekä hajauttaminen. Tiedonvälitys on elintärkeä osa-alue pilviteknologian palvelun laadun kannalta. (Youseff ym., 2008) Ohjelmistoinfrastruktuuri voidaan samalla tapaa kuin muut kerrokset tarjota palve-

luna, jolloin asiakasorganisaatiolle, tässä tilanteessa palveluntarjoajille, voidaan rakentaa tilapäistarpeen täyttäviä järjestelmiä. Ohjelmistoinfrastruktuuripalvelua voidaan kutsua yksinkertaisesti palveluinfrastruktuuriksi (Infrastructure as a service, IaaS). (Vaquero ym. 2009.)

Mallin neljännessä kerroksessa on ohjelmistoydin. Ohjelmistoytimen tehtävänä on toimia väliohjelmistona, joka hallitsee fyysisien palvelimien ohjelmistoja. Ontologian viidentenä ja alimmaisena kerroksena toimii laitteistokerros, joka on myös pilviteknologian selkäranka. (Youseff ym., 2008.)

2.4 Pilviteknologialle tyypillisiä piirteitä

Pilviteknologiaa edeltävässä hilalaskennassa on havaittavissa samanlaisia piirteitä kuin pilviteknologiassa, jolloin sekaannusta termeissä ja käsitteissä tapahtuu helposti. Näin ollen on relevanttia tarkastella juuri pilviteknologialle tyypillisiä piirteitä. (Vaquero ym., 2009.)

Pilviteknologialle on tyypillistä kysyntäperusteinen resurssien tarjonta virtualisointia hyödyntäen. Tällöin asiakkaille muodostuu käsitys yhdestä, tähän tarkoitukseen varatusta resurssista, vaikka todellisuudessa virtualisoinnin takia varsinaista resurssien erottamista eri tahojen kesken ei tarvitse toteuttaa. Hilalaskennan tavoin pilviteknologialle on ominaista laaja virtualisointi. Zhang, Zhang, Chen & Huo (2010) esittävät virtualisoinnin mahdollisuutta laitteistolle, ohjelmistoille, käyttöjärjestelmille ja tallennuskapasiteetille. Tiedon ja laskentaresurssien lisäksi pilviteknologiaan sisältyy myös laitteistojen virtualisointi.

Virtualisointi on keskeistä myös pilviteknologian turvallisuutta kehitettäessä. Turvallisuus on pilviteknologiassa usein ympäristöjen eristämistä. (Vaquero ym., 2009) Tyypillinen tapa eristää ympäristöjä on jakaa suoritettavat tehtävät fyysisesti eri laitteisiin. Eristäminen virtualisoimalla on kuitenkin vielä sitäkin tehokkaampaa ja halvempaa, mutta tällöin on vaarana tiedon salassapidon heikentyminen. (Raj, Nathuji, Singh & England, 2009.)

Vaqueron ym. (2009) mukaan pilviteknologian ollessa melko uusi tietojenkäsittelyparadigma muutamat osa-alueet eivät ole vielä päässeet kehittymään hilalaskennan tasolle. Näistä esimerkkeinä ovat korkean tason palvelut ja sisäisen standardisoinnin puute. Parempi standardointi mahdollistaisi laajempien pilvikokonaisuuksien paremman yhteentoimivuuden, mutta suurten yhtiöiden tarjotessa asiakkailleen pilvipalveluita on kyse jossain määrin myös yrityssalaisuuksista.

Joillain osa-alueilla pilviteknologia on kuitenkin hilalaskentaa kehittyneempi — virtualisointi takaa asiakasorganisaatioille mahdollisuuden tarjota arkkitehtuurista riippumattomia palveluita. Myös käytettävyys ja palvelun laatuun perustuva ajattelu on pilviteknologiassa kehittyneempää. (Vaquero ym., 2009.)

2.5 Pilveen liittyvät hyödyt

Kenties merkittävimpänä pilvipalveluiden avulla saavutettavana hyötynä voidaan pitää pääomamenojen ja operatiivisten kulujen vähenemistä (Jensen, Schwenk, Gruschka & Lo Iacono., 2009). Armbrustin ym. (2009) mukaan säästöjä syntyy kiinteiden kulujen siirtyessä muuttuviin kuluihin. Näin ollen innovatiivisten palvelujen tai tuotteiden lanseeraaminen ja kehittäminen eivät enää vaadi yhtä suurta riskinottoa kuin aikaisemmin. Tietojenkäsittely ostopalveluna ei aiheuta merkittäviä tappioita, vaikka tuote tai palvelu ei saavuttaisikaan suunniteltua menestystä. (Armbrust ym., 2009). Pilvipalveluiden osto voi tällä tavoin toimia yhtenä strategisena tekijänä liiketoiminnan turvaamiseksi.

Merkittävänä etuna pilvipalveluita ajatellen on myös keskittyneisyys. Armbrust ym. (2009) selittävät ilmiötä loppukäyttäjän kannalta helpolla ylläpidolla – käyttäjien ei tarvitse huolehtia mistään, vaan palveluntarjoajat tekevät ohjelmistoasennukset, korjaukset ja päivitykset, eli toisin sanoen huolehtivat kokonaan ylläpidosta. Youseff ym. (2008) pitävät tämänkaltaista ratkaisua toimivana myös sovelluskehittäjien kannalta. Kehittäjät voivat ajaa keskitettyihin ohjelmistoihin pieniä parannuspäivityksiä tai lisätä uusia ominaisuuksia ilman, että loppukäyttäjien työ vaikeutuu. Sovellusten ajaminen palvelimilla pienentää myös tarvetta hankkia loppukäyttäjille prosessointi- tai muistikapasiteetiltaan tehokkaita työasemia.

Pilviteknologian etuna on myös sen käytettävyys. Pilvipalveluiden kapasiteettiresursseja voidaan hallita ohjelmistollisesti, mikä auttaa palvelun tilaajaa keskittymään omaan liiketoimintaan pitkällisten yksityiskohtien sijaan. (Zhang, Zhang, Chen & Wu., 2010) Älykkäiden ohjelmistojen avulla voidaan analysoida historiallista sekä ajan tasalla olevaa tietoutta ja tarvittaessa helposti esimerkiksi lisätä virtuaalikoneita resurssikokonaisuuteen (Zhang, Zhang, Chen, & Huo., 2010). Vaqueron ym. (2009) mukaan juuri pilvipalveluiden käytettävyys on yksi merkittävimmistä tekijöistä, jotka edistävät sen omaksumista ja käyttöönottoa.

Kuten jo luvun alussa todettiin, kustannustehokkuus on tyypillistä pilvipalveluille. Pilvipalveluita käyttävä asiakas maksaa ainoastaan käyttämästään tietojenkäsittelystä. Koska yritysten keskimääräinen tietojenkäsittelyn resurssitarve on huomattavasti pienempi kuin ruuhka-ajan resurssitarve, voivat ylimitoitetut resurssit olla huomattava kulu yritykselle (Youseff ym., 2008). Armbrust ym. (2009) pitävätkin pilvipalveluita tehokkaana mahdollisuutena ottaa huomioon väliaikaiset, tavallisesta poikkeavat resurssitarpeet. Koska yritys maksaa ainoastaan käyttämästään tietojenkäsittelystä, resurssitarpeen yli- tai aliarviointi ei aiheuta merkittäviä kuluja. Fiton, Goirin & Guitartin (2010) mukaan resurssien nopea skaalaaminen ylös- ja alaspäin on ehtona saataville säästöille. Useiden palveluntarjoajien myötä myös hinnoittelutavat ovat erilaisia.

Youseff ym. (2008) jakavat pilvipalveluiden hinnoittelutavat kolmeen luokkaan: kerroshinnoitteluun, yksikköhinnoitteluun ja tilausperusteiseen hinnoitteluun. Kerroshinnoittelussa palveluntarjoaja jakaa palvelunsa erilaisiin paketteihin, joissa on määritelty esimerkiksi muistin määrä sekä prosessoreiden

tyyppi ja nopeus. Yksikköhinnoittelussa palvelun hinta määräytyy tiedonsiirron tai muistin käytön mukaan. Eräs yksikköhinnoittelutapa on määritellä muistin käytölle tuntihinta. Tilausperusteinen hinnoittelu on laajimmin käytetty hinnoittelutapa ja se perustuu palvelun hintaan tietylle määräajalle. (Youseff ym., 2008) Hinnoittelutapa määritellään palvelutasosopimuksessa.

Tietojenkäsittelypalveluiden ollessa äärimmäisen tärkeä osa liiketoimintaa sovitaan palveluehdoista yleensä palvelutasosopimuksin. (Buyya ym., 2009) Greenin (2006) mukaan palvelutasosopimukset ovat muodostuneet välttämättömiksi de facto -sopimuksiksi erityisesti informaatioteknologiaan liittyvillä aloilla, joissa erilaiset ulkoistamiset ovat yleisiä. Palvelutasosopimuksia käsitellään myöhemmin luvussa 4.3.1 — Sopimukseen perustuva palvelu.

Vaikka pilvipalveluiden hankkiminen ostopalveluna pienentää liiketoiminnan taloudellista riskiä, liittyy uuteen teknologiaan kuitenkin monia ongelmallisia osa-alueita (Murray, 2009). Seuraavassa kappaleessa käsitellään mm. turvallisuuteen ja palveluita tarjoavan yrityksen luotettavuuteen liittyviä asioita.

2.6 Pilveen liittyvät ongelmat

Youseffin ym. (2008) mukaan merkittävimpiä pilviteknologian laajempaa omaksumista hidastavia tekijöitä ovat turvallisuuteen ja yksityisyyteen liittyvät osa-alueet. Puutteellisen standardoinnin tähden pilven turvallisuus, tiedon yksityisyys ja omistukseen liittyvät asiat ovat jokaisen pilvipalveluita tarjoavan tahon itse määrittelemiä.

Jensenin ym. (2009) mukaan yrityksen tietojen sekä sovellusten asettaminen täysin ulkopuolisen tahon varaan, joka voi olla toisella puolella maailmaa valtiossa, jossa on erilaiset säännökset, saattaa aiheuttaa halun pitäytyä perinteisemmissä tietojenkäsittelytavoissa. Chow ym. (2009) määrittelevät kyseessä olevan tilanteen kontrollin hämärtymisenä ja läpinäkyvyyden puutteena. Tarvittava luottamus pilvipalveluita hankkivien ja pilvipalveluja tarjoavien tahojen välille rakentuu heidän mukaan ymmärryksellä panostaa turvallisuuden ylläpitoon ja kehittämiseen.

Zhang, Zhang, Chen & Huo (2010) ottavat pilvipalveluita pohtiessaan kantaa myös palvelujen helppokäyttöisyyden kääntöpuoleen. Tietojenkäsittelyn ostaminen edullisesti palveluna saattaa joissain tilanteissa synnyttää halukkuutta aloittaa monta projektia liian nopealla tahdilla. Tämän lisäksi Zhangin, Zhangin, Chenin & Huon (2010) mukaan tietojenkäsittelyn ulkoistamista tulisi aina harkita tilannekohtaisesti. Pilvipalvelu voi antaa ratkaisun joihinkin tietojenkäsittelyn ongelmiin, mutta joissain tilanteissa se saattaa aiheuttaa entistä haastavampia kysymyksiä. Subashinin & Kavithan (2011) mukaan erityinen ongelma liittyen vakioituun palvelutasoon pilvipalveluissa on juuri tietoturva-osa-alueiden, kuten palomuurien ja kuormantasauksen, alkeellinen taso.

Merkittävänä ongelmallisuutena pilviteknologiassa on palveluiden tai jopa kokonaisen pilven saatavuus. Liiketoiminnan ollessa vahvasti sidoksissa tietojenkäsittelypalveluihin asiakasyritykset eivät ole halukkaita ostamaan pal-

veluita, jos palveluja tarjoavalla organisaatiolla ei ole strategiaa palvelun tarjonnan keskeytyessä äkillisesti (Armbrust ym., 2009.). Ulkoistettaessa tietojenkäsittelyä kontrolli siirtyy pois yrityksen omista käsistä, ja ongelmatilanteissa liiketoimintaan kohdistuu vakava uhka. Luotettavuus on koetuksella, kun aika on rahaa. Jotta useiden pilvien välinen saatavuus ja toiminnallisuus voidaan taata, tulee myös pilvien kehittämisessä ottaa huomioon yhteenliitettävyys. (Rimal ym., 2009.) Eräs tapa kehittää saatavuutta ja toiminnallisuutta on standardointi.

Pilviteknologian kehittymisen edellytyksenä on Kaufmanin (2009) mukaan ennakoiva toiminta, esimerkiksi standardoinnin avulla. Hilalaskennasta perityistä, standardoiduista teknologioista huolimatta pilviteknologiaan ja pilvipalveluihin liittyy monia osa-alueita, joissa standardointi olisi välttämätöntä. Valitettavasti useat näistä osa-alueista ovat palveluntarjoajien sisäisiä, liikesalaisuuksiin verrattavissa olevia ratkaisuja (Vaquero ym., 2009). Standardoinnin avulla voitaisiin välttää erilaiset yhteensopivuusongelmat sekä tiedon lukkiutuminen yhteen formaattiin jonkin yksittäisen palveluntarjoajan ongelmatilanteessa (Chow ym., 2009).

Erityisesti pilviteknologian turvallisuutta pohdittaessa erilaiset standardit tulisi ottaa huomioon jo palvelujen kehityksen alkuvaiheissa — on kyseessä sitten pilviteknologian ylimmät sovelluskerrokset tai alimmat fyysisiä laitteita sisältävät kerrokset. Boden, Fischerin, Kühnhauserin & Riebischin (2009) mukaan niin sovellus- kuin arkkitehtuurisuunnittelussa on tärkeää huomioida erilaiset standardit turvallisuuden takaamiseksi. Jensen ym. (2009) painottavat myös internetselaimien turvallisuuden kehittämistä useiden pilvisovellusten ollessa loppukäyttäjälle selainpohjaisia.

Kaufmanin (2009) mukaan on relevanttia pohtia myös globaalin ulkoistamisen vaikutuksia pilvipalveluihin. Mitä pikimmiten tulisi selvittää eri maiden lakien vaikutukset tiedon liikkuessa yli valtiorajojen.

2.7 Yhteenveto

Pilviteknologian avulla toteutetut pilvipalvelut virtuaaliresursseineen haastavat aikaisemmat tietojenkäsittelymenetelmät kustannustehokkuudellaan, joustavuudellaan ja helppokäyttöisyydellään. Vaqueron ym. (2009) määritelmää mukaillen pilvet ovat monipuolisia tietojenkäsittelyresursseja, jotka voidaan mukauttaa muuttuvan tarpeen myötä kustannustehokkaasti. Pilvipalvelu on myös erittäin käytännöllinen asiakasyrityksen kannalta tiedon ja sen käsittelyn siirtyessä pois loppukäyttäjän tietokoneelta pilveen, jonka ylläpidosta huolehtii palveluntarjoaja (Armbrust ym., 2009).

Tämänkaltainen palveluna tarjottava tietojenkäsittely edellyttää kuitenkin luottamusta osapuolien välillä. Palvelun laatu rakentuu teknisesti toimivasta kokonaisuudesta, jossa on otettu huomioon erityisesti palvelun saatavuus ja tietoturvallisuus. Teknologian menestyminen edellyttää tehokasta standardoin-

tia, jonka avulla voidaan kehittää tietoturvaa, parantaa saatavuutta ja estää tilanteet, jossa tieto lukkiutuu yhden pilvipalveluntarjoajan formaattiin.

Pilviteknologian kehittymisen kannalta aihealueen tutkimus on tärkeää. Jotta tutkimus olisi menestyksellistä, tulee ymmärtää, miten pilviteknologia on kehittynyt nykyiseen muotoonsa ja miten se eroaa edeltäjistään.

Yhteenvetona luvulle voidaan määritellä pilvipalveluiden houkuttelevuus kuluja pienentävinä, joustavina ja helposti skaalattavina tietojenkäsittelypalveluina unohtamatta kuitenkaan riskejä, joita palveluihin väistämättä liittyy. Pilvipalveluissa on ongelmallista kontrollin siirtyminen yrityksestä ulkoiselle taholle sekä tietoturvan eri osa-alueet.

Seuraavassa luvussa käsitellään tietoturvaan liittyviä osa-alueita, jotka ovat keskeisessä roolissa pilviteknologian ja pilvipalveluiden menestystä ajatellen.

3 TIETOTURVA JA TIETOSUOJA

Tässä luvussa tarkastellaan tietoturvan ja tietosuojan osa-alueita pilviteknologiassa. Tietoturvaa käsitellään tietosuojaa edistävänä tekijänä, joka on edellytys mm. yksityisyyden suojaamiselle. Luvun alussa pohditaan yleisesti tietoturvaan liittyviä asioita, ja tämän jälkeen tietoturvaa käsitellään pilviteknologian näkökulmasta. Yleisen käsittelyn jälkeen tarkastellaan erilaisia tietoturvauhkia ja haavoittuvuuksia. Luvun lopussa sivutaan Suomen lainsäädäntöä tietoturvaan ja tietosuojaan liittyen, käsitellään aihealueen haasteita pilviteknologian näkökulmasta sekä esitellään tietoturvaan liittyviä standardeja. Kohdan 3.7 Yhteenveto-kappaleessa käsitellään vielä lyhyesti koko luvun oleellisimmat asiat.

3.1 Yleistä

Tietoturvaa voitaneen määritellä monella tapaa ja näkökulmasta riippuen, mutta useimmiten määritelmään liitetään keskeisesti seuraavat kolme osa-aluetta:

- luottamuksellisuus
- käytettävyys
- eheys

Hakala ym. (2006, s. 4) määrittelevät tietoturvan tiedon arvoon perustuvan määritelmän ja laajennetun määritelmän avulla. Klassinen tapa määritellä tietoturvaa on käsitellä tiedon arvoa. Tähän liittyen luottamuksellisuudella tarkoitetaan tilannetta, jossa ”tietojärjestelmän tiedot ovat vain niihin oikeutettujen henkilöiden käytettävissä”. Käytettävyys on sen sijaan määritelty niin, että ”tiedot ovat saatavissa tietojärjestelmästä oikeassa muodossa riittävän nopeasti”. Joissain yhteyksissä käytettävyys on suomennettu myös saatavuutena (Jordan, 2006, s. 18). Eheydellä tarkoitetaan tietojärjestelmän tietojen paikkansapitävyyttä ja että tiedot eivät sisällä tahallisia tai tahattomia virheitä. Hakalan ym. (2006, s. 4) mukaan luottamuksellisuutta vaalitaan käyttäjätunnuksin ja salasanoin

sekä erilaisten salausmenetelmien avulla. Käytettävyyttä ja eheyttä pyritään turvaamaan niin laitteistotason kuin ohjelmistoteknisin ratkaisuin.

Aiemmin mainittu laajennettu määritelmä pitää sisällään edellisen kolmen lisäksi myös kiistämättömyyden ja pääsynvalvonnan. Kiistämättömyydellä tarkoitetaan varmuutta siitä, että tietojärjestelmää todella käyttää sama taho, joka on oikeutettu siihen ja että tallennettava tieto on luotettavaa. Pääsynvalvonnalla taas kontrolloidaan ja rajoitetaan organisaation tietojärjestelmän käyttöä. Ulkopuolisten tahojen pääsy tietojärjestelmään voidaan estää erilaisin laitteistollisin ratkaisuin (Hakala ym., 2006, s. 86).

Tietosuojan ja tietoturvan ero on tärkeää ymmärtää, sillä termejä käytetään joissain tilanteessa virheellisesti sekaannuksia aiheuttaen (Järvinen, 2010, s. 15). Järvisen (2010, s. 15) mukaan tietosuojassa on kyse ”henkilöön tai hänen toimintaansa liittyvien tietojen suojaamisesta luvatonta keräämistä ja käyttöä vastaan”. Tällöin suojauksen kohteena on ihminen, kun taas tietoturvan kohteena on itse tieto (Järvinen 2010, s. 15). Tietosuojaa pyritään edistämään mm. lainsäädännön avulla, jota käsitellään tutkielman kohdassa 3.4.

3.2 Pilviteknologian tietoturva

Aikaisemmista tietojenkäsittelyparadigmoista poiketen pilviteknologian myötä tietojen hajauttaminen ympäri maailmaa on tullut mahdolliseksi ja samalla nostanut esiin kysymyksen: Kuka on vastuussa tietojen turvaamisesta - palveluja tarjoava taho vai palveluita ostava taho? (Kaufman, 2009) Hajautetut, verkottuneet tietojärjestelmät sisältävät yhä enemmän henkilökohtaisia ja arkaluontoisia tietoja niin yrityksistä kuin yksityishenkilöistä. Tietojen liikkumisen hallinnan väheneminen aiheuttaa vakavia riskejä tietoturvalle ja erityisesti yksityisyydelle. (Petković & Jonker, 2007, s. 5.) Perinteiset tavat suojata tietoa esimerkiksi erilaisin salausmetodein eivät välttämättä ole tulevaisuudessa enää riittävän tehokkaita tiedon pirstaloituessa ympäri maailmaa hajautettujen verkkojen myötä (Parakh & Kak, 2009).

Chowin ym. (2009) mukaan pilviteknologiaan liittyvät huolenaiheet voidaan jakaa kolmeen kategoriaan: yleiseen turvallisuuteen, saatavuuteen ja kolmannen osapuolen olemassaoloon. Kategoriat ovat sovellettavissa aikaisemmin määriteltyyn tietoturvan klassiseen määritelmään. Tässä yhteydessä yleisen turvallisuuden kategoriaan voidaan ajatella kuuluvan ne ratkaisut, joilla tiedon eheys ja oikeellisuus turvataan. Saatavuuden ajatellaan olevan niitä käytettävyyden osa-alueita, joilla varmistetaan, että haluttu tieto on saatavilla. Kolmannen osapuolen olemassaolo on verrattavissa luottamuksellisuuden osa-alueeseen.

Tietojen suojaamisen kannalta kenties keskeisimpänä Chowin ym. (2009) luokittelussa on kolmannen osapuolen olemassaolo. Tähän liittyen ongelmallisia osa-alueita on useita. Epäilyjä herättävät mm. lainsäädännön asettamat vaatimukset vasteajoille ja tietojen tuhoamiselle. Tämän lisäksi erilaisten auditointien toteutus voi olla mahdotonta pilviresurssien ollessa laajasti hajautettuja.

Edellisten lisäksi eri maiden välisten sopimusoikeudellisten poikkeavuuksien takia liiketoiminta voi kohdata ennalta odottamattomia vaikeuksia. Myös luottamukseen liittyvät tekijät aiheuttavat huolta pilvipalveluita harkitseville yrityksille — teollisuusvakoilu, tiedon lukkiutuminen tietyn palveluntarjoajan formaattiin ja mahdolliset alihankkijoiden kautta toteutettavat palvelut ovat merkittäviä tekijöitä lisäämään epäluottamusta pilviteknologioita kohtaan. (Chow ym., 2009.)

Wangin ym. (2009) mukaan hajautettujen tietojärjestelmien täysimääräinen hyödyntäminen edellyttää yksityisyyteen ja tietoturvaan liittyvien asioiden huomioimista arkaluontoisen tiedon ollessa hajallaan eri puolilla internetiä. Wangin kanssa yhtenevällä linjalla on myös Kaufman (2010), jonka mukaan tehokkaan tietoturvan edellytyksenä on ymmärtää hajautettujen järjestelmien olevan turvallisuudeltaan heikompia kuin yritysten sisäinen tietojärjestelmäarkkitehtuuri ja näin ollen tietoturvaan on kiinnitettävä erityisellä tavalla huomiota. Tämän lisäksi Kaufman (2010) painottaa, että pilvipalvelun tilaavalla taholla tulisi olla mahdollisuus määrittää tietoturvaan ja riskienhallintaan liittyviä menetelmiä, jotka ovat linjassa heidän yrityksensä päämäärien sekä operatiivisen riskienhallinnan kanssa.

Wangin, Zhaon, Jiangin & Len (2009) mukaan tiedon saatavuus on ensisijaisen tärkeää pilven turvallisuuden kannalta. Tiedon saatavuuteen liittyy myös ongelma pilvipalveluita tarjoavan yrityksen lopettaessa toimintansa. Kandukurin, Paturin & Rakshitin (2009) mukaan palvelutasosopimuksissa tulisi määritellä tiedon saatavuus palvelutarjoajan muuttuessa. Pilviteknologiaa tulee kuitenkin kehittää jo ennen palvelusopimuksien laatimista; jo pilvipalveluita kehitettäessä tulisi ottaa huomioon tiedon saatavuus (Sripanidkulchai, Sahu, Ruan, Shaikh & Dorai, 2010). Sripanidkulchain ym. (2010) mukaan pilven saatavuus on myös paljolti kiinni eri palvelutarjoajien yhteistyöstä. Pilvien arkkitehtuureja suunniteltaessa tulisi ottaa huomioon pilvien välinen yhteenliitettävyys.

Yleisen tietoturvallisuuden kehittämiseen liittyy muutamia avaintekijöitä, joiden tulee olla kunnossa. Ensimmäisenä osa-alueena voidaan pitää tiedon tallentamista. Samaratin & di Vimercatin (2010) mukaan ulkoistettaessa tietojen tallennus tai säilytys tietojen suojaamisessa käytetään erilaisia pirstaloimis- ja segmentoimismenetelmiä yhdessä salausmenetelmien kanssa. Yonghong (2010) kuitenkin pitää käytössä olevia salausmenetelmiä tehottomina ja ehdottaa tiedon pirstaloimista eri palvelimille, joilta tieto voitaisiin koota palvelinten tietämättä toisistaan.

Samalla tapaa tulee turvata tiedon liikkuminen järjestelmien tai sovellusten välillä. Spiekermannin & Cranorin (2009) mukaan järjestelmäkehittäjien tulee minimoida sopimattomiin tai kontrolloimattomiin tiedonsiirtoihin liittyvät riskit turvaamalla siirtotie asianmukaisin keinoin.

Myös tietokantoihin tehtävät haut ja niihin liittyvä indeksointi tulee turvata. Samarati & di Vimercati (2010) pitävät indeksoinnin tehokkuutta ongelmallisena yksityisyyden kannalta. Tähän mennessä on pystytty kehittämään ainoastaan metodeja, joissa tehokkaiden indeksointien edellytyksenä on jonkinasteinen yksityisyyden vaarantumisen todennäköisyys (Samarati & di Vi-

mercati, 2010). Tietosuoja saattaa vaarantua myös, jos tehtävien tietokantakyselyjen salassapito vaarantuu.

Tiedon eheys ja oikeellisuus ovat vähintäänkin yhtä merkittävä tietoturvan osa-alue kuin tiedon turvallinen tallentaminen, tietoliikenteen suojaaminen ja tietokantahaut. Samaratin & di Vimercatin (2010) mukaan lähtökohtana tiedon eheydelle ja oikeellisuudelle on palvelin, joka ei voi nähdä tiedon sisältöä, mutta on luotettava tehtävissä tietokantakyselyissä. Ferrarin (2009) mukaan tulee kiinnittää myös entistä enemmän huomiota kolmansien osapuolien tuottaman datan oikeellisuuteen. Tietoa tuottavan tahon todentaminen toteutetaan usein käyttämällä digitaalisia allekirjoituksia tai ketjurakenteita (Samarati & di Vimercati, 2010).

Pääsynvalvonnan hallintaan liittyy riskejä. Samaratin & di Vimercatin (2010) mukaan hajautettujen järjestelmien pääsynvalvontaan liittyy ongelmia esimerkiksi silloin, jos tieto menetelmästä, jolla tietoon pääsee käsiksi, on arkaluontoista. Toisena ongelmana kirjoittaja mainitsee tilanteen, jossa tieto itsessään on tietyn valtuutustason edellyttämää ja johon palvelimella itsellään ei ole lupaa päästä käsiksi. Yleisesti erilaiset sisäänpääsyn oikeuttavat todentamismenetelmät voivat perustua käyttäjän rooliin, tehtävään tai projektiin (Chen, Hu, Du, Zhou & Ji, 2009).

3.3 Tietoturvauhat ja haavoittuvuudet

Tietojenkäsittelyn siirtyessä pilveen tietoturvauhat seuraavat perässä. Kellerman (2010) pitää pilviteknologiaa alttiina useille erilaisille tietoturvauhille. Ongelmallisena voidaan pitää liiallista luottoa salausmenetelmiin ja toisaalta esimerkiksi virtualisoituihin järjestelmiin liittyviä haavoittuvuuksia (Kellerman, 2010). Grobauerin, Walloschekin, & Stockerin (2010) mukaan pilviteknologiaan liittyviä tietoturvauhkia ja -haavoittuvuuksia tarkasteltaessa tulee terminologia määrittää oikein. Tietoturvauhka voidaan ajatella yksinkertaisesti uhkatekijänä tietoturvan toteutumiselle (Mellado, Blanco, Sanchez & Fernandez-Medina, 2010). Haavoittuvuus on hiukan eri asia. Hakala ym. (2006, s. 83) määrittelevät haavoittuvuuden *tietojärjestelmän tai organisaation tunnetuksi ominaisuudeksi, joka suurentaa riskin realisoitumistodennäköisyyttä tai pahentaa sen seuraamuksia.* Terminologian ymmärtämisen lisäksi on tärkeää tiedostaa, minkälaisia tyypilliset pilviteknologiaan liittyvät tietoturvauhat ja haavoittuvuudet ovat.

Grobauerin ym. (2010) mukaan tietoturvauhkia käsiteltäessä tulee ymmärtää nimenomaan pilviteknologialle tyypilliset tietoturvauhat liittyen esimerkiksi virtualisointiin, sessioihin ja kryptografiaan. Tämän lisäksi on joukko muita potentiaalisia uhkatekijöitä: luvaton tunkeutuminen hallintajärjestelmiin, internetprotokollan haavoittuvuudet, tiedon palauttamisen haavoittuvuudet sekä palvelun mittaukseen ja laskutukseen liittyvät haavoittuvuudet (Grobauer ym., 2010). Pilviteknologian ollessa läpitunkeva ja moniulotteinen myös siihen liittyvät tietoturvauhat ovat moninkertaisia.

Pilvipalvelu altistuu hyökkäyksille eri palvelutasoilla (Jensen ym., 2009). palveluohjelmistotasolla tietoturvaa on pyritty murtamaan esimerkiksi internetselaimista löytyneiden haavoittuvuuksien kautta. Tämän lisäksi on myös hyödynnetty nk. wrapping-tekniikkaa, jossa tiedoston otsaketietoja on muokattu ja näin ollen on voitu suorittaa laittomia komentoja kohdetietokoneella. Hyökkäys voi kohdistua myös pilven alustaan tai infrastruktuuriin. Jensenin ym. (2009) mukaan haittaohjelmia voidaan hyödyntää esimerkiksi soluttamalla vahingollinen palvelumoduuli tai virtuaalikone osaksi pilvikokonaisuutta ja näin vakoilla tietoliikennettä.

