

Tomi Ahveninen

**PILVIPALVELUIDEN PALVELUTASOSOPIMUSTEN  
RISKIT ASIAKKAAN NÄKÖKULMASTA**



JYVÄSKYLÄN YLIOPISTO  
TIETOJENKÄSITTELYTIEDEIDEN LAITOS  
2014

## TIIVISTELMÄ

Ahveninen, Tomi

Pilvipalveluiden palvelutasosopimusten riskit asiakkaan näkökulmasta

Jyväskylä: Jyväskylän yliopisto, 2014, 29 s.

Tietojärjestelmätiede, kandidaatin tutkielma

Ohjaaja: Laatikainen, Gabriella

Pilvilaskentaan perustuvien palveluiden suosio on kasvanut kiihtyvällä nopeudella viime vuosina. Niin yritykset kuin yksityiset käyttäjätkin ovat alkaneet hyödyntämään pilvipalveluita. Eri alojen yritykset siirtävät ydintoimintojaankin pilvipalveluiden tarjoajille. Pilvipalveluiden kasvava hyödyntäminen on luonut myös tarpeita palveluntarjoajien antamille takeille. Kun yritys ulkoistaa joiain tai jopa suurimman osan IT - toiminnoistaan palveluntarjoajalle, tarvitaan takeita, jotka varmistavat asiakasyrityksen toiminnan jatkuvuutta. Palvelutasosopimukset (Service level agreement, SLA) ovat keino rakentaa luottamusta asiakkaan ja palveluntarjoajan välille ja sopia palvelun tasosta. Palvelutasosopimukset ovat tärkeitä asiakkaille takeiden kannalta ja palveluntarjoajalle imagonsa rakentamisen kannalta, mutta palvelutasosopimukset ja niiden neuvottelu aiheuttavat kuitenkin omat riskinsä. Tässä tutkimuksessa havaittiin palvelutasosopimusten neuvotteluun liittyviä riskejä, kuten sopimusneuvottelijan riittämättömät tekniset taidot, tilastollisten tietojen harhaanjohtavuus ja korvausten huono vastaavuus koettuun tappioon. Lisäksi havaittiin myös turvallisuuteen liittyvinä riskejä, kuten datan fyysinen sijainti, eri asiakkaiden datan erotteleminen, jatkuvuus ja palautuminen sekä palveluntarjoajan työntekijöiden pääsy asiakkaan dataan. Tämä tutkimus perustuu kirjallisuuskatsaukseen ja keskittyy palvelutasosopimusten riskeihin pilvipalvelun asiakkaiden näkökulmasta. Tutkimuksessa määritellään myös pilvipalvelut, niiden palvelu- ja toteutusmallit, palvelutasosopimukset ja pilvipalveluiden palvelutasosopimusten erityispiirteet.

Asiasanat: pilvipalvelu, palvelutasosopimus, toteutusmalli, riski, ulkoistus

## ABSTRACT

Ahveninen, Tomi

The risks of cloud SLA's from a customer perspective

Jyväskylä: University of Jyväskylä, 2014, 29 p.

Information Systems science, Bachelor's thesis

Supervisor: Laatikainen, Gabriella

The popularity of cloud computing has grown rapidly in the past few years and the pace is definitely not slowing down. Cloud based services are widely used by businesses and individuals. Corporations from different areas of expertise move their core IT -functions to cloud service providers. The accelerating adoption of cloud services has also generated a need for guarantees from the service provider. When a company outsources some or even most of its IT -functions to a service provider, the level of service has to be guaranteed in order to secure to continuity of these functions. Service level agreements (SLA) are a way for the customer and the service provider to build trust and agree on the level of service. Whereas SLA's are a good tool for customers to get guarantees on the service and for service providers to improve their image, they pose possible risks as well. Risk factors related to SLA negotiation are e.g. the negotiators' lack of technical expertise, deceptive averages and the penalties from SLA violations being not enough to cover the losses experienced by the customer. The security risks discovered during this research are the physical location of the data, data segregation, continuity and recovery and the privileged access of a service provider's employees to customer data. This research is a literature review that focuses on identifying the risks that SLA's may pose to the customers of cloud services. The thesis defines the concepts of cloud computing, different cloud service models and deployment models, service level agreements and the characteristics of SLA's between cloud service providers and their customers.