Pääsy tietoon voi estyä myös erilaisten hyökkäysten takia. Jensenin ym. (2009) mukaan palvelunestohyökkäykset voivat olla erityisen hankalia pilviteknologialle järjestelmän lisätessä resursseja sitä mukaa kun hyökkääjä kuormittaa palvelua.

Tietoturvauhka liittyy aina jossain määrin tiedon altistumiseen taholle, jonka ei tulisi päästä tietoon käsiksi. Näin ollen tietoturva integroituu olennaisesti osaksi tietosuojaa. Seuraavassa kappaleessa käsitellään tietosuojan turvaamista lainsäädännön avulla.

3.4 Lainsäädäntö, direktiivit ja suositukset

Henkilökohtaisten tietojen suojaamista on pyritty vahvistamaan lainsäädännön avulla. Suomessa yksityisyyden suojan käsite perustuu ihmisoikeussopimuksiin, kansainvälisiin säädöksiin ja Suomen perustuslakiin. (Syrjänen, 2008, s. 124.) Euroopan unionin jäsenmaana Suomen tulee ottaa lainsäädännössään huomioon myös EU-maita koskevat direktiivit (Syrjänen, 2006, s. 23).

Laajemmassa merkityksessä tietosuojaa ja yksityisyyttä voidaan pitää osana yksilön perusoikeuksia, joista säädetään Suomen perustuslaissa. Perustuslain toisen luvun kymmenennessä pykälässä on säädetty yksityiselämän ja luottamuksellisen viestin suojasta (Suomen perustuslaki 11.6.1999/731, 1999). Syrjäsen (2006, s. 35) mukaan Euroopan neuvoston tietosuojasopimus ja suositukset sekä tietosuojadirektiivi ovat ohjanneet Suomen lainsäädäntöä merkittävimmin. Tietosuojadirektiivin pohjalta on säädetty vuonna 1999 voimaan tullut henkilötietolaki (Järvinen, 2010, s. 255).

Henkilötietolain mukaan lain tarkoituksena on ”toteuttaa yksilön yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista” (Henkilötietolaki 22.4.1999/523, 1999). Alkuperäisessä direktiivissä henkilötietojen käsittelyllä tarkoitetaan mm. tietojen keräämistä, tallentamista, järjestämistä, säilyttämistä, luovuttamista, suojaamista ja tuhoamista (Tietosuojadirektiivi 95/46/EY, 1995). Vaikka henkilötietolaki onkin ensisijaisesti säädetty henkilötietoja käsitteleviä tahoja ajatellen, asettaa lainsäädäntö luonnollisesti vaatimuksia myös henkilötietoja käsittelevien järjestelmien suunnittelemiselle.

Taloudellisen yhteistyön ja kehityksen järjestö OECD:n (Organization for Economic Cooperation and Development) antama yksityisyyden suojaamisen suositus vuodelta 1981 on kenties merkittävin kansainvälisistä suosituksista, joihin useat eri lähteet viittaavat käsiteltäessä tietosuojaa tietojenkäsittelyssä. Gadzheva (2008), Lahlou (2008) ja Tavani (1999) pitävät OECD:n suositusta merkittävänä virstanpylväänä, joka oli omiaan kehittämään useiden eri maiden sisällä tietojenkäsittelyyn ja sen suojaamiseen liittyviä periaatteita. OECD:n suositus käsittelee mm. kerättävän tiedon rajoittamista, tiedon oikeellisuuden ja laadun huomioimista, henkilökohtaisen tiedon suojaamista sekä avoimien menetelmien käyttöä (OECD, 1980). Lahlou (2008) pitää OECD:n suositusta pohjana monille suosituksille ja ohjeistuksille, joita käytetään paikallisesti tietojärjestelmiä kehitettäessä.

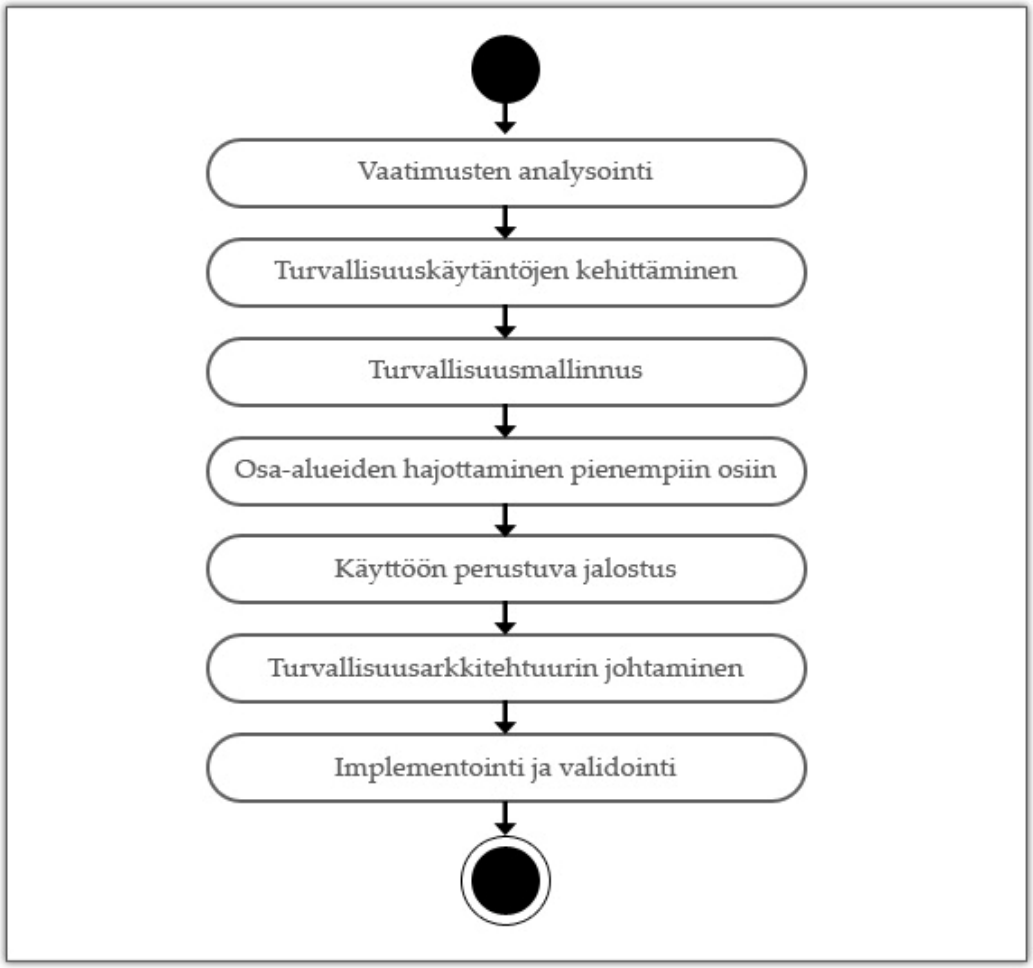
3.5 Turvallisuuden huomioiva järjestelmäkehitys

Ohjelmistokokonaisuuksien turvallisuuden takaamiseksi ja riskien minimoimiseksi on kehitetty erilaisia kehitysprosessiin implementoitaviksi tarkoitettuja järjestelmäkehitysmenetelmiä ja -malleja (Khan & Zulkernine, 2009). Toimintamalleja ja metodeja on standardisoitu, jotta ohjelmistojen turvallisuus entisestään kehittyisi (Cheng ym., 2009). Turvallisuuden huomioiva järjestelmäkehitys kestää koko ohjelmiston elinkaaren ajan (Byers & Shahmehri, 2007). Ohjelmiston elinkaarta ajatellen Melladon ym. (2010) mukaan turvallisuustarpeiden huomioiminen tulee aloittaa ohjelmistokehitysprosessin alkuvaiheessa, jotta toiminta olisi kustannustehokasta ja toteutettava järjestelmä olisi lopputulokseltaan vakaa.

On tärkeää erottaa turvallisuuteen keskittyvä järjestelmäkehitys sovellustason turvallisuudesta. Sovellustason turvallisuus on ohjelmiston suojausta sen valmistuttua suodattimien, tunkeutumisenhavaitsemisjärjestelmien ja palomuurien avulla (Khan & Zulkernine, 2009). Riskien minimoimiseksi turvallisuuden huomioiminen tulee aloittaa aikaisemmin. Sultanin, En-Nouaaryn & Hamou-Lhadjin (2008) mukaan turvallisuuden huomioiminen alkaa vaatimustenmäärittelyvaiheessa kysymyksellä ”Miten turvallisuus määritetään vaatimustenmäärittelyssä?”

Yksi turvallisuuden huomioivan järjestelmäkehityksen kulmakivistä on järjestelmäarkkitehtuuri. Boden ym. (2009) mukaan ei-toiminnallisten turvallisuusvaatimusten huomioiminen komponenttikeskeisessä arkkitehtuurisuunnittelussa vaatii iteratiivisen lähestymistavan, jossa toiminnallisten vaatimusten ohella huomioidaan ei-toiminnallisten vaatimusten aito toteutuminen esimerkiksi erilaisten skenaariomallinnusten ja simulaatioiden avulla. Boden ym. (2009) arkkitehtuuriprosessin iteraatio on selkeytetyy graafisessa muodossa (kuvio 2). Sommervillen (2007, s. 729) mukaan arkkitehtuurisuunnittelussa tulee huomioida tiedon suojaus ja ongelmatilanteessa sen jakautuminen. Tämä tarkoittaa arkkitehtuurin suunnittelua niin, että tieto on mahdollisimman suo-

jattua, mutta suojan pettäessä tietoon käsiksi pääsy on mahdollisimman minimaalista.



KUVIO 2 Boden ym. (2009) arkkitehtuurisuunnittelun iteraatio

Arkkitehtuurisuunnittelussa turvallisuusmenettelyjen määrittelemisen tulisi olla osa suunnitteluprosessia. Boden ym. (2009) mukaan melko yleinen, käyttäjän rooliin perustuva pääsynvalvonta on toimiva tapa parantaa luottamuksellisuutta ja tiedon eheyttä osana turvallisuusmenettelyä sekä turvallisuuden suunnittelua. Turvallisuuden kannalta merkittävien arkkitehtuurin osien hajottaminen pienempiin osiin on tehokas keino edistää turvallisuuden toteutumista. Erilaisten komponenttien välisten turvallisuusmääritelmien jälkeen turvallinen arkkitehtuuri on implementoitavissa ja arvioitavissa. Järjestelmäkehitys arkkitehtuurisuunnitteluineen voi perustua myös turvallisuusvaatimuksiin.

Valmiiden tietojärjestelmien turvallisuusvaatimukset täytetään usein ainoastaan lain vaatimien vähimmäisvaatimusten mukaan (Mellado ym., 2010). Melladon ym. (2010) mukaan turvallisuusvaatimuksien täyttäminen edellyttää

helposti toistettavissa olevaa, systemaattista menettelytapaa, jonka avulla voidaan määrittää niin toiminnalliset kuin ei-toiminnalliset vaatimukset: laatu, suorituskyky, siirrettävyys ja turvallisuus. Turvallisuusvaatimusten määrittämiseen on olemassa puolivirallisia ja virallisia metodeja (Hassan, Eltoweissy, Bohner, & El-Kassas, 2009). Hassan ym. (2009) pitävät kuitenkin puolivirallisia metodeja melko tehottomina ja virallisia metodeja taas usein vaikeaselkoisina ja kalliina.

Turvallisuusvaatimusten määritteleminen auttaa turvallisuusmenetelmien nimeämisessä (Firesmith, 2004). Määrittämällä tarkasti vaatimukset dokumentteihin voidaan turvallisuusvaatimukset myös paremmin tarkistaa jälkeenpäin ja hyväksyä toteutetut ratkaisut turvallisuuden takaamiseksi. Firesmithin (2004) mukaan ohjelmistojen turvallisuuden laatu ja oikeanlaisuus paranee, jos vaatimusten määrittäminen ja analysointi tapahtuu ottamalla huomioon edut ja hyödyt, joita suojellaan sekä riskit, joita turvallisuuden laiminlyömiseen liittyy. Turvallisuusvaatimusten kokoamisessa voidaan hyödyntää erilaisia uudelleen hyödynnettäviä mallipohjia ja käyttötapauskaavioita (Mellado ym., 2010).

Turvallisuusvaatimuksien määrittelemisessä voidaan ottaa käyttöön myös erilaisia kansainvälisiä standardeja. Horien, Morimoton, Azimahin, Goton & Chengin (2008) mukaan ISO-standardit ovat parhaiten sopivia yleisesti hyväksytyiksi käytänteiksi. Melladon ym. (2010) mukaan standardien integrointi osaksi turvallisuusvaatimuksien määrittelemistä parantaisi yhdenmukaisuutta ja todennettavuutta.

3.6 Tietoturvaan liittyviä standardeja

Tietojärjestelmien kokonaisvaltaisen laadun takaamiseksi on kehitetty suuri joukko erilaisia standardeja. Suomen Standardoimisliiton (2010) mukaan standardi voidaan määritellä *konsensusperiaatteella määritellyksi, asianmukaisten sidosryhmien vahvistamaksi, puolueettoman tahon hyväksymäksi asiakirjaksi, joka on yleisesti saatavilla, tarkoitettu yleiseen käyttöön ja vapaaehtoinen, mutta viranomaisten niin määritellessä pakollinen käytettäväksi*. Yksinkertaistaen standardi on siis määrätynlainen paras käytäntö, jonka käyttö voi toimia myös osoituksena laadukkaista tuotteista tai palveluista. Zhulingin, Kaihun, Xiaon, & Shihuanin (2009) mukaan standardointi liittyy laadun paranemisen lisäksi myös tekniseen kehitykseen, teollisuuden paranemiseen ja ympäristön suojelun kehittymiseen. Standardointi liittyy usein joko prosessin tai tuotteen standardointiin (Thayer & McGettrick, 2007).

Tutkielmassa käsiteltävät standardit ovat pääosin ISO:n (International Organization for Standardization) ja IEEE:n (Institute of Electrical and Electronics Engineers) standardeja. Lin, Dongin, Zhengin, Zhoun & Guon (2009) mukaan edellä mainitut organisaatiot ovat kaikista edistyneimpiä kansainvälisiä standardeja kehittäviä tahoja.

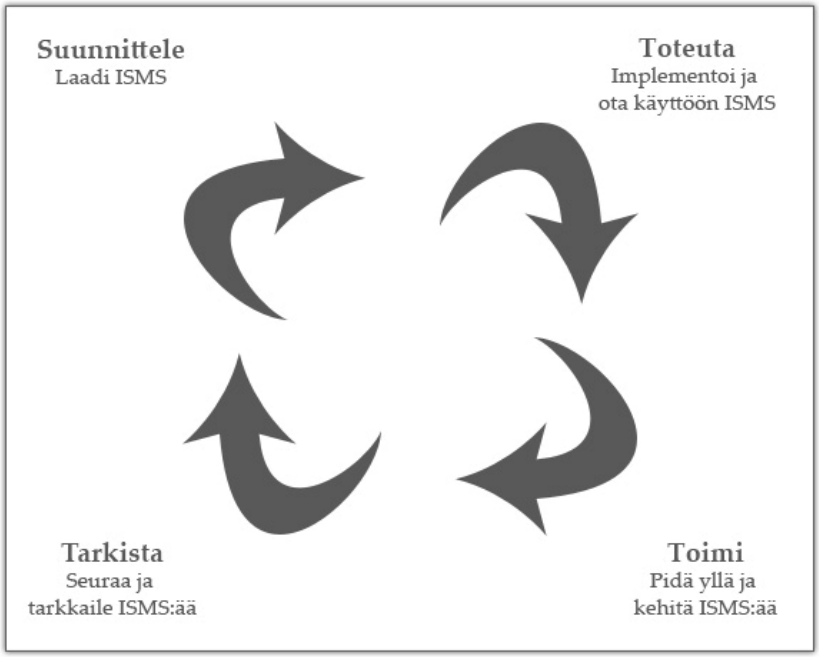
Standardien merkitys korostuu myös tietojärjestelmien turvallisuutta käsiteltäessä. Järjestelmän turvallisuus on äärimmäisen moniulotteinen asia ja ulot-

tuu järjestelmän koko elinkaarelle. Nordbottenin (2009) mukaan turvallisuuden takaamiseen liittyvää standardointia esiintyy tietojenkäsittelypalveluiden standardoinnista aina ohjelmointikoodin standardointiin; ISO:n ja IEEE:n lisäksi myös OASIS (The Organization for the Advancement of Structured Information Standards) ja W3C (Word Wide Web Consortium) ovat tehneet vuosien ajan suosituksia ja standardoimistyötä. Tietojenkäsittelyn ja siihen liittyvien osa-alueiden kehittyessä valtavalla nopeudella standardisoinnin tulisi pysyä vauhdissa mukana. Ajatellen esimerkiksi pilviteknologiaa Vaqueron ym. (2009) mukaan standardien puuttuminen asettaa pilvien turvallisuuden ja yhteentoimivuuden merkittävälle koetukselle.

Hyödyntämällä standardeja, jotka painottavat kehitettävien tai olemassa olevien järjestelmien turvallisuutta, voidaan täyttää kansainväliset, yleisesti hyväksytyt turvallisuusmääräykset ja näin parantaa esimerkiksi järjestelmien välistä kanssakäymistä (Evans, Tsohou, Tryfonas & Morgan, 2010). Deyn (2007) mukaan eräs keino parantaa yrityksen tietoturvallisuutta on suunnitella ja ottaa käyttöön tietoturvallisuuden hallintajärjestelmä (Information Security Management System, ISMS) yrityksessä. Tietoturvallisuuden hallintajärjestelmän käyttöönottoa ja hyödyntämistä varten on kehitetty kansainvälinen ISO/IEC 17799 -standardi. Standardin avulla voidaan kehittää yrityksen turvallisuusjohtamisen käytäntöjä. (ISO/IEC 17799, 2006.)

Tietoturvallisuuden hallintajärjestelmää koskeva standardi pitää sisällään koko prosessin elinkaaren: standardin omaksumisen osaksi yrityksen toimintaa, resurssien asettamisen, laajuuden määrittämisen, nykyhetken analyysit, tietovarantojen luetteloinnin, riskien arvioinnin ja hallinnoinnin sekä erilaiset tavoitteiden ja hallinnoinnin määrittelyt erilaisine käytänteineen ja toimintamalleineen (Dey, 2007). ISO/IEC 17799 -standardi on myöhemmin nimetty uudelleen ISO 27002 -standardiksi (Barlette ym., 2008).

Toinen turvallisuutta edistävä standardoitu kokonaisuus on ISO 27000 -standardisarja. Standardisarja on kehitetty parantamaan yritysten kykyä hallita tietoturvallisuutta, riskejä ja valvontaa (Evans ym., 2010). Sarja koostuu seitsemästä julkaistusta ja kahdesta kehitteillä olevasta standardista. Evansin ym. (2010) mukaan sarjan suosituimpia standardeja ovat ISO 27001 ja ISO 27002 -standardit, joista ensimmäinen pitää sisällään vaatimukset dokumentoidun tietoturvallisuuden hallintajärjestelmän aloittamiselle, implementoinnille, käytölle, monitoroinnille, arvioimiselle, ylläpidolle ja kehittämiselle. Deyn (2007) mukaan ISO 27001 -standardi hyödyntää OECD:n asettamaa PDCA-käytäntöä (Plan-Do-Check-Act) hallintajärjestelmän kokonaisprosessin toteutuksessa (kuvio 3). ISO/IEC 27001 on standardina huomattavasti sitovampi kuin ISO 17799 -standardi ja toteutettu vastaamaan myös laatujärjestelmästandardien ISO 9001 ja ISO 14001 vaatimuksia (Hakala ym., 2006, s. 49).



KUVIO 3 PDCA-malli tietoturvan hallintajärjestelmälle (Dey 2007)

Barletten ym. (2008) mukaan ISO 27001 -standardin integrointi osaksi yrityskulttuuria voi toimia IT-prosessien harmonisoinnin lisäksi myös suosituksen tavoin. Deyn (2007) mukaan ISO 27001 -standardin hyödyntämisen lisäksi yritysten tulee huomioida erilaiset alakohtaiset vaatimukset ja säännöt unohtamatta auditointiin liittyviä standardeja paremman tietoturvallisuuden takaamiseksi.

3.7 Yhteenveto

Kuten jo aikaisemmissa kappaleissa on tullut ilmi, tietoturva on yksi eniten epäilyksiä herättävistä pilviteknologian osa-alueista. Teknologian kehittyessä ja tietojen ollessa hajautettuna ympäri maailmaa tietojen suojaamiseen tulee erityisesti panostaa.

Pilviteknologian kannalta tietoturvan keskeisimpiä asioita ovat tiedon eheys, luottamuksellisuus ja käytettävyys sekä pääsynvalvonnan hallinta yhdessä kiistattomuuden kanssa. Palvelurakenteinen tietojenkäsittely on ulkoistettua ja näin ollen kolmannen osapuolen läsnäolo lisää tietoturvariskejä. Kaufmanin (2009) mukaan hajautettuihin tietojärjestelmiin liittyy muutenkin aikaisempaa enemmän tietoturvauhkia. Saatavuus on keskeisessä osassa pilviteknologiaa ja näin ollen ongelmatilanteissa myös merkittävin riski asiakasorganisaatiolle.

Tietoturvallisuuden takaamiseksi ja tietoturvariskien minimoimiseksi on kehitetty erilaisia standardoituja menetelmiä, joiden avulla pyritään ottamaan erityisellä tavalla huomioon turvallisuuteen liittyvät tekijät järjestelmäkehityk-

sessä. Ohjelmistoprosessin menestyksen kannalta on tärkeää huomioida tietoturvan merkitys mahdollisimman aikaisessa vaiheessa kehitysprosessia.

Henkilökohtaisia tai arkaluontoisia tietoja käsittelevillä järjestelmillä on usein ennalta määrättyjä turvallisuusvaatimuksia. Melladon ym. (2010) mukaan tietojärjestelmien turvallisuusvaatimukset täytetään valitettavan usein ainoastaan lain vaatimien vähimmäisvaatimusten mukaan. Turvallisuusvaatimuksien yksityiskohtainen määritteleminen auttaa myös turvallisuusmenetelmien nimeämisessä.

Tietoturvan ja tietosuojan kehittämisessä on mahdollista hyödyntää standardeja. Yksi merkittävimmistä tietoturvaan liittyvistä standardeista on ISO 27000 -standardisarja. ISO 27001 ja ISO 27002 -standardien avulla yrityksessä on mahdollisuus suunnitella ja ottaa käyttöön tietoturvallisuuden hallintajärjestelmä.

Tietoturvan pettäminen johtaa tilanteeseen, jossa arkaluontoista tietoa joutuu vääriin käsiin. Tätä taustaa vasten on aiheellista pohtia, tulisiko pilvipalveluiden suunnittelu ja toteuttaminen huomioida osana yritysten riskienhallintaa. Tietoturvan vaarantuminen voi olla merkittävä riski liiketoiminnalle. Tietoturvan ja tietosuojan vaarantumisen riskeihin on mahdollista varautua ennalta. Seuraavassa luvussa käsitellään liiketoiminnan riskienhallintaan liittyviä asioita pilviteknologian kontekstissa.

4 RISKIT JA NIIDEN HALLINTA

Riskienhallinta on tärkeä osa liiketoimintaa ja keskeisessä osassa myös tässä tutkielmassa. Tässä luvussa riskienhallintaa käsitellään ensin yleisellä tasolla koskien informaatioteknologiaa ja myöhemmin koskien erityisesti pilviteknologiaa ja pilvipalveluita. Tutkimusongelmaa ja empiiristä osaa silmällä pitäen luvussa käsitellään myös tavallisista riskienhallintamenetelmistä eroavia tapoja pienentää riskejä. Näistä menetelmistä käsitellään palvelutasosopimusten, teknisen toimivuuden ja laadun sekä kypsyysmallien potentiaalia riskienhallinnan osa-alueina. Luvun lopussa esitellään keskeisiä standardeja aihepiiriin liittyen. Kohdan 4.6 Yhteenveto-kappaleessa kerrataan luvun keskeisimmät osa-alueet.

4.1 Yleistä informaatioteknologian riskienhallinnasta

Ohjelmistokehityksen riskienhallinnan tarkoituksena voidaan pitää Boehmin (1991) määritelmän mukaan menestyksen kanssa riippuvuussuhteessa olevien riskipitoisten tekijöiden formalisointia valmiiden periaatteiden ja käytäntöjen avulla. Erilaisten tekniikoiden ja ohjeiden avulla pyritään tunnistamaan, analysoimaan ja päihittämään ohjelmistokehitykseen liittyviä riskejä (Ropponen, 1999, s. 68). Sommervillen (2007, s. 104) mukaan riskienhallinnan tulisi olla dokumentoitua jo projektisuunnitelmasta lähtien sisältäen analyysin riskien toteutumisesta aiheutuvista seurauksista. Tehokkaan riskienhallinnan avulla voidaan selviytyä ongelmatilanteista välttäen merkittävät taloudelliset tappiot ja aikataululliset viivästykset.

Sommerville (2007, s. 104) jakaa ohjelmistokehitysprosesseihin liittyvät riskit kolmeen kategoriaan: projektiriskeihin, tuoteriskeihin ja liiketoimintariskeihin. Projektiriskeihin kuuluvat riskit, jotka vaikuttavat projektin aikatauluun ja resursseihin. Tuotteisiin liittyvät riskit taas vaikuttavat lopullisen tuotteen laatuun tai suorituskykyyn. Kolmannessa kategoriassa liiketoimintariskeihin lukeutuvat riskit, jotka vaikuttavat ohjelmistoja kehittäviin tai hankkiviin organisaatioihin. Sommerville (2007, s. 105) pitää ohjelmistokehitykseen liittyvää

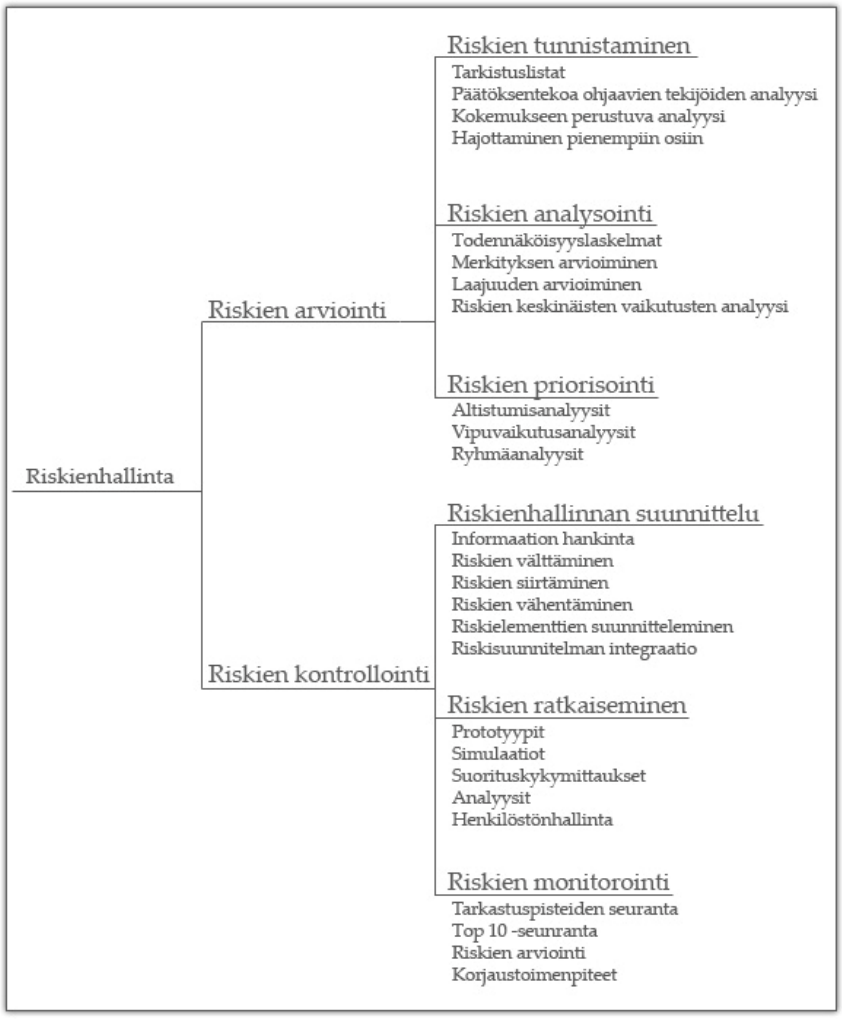
riskienhallintaa erityisen tärkeänä projektien kohdatessa monia odottamattomia tekijöitä: heikosti laadittuja vaatimuksia, resurssien allokoinnin haasteita, asiantuntijariippuvuutta ja asiakkaan tarpeiden mukaan vaihtuvia vaatimuksia.

Projektien onnistuminen on usein kiinni myös oikeanlaisesta johtamisesta. McManuksen (2004) mukaan tutkimusten perusteella on havaittu projektien epäonnistuvan hallinnollisten seikkojen takia useammin kuin teknisten ongelmallisuuksien. Boehm (1991) on samalla tapaa havainnut menestyneiden projektipäälliköiden ottaneen riskienhallinnan huomioon erityisellä tavalla ja tehdyissä päätöksissä on huomioitu riskien mahdolliset toteutumiset.

Sommervillen (2007, s. 106) mukaan riskienhallinta on neliosainen prosessi, jossa riskien tunnistaminen, analysointi, suunnittelu ja monitorointi on keskeistä. Boehm (1991) jakaa riskienhallintaprosessin alkujaan kaksiosaiseksi puumalliksi. Ensimmäinen osa pitää sisällään riskien arvioinnin ja toinen osa riskien kontrolloinnin. Puumalli jakautuu aina pienempiin osiin (kuvio 4).

Boehmin (1991) riskienhallinnan osa-alueista riskien tunnistaminen on riskien arvioinnin ensimmäinen osa-alue, joka tuottaa listan projektin onnistumista mahdollisesti uhkaavista tekijöistä. Tyypillisiä työkaluja ovat tarkistuslistojen lisäksi erilaiset päätöksien tekoa ohjaavien tekijöiden arvioinnit, kokemukseen perustuvat vertailut sekä osa-alueiden purkaminen pienempiin osiin. Sommervillen (2007, s. 107) vastaavanlaisen riskienhallintaprosessin riskien tunnistamisvaiheesta voidaan löytää muutamia erilaisia riskitekijöitä. Näitä ovat mm. teknologiaan, projektihenkilöstöön, organisaatioympäristöön, vaatimuksiin tai erilaisiin arviointeihin liittyvät riskitekijät.

Riskien analysointivaihe pitää sisällään riskien toteutumisen todennäköisyyslaskelmat sekä riskien merkityksen ja laajuuden arvioinnin. Tässä vaiheessa arvioidaan myös useiden riskien keskinäisten vaikutusten merkitys. (Boehm, 1991.) Tämänkaltaisen analysointivaiheen toteuttaminen onnistuu parhaiten kokeneilta projektijohtajilta, joilla on merkittävästi aikaisempaa kokemusta erilaisista projekteista. Riskien analysoinnin tulee olla jatkuvaa, sillä riskeistä saatava tieto saattaa muuttua projektin edetessä. (Sommerville, 2007, s. 108.) Boehm (1988) ehdottaa top-10 –listan tekemistä riskien laajuuden ja toteutumistodennäköisyyden perusteella.



KUVIO 4 Boehmin (1991) riskienhallinnan osa-alueet

Kolmantena osa-alueena Boehmin (1991) riskienhallintaprosessissa on riskien priorisointi. Riskien priorisointi tapahtuu analysoimalla riskeille altistumista sekä riskien vähentämisen vipuvaikutuksia. Myös erilaiset ryhmässä tehtävät analysointimenetelmät, kuten Delphi-arviointi liittyvät tähän vaiheeseen riskienhallintaprosessia. Tyypillisesti riskien priorisointi -vaiheen tuloksena saadaan järjestetty lista tunnistetuista ja analysoiduista riskeistä. (Boehm, 1991.)

Riskienhallinnan toinen osa, riskien kontrollointi liittyy riskien arvioinnin pohjalta riskien minimoimiseksi tehtäviin jatkotoimenpiteisiin. Boehmin (1991) riskien kontrolloinnin osa-alueita ovat riskien hallinnoinnin suunnittelu, riskien ratkaiseminen ja riskien monitorointi. Riskien hallinnoinnin suunnittelu sisältää tyypillisesti jokaisen riskin kohdistamisen osaksi projektia ja jokaisen riskin yksilöllisen suunnitelman riskin käsittelystä. Tyypillisiä työkaluja ovat mm. tarkistuslistat ja perinteiset riskienhallinnan suunnitelmien luonnokset. Riskien

ratkaiseminen nimensä mukaisesti pitää sisällään toiminnon, jonka avulla riskikohteet poistetaan tai ratkaistaan. Tämänkaltaisessa toiminnassa voidaan hyödyntää esimerkiksi prototyyppejä ja simulointia. Riskien kontrolloinnin viimeinen vaihe liittyy riskien monitorointiin. Monitorointi on tyypillisesti riskien kartoittamista toistuvasti ja niiden yhdistämistä erilaisiin ratkaisumalleihin. Näin projektin kehittyessä varmistetaan myös riskien kontrollointi. (Boehm, 1991.)

4.2 Ulkoistamiseen liittyvät riskit pilvipalveluissa

Tehokas riskienhallinta edellyttää liiketoiminnan riskien tunnistamista ja analysointia. Pilvipalveluille tyypillinen palvelujen ulkoistaminen on merkittävä riskitekijä. (Hoque, 2010.) Samaratin ym. (2010) mukaan ulkoistaminen koetaan kustannustehokkaana, tiedon saatavuutta edistävänä tekijänä sekä vaihtoehtona yrityksen sisäiselle tietojenkäsittelylle. Tietojenkäsittelyn ulkoistamiseen liittyy kuitenkin useita riskitekijöitä. Käyttäjien, pilvipalveluita ostavien ja pilvipalveluita tarjoavien ollessa ulkoistamisen eri osapuolina tietojen suojaamisen, eheyden ja oikeellisuuden sekä tietokantahakujen suorittamisen ja pääsynvalvonnan tulee olla tarkasti määriteltyä (Samarati ym., 2010). Edellä mainituista vaatimuksista voidaan sopia palvelutasosopimuksin. Sopimukset eivät kuitenkaan ratkaise kaikkia kolmannen osapuolen läsnäoloon liittyviä ongelmia.

Jordanin (2006, s. 194) mukaan palvelutasojen täyttämisen lisäksi ulkoistamispalvelua tarjoavien yritysten tulisi olla oikealla tapaa johdettuja, suhtautua joustavasti muuttuviin tarpeisiin, sisäistää ja hyödyntää toimialan standardit. Tietojenkäsittelypalveluiden ulkoistamiseen liittyy oleellisesti myös riski palveluntarjoajan kyvyttömyydestä toimittaa sovittu projektipalvelu (Jordan, 2006, s. 195). Jordan (2006, s. 195) on listannut tietojenkäsittelyn ulkoistamiseen liittyviä riskejä, joita ovat esimerkiksi:

- samanlaisena pysynyt palvelutasosopimus liiketoiminnan vaatimusten muututtua
- riippuvuus vanhentuneesta teknologiasta
- liian monta standardia ja ratkaisemattomia ongelmia vanhojen järjestelmien kanssa.
- haluttomuus ottaa käyttöön molemmille osapuolille hyödyllisiä parannuksia

Pilvipalveluita hankittaessa tietojen sirpaloituminen eri puolille maailmaa voi olla merkittävä riski erilaisten sopimusoikeudellisten tekijöiden näkökulmasta. Kolmannen osapuolen rooli ja kohdemaahan liittyvät epäselvyydet lisäävät ulkoistamisen riskejä. Chowin ym. (2009) mukaan esimerkiksi lainsäädäntöön ja tietojen kontrollointiin liittyy vaikeaselkoisuutta. Tietojen kontrollointi edellyttää pilvipalveluntarjoajalta läpinäkyvyyttä, mutta tietojenkäsittelyn auditointiin

hajautetussa, ympäri maailmaa levittyvässä tietojenkäsittelykäytännössä liittyy joka tapauksessa paljon haasteita (Chow ym., 2009). Taftin (2005) mukaan tietojen kontrollointi tietojenkäsittelyä ulkoistettaessa on äärimmäisen haasteellista maakohtaisten lainsäädäntöjen ja säännösten puutteellisuuden takia – kohdemaassa ei välttämättä ole säädetty lakia esimerkiksi tietosuojan turvaamiseksi tai sitten laista ei piitata korruption vallitessa. Tämän takia Aundhen & Mathewin (2009) mukaan ulkoistamisen riskeihin valvonnan vaikeudesta johtuen liittyy myös alisuorittamista ja suoraa tietojen varastamista tai arkaluontoisten tietojen kauppaamista esimerkiksi kilpailijoille.

4.3 Vaihtoehtoisia tapoja minimoida ja hallita riskejä

Pilvipalveluihin liittyviä riskejä voidaan pyrkiä minimoimaan monella tapaa, mutta se voi olla haasteellista. Ropposen (1999) mukaan alihankintaan ja ulkoistamiseen liittyvät riskienhallinnan harjoitteet eivät suoraan vaikuta alihankinnan kontrollointiin tai riskien vähenemiseen. Ropposen (1999) mukaan tämä voi kertoa myös riskienhallintametodien kapea-alaisesta käytöstä. Tässä tutkielmassa käsitellään kolmea potentiaalista tapaa, joilla pilvipalveluihin liittyviä riskitekijöitä voidaan hallita tai vähentää.

Pilvipalveluihin liittyviä riskejä voidaan mahdollisesti minimoida ja hallita esimerkiksi palvelutasosopimuksin, teknisellä toimivuudella ja laadulla sekä kypsyysmallien avulla. Seuraavissa kappaleissa käsitellään kolmea edellä mainittua tapaa pienentää riskejä liittyen pilvipalveluiden kehittämiseen ja tarjoamiseen. Teoreettinen käsittely luo pohjan edellä mainitulle oletukselle ja yhdessä haastatteluista saadun aineiston kanssa voidaan tehdä päätelmiä, pienentävätkö edellä mainitut keinot riskejä. Vastaus tähän alatutkimusongelmaan käsitellään luvussa 8.

4.3.1 Sopimukseen perustuva palvelu

Pilvipalveluihin, kuten myös moniin muihin palveluihin liittyvä palvelutasosopimus sitoo palveluntarjoajan asiakkaaseen ja määrittää palveluun liittyvät osatekijät liiketoimintatavoitteiden täyttämiseksi (Goo, Kim & Cho, 2006). Goon ym. (2006) mukaan sopimuksen tekemisellä on vastuiden selventämisen lisäksi merkittävä rooli luottamuksen, viestinnän lisäämisessä sekä konfliktien vähentämisessä. Kandukuri ym. (2009) lisäävät palvelutasosopimusten tarkoituksiin myös monimutkaisten asioiden yksinkertaistamisen ja epärealististen odotusten poistamisen. Tällä tavoin syntyy ymmärrettävä palvelukokonaisuus, joka on molempien osapuolten kannalta hyödyllinen.

Tarkasti laadittu sopimus selventää molemmille osapuolille palvelukokonaisuuden sisällön. Merkittävimpänä osana voidaan pitää palveluiden määrittelyosaa. Yleisten ja räätälöityjen palveluiden määrittelyn tulisi olla tarkasti toteutettu, jotta tilaava taho tietää tarkalleen, mistä ja minkälaisesta palvelusta se

maksaa. Jotta palvelun laatua voidaan tarkkailla ja mitata, tulee sopimuksesta käydä ilmi myös suorituskyky erilaisine metriikoineen. Kolmas merkittävä osa, joka tulisi myös käydä ilmi sopimuksesta, on ongelmatilanteiden hallinta. Tyypillisesti palveluntarjoaja esittää suunnitelman, jossa on selvitys niistä toimenpiteistä, jotka suoritetaan ennalta odottamattoman tilanteen ilmaantuessa. Edellisten osa-alueiden lisäksi sopimuksissa on erittelyt osapuolten vastuista, korvaustilanteista ja sopimuksen päättämisestä. (Kandukuri ym., 2009.)

Palvelutasosopimusten avulla vastuu erilaisista virhetilanteista konkretisoituu palveluntarjoajan tai asiakkaan kohdalle. Pilviteknologiaan liittyvien asiakasosapuolen virhetilanteiden lukumäärän on havaittu pienenevän merkittävästi verrattuna aikaisempiin tietojenkäsittelyparadigmoihin (Sripanidkulchai ym., 2010). Green (2006) liittää kokemuksen laadun osaksi palvelujen toimitusta ja näin ollen hänen mukaansa myös palvelutasosopimusten tulisi olla luonteeltaan mahdollisimman dynaamisia. Sopimukseen perustuva pilvipalveluiden kehittäminen ja tarjoaminen on vahvasti myös tietoturvallisuuteen liittyvä tekijä.

Tietoturvallisuutta ei voida kuitenkaan taata ainoastaan sopimusten avulla, vaan tarvitaan myös hyvin toteutettu ja toimiva tekninen tietojenkäsittelyratkaisu (Rimal ym., 2009).

4.3.2 Teknisesti toimiva ja laadukas palvelu

Kehitettäessä ja tarjottaessa pilvipalveluita tekninen toimivuus on ensisijaisen tärkeää. Teknisen toimivuuden takaamiseksi riskit huomioiva toiminta voidaan jakaa ennakoiviin ja reaktiivisiin toimintamalleihin. Jensenin ym. (2009) mukaan pilvipalveluiden teknistä toimivuutta käsiteltäessä on tärkeintä ottaa huomioon verkkopalveluihin liittyvä turvallisuus. Tähän liittyvät oleellisesti tiedon luottamuksellisuus, eheys ja käytettävyys.

Tiedon suojaaminen ja salassapito on mahdollista toteuttaa usealla eri tavalla pilviteknologiassa. Itani, Kayssi & Chehab (2009) ehdottavat tiedon suojaamisen myymistä palveluna, joka koostuu erilaisista metodeista kryptografiaa ja luotettavia kolmansia osapuolia hyödyntäen. Chow ym. (2009) esittävät pilvessä olevan tiedon suojaamiseksi älykkään datan menetelmän, jossa haluttu tietosisältö aukeaa käyttäjälleen ainoastaan, jos data havaitsee ympäristön turvalliseksi. Wangin, Lin, Owensin & Bhargavan (2009) mukaan turvalliseen pilviteknologiaan liittyy olennaisesti vahva salaus skaalautuvalla avainhallinnolla, käyttöoikeuksienhallinta, tiedon elinkaaren hallinta sekä järjestelmien saatavuus ja suorituskyky.

Käyttöoikeuksienhallinta ja pääsynvalvonta ovat kriittisiä osa-alueita pilven turvallisuuden takaamisessa. Todennus ja valtuutus toteutetaan pilvessä usein Public Key -infrastruktuurin ja X.509 SSL -sertifikaatin avulla (Youseff ym. 2008). Pilviteknologian perustuessa ulkoisiin tietojenkäsittelyresursseihin käyttäjät kirjautuvat ohjelmistotasolla pilveen, jolloin käytettävänä rajapintana on usein tavallinen internetselain (Jensen ym., 2009). Näin ollen pilviteknologian turvallisuuteen linkittyy oleellisesti myös internetselainten kehittäminen tieto-

turvallisiksi. Internetpohjaisten pilvipalveluiden suojaamisessa XML-pohjaiset ratkaisut ovat usein melko tyypillisiä (Yildiz, Abawajy, Ercan & Bernoth, 2009). Myös erilaiset Single Sign on -kirjautumiset ovat mahdollisia pilviteknologialle (Pervez, Sungyoung & Young-Koo, 2010).

Sripanidkulchain ym. (2010) mukaan laajojen hajautettujen järjestelmien hyödyntämisen lisäksi pilviteknologiaan liittyvät oleellisesti myös saatavuuden ja ongelmanratkaisun näkökulmat. Saatavuuden turvaamiseksi pilviteknologiassa oleellisina osina ovat vaihtoehtoiset sisällöntoimitusverkostot, erilaiset kuormantasauskomponentit sekä automaattinen skaalaus. Edelliset saatavuutta turvaavat tekijät eivät välttämättä kuitenkaan riitä kokonaisen pilven kohdatessa ongelmatilanteen. Näin ollen olisi äärimmäisen tärkeää myös kehittää pilvien välistä saatavuutta pilvipalveluita tarjoavien tahojen liiketoimintojen häiriintymättä. (Sripanidkulchai ym., 2010.)

Saatavuuden vastakohtana voidaan pitää ongelmatilannetta, jossa pilvipalvelun käyttö estyy. Ongelmatilanteita varten pilvipalveluita tarjoavilla organisaatioilla tulisi olla jonkinlainen suunnitelma, kuinka palvelu saadaan mahdollisimman nopeasti takaisin saataville (Youseff ym., 2008). Kontion (2001) mukaan ongelmatilanteita varten laaditut toimintasuunnitelmat auttavat yritystä ratkaisemaan vaikean tilanteen ja toimivat ennalta suunniteltuina riskienhallintadokumentteina. Stoneburner, Goguen & Feringa (2002) pitävät riskienhallintadokumenttia työkaluna tunnistaa, raportoida ja ratkaista ilmentyneeseen ongelmaan liittyvät osa-alueet.

Hakala ym. (2006, s. 98) jakavat riskienhallintadokumentit toipumissuunnitelmaan ja valmiussuunnitelmaan. Toipumissuunnitelman avulla varaudutaan toimimaan tietyllä tapaa määrittelyvaiheessa löytyneiden riskien realisoituessa, kun taas valmiussuunnitelma on laajempi, poikkeustilanteita, kuten yhteiskuntaan tai ympäristöön liittyviä katastrofeja varten laadittu toimintasuunnitelma.

Tämän lisäksi pilviteknologian turvallisuutta on mahdollista parantaa läpinäkyvyyttä parantamalla, jolloin erilaiset auditoinnit ja pilvipalvelun monitorointi helpottuvat (Chow ym., 2009). Pearson & Charlesworth (2009) laajentavat läpinäkyvyyden koskemaan myös tavallisia kuluttajia, joiden tietoja pilvipalveluita ostavat organisaatiot käsittelevät. Vastuullinen pilvipalveluiden kehittäminen ja tarjoaminen on omiaan lisäämään luottamusta pilvipalveluita kohtaan (Pearson & Charlesworth, 2009).

Kolmas riskienhallintaan liittyvä metodi sekä menettelytapa, jonka avulla voidaan kehittää laadukkaita ohjelmistoja ja varmistaa palveluntarjoajan palveluiden laatu, on hyödyntää kypsyysmallien avulla saatavaa tietoa kohdeyrityksen prosesseista ja toiminnasta.

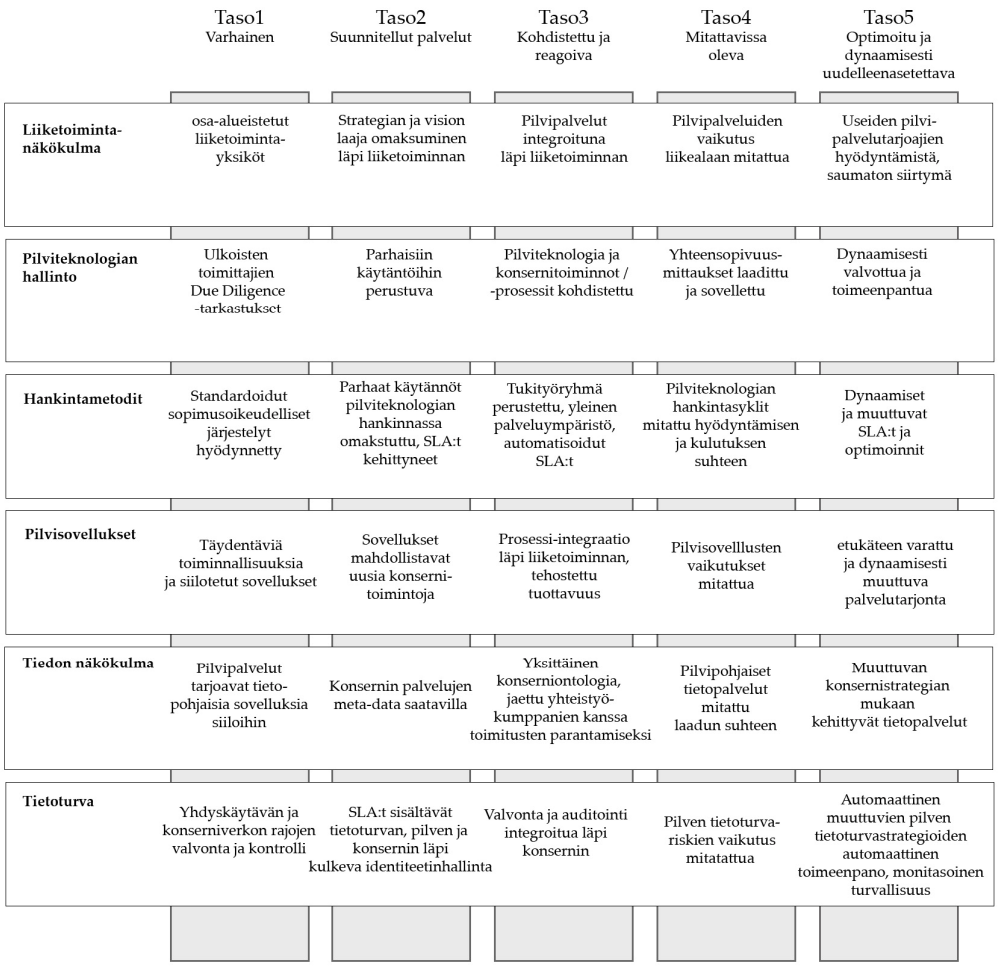
4.3.3 Kypsyysmallit

Ohjelmisto- ja sovelluskehityksen historiassa on monia esimerkkejä epäonnistuneista projekteista, joissa perustavanlaatuisena virheenä on ollut huonosti onnistunut projektinhallintaprosessi (Paulk, Curtis, Chrissis & Weber, 1993).

Projektinhallinnan kypsyysmalleja noudattamalla voidaan saada aikaan laadukkaampia ohjelmistoja, joiden avulla saatava tuotto paranee ja liiketoiminnan jatkuvuus on parempi (Kemerer & Paulk, 2009).

Kypsyysmallien tarkoituksena voidaan pitää paremman liiketoimintatuloksen aikaansaamista arvioimalla organisaation projektinhallinnan heikkouksia ja vahvuuksia, vertaamalla kypsyyttä kilpailijoihin sekä mittaamalla projektihallintatason ja saatujen tulosten riippuvuutta (Khoshgoftar ym., 2009). Münstermann & Weitzelin (2008) mukaan prosessien standardointi helpottaa ulkoistamisen onnistumista. Tiukentunut ohjelmistokehityskilpailu on lisännyt erilaisten projektinhallintastandardien kehitystä (Crawford, 2005). Vaikka on melko yleistä, että ohjelmistotalot kehittävät ja laativat omat sisäiset standardinsa ja toimintamallinsa, voidaan kehitystä tehostaa valmiiden menetelmien avulla, jotka sisältävät vankan perustan prosessikehitykselle (Schaffner & White, 1999).

Kuinka kypsyysmallit sopivat pilvipalvelujen kehittämiseen tai asiakasyrityksen arviointiin? Creesen, Hopkinsin, Pearsonin, & Shenin (2009) mukaan kypsyysmalleja on mahdollista hyödyntää konsernitasolla, jolloin otetaan huomioon erilaisia liiketoiminnan osa-alueita pilveä tai pilviä käytettäessä (kuvio 5). Creesen ym. (2009) mallin lisäksi pilviteknologiaan ja pilvipalveluihin on kehitelty muutamia muita kypsyysmalleja. Wardleyn (2008) kypsyysmallissa kypsyyttä voidaan määritellä esimerkiksi arkkitehtuurin joustavuudella, palvelutasosopimusten hyödyntämisellä, palveluntarjoajien vaihdettavuudella sekä kolmannen osapuolen vakuus- ja monitorointipalveluilla. Vaikka pilvien hyödyntäminen yrityksissä yleistyy jatkuvasti, pilviteknologiaan ja pilvipalveluihin liittyviä kypsyysmalleja ei ole vielä juurikaan esiintynyt tieteellisissä artikkeleissa.



KUVIO 5 Creesen ym. (2009) pilvipalveluiden kypsyysmalli

Kypsyysmallien avulla voidaan myös vertailla asiakasyritysten kypsyyttä tai esimerkiksi arvioida oman yrityksen prosesseja. Samalla tapaa pilvipalveluiden kehitysprosessien kypsyyttä on mahdollista arvioida laadittujen kypsyysmallien pohjalta. Seuraavissa kappaleissa käsitellään keskeisimpiä ohjelmisto-kehitykseen liittyviä kypsyysmalleja.

CMM ja sen johdannaiset

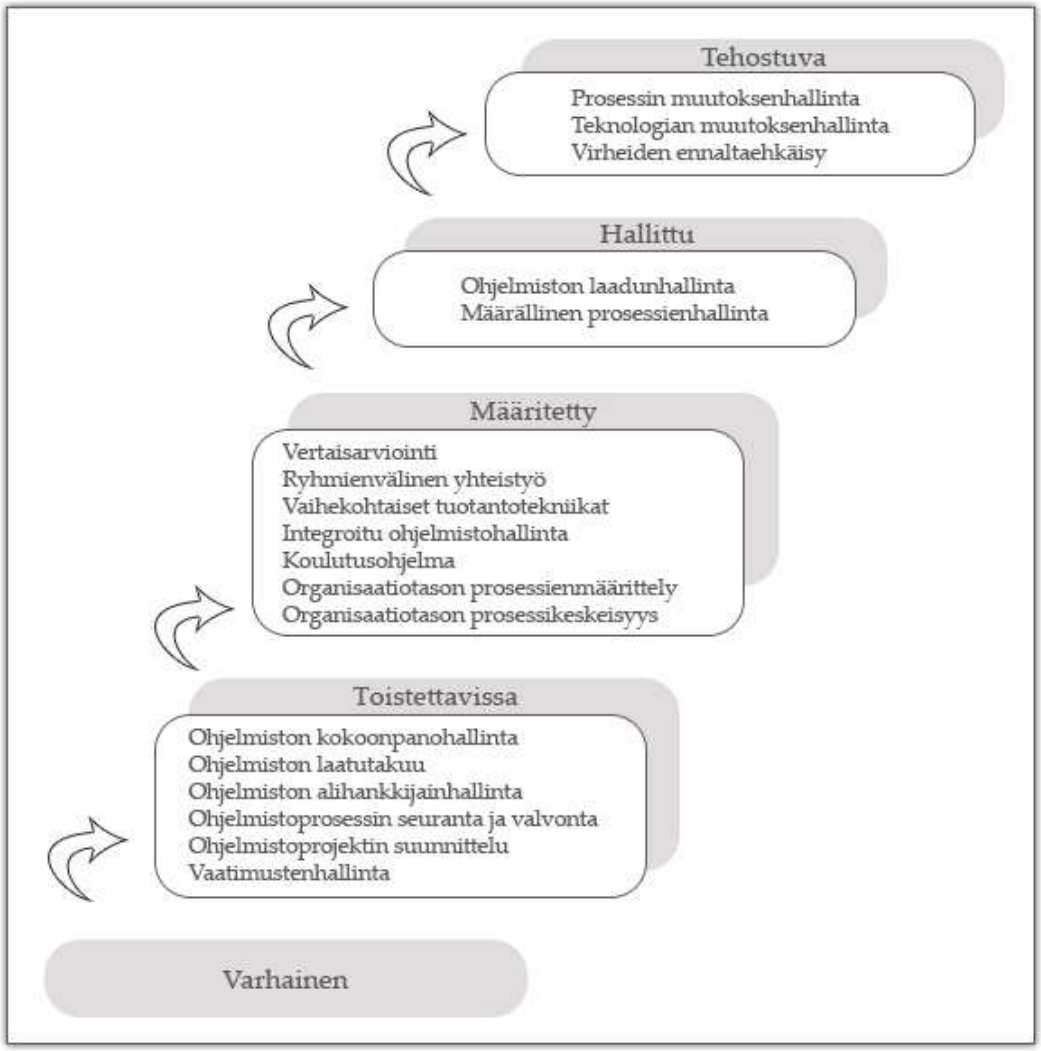
CMM, eli Capability Maturity Model, kehittiin SEI:n (Software Engineering Institute) projektissa U.S. Air Force:lle Carnegie Mellon –yliopistossa vuonna 1987 (Humphrey, 1989). SW-CMM (Capability Maturity Model for Software), jolla nimellä CMM-malli myös tunnetaan, on vanhin, tunnetuin ja eniten käytetty arviointimenetelmä (Komi-Sirviö, 2004). Paulkin ym. (1993) mukaan CMM on joukko erilaisia suositeltavia suoritteita avainasemassa olevien prosessien pa-

rantamiseksi. Lisäksi ne ovat omiaan parantamaan ohjelmistokehitystä sekä ylläpidon kyvykkyyttä.

CMM laadittiin parantamaan ohjelmistokehittäjien mahdollisuuksia kehittää ja ylläpitää ohjelmistoja. Yhtä lailla tarkoituksena oli parantaa ohjelmistoyritysten kyvykkyyttä kehittyä organisaationa ja näin saada parempaa tulosta aikaan niin liiketoiminnallisesti kuin laadullisesti. CMM-malli koostuu viidestä tasosta, jotka pitävät sisällään erilaisia ohjelmistokehitykseen liittyviä kypsyyden osa-alueita. Osa-alueita on selvennetty kuviossa 6. (Paulk ym., 1993.)

CMM:n perustavanlaatuisina osa-alueina voidaan pitää ohjelmistoprosessin kyvykkyyttä, suorituskykyä ja kypsyyttä. Paulkin ym. (1993) mukaan ohjelmistoprosessin kyvykkyytenä voidaan pitää niitä tavoitteita, jotka voidaan saavuttaa ohjelmistoprosessia seuraamalla. Aiemmin toteutettu projekti voi toimia kokemusta lisäävänä tekijänä seuraaville projekteille ja niin ikään lisätä kykyä saavuttaa tulevia päämääriä. Suorituskyky sen sijaan keskittyy saavutettuihin tavoitteisiin. Saavutetut tavoitteet verrattuna asetettuihin tavoitteisiin antavat ohjelmistoprosessille konkreettisen suorituskyvyn. Merkittävimpänä osa-alueena CMM-mallissa voidaan pitää kypsyyttä. Ohjelmistoprosessin kypsyys määräytyy kokonaislaajuudeltaan yksiselitteisesti määritellyn, hallitun, mitatun, kontrolloidun ja tehokkaan prosessin kautta. Kypsyys on näin ollen organisaation ohjelmistoprosessin monipuolisuutta yhdessä sen kanssa, miten koko organisaatio prosessin hyödyntää. (Paulk ym., 1993.)

CMM:n seuraaja, CMMI (Capability Maturity Model-Integrated), on laajempi kokonaisuus, johon liittyy ohjelmistokehityksen lisäksi myös tuotekehitys. CMMI:tä on mahdollista hyödyntää myös palveluiden laatimisessa, hallinnassa ja toimittamisessa. (SEI, 2010) Näin ollen se soveltuu riskienhallintatyökaluna myös pilviteknologiaan. Edellisten lisäksi CMMI pitää sisällään kaksi erilaista esitystä; asteittaisen mallin, joka on verrattavissa CMM:ään sekä jatkuvan mallin, jossa jokainen prosessi voi saada oman arvion kypsyyydestä. (Jokela, Siponen, Hirasawa & Earthy, 2006) CMMI sisältää kolme erilaista arviointimenetelmää, jotka vaihtelevat laajuudeltaan ja formaaliudeltaan (Komi-Sirviö, 2004).



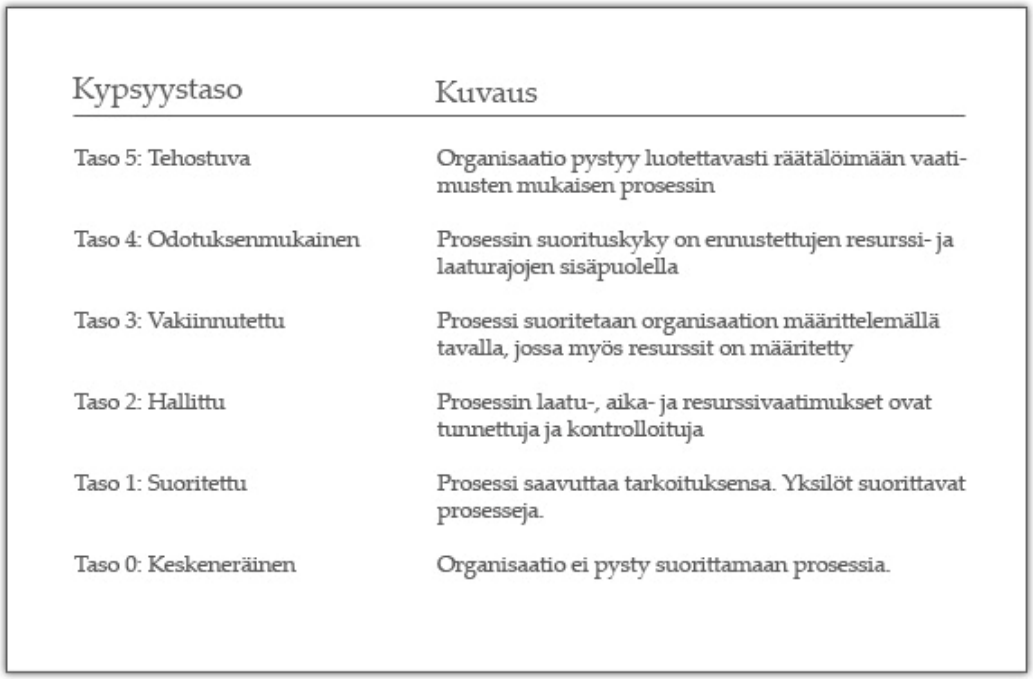
KUVIO 6 Paulkin ym. (1993) CCM-kypsyysmallin viisi tasoa

SPICE-malli

ISO/IEC 15504 -standardi tunnetaan myös nimellä SPICE, joka on prosessien arviointiin tarkoitettu kehysmalli (Ehsan, Perwaiz, Arif, Mirza & Ishaque, 2010). Ehsanin ym. (2010) mukaan SPICE-malliin kuuluvat arviointiprosessin lisäksi arviointimalli ja siihen liittyvät työkalut. Alun perin SPICE-malli kehitettiin CMM:n yhdistyessä sen johdannaismalleihin Trilliumiin ja Bootstrapiin. SPICE-mallia voidaan käyttää prosessien arvioinnin lisäksi myös niiden kyvykkyyden määrittämiseen. Erilaiset prosessiominaisuudet täyttämällä organisaatio voi saavuttaa parempia kypsyystasoja (kuvio 5). (Ehsan ym., 2010.)

SPICE-malli painottaa ohjelmistotekniikan prosessien, projektien ja liiketoimintaorganisaation merkitystä. Mallista on havaittavissa viisi erilaista prosessikategoriaa: asiakas-toimittaja-prosessi, tekninen prosessi, projektiin liittyvä prosessi, tukiprosessi ja organisaatioprosessi. Jokainen yksittäinen prosessi ar-

vioidaan kuusiportaisella järjestelmällä ja on näin ollen vertailukelpoinen muidenkin prosessien kanssa. (Wang ym., 1997.)



Kypsyystaso	Kuvaus
Taso 5: Tehostuva	Organisaatio pystyy luotettavasti räätälöimään vaatimusten mukaisen prosessin
Taso 4: Odotuksenmukainen	Prosessin suorituskyky on ennustettujen resurssi- ja laaturajojen sisäpuolella
Taso 3: Vakiinnutettu	Prosessi suoritetaan organisaation määrittelemällä tavalla, jossa myös resurssit on määritetty
Taso 2: Hallittu	Prosessin laatu-, aika- ja resurssivaatimukset ovat tunnettuja ja kontrolloituja
Taso 1: Suoritettu	Prosessi saavuttaa tarkoituksensa. Yksilöt suorittavat prosesseja.
Taso 0: Keskeneräinen	Organisaatio ei pysty suorittamaan prosessia.

KUVIO 7 SPICE-mallin kypsyystasot (Jokela ym., 2006)

SPICE-mallia voidaan pitää jatkuvana mallina ja tässä suhteessa vastakohtana asteittaisille malleille. Jokelan ym. (2006) mukaan jatkuvassa mallissa on kyse jokaisen prosessin arvioimisesta erikseen, kun taas asteittaisissa malleissa on kyse koko organisaation arvioinnista yhdellä kuvauksella. Aikaisemmin käsitelty CMM-kypsyysmalli on asteittainen malli.

4.4 Riskienhallintaan ja prosesseihin liittyviä standardeja

Standardeja on yleisesti mahdollista hyödyntää yrityksen riskienhallinnassa. Myös konkreettisesti riskienhallintaa käsitteleviä standardeja on kehitetty. Kansainvälisistä standardeista esimerkiksi ISO 27005 -standardi liittyy läheisesti riskienhallintaan (ISO 27005, 2008). ISO 27005 -standardi sisältää ohjeistuksen organisaation riskienhallintaan painottaen erityisesti tietoturvallisuuden hallintajärjestelmään liittyviä osa-alueita (Singh & Lilja, 2009). Singhin & Liljan (2009) mukaan varsinainen riskien arviointi jää organisaation päätettäväksi.

Riskienhallinnasta on tullut yhä enenevässä määrin osa informaatioteknologian prosesseja. Kontion (2001) mukaan osassa ohjelmistokehittäjille laadituista standardeista on huomioitu riskienhallinta, mikä kertoo riskienhallinnan ke-

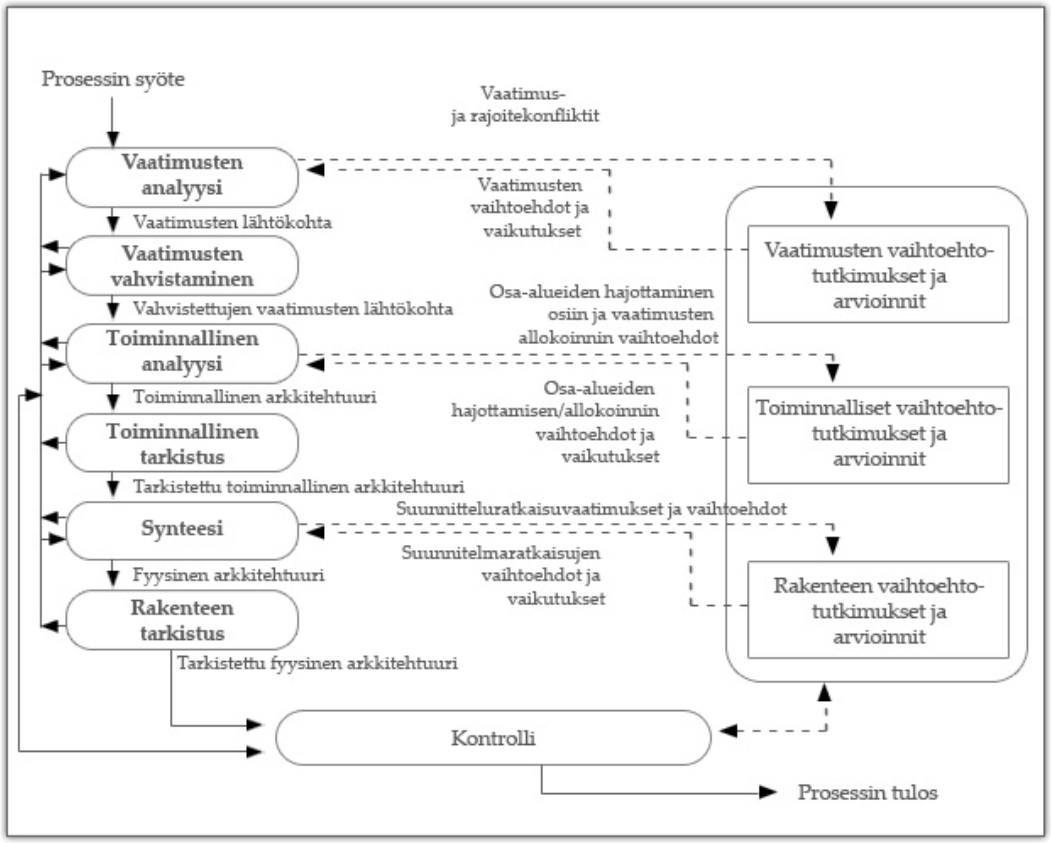
hittymisestä osaksi ohjelmistoyritysten systemaattista liiketoimintaa. IEEE:n ohjeistuksessa (2008) koskien ISO 90003 -standardin hyödyntämistä mainitaan myös riskienhallinta, niin järjestelmää kehittävän kuin järjestelmää hankkivan tahon näkökulmasta.

Yksi mainituista tavoista hallita riskejä on prosessiarviointi, jonka avulla voidaan saada käsitys järjestelmää kehittävän yrityksen prosessien kyvykkyydestä ja kypsyydestä. Järjestelmää kehittävän tahon näkökulmasta riskejä käsitellään osana projektin riskienhallintaa. Ensimmäisenä riskiryhmänä määritellään järjestelmän kriittisyyteen ja turvallisuuteen liittyvät osa-alueet. (IEEE:n ohjeistus, 2008) Riskienhallinta liittyy osin myös prosessistandardeihin. Osin myös prosessistandardeihin lukeutuva ISO/IEC 16085 -standardi sisältää riskienhallintaan liittyvän prosessikuvauksen tietojärjestelmän tai ohjelmiston hankkimiseen, toimittamiseen, kehittämiseen, operaatioihin ja ylläpitämiseen (ISO/IEC 16085, 2006). Standardi noudattaa yleisesti jo aiemmin käsiteltyä riskienhallintaprosessia. Asnarin, Morettin, Sebastianisin & Zannonen (2008) mukaan standardissa on kyse systemaattisesta, koko tuotteen tai palvelun elinkaaren kestävästä riskien tunnistamisesta, analysoinnista, käsittelemisestä ja seuraamisesta. Yrityksen kypsyyden ja riskienhallinnan kannalta tulee kiinnittää huomiota myös yrityksen sisäisiin prosesseihin.

Eräs merkittävimmistä ohjelmistoprosesseja koskevista standardeista lienee ISO/IEC 26702 -standardi. Standardi käsittelee järjestelmäkehitysprosessin soveltamista ja hallintaa (ISO/IEC 26702, 2007). Standardi sisältää seuraavanlaiset osa-alueet:

1. Laajuus, tarkoitus ja organisaatio
2. Huomautukset
3. Terminologia ja akronyymit
4. Yleiset vaatimukset
5. Elinkaaren vaiheet
6. Järjestelmäkehitysprosessi

Standardin merkityksellisin osa on viimeisenä mainittu järjestelmäkehitysprosessi. Järjestelmäkehitysprosessi koostuu kahdeksasta alaprosessista: vaatimusten analyysistä, vaatimusten vahvistamisesta, toiminnallisesta analyysista, toiminnallisesta vahvistamisesta, synteesistä, suunnittelun varmennuksesta, järjestelmäanalyysistä ja kontrollista (kuvio 8).



KUVIO 8 ISO/IEC 26702 -standardin mukainen järjestelmäkehitysprosessi

Evansin ym. (2010) mukaan standardia on hyödynnetty aiemmin ainoastaan suurissa avaruushankkeissa ja sotilaallisia hankintoja tehtäessä. Viime vuosina standardin käyttö on alkanut levitä myös tavalliseen liiketoimintaan. Standardin hyödyntäminen on Evansin ym. (2010) mukaan yksi tapa kasvattaa liiketoiminnan arvoa laajoja järjestelmiä kehittävien yritysten keskuudessa.

Toinen merkittävä prosessistandardi on ISO/IEC 12207 -standardi. Standardi on perustavanlaatuinen ohjelmistokehitysstandardi, joka sisältää kehysmallin ohjelmiston elinkaaren prosesseille tarkasti määriteltyine termeineen (ISO/IEC 12207, 2008). Horien ym. (2008) mukaan ISO/IEC 12207 -standardin avulla voidaan käynnistää joukko prosesseja, jotka tehostavat ohjelmiston toiminnallisuutta, luotettavuutta, ylläpidettävyyttä, tuottoisuutta, turvallisuutta ja muita laatutekijöitä. Baldassarren ym. (2009) mukaan standardi helpottaa hankkijoiden, tuottajien ja muiden sidosryhmien välistä ja keskinäistä kommunikaatiota. Prosessikehitystyökaluna ISO/IEC 12207 -standardi on myös verrattavissa aikaisemmin käsiteltyihin kypsyysmalleihin (Baldassarre ym., 2009).

4.5 Muut standardit ja kehysmallit

Standardien kehittäessä yleisesti tuotteiden ja prosessien laatua on myös kehitetty standardeja, jotka painottuvat nimenomaan laadun hallintaan ja parantamiseen. Laadun ollessa melko vaikeasti määriteltävissä ISO ja IEEE ovat määritelleet laadun melko samalla tapaa tuotteen tai palvelun kyvyksi täyttää sille asetetut odotukset (Al-Kilidar, Cox & Kitchenham, 2005). Tässä tutkielmassa laatu rajataan koskemaan tuotteiden ja palveluiden osa-alueita toimittajan näkökulmasta eikä niinkään asiakkaan kokemukseen perustuvaksi asiaksi. Tietojenkäsittelyyn sovellettavissa olevia laatustandardeja on muutamia, joista tässä kappaleessa käsitellään tutkielman kannalta tärkeimpiä.

ISO 9000 -standardi julkaistiin vuonna 1987 ja se on yksi laajimmin levinneistä laatustandardeista; 2007-vuoden loppuun mennessä standardia oli sertifioitu yli 950000 kertaa, 161 eri maassa (Yongqing & Jiatao, 2009) ja (Barlette & Fomin, 2008). ISO 9000 -standardi on osa standardisarjaa, joka sisältää joukon vaatimuksia laadunhallintajärjestelmälle (ISO 9000, 2010). Standardisarjaan kuuluu kolme standardia: ISO 9000-, ISO 9001- ja ISO 9004-standardit (Hoyle, 2007, s. 80). ISO 9000 -standardi määrittää perusperiaatteet ja sanaston muille sarjan standardeille, kun taas ISO 9001 -standardi toimii vaatimusmäärittelynä laadunhallintajärjestelmälle, joka on sertifioitavissa merkkinä asiakastyytyväisyyteen panostavasta organisaatiosta. Nämä kaksi standardia pitävät sisällään kymmeniä määritelmiä, osa-alueita, lausekkeita ja yli 250 vaatimusta, jotka organisaation tulee täyttää sertifioinnin saadakseen. ISO 9004 -standardi täydentää edellisiä standardeja sisältäen ohjeita, joiden avulla organisaatio voi kehittää suorituskykyään. (Hoyle, 2007, s. 81.) Hoylen (2007, s. 78) mukaan standardisarjassa on ennen kaikkea kyse tyytyväisistä asiakkaista; standardin ensisijaisena tarkoituksena on kehittää organisaatioiden kykyä täyttää asiakkaiden tarpeet ja vaatimukset.

ISO 9000 -sarjan standardeja on mahdollisuus hyödyntää myös järjestelmäkehityksessä (Wang ym., 1997). Tähän tarkoitukseen on laadittu erillinen standardi, ISO/IEC 90003, joka ohjeistaa 9001-standardin käytöstä järjestelmäkehityksessä (ISO/IEC 90003, 2010). ISO 90003 -standardia voidaan hyödyntää laajasti eri tilanteissa; järjestelmää hankittaessa, tarjottaessa, kehitettäessä, käytettäessä ja ylläpidettäessä (IEEE:n ohjeistus, 2008).

ISO 9000 -sarjan lisäksi on kehitetty mm. ohjelmistotuotteiden laatua koskeva ISO/IEC 9126 -standardi sekä palvelujen laatua koskeva ISO/IEC 13236 -standardi. ISO/IEC 9126 -standardi on neliosainen standardi, jonka ensimmäiset kolme osaa perustuvat ohjelmistotuotteen laadun määrittelemiseen ja arvioimiseen. Neljäs ja viimeinen osa pitää sisällään käyttäjäarvion laadun mittarina. Standardin ensimmäisessä vaiheessa pyritään arvioimaan ohjelmiston laatua — tällöin arvioidaan toiminnallisuutta, luotettavuutta, käytettävyyttä, suorituskykyä, ylläpidettävyyttä ja siirrettävyyttä. Toisessa vaiheessa arvioinnin kohteena on käytön laatu. Tällöin arvioidaan tehokkuutta, tuotteliaisuutta, turvallisuutta ja tyydyttävyyttä. (Al-Kilidar ym., 2005.) ISO/IEC 9126 -standardista

on olemassa uudempi versio ISO/IEC 9126-1, jonka käyttöä on ohjeistettu ISO/IEC 25001:2007 -standardissa (ISO/IEC 25001, 2010).

Palvelujen laatuun keskittyvä ISO/IEC 13236 -standardi määrittelee terminologian ja useita käsitteitä palvelun laadun takaamiseksi (Jean, Losavioy, Matteoy & Levyz, 2010). Jeanin ym. (2010) mukaan standardiin liittyvät käsitteet ovat pitkälti aika-, kapasiteetti-, luotettavuus- ja turvallisuussidonnaisia. Standardin avulla voidaan arvioida esimerkiksi turvallisuuden kategoriaan liittyviä käsitteitä ”pääsynvalvonta” ja ”tiedon suojaaminen”.

Edellä käsiteltyjen laatustandardien lisäksi on olemassa joukko muita tietojenkäsittelyyn liittyviä standardeja, kehysmalleja ja käytänteitä, joista seuraavaksi pienimuotoinen esittely.

Standardeista ja kehysmalleista ensimmäisenä on Common Criteria -turvallisuusarvio. Common Criteria -arviointi perustuu joukkoon toiminnallisia turvallisuusvaatimuksia ja toimii näin vakuutena hankittavalle tai tarjottavalle tuotteelle (Common Criteria, 2009). Arviointimenetelmä perustuu kansainväliseen standardiin ISO/IEC 15408 ja on tarkoitettu laaja-alaisesti informaatioteknologian tuotteiden arviointiin; kortinlukijalaitteista aina laajoihin tietojärjestelmiin ja tietokantoihin (Taguchi, Yoshioka, Tobita & Kaneko, 2010). Taguchin ym. (2010) mukaan kyseessä on kolmiosainen arviointikokonaisuus, jossa ensimmäinen osa käsittelee terminologiaa ja metodologiaa, toinen osa turvallisuuteen liittyviä toiminnallisia vaatimuksia ja kolmas turvallisuuden vakuusvaatimuksia.

Toisena, tutkielman kannalta tärkeänä, tietojärjestelmien turvallisuuden arviointimenetelmänä voidaan pitää tietosuojan merkitykseen perustuvaa arviointimenetelmää. Rahoitusalan järjestelmiä koskeva arviointimenetelmä, ISO 22307 -standardi on saavuttanut kansainvälisen standardin aseman. Standardi on laadittu ensisijaisesti tietosuojaan liittyvien riskitekijöiden arviointimenetelmäksi ja työkaluksi kehitettäviä rahoitusalan järjestelmiä varten (ISO 22307, 2008). Wrightin ym. (2010) mukaan PIA:t (Privacy Impact Assessment) ovat kehittyneet vuodesta 1995 lähtien joko yleisenä vastalauseena hallitusten ja yritysten tietosuojaa heikentäville toimille tai yritysten rationaalisena, hallinnollisena tekniikkana pyrkiä ottamaan huomioon tietosuojan merkitys strategisena osana riskienhallintaa.

Käsiteltävistä kehysmalleista tunnetuin lienee informaatioteknologian palveluiden hallintaan liittyvä ITIL (Information Technology Infrastructure Library). ITIL perustuu ohjeistukseen, jonka avulla organisaatiot voivat parantaa IT-palveluitaan ja näin ollen parantaa yrityksen liiketoimintaa (Arraj, 2010). IT-palveluiden hallinnan kehysmalli jakautuu viiteen osaan: palvelustrategiaan, palvelusuunnitteluun, palvelumuutokseen, palvelutoimintaan ja jatkuvaan palveluiden kehittämiseen. ITIL-mallin rakenne on laadittu niin, että jokaista viittä osa-aluetta käsitellään ikään kuin palvelun elinkaaren eri osina. Tämän lisäksi jokaisessa osa-alueessa on määritelty osa-alueen merkitys, tärkeimmät käsitteet, tärkeimmät prosessit ja toiminnot sekä tärkeimmät roolit ja vastuut joitain poikkeuksia lukuun ottamatta. Esimerkiksi palvelutoiminnan osa-alueessa on määritetty tarkemmin riskienhallinnallisia osa-alueita. (ITIL Introduction, 2007.)

Zhangin, Wangin, Dingin & Zongin (2009) mukaan ITIL on laajasti omaksuttu kehysmallin vaikuttaessa positiivisesti liiketoimintatuloksiin. Tuloksia ovat mm. kustannussäästöt, tehostunut suhdetoiminta, kehittynyt asiakastyytyväisyys ja parantunut kykyjen hyödyntäminen.

Viimeisenä käsiteltävänä turvallisuuden ja tietosuojan edistämisen käytänteenä on tietojärjestelmien tai ohjelmistojen tarkistus sekä auditointi. Tähän tarkoitukseen on kehitetty IEEE:n standardi 1028 (IEEE Std 1028, 2008). Mishran & Mishran (2007) mukaan ohjelmistojen tarkistus jakautuu kolmeen vaiheeseen: yksilölliseen analyysiin, tiimianalyysiin ja korjausvaiheeseen. Ohjelmistojen tarkistus on kokonaislaadun kannalta kriittinen osa-alue, ja aikaisessa vaiheessa havaitut ongelmat voivat ehkäistä merkittäviä kustannuksia myöhemmissä vaiheissa (Humayun, Basit, Farrukh, Lodhi& Aden, 2010).

4.6 Yhteenveto

Boehmin (1991) määritelmää mukaillen riskienhallinta on menestyksen kanssa riippuvuussuhteessa olevien riskitekijöiden formalisointia erilaisten valmiiden menetelmien avulla. Ohjelmistokehitysprojektissa riskitekijöitä liittyy ainakin projektin aikatauluun ja resursseihin, lopullisen tuotteen laatuun ja suorituskykyyn sekä koko liiketoimintaan.

Pilvipalveluita pohdittaessa yksi merkittävimmistä riskeistä liittyy tietojenkäsittelyn ulkoistamiseen. Ulkoistettujen palveluiden tietoturvallisuus tulisi olla taattua sekä mitattavissa ja arvioitavissa. Näin ollen molempien osapuolien, palvelun tarjoajan ja palvelun hankkivan tahon, riskienhallinta olisi tehokasta. Tässä tutkielmassa pohditaan, voidaanko riskien minimoiminen toteuttaa sopimuksin, teknisesti toimivalla ja laadukkaalla ratkaisulla tai palvelulla, tai kypsyysmallien avulla.

Kandukurin ym. (2009) mukaan sopimuksien avulla voidaan yksinkertaistaa monimutkaisia asioita ja poistaa epärealistisia odotuksia määrittelemällä tarkasti palvelukokonaisuus. Myös ongelmatilanteiden hallinta ja palveluiden suoritusteho erilaisine metriikoineen tulisi käsitellä sopimustasolla. Näin ollen osapuolten vastuut, velvoitteet ja korvaustilanteet selkiintyvät, mikä taas vaikuttaa riskien vähenemiseen.

Teknisesti toimiva palvelu vähentää riskejä. Pilvipalveluissa tekninen toimivuus on ennen kaikkea saatavuuden takaamista. Ongelmatilanteita varten tulisi olla laadittuna dokumentti, joka määrittää toimenpiteet palvelun palauttamiseksi ennalleen. Osana teknistä toimivuutta voidaan pitää palveluiden läpinäkyvyyttä. Tällöin erilaiset auditoinnit ovat mahdollisia ja pilvipalveluiden monitorointi helpottuu.

Pilviteknologiaan liittyviä riskejä on mahdollista myös hallita hyödyntämällä kypsyysmalleja. Kypsyysmalleja noudattamalla voidaan saada aikaan laadukkaita ohjelmistoja, mikä vaikuttaa positiivisesti liiketoiminnan menestykseen (Kemerer ym., 2009). Kypsyysmallien avulla voidaan myös vertailla eri yrityksiä ja niiden palveluita. Eniten käytetty kypsyysmalli, CMM-malli, mittaa

ohjelmistoprosessin kyvykkyyttä, suorituskykyä ja kypsyyttä. CMM-pohjaisen CMMI-mallin ja ISO/IEC 15504 -standardiin perustuvan SPICE-mallin avulla voidaan arvioida jokainen ohjelmistotekniikan prosessi omana kokonaisuutenaan.

Myös riskienhallintaan on kehitetty monia standardeja. Keskeisenä tietoturvaan liittyvänä riskienhallintastandardina voidaan pitää ISO 27005 -standardia. Tämän lisäksi erilaisten prosessi- ja laatustandardien sekä kehysmallien avulla voidaan vaikuttaa tietoturvan toteutumiseen pilviteknologiaa ja pilvipalveluita kehitettäessä

5 ANALYYSI TEORIAN POHJALTA

Tässä luvussa kootaan yhteen tutkielman eri osa-alueita ennen empiiristä osiota. Koska tutkimusongelma yhdessä alaongelman kanssa on hyvin moniulotteinen ja sivuaa tietojenkäsittelyn, projektinhallinnan ja liiketoiminnan eri osa-alueita, on tärkeää, että eri osat muodostavat ymmärrettävän ja helposti lähestyttävän kokonaisuuden. Seuraavissa kappaleissa käsitellään kootusti teoriaosan tärkeimmät kohdat. Näiden osa-alueiden pohjalta on laadittu empiirisen osion haastattelukysymykset.

5.1 Edellytykset pilvipalveluiden yleistymiselle

Tehokas liiketoiminta edellyttää nykyään yhä useammin luotettavia ja mukautettavia tietojenkäsittelyratkaisuja. Pilviteknologia voi olla tällaiset vaatimukset täyttävä ratkaisu. Pilvipalveluiden yleistyminen pilviteknologiaan liittyvien ratkaisujen avulla edellyttää kuitenkin useiden eri osatekijöiden huomioimista ja kehittämistä sekä yhteistyötä ja luottamusta eri osapuolien välillä. Terminologian määrittely lienee ensisijaisen tärkeää, jotta palvelun eri osapuolet ymmärtävät toisiaan. Empiirisessä osiossa havainnollistetaan pilviteknologian ja pilvipalveluiden määrittelyä sekä niiden hyödyntämistä eri yrityksissä.

Kuten on jo todettu, pilviteknologian avulla on mahdollista toteuttaa palveluja, joiden etuina ovat kustannustehokkuus, joustavuus ja helppokäyttöisyys. Edut ovat kuitenkin saavutettavissa ainoastaan, jos pilvipalveluita kehitetään turvallisiksi ja luotettaviksi. Turvallisuus pitää sisällään tietoturvan ja tietosuojan eri osa-alueet. Tiedon luottamuksellisuus, eheys ja käytettävyys tulee turvata asianmukaisin salauskeinoin unohtamatta pääsynvalvontaa ja kiistattomuutta. Nämä osa-alueet tulee huomioida jo pilvipalveluita kehitettäessä. Tämä taas edellyttää, että tietoturva ja tietosuoja koetaan tarpeeksi merkittävinä osa-alueina, jotta niihin panostetaan aidosti teknologiaa ja palveluja kehitettäessä.

Pilvipalveluille tyypilliseen tietojenkäsittelyn ulkoistamiseen liittyy riskitekijöitä. Kolmannen osapuolen olemassaolo vaarantaa aina jossain määrin tietosuojan. Ulkoistamisen ja sen eri osa-alueiden riskitekijöitä voidaan kuitenkin hallita aivan kuten liiketoiminnan muitakin riskejä. Riskitekijöihin voidaan vaikuttaa esimerkiksi sopimalla osapuolten vastuista ja velvollisuuksista palvelutasosopimuksin. Sopimukset eivät voi kuitenkaan poistaa kaikkia riskejä, joita liittyy arkaluontoisten tietojen vaarantumiseen.

Tietosuojan vaarantumiseen liittyviä riskejä on mahdollista hallita ja minimoida erilaisten riskienhallintametodien avulla. Tässä tutkielmassa on käsitelty perinteisten riskienhallintametodien lisäksi tarkasti määriteltyjen palvelutasosopimusten, toimivien ja laadukkaiden tuotteiden tai palvelujen toteuttamisen sekä kypsyysmallien hyödyntämisen potentiaalia riskejä pienentävinä menetelminä. Pilvipalveluihin liittyviä kypsyysmalleja ei ole vielä juurikaan kehitetty, joten tutkielmassa on pohdittu yleisempien CMM- ja SPICE-kypsyysmallien hyödyntämispotentiaalia. Empirian avulla haetaan vastausta kysymykseen, onko edellä mainitut tavat aidosti mahdollisia hyödynnettäviksi osana yritysten riskienhallintaa.

5.2 Riskienhallinnan implementointi osaksi prosesseja

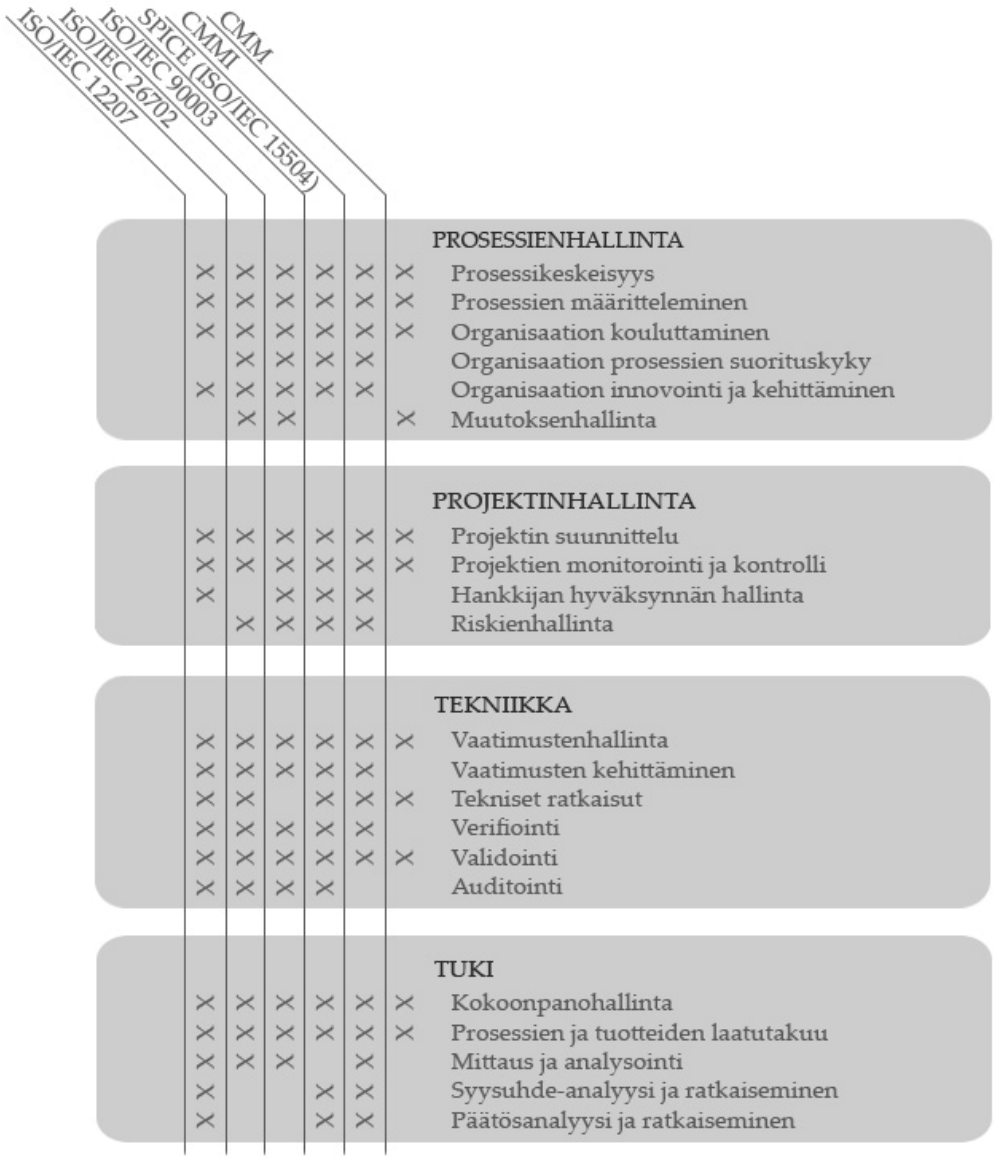
Riskienhallintaprosessin tulisi olla muun projektisuunnittelun tavoin iteratiivinen prosessi, joka jatkuu koko projektin elinkaaren ajan (Sommerville, 2007, s. 106). Boehmin (1991) mukaan monien katastrofaalisesti epäonnistuneiden projektien kautta on huomattu, että ongelmat olisi voitu välttää – tai ainakin niiden määrää huomattavasti pienentää — jos korkean riskin tekijät olisi tunnistettu ja ratkaistu riittävän ajoissa. On hyvin yleistä, että ohjelmistoja kehittävällä yrityksellä on useampia päällekkäisiä, eri määrän resursseja vieviä kehitysprojekteja ja -prosesseja, joiden aikataulut ovat tiukkoja. Näin ollen erilaiset riskienhallintamenetelmät korostuvat entisestään yksittäisten projektien muodostaessa kokonaisuuden, joka on kriittinen osa-alue liiketoiminnan jatkuvuuden kannalta.

Tehokas riskienhallinta edellyttää tiettyjen projektinhallinnan osa-alueiden huomioon ottamista korostetulla tavalla. Tähän liittyy läheisesti yrityksen sisäinen kulttuuri. Chittisterin & Haimesin (1994) mukaan monissa yrityksissä on kielteistä suhtautumista riskeistä puhumiseen ja avoin kommunikaatio eri hierarkiatasojen välillä on lähes olematonta. Näin ollen toimiva kommunikaatio on yksi merkittävä edellytys riskienhallinnan implementoinnille. Samalla tapaa on huomattu, että yrityksen riskienhallinnan implementoinnilla osaksi projekteja tulee olla ylimmän johdon tuki; ilman sitä riskienhallinta todennäköisesti epäonnistuu (Beasley, Clune & Hermanson, 2005).

Taulukossa 1 on havainnollistettu tässä tutkielmassa käsiteltyjä kypsyysmalleja ja prosessistandardeja sekä niiden sisältöä, joka pitää sisällään myös projektinhallinnan osa-alueen. Taulukon prosessit ovat CMMI v.1.1 (continuous) kypsyysmallissa määritettyjä prosesseja, ainoana lisäyksenä teknisen osan audi-

tointi (Software Engineering Institute, 2002), (Mazlan ym., 2009), (Ehsan ym. 2010), (ISO/IEC 12207, 2008), (CMM, 1999), (IEEE:n ohjeistus, 2008) ja (ISO/IEC 26702, 2007). Auditointi lisättiin taulukkoon, sillä auditointi on pilvipalveluiden kannalta keskeinen osa-alue, jolla voidaan valvoa palvelutasosopimuksen täyttämistä.

TAULUKKO 1 Kypsyysmallien sekä ohjelmistoprosessiin liittyvien standardien ja kehysmallien vertailua



Taulukosta 1 voidaan havaita, että käsitellyt ohjelmistoprosesseihin liittyvät standardit ja kehysmallit ovat sisällöltään lähes samanlaisia. Voidaan havaita

esimerkiksi, että jokaiseen standardiin ja kehysmalliin liittyy erityinen prosessikeskeisyys, jota leimaa myös projektinhallinta erilaisine monitorointi- ja kontrollointiprosesseineen. Riskienhallinta ja vaatimusten kehittäminen ovat myös lähes jokaisessa käsiteltävässä standardissa ja kehysmallissa. Tämän perusteella voidaan olettaa, että esimerkiksi CMMI- tai SPICE-kypsyysmalleja hyödyntämällä organisaatio kykenee toteuttamaan laadukkaita tuotteita ja palveluita. Näin ollen kypsyysmallien hyödyntäminen itsessään voi toimia riskejä vähentävänä metodina.

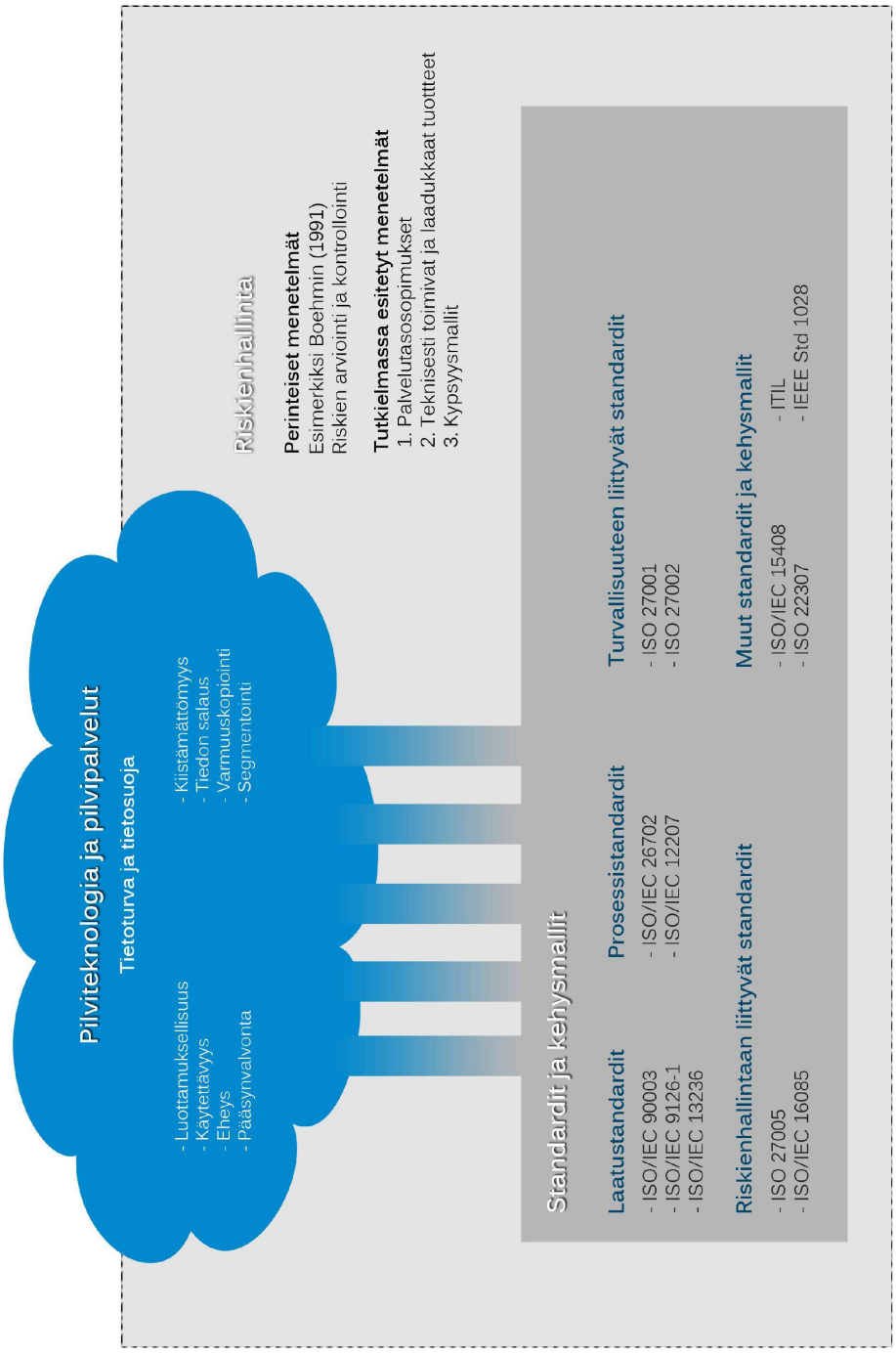
5.3 Standardit ja kehysmallit tutkielmassa

Informaatioteknologian kokonaisvaltaisen laadun parantamiseksi on kehitetty suuri joukko erilaisia standardeja. Zhulingin ym. (2009) mukaan standardien merkitys ylettyy laadun paranemisen lisäksi myös tekniseen kehitykseen, teollisuuden paranemiseen ja ympäristön suojelun kehittymiseen.

Teknologian nopea kehittyminen asettaa haasteita ajantasaiselle standardoinnille. Toisaalta voidaan ajatella, että teknologian nopea kehittyminen ja markkinoille tulo saa aikaan keskeneräisiä ja turvallisuudeltaan kyseenalaisia järjestelmiä. Pilviteknologiaan liittyy monia osa-alueita, joissa standardeja voitaisiin hyödyntää. Standardien ja kehysmallien käyttöönottoon liittyy kuitenkin omat haasteensa.

Tämän tutkielman kannalta on oleellista käsitellä standardeja, jotka liittyvät tuotteiden ja palvelujen laatuun. ISO ja IEEE määrittelevät laadun tuotteen tai palvelun kyvyksi täyttää sille asetetut odotukset (Al-Kilidar ym., 2005). Tietoturvallisuutta voidaan pitää merkittävänä laatutekijänä pilviteknologiassa. Toisaalta tutkimusongelmia silmällä pitäen on aiheellista pohtia myös riskienhallintaan liittyviä standardeja.

Tässä tutkielmassa on käsitelty standardeja ja kehysmalleja, jotka ovat abstraktimpia verrattaessa aidosti teknisiin ratkaisuihin liittyviin standardeihin. Tästä syystä tutkielma ei ota kantaa esimerkiksi pilvien välisten yhteensopivuuden kehittämiseksi laadittuihin teknisten ratkaisujen standardeihin. Pilviteknologiaa ja pilvipalveluita kehitettäessä tai hankittaessa on kuitenkin mahdollista hyödyntää erilaisia laatu-, turvallisuus-, riskienhallinta- ja prosessistandardeja sekä erilaisia kehysmalleja. Kuviossa 9 havainnollistetaan käsiteltyjen standardien ja kehysmallien kokonaisjoukkoa suhteessa tutkielman muuhun sisältöön.



KUVIO 9 Tutkielman kokonaiskuva

5.4 Standardien ja kehysmallien ongelmallisuudet

Standardien hyödyntämiseen liittyy tiettyjä ongelmallisuuksia, joita on syytä tarkastella ennen tutkimuksen empiiristä osiota.

Alati muuttuvassa ja kehittyvässä tietojenkäsittelyn ympäristössä standardointiorganisaatioiden kyvyttömyys tuottaa erilaisia standardeja riittävän nopealla tahdilla saattaa aiheuttaa standardien vähäistä hyödyntämistä. Blind & Gauchin (2008) mukaan viralliset, suuret standardointiorganisaatiot eivät ole yrityksistä huolimatta kyenneet nopeuttamaan vuosia kestävää standardointiprosessia niin, ettei muodostuisi alakohtaisia, reaktiivisempia standardointiyhtymiä. Alakohtaisten konsortioiden muodostumisessa haittapuolena voi olla pienten ja keskisuurien yritysten jääminen ulos standardikehityksestä. Yleisten standardien kehittymisen hitaus ei ole ainoa standardeihin liittyvä ongelma.

Merkittävä tekijä, joka saattaa estää standardien tai kehysmallien implementoinnin osaksi organisaatiokulttuuria, ainakin pienissä ja keskisuurissa yrityksissä, lienee implementointiprosessista aiheutuvat kustannukset. Qasaimehin & Abranin (2010) mukaan esimerkiksi ISO 9001 -standardin hyödyntäminen pienissä ja keskisuurissa yrityksissä saattaa olla vaikeaa pienien resurssien tähden. Barletten & Fominin (2008) mukaan tietoturvallisuuden hallintajärjestelmän implementointi vaatii pieniltä ja keskisuurilta yrityksiltä suuren määrän aikaa, vaivannäköä ja rahaa kompleksisen luonteensa tähden. Vaikka resurssit olisi olemassa, standardin implementointi ei takaa kuitenkaan automaattisesti etuja kilpailijoihin nähden.

Standardien hyödyntäminen organisaatiossa ei välttämättä ole tae organisaation paremmuudesta verrattuna kilpailijoihin. Vaikka esimerkiksi ISO 9000 -laatustandardisarja on hyödyllinen työkalu ohjelmistokehityksessä monine käytännöllisine tarkistuskohtineen, Wangin ym. (1997) mukaan standardisarja on luonteeltaan yleispätevä, eikä välttämättä kerro mitään ohjelmistokehitysyrityksen kypsyydestä. Samalla tapaa Barlette & Fomini (2008) kritisoivat standardien sisältöä. Heidän mukaansa standardit eivät ota riittävästi kantaa siihen, miten tietyt tietoturvallisuuden osa-alueet tulisi toteuttaa.

Edellä mainittujen tekijöiden lisäksi on vaarana, että standardi tai kehysmalli pyritään väkisin implementoimaan osaksi organisaatiokulttuuria. Näin ollen on syytä olla tarkkana, sopiiko mahdollinen standardi esimerkiksi joustavuudeltaan yrityksen ydinprosesseihin. Tietyt ohjelmistoprosessit eivät ole täysin mukautettavissa standardien vaatimuksiin. Qasaimehin & Abranin (2010) mukaan esimerkiksi extreme programming -ohjelmistoprosessissa on tiettyjä osa-alueita, esimerkiksi vaatimusten määrittelyssä käytettävät käyttäjäkertomukset, jotka eivät ole riittävän perusteellisia vastaamaan ISO 9001 -standardin vaatimuksia. Näin ollen standardin jäykkyys saattaa asettaa erityisiä haasteita dynaamiselle ohjelmistoprosessille, vaikka prosessi olisi muuten kaikin tavoin laadukas. Tämä saattaa toisaalta edesauttaa yritysten omien, standardinomaisten hyvien käytäntöjen määrittelyä.

Aina standardien kritiikitön implementointi osaksi projekteja ja yrityskulttuuria ei ole siis järkevää. Glassin (2009) mukaan standardien käytössä tulee olla rationaalinen. Standardien käytön tulee muidenkin käytäntöjen tavoin olla arvioitavissa ja tutkittavissa. Ennen kaikkea standardien tulee olla laadittuja yhteistyössä tietojärjestelmiä kehittävien tahojen kanssa, sillä muutoin standardit saattavat päinvastoin heikentää organisaatioiden tuotteiden tai palveluiden laatua. (Glass, 2009.)

6 TUTKIMUKSEN TOTEUTTAMINEN

Tässä luvussa käsitellään tutkielman empiirisen osan toteuttamista. Aihepiirin taustaa ja tavoitteita käsitellään sen verran, että lukija ymmärtää tutkimuksen motiivit. Jotta tutkimuksen tekeminen olisi relevanttia, tulee määritellä tapa, jolla kyseessä olevaa aihetta tutkitaan. Luvun lopussa käsitellään tutkimusprosessin eri vaiheet.

6.1 Taustaa

Pilviteknologian ollessa tietojenkäsittelyparadigma, joka perustuu tietojenkäsittelyn ulkoistamiseen sekä hajauttaa tiedon useaan eri kohteeseen, on aiheellista tutkia ja pohtia tietoturvaan ja tietosuojaan kohdistuvia uhkatekijöitä. Hoquen (2010) mukaan pilvipalveluille tyypilliseen tietojenkäsittelyjen ulkoistamiseen liittyy monia riskitekijöitä. Youseff ym. (2008) pitävät tietoturvaan ja yksityisyyteen liittyviä osa-alueita merkittävimpinä pilviteknologian yleistymistä hidastavina tekijöinä. Pilviteknologian eri osa-alueita standardoimalla voitaisiin kuitenkin mahdollisesti edistää teknologian luotettavuutta. Vaqueron ym. (2009) mukaan esimerkiksi pilvienvälistä yhteentoimivuutta ja saatavuutta voitaisiin edistää standardoinnilla.

Tietosuojan vaarantuminen on aina riski. Toisaalta se on riski asiakasorganisaatiolle, joka hyödyntää pilvipalvelua, mutta samalla tapaa se on myös riski pilvipalveluita tarjoavalle organisaatiolle. Arkaluontoisten tietojen levitessä esimerkiksi internetissä voi tiedot menettäneen organisaation liiketoiminta vaarantua merkittävästi puhumattakaan yksilöille aiheutuvista ongelmista. Se, otetaanko tietosuojan ja näin ollen myös yksityisyyden vaarantumista huomioon pilvipalveluita kehitettäessä sekä kuinka tietoturvaa ja tietosuojaa voidaan kehittää standardien ja kehysmallien avulla, ovat mielenkiintoisia kysymyksiä, joista syntyy riittävä motiivi tämän tutkimuksen toteuttamiselle.

6.2 Tavoitteet

Tämän tutkielman tarkoituksena on käsitellä kirjallisuudessa esiintyviä tutkimustuloksia, päätelmiä ja argumentteja tietoturvaan ja tietosuojaan sekä riskienhallintaan ja tietojenkäsittelystandardeihin liittyen. Teemahaastattelujen avulla pyritään kartoittamaan pilviteknologiaa ja pilvipalveluita kehittävien tahojen kokemuksia käsitellyistä teemoista — erityisesti tietoturvaan ja tietosuojaan liittyvistä standardeista ja kehysmalleista. Lisäksi tutkielman avulla pyritään selvittämään, voidaanko palvelutasosopimusten, toimivien ja laadukkaiden ratkaisujen sekä kypsyysmallien avulla pienentää tai hallita pilvipalveluihin liittyviä riskejä. Teoria- ja empiriaosuuden avulla saataneen vastaus tutkimusongelmaan ja sen alaongelmaan.

Tutkimusongelman taustalla on mielenkiintoinen aihealue, joka herättää keskustelua puolesta ja vastaan. Tutkielman taustalla on myös kirjoittajan henkilökohtainen halu selvittää yritysten suhtautumista tietoturva- ja tietosuojaasioihin. Pilviteknologian yleistyessä aihe koskettaa pian jokaista tietojenkäsittelyä välillisesti tai suoraan hyödyntävää yksilöä.

6.3 Tutkimustapa

Tässä tutkielmassa pyritään käsittelemään valittua aihealuetta eri näkökulmista, loogisena kokonaisuutena. Sisällöllisesti teoreettinen osa on jäsennetty Hirsjärven ym. (1997, s. 35) luokittelujen mukaan temaattiseksi. Tutkimusongelmia tarkastelemalla voidaan huomata, että kyseessä on laadullinen tutkimus. Varsinaiseksi tutkimustavaksi valittiin teoriaosuutta parhaiten tukeva tiedonkeruutapa: teemahaastattelu. Eskolan & Vastamäen (2001, s. 24) mukaan teemahaastattelussa tutkija pyrkii keskustelun tavoin saamaan haastateltavilta selville tutkimusongelman kannalta merkittävää tietoa.

Hirsjärvi ym. (1997, s. 168) pitävät laadullisen tutkimuksen tarkoituksena tutkimuskohteen ymmärtämistä. Tutkimusongelmien selvittämiseksi tulisi siis löytää luotettava yhteys haastattelukysymysten, saatavien vastausten ja todellisuuden välille. Eskolan & Vastamäen (2001, s. 40) mukaan tutkimuksen laajuudesta, tutkimusmenetelmästä ja oppilaitoksen suosituksista riippuen haastattelujen määrä voi vaihdella, vaikkakin on hyvä muistaa, että kyllääntyminen voi olla merkki riittävästä tutkimusaineistosta; tällöin uusien haastattelujen kautta ei ilmene enää mitään uutta tietoa.

Teemahaastattelua voidaan kutsua myös puolistrukturoiduksi haastattelumenetelmäksi (Hirsjärvi & Hurme, 2000, s. 47). Hirsjärven & Hurmeen (2000, s. 47) mukaan teemahaastattelun ominaispiirteitä ovat tutkijan alustava tutustuminen käsiteltävän ilmiön kokonaisuuteen, tietyn tilanteen kokeneet haastateltavat sekä näiden pohjalta toteutettu, oletuksiin perustuva haastattelurunko ja varsinainen haastattelu, joka suuntautuu haastateltavien subjektiivisiin kokemuksiin, joita tutkija on aikaisemmin analysoinut. Eskolan & Suorannan

(1998, s. 86) mukaan puolistrukturoidussa haastattelussa kaikille haastateltaville esitetään samat kysymykset, mutta haastateltava saa vastata omin sanoin valmiiden vastausvaihtoehtojen sijaan.

6.4 Tutkimusprosessi

Tutkimusprosessi alkoi keväällä 2010 tutkimusaiheen suunnittelulla. Alkuperäinen suunnitelma oli tutkia ainoastaan yksittäistä tietojenkäsittelystandardia eri näkökulmista, mutta aihealueeseen perehtymisen myötä syntyi ajatus useamman standardin, ja tämän lisäksi erilaisten kehysmallien, kokonaisuudesta. Neuvoteltuani kesällä ohjaajani kanssa, hän ehdotti pilviteknologian kontekstin lisäämistä osaksi tutkielmaa. Aihealue alkoi rajautua. Tämän tutkielman kohdalla alkoi syklinen prosessi, joka on muovautunut iteratiivisesti viikko viikolta. Hirsjärvi, Remes & Sajavaara (1997, s. 14) kuvaavat yhdeksi tutkimusprosessin luonteeksi sen spiraalinomaisuuden — tällöin tutkimus etenee vaihtelevasti ajallisessa järjestyksessä ja on prosessi, joka ohjaa harkitsemaan toistamiseen tehtyjä valintoja. Tämänkaltainen, vaiheittainen prosessi on tyypillinen laadulliselle tutkimukselle (Hirsjärvi, Remes & Sajavaara, 1997, s. 15). Tässä yhteydessä asetettiin myös alustava tutkimusongelma.

Tutkielman toisena vaiheena voidaan pitää teoreettisen aineiston keruuta. Kirjallisen aineiston etsintä ja keruu tapahtui kahdella tavalla. Ensisijaisesti aineiston keruussa hyödynnettiin erilaisia tunnettuja, elektronisia aineistotietokantoja, kuten ACM:ä, IEEE:iä, ScienceDirect:ia ja Elsevier:iä. Voidaan ajatella, että tutkimuksen primaarilähteet ovat valikoituneet tätä kautta. Hirsjärven, Remeksen & Sajavaaran (1997, s. 83) mukaan primaarilähteitä ovat erilaiset niin painetussa kuin sähköisessäkin muodossa olevat monografiat, raportit, tutkimukset ja artikkelit. Samaisten kirjoittajien mukaan sekundaarilähteitä ovat ne lähteet, joiden avulla löydetään tietoja primaarilähteistä. Sekundaarilähteitä tässä tutkielmassa olivat erilaisten elektronisten julkaisujen lisäksi Suomen eri yliopistojen opinnäytteet ja tutkimukset. Tutkielman toissijaisena aineistonkeruumenetelmänä oli erityisesti Jyväskylän yliopiston tietojenkäsittelytieteiden pro gradu -tutkielmat. Elektronisten ja painettujen lähteiden etsintä tapahtui tekemällä erilaisia sanahakuja tietokantoihin mahdollisimman monipuolisesti ja kattavasti. Löydettyjen lähteiden suhteen pyrittiin noudattamaan asiaankuuluvaa lähdekritiikkiä ja tästä syystä osa lähteistä rajautui pois tutkielmasta epäluotettavuuden tähden.

Varsinainen kirjoitusprosessi tapahtui osin samanaikaisesti tiedonkeruun kanssa. Kirjallisuuden lukemisen ja teorian kirjoittamisen yhteydessä myös tutkimusongelma muovautui selkeämmäksi. Hirsjärvi, Remes & Sajavaara (1997, s. 117) kuvaavat tilannetta varautumiseksi ongelman muuttumiseen kvalitatiivisen tutkimuksen yhteydessä. Tutkimusongelma haluttiin kuitenkin määritellä jo alusta alkaen, jotta tutkielman kokonaisuus hahmottuisi selkeästi ja tutkielman teoriaosuus olisi mahdollisimman tiiviisti kytköksissä tutkimusongelmaan. Tutkimusongelma muodostui lopulta kaksiosaiseksi ongelmaksi, jossa on pää-

ongelma ja yksi alaongelma. Tutkimusongelman selkeytymisen myötä oli selvää, että kyseessä olisi laadullinen tutkimus ja yhdessä ohjaajan kanssa varsinaiseksi aineistonkeruumenetelmäksi valittiin teemahaastattelu.

Haastattelujen suunnittelu lähti käyntiin pääkohtien määrittelyllä. Hirsjärvi & Hurme (2008, s. 66) korostavat suunnittelun tärkeyttä sillä, että haastattelusta saatavan aineiston avulla tulee voida tehdä luotettavia päätelmiä tutkittavasta aiheesta. Haastattelukysymyksien laatiminen oli melko suoraviivainen prosessi ja käsiteltävät teemat muodostuivat tutkielman pääkohdista. Käytetty, suuntaa antanut haastattelulomake on tarkasteltavissa liitteessä 1. Hirsjärvi & Hurme (2008, s. 66) pitävät haastatteluteemojen suunnittelua suunnitteluvaiheen tärkeimpänä tehtävänä. Teemahaastatteluun osallistuvat henkilöt valittiin yrityksistä, jotka tavalla tai toisella hyödyntävät pilviteknologiaa tai pilvipalveluita. Yhteydenotto yrityksiin tapahtui sähköpostein ja puhelinsoitoin. Tässä yhteydessä varmistettiin yrityksen sidos pilviteknologiaan tai pilvipalveluihin. Haastatteluun suostuneen yrityksen edustajan henkilökohtaisia kompetensseja vastata aihealueen kysymyksiin täsmennettiin haastateltavalle lähetetyllä sähköpostilla, jossa kerrottiin lisää haastattelun sisällöstä. Tällä tavoin varmistettiin, että haastateltava osaa vastata haastattelussa käsiteltävien teemojen kysymyksiin. Haastatteluun suostuneille lähetetty kirje on luettavissa tutkielman liitteessä 2.

Haastattelut suunniteltiin toteutettaviksi kasvotusten. Tämä ei kuitenkaan ollut jokaisen haastattelun kohdalla mahdollista johtuen pitkistä välimatkoista ja näin ollen osa haastatteluista toteutettiin puhelimitse. Haastatteluajankohta, ja kasvotusten toteutettavissa haastatteluissa haastattelupaikka, sovittiin jokaisen haastateltavan kanssa etukäteen. Jokainen haastattelu tallennettiin sekä minidisc-levylle että tietokoneelle. Tällä tavoin varmistettiin haastattelujen nauhoituksen onnistuminen sekä mahdollisimman hyvä nauhoituslaatu haastattelujen puhtaaksi kirjoittamista ajatellen.

7 HAASTATTELUVASTAUKSET

Tässä luvussa käydään läpi tutkimuksen kannalta merkittävimmät haastattelujen avulla saadut tulokset. Luvussa käsiteltävät teemat ovat yhtenevät haastatteluissa käsiteltyjen teemojen kanssa. Koska tutkimuksen kannalta oleellinen teema — pilviteknologia ja pilvipalvelut — on koko tutkimuksen ajan taustalla vaikuttamassa, käsitellään kyseistä teemaa ensimmäisenä myös tutkimustuloksissa.

7.1 Haastatellut henkilöt

Haastateltaviksi valikoitui kuusi henkilöä viidestä eri yrityksestä. Tutkimuksessa käsiteltävien yritysten edustajien anonymiteetin turvaamiseksi haastateltaviin viitataan H1-H6 merkinnöin. Seuraavassa lyhyt esittely haastateltavista:

H1: Kahden yrityksen tuotekehityksestä vastaava henkilö, kokemusta n. 20 vuotta. Yritys mm. kehittää ja tuottaa pilviteknologiaan pohjautuvia, oman toimialansa ohjelmistoja.

H2: Tekninen konsultti, kokemusta n. 3 vuotta. Yritys mm. kehittää ja tarjoaa ohjelmistopalveluja sekä -infrastruktuureja eri laitteille mm. pilviteknologiaan pohjautuen.

H3: Arkkitehti-asiantuntija, kokemusta n. 23 vuotta. Yritys kehittää ja tarjoaa monenlaisia ohjelmisto- ja alustapalveluja mm. pilviteknologiaan pohjautuen.

H4: Projektipäällikkö, kokemusta n. 20 vuotta. Yritys mm. kehittää ja tarjoaa ohjelmistopalveluja mm. pilviteknologiaan pohjautuen.

H5: Java-asiantuntija, kokemusta n. 5 vuotta. Yritys mm. kehittää ja tarjoaa ohjelmistopalveluja mm. pilviteknologiaan pohjautuen.

H6: Development Director, kokemusta n. 12 vuota. Yritys mm. tarjoaa erilaisia teknologisia ratkaisuja asiakkailleen.

7.2 Pilviteknologia ja pilvipalvelut

Vaqueron ym. (2009) mukaan pilviteknologian uutuuden vuoksi sen yhtenäinen määritteleminen on haasteellista. Tutkielman kannalta on tärkeää, että haastateltavat kertovat oman määritelmänsä pääkäsitteisiin, jolloin voidaan ymmärtää ja analysoida muitakin vastauksia. Haastattelujen ensimmäisen kysymyksen avulla pyrittiinkin kartoittamaan haastateltavien kykyä määritellä pilviteknologia ja pilvipalvelut. Keskeiset pilviteknologiaa ja pilvipalveluita määrittävät tekijät, jotka toistuivat vastauksissa, olivat mm. palveluna myytävyys, internetin yli tarjottavuus, virtuaaliset resurssit ja käytön mukaan määräytyvä laskutus.

> H3: ”..tietotekniikan, on ne sitten sovelluksia, sovellusalustoja tai infraa, tarjoamista palvelun muodossa […] jakelukanavana käytetään internettiä tai erityisesti nyt internet-tekniikoita. […] Mutta sitten ne ominaisuudet mun mielestä oleellisempia on se, että niinku se elastisuus, elikkä resurssimäärää voidaan joustavasti säätää ylös että alaspäin.. tuota tarpeen mukaan ehkä sitten käyttöpohjainen veloitus. […] Jaja sitten ehkä vielä asiakkaan näkökulmasta se niin kun itsepalveluperiaate ja siitä tuleva nopeus..”

Riippuen hieman yrityksestä ja sen toiminnasta haastateltavat painottivat eri asioita liittyen pilviteknologiaan ja pilvipalveluihin. Annettujen vastausten kautta välittyi myös selkeästi kuva haastateltavien ja heidän yrityksensä liiketoiminnallisista yhteyksistä pilviteknologiaan ja pilvipalveluihin. Esimerkiksi kysyttäessä hyötyjä ja haittoja liittyen pilviteknologiaan ja pilvipalveluihin vastauksia annettiin melko subjektiivisesti liittyen oman yrityksen toimintaan. Tämä lienee tutkielman kannalta sekä hyvä että huono asia. Joka tapauksessa pilviteknologiaan ja pilvipalveluihin liitettiin monipuolisesti hyötyjä ja haittoja. Haastateltavien rooli heijastui vastauksissa ja näin ollen vastaukset olivat hyvin erilaisia. Yhteisiä hyötyjä ja haittoja kuitenkin esiintyi ja lähes kaikissa vastauksissa merkittävänä hyötynä koettiin taloudelliset edut, joita liittyy palvelukeskeisyyteen.

> H3: ” on kyse sovelluspalveluista tai alusta-, tai infrapalvelusta niin se pienempi aloitusinvestointi jonkin uuden ratkaisun käyttöönotossa tai rakentamisessa, sen kautta et tyypillisestihän se lisenssihankinta ja laitehankinta ja muu tämmönen jää siitä pois. Ja sitten jos puhutaan sovelluspalveluista niin silloin jää myös sen sovelluksen asentamiset, pystyttämiset ja kenties jos se on vaihtoehtona, jos vaihtoehtona tarkastelee ihan suoraan jonkin verran räätälöityä pakettisovellusta tai räätälöityä pakettisovellusta, niin totta kai se rakennusvaihekin jää merkittävästi pienemmäksi. […] talousjohto tykkää siitä, että siirretään niiku pääomakuluista jatkuviin kuluihin.”

Haittapuolena vastauksissa oli huoli tietojen kontrolloinnin hämärtymisestä tietoa hajautettaessa.

> H1: ”..heillä on ollu, että se serveri seisoo siinä nurkassa ja he on tottunu, että se on siinä heidän omaa taloushallinnon dataa ja se on joillekin ollu aikamoinen vakuuttelu että kyllä se on silti suojassa vaikka se on siellä [pilvessä].”

> H2: ”Muuten saattaa olla tämä huoli, että kun ei välttämättä niiku enää, kun me abstrahoidaan se alla oleva infra pois, niin loppukäyttäjällä ei välttämättä ole enää selvä, että missä ne hänen datansa on.”

> H3: ”Ja sit totta kai yks asia selvästi mikä tulee, kun juttelee asiakasyritysten kanssa niin tuota on tietysti erilaiset huolenaiheet siitä, että missä sitä tietoa käsitellään ja säilytetään ja että onko siihen itsellä riittävän kontrolli.”

Edellä mainittujen lisäksi erilaisia hyötyjä ja haittoja listattiin monipuolisesti. Hyötyinä koettiin esimerkiksi keskitetty versionhallinta, palvelujen ylläpidon ja toisaalta palvelujen käytön helppous, kuorman siirtäminen laitteesta pilveen, nopeusedut palvelujen käyttöönotossa ja liiketoimintapotentiaali. Haittoina tai huolenaiheina taas listattiin palvelujen tai resurssien saavutettavuuteen liittyvät puutteet, juridiset ongelmat liittyen datan säilyttämispaikkoihin tai esimerkiksi alihankintasopimusten tulkinnassa, pilvipalveluntarjoajan mahdollinen konkurssi, tietoturva, tiedon lukkiutuminen tiettyyn formaattiin ja yleinen ”hype” asian tiimoilta. Eräs haastateltava muotoili sanansa näin:

> H6: ”Haittapuolet liittyy tähän yleiseen hypetykseen mikä nyt tän standardoitumisen ja koko tämän kehityksen myötä mitä luultavammin nyt sitten saadaan menemään eteenpäin alkuinnostuksen jälkeen.”

Sekä positiivista että negatiivista huomiota sai vakioitu palvelutaso. Palveluiden muokattavuuteen liittyvät rajoitteet ja toisaalta käytön helppous jakoivat mielipiteitä hiukan haastateltavasta riippuen.

> H1: ”..sitten tämmösessä meidänkin laatusessa ympäristössä, niin yks mikä on ollu sitten pienoinen haaste, on ollut sitten nää mahdolliset meidän haluamat erikoispiirteet kautta integrointi. Tämmöseen pilvipalveluun nehän on aika standardeja, ne on vähän tällaisia ota tai jätä –tyyppisiä juttuja ja sen sä sieltä saat, sen sä saat kenties hyvin mut mitään muuta sä et sit saakaan. […] mää ymmärrän kyllä tarjoojan, koska me ollaan siellä tarjoojan puolella myöskin, niin siinä häviää sitten se mielekkyys, et jos sitä ruvetaan asiakaskohtaisesti säätämään, et se on ihan niiku ymmärrettävää.. Se on toisaalta sen järjestelmän vahvuus, mutta omalla tavallaan järjestelmän heikkous..”

> H3: ”..sit jos menee niihin huonoihin asioihin, niin palvelun taso on vakioitua. Riippuen tietysti vähän minkä tyyppisestä alustasta ja minkä kokoisesta palveluntarjoajasta on kyse, mutta esimerkkinä jos käyttää meidän näitä onlinepalveluita tai tuota alustapalvelua, niin sehän on niinkun vakioitu palvelutaso, eli ysiysi piste ysi käytettävyys.. […] niinkun tuo on vähän sillä tavoin että ei se pelkkä haittakaan aina ole.”

> H5: ” siellä saattaa tulla sellanen turvallisuuden illuusio - - […] niin saattaa vaikuttaa että se on helppo, otetaan vaikka tosta tommonen PHP+MySQL+jotakin -yhdistelmäserveri, joka lähti play:llä käyntiin siitä ja sitten huomataankin, että siellä

> on tietoturva-asetukset ihan päin mäntyä. Elikkä siinä niiku tehään sellasista asioista helppoa, minkä ei pitäis olla helppoa."

7.3 Tietoturva ja tietosuoja

Tietoturvan ja tietosuojan teemaa käsiteltiin haastattelussa laajennettuna koskemaan myös yksityisyyden suojaamista. Yksityisyyden suojaa voidaan ajatella tietyllä tapaa myös osana tietosuojaa. Tässä yhteydessä haluttiin selvittää, millä tavoin haastateltavien yrityksissä otetaan huomioon tietoturva ja tietosuoja hyödynnettäessä pilviteknologiaa ja pilvipalveluita eri tavoin. Saatujen vastausten perusteella tietoturvaa ja tietosuojaa pidetään tärkeinä asioina kyseisten yritysten kehittäessä, tarjotessa, hankkiessa tai muuten hyödyntäessä pilviteknologiaa ja pilvipalveluita.

Wangin ym. (2009) mukaan turvalliseen pilviteknologiaan liittyy olennaisesti vahva salaus. Spiekermann ja Cranor (2009) peräänkuuluttavat tiedonsiirron turvaamista asianmukaisin keinoin. Siirtotien turvaaminen tuli esille kolmessa kuudesta haastattelusta.

> H5: "Se tietysti että kun siirretään tietoa meiän ja toisen firman välillä niin se tietysti aiheuttaa toimenpiteitä mutta sekin on yleensä salattua liikennettä."

> H2: "Toinen mikä siihen tietoturvaan liittyy, on myös se, että siirtotie itsessään pitäs olla suojattu."

> H1: "Jos nyt lähetään ensin vaikka siitä että, koska liikennehän tapahtuu tuossa meidän palvelumallissa internetin yli.. […] ja käytetään tätä normaalia, salattua HTTPS-protokollaa, joka jo sinällään varmaan tarjoo jotakin. Tai ainakin pitäs tarjota, se että onko se nyt pomminvarmaa ja muuta.. ainakin toistaseks tuntuu siltä että se on ihan ookoo."

Siirtotien salaamisen lisäksi tiedon kryptaus koettiin tärkeänä asiana tietoturvaan ja tietosuojaan liittyen. Yhtä lailla kolme kuudesta mainitsi kryptauksen konkreettisena tiedon turvaamisen keinona pilviteknologiassa ja pilvipalveluissa.

> H2: "..että mitä ikinä dataa meil sinne pilveen menee niin se olis kryptattua siinä muodossa että vain loppukäyttäjä ylipäätään pystys sen purkamaan."

> H3: " ..se oleellinen sisältö onkin sitten kryptattu esimerkiksi ja se vaatii niinkun taas sitten.. vaikka mä pääsisinkin lukemaan sen esimerkiksi kotikoneelta, meidän yritysverkon ulkopuolelta sen sähköpostin, mutta siinä vaiheessa mun täytyy antaa taas mun yrityskredentiaalit siihen, että saan sen viestin auki."

Jensenin ym. (2009) mukaan turvallinen pilviteknologia pilvipalveluineen edellyttää luottamusta eri osapuolien välille. Chowin ym. (2009) mukaan palvelujen ulkoistamiseen liittyvät samat ongelmat kuin aikaisemminkin — ainoastaan

uudessa muodossa. Ulkoistaminen vaatii edelleen luottamusta kumppaneiden ja yhteistyötahojen välille. Tietoturvaa ja tietosuojaa käsiteltäessä suurin osa haastateltavista mainitsi kumppanivaatimuksiin ja luottamukseen perustuvia tekijöitä.

> H1: ”Ja sitten totta kai edellytetään näiltä meidän hosting-partnereilta, että siellä heidän sisäiset prosessinsa on kunnossa. Sinne on rajotettu pääsy vaan niillä adminhenkilöillä ja kaikki tämä jutut. Ja toisaalta ne tilat on asianmukaisesti sertifioitu, jossa on tietyt tietoluokkastandardit - näissä hosting-saleilla. […] Kyl me siinä fyysisessä turvallisuudessa ja siinä hosting-centerin turvallisuudessa ja kaikkeen siihen liittyvään me luotetaan sen partnerin osaamiseen. Totta kai me tehään sitten jopa asiakkaitten, joittenkin asiakkaitten kanssa auditteja. Elikkä käydään kattomassa, nähään miten se käytännössä toimii ja näin sitten koitetaan vakuuttaa”

> H2: ”Niin kyllä mua itseäni ainakin huolettaa se, et miten paljon siihen itse palveluntarjoajaan voidaan luottaa. Vaik jos me mennään sellaiseen tilanteeseen, että sä ostat palvelun tältä firmalta A. Ja firma A huomaa, että heillä on hiukan resurssointiongelmia ja siirtää osan kuormasta firmalle B. Ja mä en siinä vaiheessa enää tiedäkään, että okei mitä firman B kanssa on sovittu siitä, että.. tai sanotaan, että mä en ole sopinut firman B kanssa yhtään mitään. Jos firma B vaikka operoikin eri maassa, sillä saattaa olla ihan erilaiset.. tai lainsäädäntö saattaa antaa ihan erilaiset oikeudet käyttää sitä dataa johonkin muuhun.”

> H5: ”..meidän rooli on haastaa täntyyppiset globaalisti tiettyä standardi-publicpilvipalvelutuottajat siitä, että miten he pystyvät tämän tiedon, asiakastiedon ja henkilötiedon rajaamaan niin, että meidän asiakkaille pystytään tietoturvallisesti tarjoamaan tiettyjä integroituja hybridi- ja julkisia pilvipalveluita.

Youseffin ym. (2008) mukaan merkittävimpiä tekijöitä, jotka hidastavat pilviteknologian laajempaa omaksumista ovat turvallisuuteen ja yksityisyyteen liittyvät osa-alueet. Kysyttäessä yksityisyyden suojaamisen merkityksestä ja haastateltavien yrityksissä tapahtuvasta sidosryhmien yksityisyyden suojaamisesta monissa vastauksissa korostettiin yksityisyyden suojaamisen merkitystä. Monet konkreettiset toiminnot yksityisyyden suojaamiseksi yritysten sisällä ovat vastausten perusteella ennalta määriteltyjä käytäntöjä.

> H2: ”No mun mielestä se on tärkeetä, mut sanotaan, että yksityisyyden suojaaminen ei sais olla este siihen, että jotain hienoja juttuja ois mahdollista saada aikaseks..[…] Että jos standardeja ei ole, niin niitä pitäisi laatia kehitysvaiheessa. Ja jos niitä ei pystytä laatimaan silloin, niin järjestelmät tulisi suunnitella niin, että ne voistais myöhemmin tuoda sinne mukaan.”

> H3: ”Meillä on esimerkiksi sillä tavalla, että meillä on olemassa niinkun kirjoitetut kirjalliset pelisäännöt siihen, että miten henkilötietoja.. niin miten henkilöt identifioivia tietoja pitää käsitellä. Et esimerkiksi, jos puhutaan vaikka asiakastietojärjestelmästä, niin konkreettisesti meillä on rajoitettu se, että esimerkiksi en minä voi vaikkapa ottaa meidän asiakastietojärjestelmästä listausta kontaktitietoineen. […] sitten toinen asia missä se näkyy on se, että tästä on myös niin kuin joka vuosi tämmöinen verkkopohjainen koulutus, joka on pakollinen kaikelle henkilöstölle. […] alihan-

kintojen seurannassa ja auditoinnissa yksi erikseen seurattava asia on, käsitteleekö tämä alihankkija meidän lukuun henkilötietoja."

H4: " Se on oikeestaan meillä kaiken toiminnan lähtökohta. Meillähän joka ikinen henkilö tänne töihin tullessaan käy tällaisen security eli turvallisuuskoulutuksen, missä käydään nämä perusteet läpi. Mutta sitten niiku esimerkiksi projektipäällikön tehtävä on huolehtia siitä, että silloin kun asiakasprojekti alkaa, niin tietyt suuntaviivat määritellään jo silloin, mutta tarvittaessa näitä täsmennetään ja määritellään aina uudelleen tarpeen mukaan, kun projekti etenee."

H6: "Että siinäkin pitää olla selkeät menettelytavat ja kriteeristöt, millä tavoin voidaan yrityksen taholta sitten päästä kiinni tämäntyyppiseen viestintätietoon tai muuhun."

Tietojen suojaamisen kannalta kenties keskeisimpänä Chowin ym. (2009) luokittelussa on kolmannen osapuolen olemassaolo. Tähän liittyen ongelmallisia osa-alueita on useita. Epäilyjä herättivät mm. lainsäädännön asettamat vaatimukset vasteajoille ja tietojen tuhoamiselle. Yksityisyyden suojaamisesta kysyttäessä monet haastateltavat ottivat vastauksessaan esille myös lainsäädännön merkityksen:

H2: "Mitä tulee sitten noiden pilvipalveluiden pystyttämisessä niin tietenkin pakolliset lainpykälät tietenkin tulisi noudattaa niiku esimerkiksi tota lait mitkä liittyy rekisterien pitämiseen ja erilaisiin muihin luetteloihin."

H3: "..että tietysti kun hankkii palvelua niin silloin sen hankkivan tahon […] ..niin sen selville otto, että missä se oikeesti sen tiedon käsittely tapahtuu ja sitten tietysti olla selvillä siitä, vaikka mitä henkilötietolaki sanoo siitä, että kuka on rekisterinpitäjä ja kuka on niinkun henkilötietojen käsittelijä."

H6: "No tietysti tää toimintahan on säädeltyä. Ja sen rooli on juurikin niin tiukka kuin miten tää säätely on voimassa ja sen mukaanhan meidän pitää toimia."

7.4 Riskienhallinta

Koska tutkimusongelman alaongelmassa ja monissa tutkielman tietojenkäsittelyyn liittyvissä standardeissa käsitellään riskienhallintaa, laadittiin haastatteluun myös kysymyksiä liittyen yritysten riskienhallintaan. Kuten jo aiemmin on todettu, Boehmin (1991), Ropposen (1999, s. 68) ja Sommervillen (2007, s. 104) mukaan riskienhallinnan tarkoituksena on tunnistaa, analysoida ja päihittää riskitekijöitä erilaisin menetelmin osana projektinhallintaa. Kysyttäessä tietoturvaan ja tietosuojaan liittyvistä riskienhallintamenetelmistä yrityksissä osa vastaajista nimesi yrityksen rakenteeseen liittyviä tekijöitä, osa seurantaan liittyviä toimenpiteitä ja osa mainitsi myös perinteisiä riskienhallintametodeja.

H1: "..että meillä nää kehitys-, testi- ja tuotantoympäristöt on täysin erotettu toisistaan. Elikkä tää meidän kehitysporukka kehittää kehitysjärjestelmissä, johon on sit-

> ten kenties liittyny osa meidän alihankintaketjua myöskin sitten, jota me käytetään tässä hommassa. Mutta se on taas sitten erotettu täysin siitä meidän tuotantoympäristöstä joka pyörii siellä aivan eri paikassa."
>
> H2: "Eli jos me esimerkiksi jätetään tarjouspyyntö, jostain järjestelmästä mikä me tehdään, niin meillä on esimerkiksi niiku jalkautettu erilaisiin teknisiin chekkilisteihin, mistä pitää käydä läpi tietyt asiat."
>
> H4: ".. ja sitten tämmösissä scrummiprojekteissa esimerkiksi.. Niinku noissa ketterissä projekteissa on tätä riskien hallintaa ja riskien status tsekataan aina niiku sprintin aikana."
>
> H5: "Projektisuunnitelmiin listataan niitä riskejä, joita olis mahdollista toteutua. Ja sitten millä tavalla niihin voitas varautua."
>
> H6: " tota tietysti meidän niikun tietoturvaan liittyvät prosessit ja tota tietoturvan hallinnoinnin prosessit ja auditoinnit ja täntyyppiset niikun tietoturvasuunnitelmat.. Ja suunnitelmathan on sentyyppisiä asioita, millä me niikun ennakoidaan niin, että täntyyppisiä tilanteita ei pääse tapahtumaan sen lisäksi että teknologinen arkkitehtuuri on sen tyyppinen että siinä pystytään erottelemaan ja segmentoimaan."

Hieman käsitellystä kirjallisuudesta poiketen kysyttäessä tietojenkäsittelyn ulkoistamiseen liittyvistä riskeistä, kaikki kuusi haastateltavaa olivat samaa mieltä siitä, että ulkoistamiseen liittyy aina joitain riskejä; jonkin palvelun ulkoistaminen sinänsä itsessään ei merkittäväsi lisää riskityyppejä verrattuna tilanteeseen, jossa kyseistä palvelua ei ulkoistettaisi.

> H3: "Mutta vois näin muuten sanoa, että en mä näe sitä.. et tuleeko siitä niinkun ulkoistamisesta uusia riskityyppejä.. vois vaan sanoo et ne samat riskit mitä itsehoidollisessa tuotannossa ehkä.. niihin on suhtauduttava niinkun järjestelmällisemmin koska ne ei ole suorassa organisaation omassa kontrollissa."
>
> H6: "..se että se ulkoistaminen on asiakkaan kannalta onnistunut, niin yleisesti se edellyttää sitä, että se asiakas myöskin ymmärtää mitä on ulkoistamassa. Toisin sanoen niin kun se, että asiakkaalla tulee olla jonkinlainen käsitys siitä heidän niikun prosesseista, minkä osin he on sitä vastuuta siirtämässä."

Tutkielman päätutkimusongelman alaongelmassa pohditaan kolmen vaihtoehtoisen riskienhallintamenetelmän potentiaalia. Kysyttäessä palvelutasosopimusten merkityksestä riskejä pienentävänä tekijänä haastatellut suhtautuivat sopimusmalleihin pääosin positiivisesti.

> H1: "Kyllähän se tiettyä turvallisuutta tuo varsinkin siinä ostavalle puolelle, että totta kai ei se sen palvelun laatua paranna. Siis SLA:han otetaan siinä vaiheessa käyttöön kun jokin menee pieleen. […] kyl se pistää sanotaan toimittajan miettimään sitä asiaa ja se pistää siihen varautumaan. Se luo tota siihen raameja, se pakottaa sut mittaamaan, se pakottaa sut niiku seuramaan ja reagoimaan näihin tota mahollisiin poikkeemiin. Etet kyl siin on tällainen ohjaava vaikutus."

> H2: ”Elikkä jos pelätään, et palvelun operointi loppuu, niin siihen voidaan sopimusteitse vaikuttaa esimerkiks sillä tavoin, et tää toinen firma takaa sen vaikka jokskin tietyks ajaks.”

> H3: ” No tietysti sillä tavalla että vaatii siltä palvelutoimittajalta niinkun kansainvälisiä sertifiointeja.. […] esimerkiksi sillä, missä määrin sillä palveluntoimittajalla on oikeus tehdä alihankintaa ja minkä osin.. ja sitten ihan myös kontrolloimalla sitä, missä se tieto käsitellään ja säilytetään.”

> H6: ”niin kyllä yhtälailla tää standardoinnin puute näkyy erityisesti näissä sopimusmalleissa, jos puhutaan palvelusanktioihin tai palvelu niikun rewardeihin taikka niinkun ostoehtoihin tai muihin asioihin, niin niissä on kyllä hyvin laajalla repertuaarilla tänä päivänä vielä valitettavasti niitä malleja.”

Palvelujen ja tuotteiden laatua ja teknistä toimivuutta voitiin pitää hyvinä riskejä alentavina tekijöinä. Tähän liittyen vastauksissa painotettiin esimerkiksi kehityksen alkuvaiheiden merkittävyyttä.

> H1: ”Ilman muuta, ilman muuta.. […] se että ne ottaa huomioon jo siellä systeemin kehityksessä ja jo tieten jättää sieltä kenties pois jotain sellaisia juttuja, jotka saattas aiheuttaa probleemia syystä tai toisesta. Että se ehkä rajottaa sitä kehitystä jonkun verran, mutta toisaalta jos sen pitää mielessä, ja tekee laatua, niin sitten niistä ei oo myöskään ongelmia tulevaisuudessa.”

> H2: ”Voidaan. Ja erityisesti nostaisin tossa ehkä nää yhteiset rajapinnat. Ja erilaiset standardit.”

Kysyttäessä kypsyysmallien hyödyntämisestä yrityksessä ja niiden riskejä pienentävästä vaikutuksesta sivuttiin mm. laatutekijöitä ja prosessiajatteluun liittyviä positiivisia ja negatiivisia puolia.

> H2: ”mun päälimmäinen kuva niistä malleista on, et siinä pyritään tietyllä tapaa varmistamaan et se softaprosessi on toistettavissa.. […] sanotaan et mä uskon, että on parempia tapoja varmistaa laatua pelkästään sitä prosessin laatua valvomalla. Et sil on merkitystä mutta mä en ehkä koe sitä hirvittävän suurena.”

> H6: ”..esimerkiksi cmmi-malleihin tai muihin tämmöisiin maturiteettimalleihin, niin nää on tietysti miten mekin niikun itseämme rankataan. Ja se on ehkä semmosia asioita yhtä lailla niikun meidän prosessiauditointeja ja muitten ja niitten standardisointien kautta miten me halutaan asiakkaille se varmistaa, että he tietää, että mitä he on ostamassa ja minkä tyyppistä maturiteettia..”

7.5 Tietojenkäsittelystandardit ja -kehysmallit

Viimeisenä käsiteltävää teemaa voidaan pitää tutkielman kannalta kenties olennaisimpana — ainakin päätutkimusongelman kannalta. Teema on samalla myös haasteellinen vähäisen akateemisen tutkimuksen tähden. Lyytisen ja Kingin (2006) mukaan standardien merkitys on korostunut vuosien mittaan, mutta

niiden tutkimus on edelleen melko vähäistä. Vaqueron ym. (2009) mukaan standardien puuttuminen asettaa pilvien turvallisuuden ja yhteentoimivuuden merkittävälle koetukselle. Osittain näistä lähtökohdista muotoutui tutkielman tutkimusongelma. Haastattelun viimeisen teeman aloitti kysymys koskien haastateltavien mielipidettä tietojenkäsittelystandardeista ja kehysmalleista. Tietojenkäsittelystandardeihin ja kehysmalleihin suhtauduttiin erittäin positiivisesti.

> H1: ”Ehottoman hyviä. Ja me pyritään tässä meidän toiminnassa noudattamaan niitä niin pitkälle kuin mahdollista. Koska kyl mun mielestä niiden merkitys vaan korostuu tässä tällasessä one-size-fits-for-all –tyyppisessä jutussa, et mitä enempi rajapinnat, mitä enempi kaikki tää perustuu standardeihin, niin tää helpottaa sanotaan molempien osapuolten elämää älyttömästi”

> H2: ”Että niiku ne standardit, mitä me käytetään, liittyy olemassa oleviin ohjelmistotuotantomenetelmiin. Ja tota tarvittaisko me omia standardeja mahdollisesti nimenomaan niiku pilvipalveluiden tuotantoon, niin tuskin meidän ehkä niiku ihan tyhjästä tarvii uusia keksiä. Mut tää on niiku uus näkökulma, joka niiku nostaa.. korostaa jotain tiettyjä uusia asioita. Niin tota jonkinlainen delta näiden vanhojen tai olemassa olevien, hyviksi havaittujen tapojen päälle pitäis ehkä vielä niiku lisätä.”

> H5: ”No siis kyllähän se helpottaa työtä kun on jokin ohje jonka mukaan mennään. Ei tarvi joka kerta itte säveltää uusiks noita. Ja tietojenkäsittelyssä yleensä nuo standardit on paljon sellasia de facto –standardeja, eli tehään joku, että ei ole varsinaista mitää ISO-numeroa tai vastaavaa.”

> H6: ”Siis näähän on niiku oleellisia tekijöitä siinä jos mietitään miten ylipäätään tällainen niikun IT-palvelumarkkina on kehittynyt. […] Oli ne sitten niiku prosessistandardia ja ITILiä ja muuta, tietoturvaan liittyviä standardeja tai muuta niinniin ilman näitä asiakkaan olisi hyvinkin paljon vaikeampi vertailla eri toimittajien kypsyyttä ja sitä palveluprosessia mitä he pystyy toimittaa.”

Haastateltavien mielipidekartoituksen jälkeen pyrittiin vielä selventämään, mitä standardeja heidän yrityksessään hyödynnetään. Jokainen yritys hyödynsi standardeja jollain tapaa, ja monissa tilanteissa yritys oli luonut omat käytänteensä jonkin aiemmin luodun yleisen standardin pohjalta.

> H1: ”Ja totta kai sitten täällä, jos esimerkiksi tuotekehityksestä puhutaan, niin kyllähän meillä täällä kehityksessä on omat kehitysprosessit, jotka on standardeja. Joskin harva standardi käy ihan heittämällä, että ainahan siitä on yrityskohtaisia ratkaisuja ja vähän säätöä.”

> H3: ”Niin niin tuota joo, sovelletaan. Ja lähinnä meillä sen nimi on [tuotteen nimi] mutta tuota se pohjautuu käytännösssä niin eniten ITILiin ja sisältää käsittääkseni jotain asetelmia sitten CobiTista.”

> H4: ”Niin kyllähän siellä aina on.. totta kai nämä niiku ylleiset standardit huomioiaan, mutta hyvin pitkälti omiin tarpeisiin räätälöityjä.”

> H6: ” Kyllä joo, meillä on, me ollaan ISO-standardoitu sekä niiku tietoturvan puolella että tota nää niiku ISO-mallin mukaisesti meil on tarkennettu useita standardeja. […] jos on niiku kriittisiä tämmösiä niikun sovelluskehitysympäristöjä ja sovelluspalve-

luita, niin siellä näitä cmmi:n vitostasoja meillä on.. nää on ne niiku mitkä pääsääntösesti ohjaa ja nää ISO 27000 security puolen asiat meillä on.. ja ITILi prosessimallin mukaista toimintaa."

Kenties merkittävämpänä kysymyksenä tutkielman kannalta voidaan pitää kysymystä, jossa haettiin vastausta siihen, voidaanko standardien ja kehysmallien avulla parantaa tietosuojaa ja yksityisyyttä. Youseff, Butrico & Da Silvan (2008) mukaan puutteellinen standardointi pilvipohjaisessa tietojenkäsittelyssä johtaa siihen, että jokaisella toimijalla on omat käytäntönsä ja näin ollen esimerkiksi tietoturvaan ja tietosuojaan liittyvät osa-alueet ovat epäselviä. Esitetty kysymys tuotti hyvinkin erilaisia vastauksia – puolesta ja vastaan.

H1: "Kyl mä luulen, kyl mä luulen. […] voisin kuvitella, jos tietosisällöt tietomallit näissä integraatiorajapinnoissa on esimerkiksi hyvin mietitty ja niitä noudatetaan ja sitten nää standardien kuljetuskerrokset on turvallisia niin ihan varmasti. Etet kyl se varmaan poistaa sellaista osittain tahatontakin paikkaa sille, mistä niitä vuotoja voisi tulla"

H2: "Hmm.. Mä oisin tähän niiku valmis sanomaan että ei. Että sinänsä niiku standardit itsessään ei vielä niiku itsessään lupaa mitään. […] mä pikemminkin uskon että tavallaan me saadaan tietosuojaa ja yksityisyyttä paremmin taklattua niiku oikeantyyppisellä valvonnalla. Ja avoimuudella. Et standardoinnilla me pystytään tietyllä tapaa edesauttamaan näiden tiettyä asioiden käyttöönottoa, et se helpottaa sitä kynnystä tehdä turvallisia palveluita, mut ei pystytä sillä takaamaan, että niitä noudatetaan."

H3: "..toki malleilla parantaa tietyllä tapaa tietosuojaa ja yksityisyyden suojaa, koska tulee perusasiat huomioitua, mutta ehkä kannattaa.. niiden orjallinen noudattaminen tai kirjaimen noudattaminen ei aina sitten tietysti välttämättä riitä, vaan tarvii olla sitten oma järki siinä asiassa.. Että nehän on vain hyviä aikaisempia käytäntöjä, jotka on dokumentoitu ja kuvattu. Ja saattaa tulla aidosti tilanteita joissa täytyy mennä pidemmälle"

H4: "No mä sanon että en.. minä en ihan.. mun mielestä se tietosuojan ja yksityisyyden.. niiku se tietosuojan ymmärtäminen ja sen, että mitä se yksityisyyden suojaaminen meidän kehittäjien näkökulmasta tarkoittaa.. niin mun mielestä se on just se, että tavallaan sen täytyy olla kaikilla niin selkärangassa […] Se on meidän jokaisen tehtävä huolehtia siitä, että nämä tietosuoja ja yksityisyys ja niiku asiakkaan yksityisyyden huomioiminen varmasti täyttyy. Et se on niiku meiän jokaisen tehtävä. Mä en niiku nää, että standardeilla ja joillain kehysmalleilla siihen niiku sillai vaikutetaan. Vaan se on jokaisen meiän nupissa."

H5: "Mutta jos ajattelee ihan taas koodaamisen näkökulmasta niin siihen ei hirveesti oo mitään sellasta valmista sapluunaa, että miten se pitäis tehdä."

H6: "sanotaan et standardien osalta voidaan varmistaa se, että että tota toimitaan.. sanotaan näin, että sen laatutason mukaisesti mikä on ennalta määritetty. Toisin sanoen pystytään varmistamaan se että toiminta vastaa sitä määritystä, mikä tota on standardeissa määritelty. Ja sen avulla pystytään niikun asettamaan selkeälle kontrollia mitä vastaan pystytään selkeästi auditoimaan sitä meidän operatiivista toimintaa. […] Sanotaan et joku tällainen niiku EU-tasoinen säädöstyö on myöskin niikun

> merkittävän tärkeää ja aivan oikealla tavalla ajaa sitä henkilötiedon ja tietosuojaan liittyvää säädöksiä että tota […] että me niikun ymmärretään meidän niikun eri dataprosessori- taikka muut roolit tai mitkä ne vastuut ja velvollisuudet on tota näissä rooleissa toimiessamme"

Aivan haastattelun loppuun tiedusteltiin, mitä mieltä haastateltavat ovat, tulisiko pilviteknologiaa jotenkin standardoida. Pääosin pilviteknologian standardoiminen nähtiin tavoittelemisen arvoisena asiana, vaikkakin haasteellisena. Toisaalta standardoiminen asetettiin kyseenalaiseksi, jos se estää innovaatioiden synnyn.

> H2: "Eli mä ite uskon että teknologiapuolella tarvitaan yhteisiä rajapintoja. […] Ja totaa mitä sitte tulee tohon prosessipuolelle niin uskon, että fiksut organisaatiot räätälöi parhaiten omat prosessinsa. Mut niitä prosesseja vois ehkä olla valvomassa joku luotettu kolmas osapuoli, jolle niiku tämä tietoturva ja ynnä muut näkökulmat olis eniten heidän sydämen asiansa."

> H3: "No siis ainakin siltä osin, että palveluiden ostajien, kautta rakentajien näkökulmasta erilaisia niinkun.. lienee tarve miettiä sitä, että miten esimerkiksi rajapintoja ja muuta tämmöstä, olisko syytä standardoida."

> H4: " Että tavallaan se on niiku kaksteräinen miekka, että okei standardoiminen on hyvä juttu, kun se antaa raamit, mutta se kolikon kääntöpuoli on, että se hyvin herkästi niiku sulkee innovoinnin pois."

> H1: " Varmaan haastava kenttä, mutta olis varmaan kaikkien etu, jos päästäs johonki tälläseen. Ilman muuta. […] kyl mä luulen, et se saattais jos siellä olis jotakin standardinomaista, niin mä luulen et se edesauttais myös sitten tän uskonnon leviämistä aika paljon."

8 TULOKSET JA PÄÄTELMÄT

Tässä luvussa käsitellään ja analysoidaan lähdekirjallisuuden sekä haastatteluvastausten avulla asetettuja tutkimusongelmia vastauksineen. Molemmat tutkimusongelmat käsitellään erikseen, minkä jälkeen arvioidaan tutkimuksen onnistumista. Aivan luvun lopussa on kirjoittajan omaa kontribuutiota tutkielmassa käsiteltävistä aiheista.

8.1 Vastaus päätutkimusongelmaan

Päätutkimusongelmassa käsitellään tietoturvan ja tietosuojan huomioimista pilvipalveluita kehitettäessä erilaisten tietojenkäsittelystandardien ja -kehysmallien avulla. Tutkimusongelmaa voitaneen lähestyä monella tapaa pohdittaessa lähdekirjallisuudessa ja haastatteluaineistossa esiintyviä seikkoja. Tässä yhteydessä pohdinnan voidaan ajatella mukailevan Tuomen & Sarajärven (2002, s. 98) teoriasidonnaista analyysiä, jossa analyysiyksiköt valitaan aineistosta, mutta aikaisempi tieto ohjaa tai auttaa analyysiä.

8.1.1 Tietoturva

Pohditaan ensiksi tietoturvan ja tietosuojan määritelmiä. Hakalan, Vainion & Vuorisen (2006, s. 4) mukaan luotettavuus, käytettävyys ja eheys ovat tietoturvan peruspilarit. Tarkasteltaessa tässä tutkielmassa esiintyviä aihealueita voidaan havaita, että erityisesti luotettavuus ja käytettävyys liittyvät keskeisesti pilviteknologian ja pilvipalveluiden tietoturvaan. Luotettavuuden merkitystä voidaan perustella pilviteknologialle luonteenomaisella palvelurakenteella ja tähän liittyvällä tietojenkäsittelyn ulkoistamisella. Käytettävyys on taas esimerkiksi Vaqueron ym. (2009) mukaan keskeinen pilviteknologian nopeaan yleistymiseen vaikuttava tekijä.

Haastattelujen avulla saaduista vastauksista voidaan päätellä, että luotettavuutta edistetään erilaisin teknisin keinoin tietoa salaten ja sidosryhmille ase-

tettavin vaatimuksin. Asetettuja vaatimuksia auditoidaan tarvittaessa. Käytettävyyden eri osa-alueista pilvipalveluiden käytön helppoutta ei nähdä pelkästään positiivisena asiana, vaan helppouteen liittyy aina jonkinlaisia rajoitteita — esimerkiksi tietoturvan määrittelyssä yrityskohtaisesti. Saatavuuteen liittyviä tekijöitä tulee esiin vastauksissa pilvien ja palvelurakenteen eri osa-alueiden välisen yhteentoimivuuden turvaamiseksi.

Tutkielmassa on käsitelty tietoturvaan läheisesti liittyviä tietojenkäsittelystandardeja. Näistä esimerkiksi ISO/IEC 9126 ja ISO/IEC 13236 -standardit sekä Common Criteria- ja ITIL-kehysmallit ottavat huomioon luotettavuuteen ja käytettävyyteen liittyviä tekijöitä kehitettäessä tietojenkäsittelypalveluita ja -sovelluksia. Mitä tulee muuhun standardointiin, vastausten perusteella sidosryhmille asetettavia vaatimuksia voitaisiin standardoija ja erityisesti saatavuuden suhteen teknisten ratkaisujen standardoinnille olisi tarvetta.

8.1.2 Tietosuoja

Käsiteltäessä tutkimusongelman toista merkittävää osa-aluetta, tietosuojaa, lähtee pohdinta ja analyysi liikkeelle jälleen termin määrittelyllä lähdekirjallisuudessa. Järvisen (2010) mukaan tietosuojassa on kyse ”henkilöön tai hänen toimintaansa liittyvien tietojen suojaamisesta luvatonta keräämistä ja käyttöä vastaan”. Tässä yhteydessä havaitaan konkreettinen ero tietoturvaan liittyen. Pilviteknologiaa ja pilvipalveluita ajatellen tietosuoja on uhattuna ainakin kahdesta eri näkökulmasta: Ensinnäkin tietojenkäsittelyn ulkoistamiseen liittyen ja toiseksi teknologialle luonteenomaisen tietojen hajauttamisen tähden. Chowin ym. (2009) mukaan kolmannen osapuolen läsnäolo luo tilanteen, jossa tiedon kontrollointi hämärtyy.

Saatujen haastatteluvastausten perusteella tietosuojan ja yksityisyyden turvaaminen on tärkeä asia. Useimmissa vastauksissa korostettiin yrityksessä määriteltyjä käytäntöjä tietojen suojaamiseksi unohtamatta erilaisia lakeja ja viranomaisvaatimuksia. Erilaiset prosessit, kirjalliset määritelmät ja tietosuojaan liittyvät koulutukset olivat konkreettisia tapoja edistää tietosuojan toteutumista. Tämän lisäksi tietosuojan merkitys korostui jokaista työntekijää koskevana asiana.

Näin ollen voidaan päätellä, että tehokas tietosuoja edellyttää suunnittelua, asetettuja rajoitteita ja koulutusta, joiden avulla yrityksen työntekijät käsittelevät tietoa riittävällä tietosuojatasolla. Tietosuojan aitoa toteutumista ja tietojenkäsittelyn ulkoistamista on aiheellista pohtia tästä näkökulmasta. Tietosuojan toteutumisen valvonta tai erilaiset auditoinnit lienevät keino lisätä luottamusta entisestään toimijoiden välillä. Oikeanlainen avoimuus ja läpinäkyvyys voivat olla merkittävässä roolissa tietosuojan toteutumiselle eri sidosryhmien välillä.

Käsitellyistä tietojenkäsittelystandardeista esimerkiksi ISO/IEC 17799 - ja ISO 27001 -standardit pitävät sisällään määrittelyt erilaisille tietoturvaa ja tietosuojaa edistäville toiminnoille ja käytänteille yrityksessä. Näiden lisäksi ISO 22307 ja IEEE 1028 -standardit käsittelevät tietosuojan merkityksen ja toteutumisen arviointia. Haastatteluvastausten perusteella voitaisiin varovaisesti pää-

tellä, että useimmissa haastatelluista yrityksistä on käytössään jonkinlainen tietoturvallisuuden hallintajärjestelmä — tai ainakin osia siitä. Tämän lisäksi vastausten perusteella yrityksissä on erilaisia arviointiprosesseja asetettujen tietosuojavaatimusten toteutumiselle. Standardointia voitaisiin kehittää esimerkiksi tietosuojan auditointien ja valvonnan suhteen.

Jotta voitaisiin arvioida standardien ja kehysmallien merkitystä tietoturvaa ja tietosuojaa edistävinä tekijöinä, tulee käsitellä myös yritysten omia, standardinomaisia käytänteitä tai prosesseja tietoturvan ja tietosuojan takaamiseksi. Näin ollen joudutaan käsittelemään jossain määrin tutkielman kannalta ongelmallista kysymystä siitä, voidaanko yritysten omia erikseen määriteltyjä käytänteitä ja prosesseja tarkastella rinnan esimerkiksi ISO-standardien kanssa. Lähdekirjallisuuden ja saatujen vastausten perusteella suuri osa yrityksistä räätälöi valmiiden standardien pohjalta omat, kyseiseen yritykseen soveltuvat standardit. Tarkasteltaessa esimerkiksi prosessi- ja riskienhallintastandardeja voidaan havaita, että niille on luonteenomaista korkeampi abstraktiotaso, joka antaa standardin soveltamiselle laajemmat ja joustavammat lähtökohdat. Tällöin esimerkiksi standardin osittainen hyödyntäminen saattaa realisoitua yrityksessä

8.1.3 Yhteenveto

Tutkimusongelmalle voitaisiin määritellä seuraavanlainen vastaus: Tietoturva ja tietosuoja voidaan huomioida monella tapaa tietojenkäsittelystandardien ja -kehysmallien avulla kehitettäessä pilviteknologiaa ja pilvipalveluita. Tietoturvan huomioiminen voi olla esimerkiksi osana prosessi- tai laatustandardin mukaista toimintaa yrityksessä. Samalla tavalla tietosuoja voi olla huomioituna tietoturvan hallintajärjestelmässä, esimerkiksi tietojenkäsittelykäytäntöinä. Tässä tutkielmassa käsiteltyjen tietojenkäsittelystandardien luonteeseen kuuluu hyvin spesifien tietoteknisten ratkaisujen rajautuminen standardien ja kehysmallien ulkopuolelle. Näin ollen tietoturvaa ja tietosuojaa pohdittaessa erilaisten kansainvälisten sekä kansallisten säädöksien ja määräysten merkitys korostuu pilviteknologiaa tai -palveluita kehitettäessä. Voidaan myös huomata, että pilviteknologiaan liittyviin erityispiirteisiin voitaisiin kehittää standardeja.

8.2 Vastaus tutkielman alaongelmaan

Tutkielman alaongelmassa haettiin vastausta kysymykseen, kuinka palvelutasosopimusten, teknisesti toimivien ja laadukkaiden ratkaisujen sekä kypsyysmallien avulla voidaan pienentää pilvipalveluihin liittyviä riskejä. Koska pilvipalveluita hankitaan palvelunomaisesti, liittyy tietojenkäsittelyn ulkoistaminen oleellisesti aihealueeseen. Tämän lisäksi, kuten aikaisemminkin on todettu, kolmannen osapuolen olemassaolo lisää tietoturvan ja tietosuojan rikkoontumisen riskejä. Kaufmanin (2010) mukaan tietoturva-asioita pohdittaessa tulee

ottaa huomioon, että hajautettu tietojenkäsittely on turvallisuudeltaan aina yrityksen sisäistä arkkitehtuuria heikompaa.

8.2.1 Palvelutasosopimukset riskienhallinnan instrumenttina

Kolmiosainen tutkimuskysymys osoittautui haasteelliseksi, ja vaihtoehtojen asettaminen jollain tapaa paremmuusjärjestykseen lienee mahdotonta. Tässä yhteydessä jokaista vaihtoehtoa käsitellään rinnakkain kirjallisuuden ja saatujen vastausten kanssa.

Kysymyksen ensimmäinen vaihtoehto koskee palvelutasosopimuksia. Lähdekirjallisuuden pohjalta voidaan väittää, että palvelutasosopimusten tarkoituksena on poistaa sopijaosapuolien välistä epäselvyyttä vastuista ja velvollisuuksista. Palvelutasosopimusten avulla myös määritellään palveluiden sisältö. Karkeasti yleistäen voitaisiin siis ajatella, että palvelutasosopimuksilla on yhteyksiä ainakin epävarmuuden hallintaan. Onko kyseessä varsinainen riskienhallinnan instrumentti, lienee määrittelykysymys.

Haastatteluista saatujen vastausten perusteella palvelutasosopimuksia voidaan hyödyntää ainakin osittain riskienhallinnallisena työkaluna. Sopimusteitse on mahdollista sopia esimerkiksi palvelun jatkuvuudesta palveluntarjoajan kohdatessa vaikeuksia toimittaa palveluaan. Samalla tapaa palvelutasosopimus ohjaa palveluntarjoajaa tuottamaan palveluita, jotka esimerkiksi vastaavat sopimuksissa määriteltyjen palveluiden suorituskykyä. Näin ollen voidaan ajatella, että palvelutasosopimukset toimivat osittain asiakkaan riskejä pienentävinä instrumentteina, osittain palveluntarjoajan toimintaa ohjaavina kirjallisina määritelminä.

8.2.2 Toimivat ja laadukkaat ratkaisut riskejä pienentävinä tekijöinä

Alaongelman tässä osassa on oleellinen yhtymäkohta päätutkimusongelmaan. Lähdekirjallisuuden perusteella esimerkiksi prosessi- ja laatustandardien avulla voidaan ennaltaehkäistä riskitekijöiden realisoitumista lopullisessa tuotteessa tai palvelussa. Näin ollen esimerkiksi tietoturvaan liittyviä osa-alueita voidaan huomioida tehokkaammin erilaisten standardien ja kehysmallien avulla.

Haastatteluista saatujen vastausten perusteella voidaan kritisoida kysymyksen asettelua. Toimivuus on melko suoraviivaisesti yhdistettävissä esimerkiksi palvelun saatavuuteen ja määritellyn suorituskyvyn toteutumiseen, mutta se, mitä laadulla tarkoitetaan tässä yhteydessä, oli epäselvästi määriteltyä. Tässä yhteydessä laadulla pyrittiin tarkoittamaan vastaavanlaisia tekijöitä kuin toimivuudellakin. Näin ollen asiakasyrityksen laadun kokemus rajautuu pois. Saaduissa vastauksissa korostui kirjallisuuden tavoin proaktiivisuus ja standardien merkitys.

8.2.3 Kypsyysmallit riskienhallinnan työkaluna

Alaongelman kolmas vaihtoehtoinen tapa hallita riskejä liittyi kypsyysmallien hyödyntämiseen. Pilviteknologiaan ja pilvipalveluihin liittyviä kypsyysmalleja ei vielä esiinny akateemisessa kirjallisuudessa juurikaan, mutta tutkielmassa käsitellyt kypsyysmallit ovat sovellettavissa myös tässä yhteydessä. Intuitiivisesti voitaisiin olettaa, että organisaation ja prosessien kypsyys vaikuttaisi riskejä pienentävällä tavalla kehitettäviin tuotteisiin ja palveluihin. Lähdekirjallisuudessa esiintyi intuitiota osittain tukevaa argumentaatiota. Khoshgoftarin ym. (2009) mukaan kypsyysmallien tarkoituksena voidaan pitää paremman liiketoimintatuloksen aikaansaamista arvioimalla organisaation projektinhallinnan heikkouksia ja vahvuuksia, vertaamalla kypsyyttä kilpailijoihin sekä mittaamalla projektihallintatason ja saatujen tulosten riippuvuutta. Münstermannin & Weitzelin (2008) mukaan prosessien standardointi on menestystekijä ulkoistamisen onnistumisen kannalta.

Mielipiteet ja kokemukset kypsyysmalleista riskienhallintatyökaluina vaihtelivat haastateltavien kesken. Tässä yhteydessä lienee aiheellista pohtia myös kypsyysmallien ensisijaista käyttötarkoitusta yrityksessä. Jos prosessien toistettavuus ja tehokkuus on lähtökohtana, voi riskienhallinnallinen näkökulma olla pienempi. Toisaalta sitten, jos yrityksen tarkoituksena on kehittyä ja toteuttaa laadukkaampia palveluja kypsyyttä mittaamalla ja arvioimalla, voi riskien pienentyminen olla merkityksellisempää.

Lähdekirjallisuuden ja haastatteluvastausten avulla voidaan päätellä, että kypsyysmalleilla voi olla riskejä pienentäviä vaikutuksia, mutta ensisijaisesti kysymyksessä on prosessien kyvykkyyteen, suorituskykyyn ja kypsyyteen liittyvä arviointityökalu.

8.3 Tutkimuksen arviointi

Hirsjärven, Remeksen & Sajavaaran (1997) mukaan tutkimuksessa pyritään välttämään virheitä, mutta silti tutkimuksen luotettavuutta on aiheellista pohtia. Tuomen & Sarajärven (2006) mukaan laadullisen tutkimuksen arviointi on aina kokonaisuuden arviointia, ja arvioinnissa voidaan käsitellä esimerkiksi tutkimuksen kohdetta, tutkimuksen tarkoitusta, aineiston keruuta ja tutkimuksen luotettavuutta.

Tässä tutkielmassa on tutkittu tietojenkäsittelystandardeja, joissa huomioidaan tietoturva ja tietosuoja. Kirjoittajan tarkoituksena on antaa lukijalleen mahdollisimman monipuolinen kuva tietoturvaan ja tietosuojaan liittyvistä asioista pilviteknologiaa ja pilvipalveluita kehitettäessä erilaisten standardien ja kehysmallien avulla. Tavoite on pyritty saavuttamaan käsittelemällä kirjallisuudesta löytyviä teemoja aiheeseen liittyen, toteuttamalla empiirinen tutkimus ja analysoimalla löydettyjä yhtäläisyyksiä sekä eroavaisuuksia. Mielestäni tässä on onnistuttu melko hyvin.

Tiedon ja aineiston keruuta on aiheellista pohtia erikseen — ensinnäkin lähdekirjallisuuden suhteen ja toiseksi haastattelujen avulla saadun aineiston suhteen. Lähdekirjallisuuden hankinta pyrittiin toteuttamaan mahdollisimman kattavasti hyödyntäen käytettävissä olevia tietolähteitä. Tiedon keruu rajoittui tunnetuimpiin IT-alan tietokantalähteisiin, akateemiseen materiaaliin internetissä ja paikallisiin monografioihin. Kokonaisuutta ajatellen jokaista teemaa käsiteltiin monipuolisesti, joten tiedon keruu onnistui hyvin.

Haastattelujen onnistuminen tulee analysoida tiedon keruuta kriittisemmin — kenties jopa hieman kyseenalaistaa. Saatujen haastatteluvastausten perusteella on mahdollista ymmärtää jotain tutkimuksen moniulotteisuudesta. Vaikka laaditut kysymykset oli suunniteltu tarkkaan, niiden tulkinta oli kuitenkin tapauskohtaista ja toisaalta haastattelutilanteesta riippuvaa. Hirsjärven, Remeksen & Sajavaaran (1997) mukaan on aiheellista pohtia miten tutkijan kielenkäyttö on vaikuttanut haastattelukysymysten ymmärtämiseen ja toisaalta onko tutkija itse ymmärtänyt tutkittaviaan. Tähän liittyen huomattiin, että esimerkiksi standardin määritelmän moniulotteisuus asetti haasteita haastatteluvastausten analysoinnissa. Ymmärrettiinkö standardi vain esimerkiksi ISO- tai IEEE-standardointiorganisaation määrittelemäksi vai voitiinko yrityksen omia, määriteltyjä käytänteitä tai prosesseja pitää standardeina? Jos käsitellyt standardit olisivat olleet luonteeltaan teknisempiä, saadut tutkimustulokset olisivat olleet mahdollisesti selkeämpiä tutkielmassa saatuihin tuloksiin verrattuna.

Kenties merkittävimpänä haasteena tutkielman kannalta oli sen oikeanlainen rajaus. Hirsjärven, Remeksen & Sajavaaran (1997) mukaan aloittelevat tutkijat tekevät perusvirheen valitsemalla aiheita, jotka ovat liian laajoja. Yhden tutkimusongelman käsitteleminen olisi kenties rajannut kokonaisuutta tehokkaammin.

Saavutettujen tulosten perusteella voidaan kuitenkin havaita tietojenkäsittelystandardien kokonaisvaltainen merkitys osana turvallista tietojenkäsittelyä. Näin ollen saatujen tutkimustulosten voidaan ajatella antavan suuntaa pohdittaessa tietojenkäsittelyn kehitystä lähivuosina — erityisesti pilviteknologiaa ja pilvipalveluita ajatellen.

8.4 Kontribuutio tutkielmasta

Tässä tutkielmassa on käsitelty tietojenkäsittelystandardeja ja -kehysmalleja sekä niissä esiintyvää tietoturvan ja tietosuojan huomioimista. Koska tietoturvan ja tietosuojan vaarantuminen on merkittävä riski, on tutkielmassa käsitelty myös riskienhallinnallista näkökulmaa. Kokonaisuus on pilviteknologian kontekstissa.

Tutkielman avulla voidaan havaita, että pilviteknologiassa ja pilvipalveluissa on tarvetta standardoimiselle. Haasteena on, kuinka laajasti standardointia tulisi toteuttaa, että tietoturva ja tietosuoja olisivat riittävällä tasolla. Haastatteluvastausten perusteella voidaan havaita, että tässä tutkielmassa rajauksen

ulkopuolelle jäänyt pilviteknologian ja pilvipalveluiden teknisten ratkaisujen standardointi on erittäin ajankohtaista.

Tärkeintä pilviteknologian ja pilvipalveluiden yleistymisen kannalta on kuitenkin se, että tietoturva- ja tietosuoja-asioihin kiinnitetään erityistä huomiota — tapahtuipa huomioiminen sitten standardien, kehysmallien, hyvien käytäntöjen tai yritysten itse määrittelemien prosessien avulla.

9 POHDINTA

Tässä tutkielmassa on käsitelty tietoturvan ja tietosuojan huomioimista hyödynnettäessä tietojenkäsittelystandardeja pilviteknologiaa ja pilvipalveluita kehitettäessä. Motiivi tutkielman aiheelle nousi pilviteknologian ajankohtaisuudesta ja henkilökohtaisesta kiinnostuksesta standardeja kohtaan.

Pilviteknologian yhdistäessä aikaisempia teknologisia ratkaisuja on kehittynyt tietojenkäsittelymenetelmä, jossa tietojenkäsittelyä myydään hyödykkeenä veden tai sähkön tapaan. Kustannustehokas, skaalautuva, helppokäyttöinen ja internetin yli tarjottava tietojenkäsittelyparadigma on nopeaa vauhtia yleistymässä globaalisti. Pilviteknologian turvallisuus herättää kuitenkin huolta monessa organisaatiossa.

Tästä syystä tietoturvaan ja tietosuojaan liittyviä aihealueita tulee ottaa erityisellä tavalla huomioon pilviteknologiaa ja pilvipalveluita kehitettäessä, jotta luottamus pilvipalveluihin kasvaisi. Kolmannen osapuolen olemassaolo, tietojen hajauttamisesta aiheutuva tiedon kontrollin hämärtyminen ja teknologian kehittymättömyys ovat merkittäviä riskejä aiheuttavia uhkatekijöitä tietoturvalle ja -suojalle. Nämä asiat tulee ottaa huomioon kehitettäessä pilviteknologiaa ja pilvipalveluita.

Tietoturvaa ja tietosuojaa on mahdollista huomioida hyödynnettäessä erilaisia tietojenkäsittelystandardeja ja -kehysmalleja. Vaikka määriteltyjä standardeja ei ole suoraan tarkoitettu pilviteknologian kontekstiin, voidaan niitä kuitenkin hyödyntää monella tapaa. Tässä tutkielmassa on käsitelty tietoturva-, laatu, prosessi- ja riskienhallintastandardeja. Lähdekirjallisuuden avulla on käsitelty myös aikaisempaa tutkimusta ja standardeihin liittyviä osa-alueita.

Varsinainen tutkimusongelma käsittelee tietoturvan ja tietosuojan huomioimista tietojenkäsittelystandardeja ja -kehysmalleja hyödynnettäessä. Tutkielman alaongelma sen sijaan keskittyy riskienhallintaan ja tässä palvelutasosopimusten, toimivien ja laadukkaiden ratkaisujen sekä kypsyysmallien potentiaaliin riskejä pienentävinä tekijöinä.

Tutkielman empiirinen osa toteutettiin laadullisena tutkimuksena ja aineisto kerättiin teemahaastattelujen avulla. Haastatteluihin osallistui yhteensä kuusi henkilöä viidestä eri yrityksestä. Saatujen vastausten avulla pohdittiin

lähdekirjallisuudessa esiintyvien määritelmien, väitteiden ja tutkimustulosten yhtenevyyttä.

Analyysin ja pohdinnan perusteella voidaan todeta, että tietoturva ja tietosuoja voidaan ottaa monella eri tavalla huomioon hyödynnettäessä erilaisia tietojenkäsittelystandardeja ja -kehysmalleja. Konkreettisimpina tekijöinä haastatteluissa mainittiin yritysten itse laatimat prosessit, joissa tietoturva otetaan huomioon pilviteknologiaa tai pilvipalveluita kehitettäessä tai tarjottaessa. Tietosuojan takaamisen kannalta oli havaittavissa, että esimerkiksi tietoturvallisuuden hallintajärjestelmien hyödyntäminen yrityksissä voisi olla järkevää.

Haastatteluiden perusteella voidaan päätellä, että palvelutasosopimukset, toimivat ja laadukkaat tietojenkäsittelyratkaisut sekä kypsyysmallit pienentävät tietoturvan ja tietosuoja pettämiseen liittyviä riskejä. Erityisesti palvelutasosopimusten vaikutukset epävarmuudenhallintaan olivat aidosti olemassa. Näin ollen myös riskejä pienentävä vaikutus oli konkreettinen, vaikkakin ehkä enemmän ohjaava luonteeltaan.

Kokonaisuudessaan tutkielman tarkoituksena oli käsitellä ajankohtaista teemaa mahdollisimman monipuolisesti tutkimusongelmien ja niihin saatavien vastausten avulla. Tutkielman avulla on mahdollista herättää keskustelua standardoinnin tarpeesta pilviteknologian ja pilvipalveluiden turvallisuuden takaamiseksi.

LÄHTEET

Al-Kilidar, H., Cox, K. & Kitchenham, B. (2005). The use and usefulness of the ISO/IEC 9126 quality standard. *International Symposium on Empirical Software Engineering, November 17-18* (s. 1-7).

Armbrust, M., Fox, A., Griffith, R., Joseph A.D., Katz R.H., Konwinski A., Lee, G., Patterson D.A., Rabkin A., Stoica I. & Zaharia M. (2009) *Above the Clouds: ABerkeley view of cloud computing*. (Technical Report UCB/EECS-2009-28), University of California at Berkeley, Electrical Engineering and Computer Sciences.

Arraj, V. (2010). ITIL The Basics. APM Group Limited. Haettu 17.8.2010 osoitteesta http://www.best-management-practice.com/gempdf/ITIL_The_Basics.pdf

Asnar, Y., Moretti, R., Sebastianis, M. & Zannone, N. (2008). Risk as Dependability Metrics for the Evaluation of Business Solutions: A Model-driven Approach. *Third International Conference on Availability, Reliability and Security (ARES), March 4-7* (s. 1240-1247).

Aundhe, M.D & Mathew, S.K. (2009). Risks in offshore IT outsourcing: A service provider Perspective. *European Management Journal, 27*(6). 418– 428.

Baldassarre, M.T., Piattini, M., Pino, F.J. & Visaggio, G. (2009). Comparing ISO/IEC 12207 and CMMI-DEV: Towards a mapping of ISO/IEC 15504-7. In *Proceedings of the International Conference on Software Engineering (ICSE) Workshop on Software Quality (WOSQ), Vancouver, Canada, May 16* (s. 59-64).

Barlette, Y. & Fomin, V.V. (2008). Exploring the Suitability of IS Security Management Standards for SMEs. In *Proceedings of the 41st Annual Hawaii international Conference on System Sciences (HICSS) January 7-10* (s. 308). Washington: IEEE Computer Society.

Beasley, M.S., Clune, R. & Hermanson, D.R. (2005). Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy 24*(6), 521-531.

Blind, K. & Gauch, S. (2008). Trends in ICT standards: The relationship between European standardisation bodies and standards consortia. *Telecommunications Policy, 32*(7), 503-513.

Bode, S., Fischer, A., Kühnhauser, W. & Riebisch, M. (2009). Software Architectural Design Meets Security Engineering. In *Proceedings of the 16th Annual IEEE international Conference and Workshop on the Engineering of Computer Based Systems (ECBS), April 14-16* (s. 109-118) Washington: IEEE Computer Society.

Boehm, B.W. (1988). A spiral model of software development and enhancement. *Computer , 21*(5), 61-72.

Boehm, B.W. (1991). Software risk management: principles and practices. *Software, IEEE , 8*(1), 32-41.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg J. & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems archive, 25*(6), 599-616.

Byers, D. & Shahmehri, N. (2007). Design of a Process for Software Security. *The 2nd International Conference on Availability, Reliability and Security (ARES) April 10-13* (s. 301-309).

Chen, D., Hu, R., Du, Z., Zhou, Z. & Ji, C. (2009). Research on an SOA-based virtual enterprise access control model. *7th IEEE International Conference on Industrial Informatics (INDIN) June 23-26* (871-874).

Cheng, J., Goto, Y., Horie, D., Miura, J., Kasahara, T. & Iqbal, A. (2009). Development of ISEE: An Information Security Engineering Environment. *IEEE International Symposium on Parallel and Distributed Processing with Applications, August 10-12* (s. 505-510).

Chittister, C. & Haimes, Y.Y. (1994). Assessment and management of software technical risk. *Systems, Man and Cybernetics, IEEE Transactions 24*(2), 187-202.

Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R. & Molina, J. (2009). Controlling data in the cloud: outsourcing computation without outsourcing control. *Proceedings of the ACM Workshop on Cloud Computing Security (CCSW 2009), Chicago, November 13* (s. 85-90) New York: ACM.

CMM. (1999). *Pathways to Process Maturity: The Personal Software Process and Team Software Process*. Carnegie Mellon University. Haettu 3.9.2010 osoitteesta http://www.sei.cmu.edu/library/abstracts/news-at-sei/backgroundjun99.cfm

Common Criteria. (2009). Common Criteria for Information Technology Security Evaluation. Common Criteria Portal. Haettu 17.8.2010 osoitteesta http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf

Crawford, L. (2005). Senior management perceptions of project management competence. *International Journal of Project Management 23*(1), 7-16.

Creese, S., Hopkins, P., Pearson, S. & Shen, Y. (2009). Data Protection-Aware Design for Cloud Services. In *Proceedings of the 1st international Conference on Cloud Computing, Beijing, China, December 01-04*. Teoksessa M. G. Jaatun, G. Zhao, and C. Rong, (toim.), Lecture Notes In Computer Science (s. 119-130). Berlin: Springer-Verlag.

Croft, J. & Signorile, R. (2009). Secure distribution of confidential information via self-destructing data. In *Proceedings of the 8th World Scientific and Engineering Academy and Society (WSEAS) international conference on on Data networks, communications, computers Baltimore, USA, November 7-9* (s. 124-129).

Dey, M. (2007). Information security management - a practical approach. In *Proceedings of AFRICON 2007 Windhoek, Republic of Namibia, September 26-28* (s. 1-6).

Ehsan, N., Perwaiz, A., Arif, J., Mirza, E. & Ishaque, A. (2010). CMMI / SPICE based process improvement. *IEEE International Conference on Management of Innovation and Technology (ICMIT), June 2-5* (s. 859-862).

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Tampere:Vastapaino.

Eskola, J. & Vastamäki, J. (2001). *Teemahaastattelu: Opit ja opetukset*. Teoksessa Aaltola J. ja Valli R. (toim.), Ikkunoita tutkimusmetodeihin I - Metodin valinta ja aineiston keruu: virikkeitä aloittelevalle tutkijalle. Jyväskylä: PS-kustannus.

Evans, R., Tsohou, A., Tryfonas, T. & Morgan, T. (2010). Engineering secure systems with ISO 26702 and 27001. *5th International Conference on System of Systems Engineering (SoSE), June 22-24* (s. 1-6).

Ferrari, E. (2009). Database as a Service: Challenges and solutions for privacy and security. *IEEE Asia-Pacific Services Computing Conference (APSCC) December 7-11* (46-51).

Firesmith, D. (2004). Specifying Reusable Security Requirements. *Journal of Object Technology 3*(1), 61-75.

Fito, J.O., Goiri, I. & Guitart, J. (2010). SLA-driven Elastic Cloud Hosting Provider. In *Proceedings of 18th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), Pisa, Italy, February 17-19* (s. 111-118).

Gadzheva, M. (2008). Privacy in the Age of Transparency: The New Vulnerability of the Individual. *Social Science Computer Review, 26*(1), 60-74.

Glass, R.L. (2009). Doubt and Software Standards. *Software, IEEE , 26*(5) 104-104.

Goo, J., Kim, D.J. & Cho, B. (2006). Structure of Service Level Agreements (SLA) in IT Outsourcing: The Construct and Its Measurement. *12th Americas Conference on Information Systems (AMCIS), Acapulco, Mexico, August 4-6*.

Green, L. (2006). Service level agreements: an ontological approach. In Proceedings of the 8th international Conference on Electronic Commerce: the New E-Commerce: innovations For Conquering Current Barriers, Obstacles and Limitations To Conducting Successful Business on the internet (ICEC), Fredericton, New Brunswick, Canada, August 13-16, 156 (s. 185-194). New York: ACM.

Grobauer, B., Walloschek, T. & Stocker, E. (2010). Understanding Cloud-Computing Vulnerabilities. *Security & Privacy, IEEE , 99*. 1-14.

Hakala, M., Vainio, M. & Vuorinen, O. (2006). *Tietoturvallisuuden käsikirja*. Porvoo: WS Bookwell.

Hassan, R., Eltoweissy, M., Bohner, S. & El-Kassas, S. (2009). Goal-Oriented Software Security Engineering: The Electronic Smart Card Case Study. *International Conference on Computational Science and Engineering (CSE) August 29-31, 3* (s. 213-218).

Henkilötietolaki 22.4.1999/523. (1999). Haettu 31.5.2010 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Hirsjärvi, S. & Hurme, H. (2000). *Tutkimushaastattelu*. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S. & Hurme, H. (2008). *Tutkimushaastattelu*. Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (1997). *Tutki ja kirjoita*. Helsinki:Kirjayhtymä.

Hoque, F. (2010, 12. helmikuuta). *Is Your IT Strategy Optimized for Risk Management?* CIO Update. QuinStreet Inc. Haettu osoitteesta http://www.cioupdate.com/insights/article.php/3864746/Is-Your-IT-Strategy-Optimized-for-Risk-Management.htm

Horie, D., Morimoto, S., Azimah, N., Goto, Y. & Cheng, J. (2008). ISEDS: An Information Security Engineering Database System Based on ISO Standards. *3rd International Conference on Availability, Reliability and Security (ARES), March 4-7* (s. 1219-1225).

Hoyle, D. (2007). *Quality: management essentials*. Oxford:Butterworth-Heinemann.

Humayun, A., Basit, W., Farrukh, G.A., Lodhi, F. & Aden, R. (2010). An empirical analysis of team review approaches for teaching quality software development. In *Proceedings of the 32nd ACM/IEEE international Conference on Software Engineering - Volume 1 (ICSE), Cape Town, South Africa, May 01-08* (s. 567-575) New York: ACM.

Humphrey, W.S. (1989). *Managing the software process*. SEI series in software engineering. Reading: Addison-Wesley.

IEEE:n ohjeistus. (2008). *IEEE Guide--Adoption of ISO/IEC 90003:2004 Software Engineering--Guidelines for the Application of ISO 9001:2000 to Computer Software*. (IEEE Std 90003-2008, C1-71).

IEEE Std 1028. (2008). *IEEE Standard for Software Reviews and Audits*. (IEEE STD 1028-2008). (s. 1-52).

ISO 9000. (2010). ISO 9000 Essentials. International Organization for Standardization. Haettu 3.8.2010 osoitteeesta http://www.iso.org/iso/iso_catalogue/management_standards/iso_9000_iso_14000/iso_9000_essentials.htm

ISO 22307. (2008). *Financial services – Privacy impact assessment*. (Std ISO 22307 – 2008). (s. 1-28).

ISO 27005. (2008). Introduction To ISO 27005 (ISO27005). ISO 27000 Directory 2008 - The Information Portal for ISO 27000 Contact Page. Haettu 2.8.2010 osoitteeesta http://www.27000.org/iso-27005.htm

ISO/IEC 12207. (2008). *ISO/IEC/IEEE Standard for Systems and Software Engineering - Software Life Cycle Processes*. (IEEE STD 12207-2008). (s. 1-138).

ISO/IEC 16085. (2006). *Systems and Software Engineering - Life Cycle Processes - Risk Management*. (Std ISO IEC 16085 – 2006). (s. 1-36).

ISO/IEC 17799. (2006). *Kansainväliset uudet tietoturvastandardit nyt suomeksi*. Suomen Standardisoimisliitto SFS ry. Haettu 16.8.2010 osoitteesta http://www.sfs.fi/ajankohtaista/tiedotteet/20060803150421.html

ISO/IEC 25001. (2010). *ISO/IEC 25001:2007 Software engineering -- Software product Quality Requirements and Evaluation (SQuaRE) -- Planning and management*. International Organization for Standardization. Haettu

19.8.2010 osoitteesta http://www.iso.org/iso/catalogue_detail.htm?csnumber=35724

ISO/IEC 26702. (2007). *ISO/IEC Standard for Systems Engineering - Application and Management of the Systems Engineering Process*. (ISO/IEC 26702 IEEE Std 1220-2005 First edition 2007-07-15). (s. 1-88).

ISO/IEC 90003. (2010). *ISO/IEC 90003:2004 Software engineering -- Guidelines for the application of ISO 9001:2000 to computer software*. International Organization for Standardization. Haettu 6.8.2010 osoitteesta http://www.iso.org/iso/catalogue_detail?csnumber=35867

Itani, W., Kayssi, A. & Chehab, A. (2009). Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. *8th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), December 12-14* (s. 711-716).

ITIL Introduction. (2007). An Introductory Overview of ITIL® V3. APM Group Ltd. Haettu 1.12.2010 osoitteesta http://www.best-management practice.com/gempdf/itSMF_An_Introductory_Overview_of_ITIL_V3.pdf

Jean, S., Losavioy, F., Matteoy, A. & Levyz, N. (2010). An extension of OWL-S with quality standards. *Fourth International Conference on Research Challenges in Information Science (RCIS), May 19-21* (s. 483-494).

Jensen, M., Schwenk, J., Gruschka, N. & Lo Iacono, L. (2009). On Technical Security Issues in Cloud Computing. *IEEE International Conference on Cloud Computing, Bangalore, India, September 21-25* (s. 109-116).

Jokela, T., Siponen, M., Hirasawa, N. & Earthy, J. (2006). A survey of usability capability maturity models: implications for practice and research. *Behaviour & Information Technology 25*(3), 263–282.

Jordan, E. (2006). *Strateginen IT-riskien hallinta*. Toim. Jordan, E. & Silcock, L. Helsinki: Edita.

Järvinen, P. (2010). *Yksityisyys: Turvaa digitaalinen kotirauhasi*. Jyväskylä: WSOYpro.

Kandukuri, B.R., Paturi, V.R. & Rakshit, A. (2009). Cloud Security Issues. In *Proceedings of IEEE International Conference on Services Computing (SCC), Bangalore, India, September 21-25* (s. 517-520).

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

Kauffman, R.J. & Tsai, J.Y. (2010). With or without you: The countervailing forces and effects of process standardization. *Electronic Commerce Research and Applications, 9*(4), 305-322.

Kellerman, T. (2010). Cyber-Threat Proliferation: Today's Truly Pervasive Global Epidemic. *Security & Privacy, IEEE , 8*(3) 70-73.

Kemerer, C.F. & Paulk, M.C. (2009). The Impact of Design and Code Reviews on Software Quality: An Empirical Study Based on PSP Data. *Software Engineering, IEEE Transactions 35*(4), 534-550.

Khan, M.U.A. & Zulkernine, M. (2009). On Selecting Appropriate Development Processes and Requirements Engineering Methods for Secure Software. In

Proceedings of 33rd Annual IEEE International Computer Software and Applications Conference (COMPSAC), July 20-24, 2 (s. 353-358).

Khoshgoftar, M. & Osman, O. (2009). Comparison of maturity models. In *Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT). August 8-11* (s. 297-301).

Komi-Sirviö, S. (2004). *Development and Evaluation of Software Process Improvement Methods*.VTT Publications 535. Espoo.

Kontio, J. (2001). *Software Engineering Risk Management: A Method, Improvement Framework, and Empirical Evaluation*. Doctoral dissertation, Helsinki University of Technology. Center of Excellence.

Lahlou, S. (2008). Identity, social status, privacy and face-keeping in digital society. *Social Science Information 47*(3), 299-330.

Li, G., Dong, H., Zheng, Q., Zhou, M. & Guo, Y. (2009). Research on National and International Software Engineering Standard Bodies. *International Conference on Computational Intelligence and Software Engineering (CiSE) December 11-13* (s. 1-4).

Lyytinen, K. & King, J. (2006). Standard Making: A Critical Research Frontier for Information Systems Research. *MIS Quarterly, 30*, 405-411.

Mazlan, E.M., Rahim, L.A., Shazi, A.R. & Mazlan, W.M. (2009) Asset Management System: Supporting Organization in Achieving Process Maturity. In *Proceedings of International Conference on Computing, Engineering and Information (ICC),California, USA, April 2-4* (s. 357-362).

McManus, J. (2004). *Risk Management in Software Development Projects*. Oxford: Elsevier Butterworth Heinemann

Mellado, D., Blanco, C., Sanchez, L.E. & Fernandez-Medina, E. (2010). A systematic review of security requirements engineering, *Computer Standards & Interfaces 32*(4), 153-165.

Mishra, D. & Mishra, A. (2007). Efficient software review process for small and medium enterprises. *Software, IET , 1*(4). 132-142.

Murray, P. (2009). Enterprise grade cloud computing. In *Proceedings of the Third Workshop on Dependable Distributed Data Management (WDDM), Nuremberg, Germany, March 31* (s. 1). ACM: New York.

Münstermann, B. & Weitzel, T. (2008). What is Process Standardization? *Proceedings of the International Conference on Information Resources Management (Conf-IRM 2008), Niagara Falls, Ontario, Canada, May 18-20*. Paper 64.

Nordbotten, N.A. (2009). XML and Web Services Security Standards. *Communications Surveys & Tutorials, IEEE , 11*(3) 4-21.

OECD. (1980). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Haettu 31.5.2010 osoitteesta http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

Parakh, A. & Kak, S. (2009). Online data storage using implicit security. *Information Sciences, 179*(19). 3323-3331.

Paulk, M.C., Curtis, B., Chrissis, M.B. & Weber, C.V. (1993). Capability maturity model, version 1.1. *Software, IEEE 10*(4), 18-27.

Pearson, S. & Charlesworth, A. (2009). Accountability as a Way Forward for Privacy Protection in the Cloud. In *Proceedings of the 1st international Conference on Cloud Computing, Beijing, China, December 01- 04*. Teoksessa M. G. Jaatun, G. Zhao, & C. Rong (toim.), Lecture Notes In Computer Science, vol. 5931. (s. 131-144) Berlin: Springer-Verlag.

Pervez, Z., Sungyoung, Lee & Young-Koo, Lee. (2010). Multi-Tenant, Secure, Load Disseminated SaaS Architecture. *The 12th International Conference on Advanced Communication Technology (ICACT), February 7-10, 1* (s. 214-219).

Petković, M. & Jonker, W. (2007). Security, Privacy and Trust in Modern Data Management (Data-Centric Systems and Applications). New York: Springer-Verlag.

Qasaimeh, M. & Abran, A. (2010). Investigation of the Capability of XP to Support the Requirements of ISO 9001 Software Process Certification. *8th ACIS International Conference on Software Engineering Research, Management and Applications (SERA), May 24-26* (s. 239-247).

Raj, H., Nathuji, R., Singh, A. & England, P. (2009). Resource management for isolation enhanced cloud services. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW), Chicago, Illinois, USA, November 13* (s. 77-84) New York: ACM.

Rimal, B.P., Choi, E. & Lumb, I. (2009). A Taxonomy and Survey of Cloud Computing Systems. In *Proceedings of 5th International Joint Conference on INC, IMS and IDC, Seoul, Korea, August 25- 27* (s. 44-51).

Ropponen, J. (1999). *Software Risk Management – Foundations, Principles and Empirical Findings*. Jyväskylä: Jyväskylä University Printing House.

Samarati, P. & di Vimercati, S.D. (2010). Data protection in outsourcing scenarios: issues and directions. In *Proceedings of the 5th ACM Symposium on information, Computer and Communications Security (ASIACCS), Beijing, China, April 13–16* (1-14). New York: ACM.

Schaffner, S.K. & White, K.S. (1999). Software engineering practices for control system reliability. *Proceedings of the Particle Accelerator Conference, New York, USA, March 27-April 2, 2* (s. 729-731).

SEI. (2010). CMMI Overview. Software Engineering Institute, Carnegie Mellon University. Haettu 8.7.2010 osoitteesta http://www.sei.cmu.edu/cmmi/index.cfm

Singh, A. & Lilja, D. (2009). Improving risk assessment methodology: a statistical design of experiments approach. In *Proceedings of the 2nd international Conference on Security of information and Networks (SIN) Famagusta, North Cyprus, October 06-10* (s. 21-29). New York: ACM.

Software Engineering Institute. (2002). *Capability Maturity Model Integration (CMMISM), Version 1.1.* CMMISM for Systems Engineering, Software Engineering, Integrated Product and Process Development and Supplier Sourcing (CMMI-SE/SW/IPPD/SS, V1.1), Continuous Representation. Pittsburgh.

Sommerville, I. (2007). *Software engineering*. New York : Addison-Wesley.

Spiekermann, S. & Cranor, L.F. (2009). Engineering Privacy. *Software Engineering, IEEE Transactions on 35*(1). 67-82.

Sripanidkulchai, K., Sahu, S., Ruan, Y., Shaikh, A. & Dorai, C. (2010). Are clouds ready for large distributed applications? *SIGOPS Operating Systems Review, 44*(2), 18-23.

Stoneburner, G., Goguen, A.Y. & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology*. (National Institute of Standards and Technology Special Publication 800-30). Technology department, US Department of Commerce. Washington: US Government Printing.

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

Sultan, K., En-Nouaary, A. & Hamou-Lhadj, A. (2008). Catalog of Metrics for Assessing Security Risks of Software throughout the Software Development Life Cycle. *International Conference on Information Security and Assurance (ISA) April 24-26* (s. 461-465)

Suomen perustuslaki 11.6.1999/731. (1999). Haettu 31.5.2010 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Suomen Standardoimisliitto. (2010). *Mikä on standardi?* Suomen Standardisoimisliitto SFS ry. Haettu 11.8.2010 osoitteesta http://www.sfs.fi/standardisointi/tietoa_standardeista/mika_standardi/

Syrjänen, P. (2006). *Yksityisyyden suoja ja henkilöarviointi*. Acta Universitatis Tamperensis 1155. Väitöskirja. Tampereen yliopisto. Haettu 31.5.2010 osoitteesta http://acta.uta.fi/pdf/951-44-6646-2.pdf

Syrjänen, P. (2008). *Luotettava henkilöarviointi ja yksityisyyden suoja*. Helsinki: Talentum.

Tafti, M. (2005). Risk factors associated with offshore IT outsourcing. *Industrial Management & Data Systems*, *105*(5). 549-560.

Taguchi, K., Yoshioka, N., Tobita, T. & Kaneko, H. (2010). Aligning Security Requirements and Security Assurance Using the Common Criteria. *Fourth International Conference on Secure Software Integration and Reliability Improvement (SSIRI), June 9-11* (s. 69-77).

Tavani, H.T. (1999). Privacy online. *ACM SIGCAS Computers and Society 29*(4), 11-19.

Thayer, R.H. & McGettrick, A.D. (2007). IEEE Software Engineering Standards: A Student's Version. *20th Conference on Software Engineering Education & Training (CSEET) July 3-5* (s. 229-236).

Tietosuojadirektiivi 95/46/EY. (1995). Virallinen lehti nro L 281 , 23/11/1995 (s. 31-50). Haettu 31.5.2010 osoitteesta http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FI:HTML

Tuomi, J. & Sarajärvi, A. (2002). *Laadullinen tutkimus ja sisällönanalyysi*. Helsinki: Tammi

Vaquero, L. M., Rodero-Merino, L., Caceres, J. & Lindner, M. (2009). A break in the clouds: towards a cloud definition. *SIGCOMM Computer Communication Review, 39*(1), 50-55.

Wang, Y., Court, I., Ross, M., Staples, G., King, G. & Dorling, A. (1997). Quantitative evaluation of the SPICE, CMM, ISO 9000 and BOOTSTRAP. In *Proceedings of the Third IEEE International Software Engineering Standards Symposium and Forum (ISESS), June 1-6* (s. 57-68).

Wang, W., Li, Z., Owens, R. & Bhargava, B. (2009). Secure and efficient access to outsourced data. In *Proceedings of the 2009 ACM Workshop on Cloud Computing Security (CCSW) Chicago, Illinois, USA, November 13* (s. 55-66) New York: ACM.

Wang, J., Zhao, Y., Jiang, S. & Le, J. (2009). Providing privacy preserving in cloud computing. *International Conference on Test and Measurement (ICTM), Hong Kong, December 5-6, 2* (s. 213-216).

Wardley, S. (2008). *Maturity models for the cloud*. Haettu 4.10.2010 osoitteesta http://blog.gardeviance.org/2008/12/maturitymodels-for-cloud.html

Weiss, A. (2007). Computing in the clouds. *netWorker, 11*(4), 16-25.

Wright, D., Friedewald, M., Gutwirth, S., Langheinrich, M., Mordini, E., Bellanova, R., De Hert, P., Wadhwa, K. & Bigo, D. (2010). Sorting out smart surveillance, *Computer Law & Security Review 26*(4). 343-354.

Yildiz, M., Abawajy, J., Ercan, T & Bernoth, A. (2009). A Layered Security Approach for Cloud Computing Infrastructure. *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN), December 14-16* (s. 763-767).

Yonghong, Y. (2010). Privacy Protection in Secure Database Service. In Proceedings of the Second International Conference on Networks Security Wireless Communications and Trusted Computing (NSWCTC), April 24-25, 1 (s. 218-222).

Yongqing, C. & Jiatao, H. (2009). The Study of a Comprehensive Assessment Method for Service Quality of ISO 9000 Consulting Service Based on a Hierarchical Grey Analysis. *International Conference on Management and Service Science (MASS), September 20-22* (s. 1-6).

Youseff, L., Butrico, M. & Da Silva, D. (2008). Toward a Unified Ontology of Cloud Computing. In *Proceedings of Grid Computing Environments Workshop, (GCE), Texas, USA, November 12-16* (s. 1-10).

Zhang, S., Wang, P., Ding, Z. & Zong, Y. (2009). Organization ITIL Process Integration Based on Web Services. *WRI World Congress on Software Engineering (WCSE) May 19-21, 1* (s. 412-416).

Zhang, S., Zhang, S., Chen, X. & Wu, S. (2010). Analysis and Research of Cloud Computing System Instance. *Second International Conference on Future Networks (ICFN), Sanya, Hainan, China, January 22-24* (s. 88-92). Los Alamitos: IEEE Computer Society.

Zhang, S., Zhang, S., Chen, X & Huo, X. (2010). Cloud Computing Research and Development *Second International Conference on Future Networks (ICFN), Sanya, Hainan, China, January 22-24* (s. 93-97). Los Alamitos: IEEE Computer Society.

Zhuling, Y., Kaihu, H., Xiao, N. & Shihuan, Q. (2009). Study on Standardization Strategy for SMEs. *International Conference on Information Management,*

Innovation Management and Industrial Engineering, December 26-27, 4 (s. 145-148).

LIITE 1 HAASTATTELUKYSYMYKSET

Yleiset tiedot

1. Nimi
2. Yrityksen nimi
3. Työnkuva/ Toimialue
4. Kokemus (vuosia)
5. Yrityksenne ensisijainen toimiala

"Tietojenkäsittely pilvessä on melko tuore aihealue ja näin ollen siihen liittyy epäselvyyttä.."
Pilviteknologia ja pilvipalvelut:

1. Miten määrittelet pilviteknologian? Entä pilvipalvelut?
2. Hyödynnetäänkö yrityksessänne pilviteknologiaa tai pilvipalveluita? Miten?
3. Minkälaisia hyötyjä ja haittoja pilviteknologiaan tai pilvipalveluihin mielestäsi liittyy?

"Pilviteknologiaan ja tietojen hajauttamiseen liittyy oleellisesti tietoturva ja tietosuoja.."
Tietosuoja & yksityisyys:

1. Miten tietoturva ja tietosuoja huomioidaan yrityksessänne pilviteknologiaa tai pilvipalveluita hyödynnettäessä? Miten niitä tulisi kenties kehittää?
2. Miten tietoturva ja tietosuoja tulisi yleisesti huomioida pilvipalveluita kehitettäessä tai hankittaessa?
3. Onko yksilöiden yksityisyyden suojaaminen mielestäsi tärkeää tietojenkäsittelyssä?
4. Miten asiakkaidenne tai yhteistyökumppaneidenne yksityisyys huomioidaan yrityksessänne
5. Miten yksityisyys tulisi huomioida pilvipalveluita kehitettäessä tai hankittaessa?
6. Miten yksilöt voisivat olla vaikuttamassa omaan yksityisyyteensä tietojen ollessa pilvessä (vai voivatko?)

"Tietoturvan pettäminen ja tietosuojan rikkoontuminen on riski.."
Riskienhallinta

1. Miten yrityksessänne hallitaan riskejä?
2. Liittyykö tietojenkäsittelyn ulkoistamiseen mielestäsi riskejä? Minkälaisia?
3. Miten pilvipalveluihin liittyviä riskejä voidaan hallita?
4. Voidaanko pilvipalveluiden riskeihin vaikuttaa:

a.) Sopimuksin (esimerkiksi palvelutasosopimukset)
b.) Teknisesti toimivilla ja laadukkailla palveluilla
c.) Kypsyysmallien avulla

5. Jos voidaan, niin millä edellisistä mielestäsi parhaiten? Edellisiä yhdistelemällä?
6. Hyödynnetäänkö yrityksessänne kypsyysmalleja?
7. Onko tietosuojan vaarantuminen niin merkittävä riski, että se tulee huomioida osana yrityksen kokonaisvaltaista riskienhallintaa? Vai riittääkö, että tietosuoja on huomioitu pilvipalveluiden kehitysprosessissa?
8. Kuinka palvelutasosopimusten täyttämistä tulisi valvoa?

”Niin pilviteknologiaa kuin pilvipalveluita kehitettäessä tai hankittaessa voidaan hyödyntää tietojenkäsittelystandardeja..”

Standardit:

1. Mitä mieltä olet tietojenkäsittelyyn liittyvistä standardeista ja kehysmalleista?
2. Hyödynnetäänkö yrityksessänne tietojenkäsittelyyn liittyviä standardeja tai kehysmalleja? Mitä?
3. Voidaanko standardien ja kehysmallien avulla parantaa tietosuojaa ja yksityisyyttä?
4. Pitäisikö pilviteknologian eri osa-alueita standardoida?

(Tähän teemahaastattelun loppuun voit kertoa yleisellä tasolla mitä mieltä olet pilviteknologiasta ja sen kehittymisestä)

KIITOS..

LIITE 2 HAASTATTELUUN SUOSTUNEILLE LÄHETETTY KIRJE

Hyvä tutkimuksen osanottaja,

Yleistä

Kiitän mahdollisuudesta haastatella sinua liittyen pro gradu –tutkielmaani. Toteutettava haastattelu nauhoitetaan ja kirjoitetaan puhtaaksi, jotta haastatteluvastauksia voidaan hyödyntää analysoitaessa tutkimusongelmaa ja haastatteluja. Puhtaaksi kirjoitettu versio lähetetään haastateltaville tarkasteltavaksi ja tarvittaessa korjataan haastateltavan niin halutessa. Haastattelut ovat täysin luottamuksellisia ja henkilöiden tai yritysten tietoja ei missään vaiheessa luovuteta ulkopuolisille. Tutkielmassa lähteisiin viitataan muodossa: Haastateltava1, Haastateltava2.. jne.

Tutkimuksen aihe

Tutkimuksen lähtökohtana on pilviteknologiaa tai pilvipalveluita hyödyntävät yritykset. Varsinainen tutkimusongelma liittyy pilvisovellusten ja –järjestelmien tietosuojaan. Tietoa hajautettaessa tietosuojan vaarantuminen on riski. Riski voi konkretisoitua esimerkiksi henkilötietojen vuotaessa internetiin kenen tahansa saataville. Usein yrityksissä pyritään jollain tapaa hallitsemaan riskejä ja riskienhallintaan saattaa liittyä erilaisia metodeja tai toimenpiteitä.

Motiivi

Tietosuoja ja yksityisyys ovat mielestäni merkittäviä asioita ajatellen pilviteknologiaa ja pilvipalveluita. Tietojenkäsittelyyn liittyviä standardeja ja kehysmalleja on lukematon määrä. Osa standardeista liittyy ohjelmistoprosesseihin, osa esimerkiksi riskienhallintaan tai toteutettavan palvelun laatuun. Suoritettavien haastattelujen perusteella analysoin erilaisten standardien ja kehysmallien hyödyntämistä yrityksissä sekä niiden potentiaalia tietosuojan kehittämiseksi.

Tutkielman tekijä

Opiskelen Jyväskylän yliopistossa tietojärjestelmätieteitä viidettä vuotta digitaalisen median suuntautumislinjalla. Muutamaa kurssia vaille valmis kauppatieteiden maisterin tutkinto pitää sisällään mm. yritystaloustieteiden ja kauppaoikeuden sivuainekokonaisuudet. Henkilökohtainen mielenkiinto tietosuojaa kohtaan sai minut valitsemaan tämän aiheen tutkielmalle. Pilviteknologiaan liittyvä gradu oli ohjaajani, professori Pasi Tyrväisen idea, mikä täydentää kokonaisuutta hyvin.

Myöhemmin syksyllä valmistuvan tutkielman tulokset lähetetään jokaiselle haastateltavalle, jos haastateltava niin haluaa.

Kunnioittaen,
Vesa Lehtinen