Keywords: cloud computing, service level agreement, SLA, service model, risk, outsourcing

## KUVIOT

KUVIO 1 Vastuun jakautuminen pilvipalveluiden eri päätyypeissä .....	10
--	----

## TAULUKOT

TAULUKKO 1 Yhteenveto erilaisten toteutusmallien eduista .....	14
TAULUKKO 2 Yhteenveto erilaisten toteutusmallien haitoista.....	15
TAULUKKO 3 Erilaisten toteutusmallien yhteiset sopimusehdot .....	19
TAULUKKO 4 Kooste pilvipalveluiden asiakkaiden palvelutasosopimukseen liittyvistä riskeistä.....	24

# SISÄLLYS

TIIVISTELMÄ .....	2
ABSTRACT .....	3
KUVIOT .....	4
TAULUKOT .....	4
SISÄLLYS.....	5
1 JOHDANTO.....	6
2 PILVIPALVELUT .....	8
2.1 Pilvilaskenta ja pilvipalvelut.....	8
2.2 Pilvipalveluiden kolme palvelumallia.....	10
2.2.1 Infrastructure as a Service (IaaS).....	11
2.2.2 Platform as a Service (PaaS).....	11
2.2.3 Software as a Service (SaaS).....	12
2.3 Pilvipalveluiden toteutusmallit .....	12
2.3.1 Julkinen pilvi.....	12
2.3.2 Yksityinen pilvi.....	13
2.3.3 Hybridi pilvi.....	13
3 PILVIPALVELUIDEN PALVELUTASOSOPIMUKSET .....	16
3.1 Palvelutasosopimukset .....	16
3.1.1 Palvelutasosopimusten neuvottelu .....	17
3.1.2 Palvelutasosopimusten monitorointi .....	17
3.2 Palvelutasosopimukset pilvipalveluissa .....	18
3.2.1 IaaS-sopimusten erityispiirteet.....	19
3.2.2 PaaS-sopimusten erityispiirteet.....	19
3.2.3 SaaS-sopimusten erityispiirteet.....	19
4 PILVIPALVELUIDEN PALVELUTASOSOPIMUSTEN RISKIT ASIAKKAALLE .....	21
4.1 Neuvottelun riskit.....	21
4.2 Turvallisuusriskit.....	22
5 YHTEENVETO .....	25
LÄHTEET .....	28

# 1 JOHDANTO

Pilvilaskennan kehityksen myötä pilvipalveluista on tullut maailmanlaajuinen ilmiö ja niiden käyttö laajenee jatkuvasti. Ne kuuluvat jo monen yksittäisen ihmisen jokapäiväiseen elämään. Yritystenkin piirissä IT-palveluiden ulkoistus-trendi on siirtynyt vahvasti kohti pilvipalveluita. Tämä kehitys aiheuttaa sen, että fyysisesti tieto alkaa siirtymään yritysten ja yksityiskäyttäjien laitteilta pilvipalveluiden tarjoajien keskitettyihin palvelinkeskuksiin. (Chen, Li & Chen, 2011.) Tilanteessa, jossa asiakas ulkoistaa ydintoimintonsa pilvipalveluun, on oltava selvät ja dokumentoidut takeet palvelun toimivuudesta. Palvelutasosopimukset (Service level agreement, SLA) ovat keino antaa näitä takeita ja rakentaa luottamusta asiakkaan ja palveluntarjoajan välille. (Dillon, Wu & Chang, 2010.) Pilvipalveluiden turvallisuus onkin suurin yksittäinen yritysten intoa pilvipalveluiden käyttöön hillitsevä tekijä (Subashini & Kavitha, 2011).

Palvelutasosopimus antaa parhaimmillaan asiakkaalle selvän kuvauksen palvelusta ja siitä, millä tasolla sen on pysyttävä. Kattavan ja sopivan palvelutasosopimuksen tekeminen ei kuitenkaan ole helppoa. (Sun, Singh & Hussain, 2012.) Tilanne on sama kuin minkä tahansa muunkin työkalun kanssa: mikäli käyttöön ei löydy vaadittua taitoa, lopputuloksestakaan ei saada toivottua. Esimerkiksi, jos asiakkaan neuvottelijalla ei ole tarpeeksi teknistä ymmärrystä, sopimuksesta voi tulla sopimaton asiakkaan tarpeisiin nähden (Tripathy & Patra, 2011). Sopimusta tehtäessä on siis tärkeää tuntea konteksti hyvin. Kun asiakas tiedostaa riskit jo sopimuksen tekovaiheessa, pystyy hän ottamaan ne huomioon ja rakentamaan sopimuksen, josta on yritykselle todellista lisäarvoa.

Taloudellisesta näkökulmasta katsottuna pilvipalveluissa on jo nyt kyse hyvin merkittävästä liiketoiminnasta ja palvelutasosopimusten kehittyminen on avainroolissa pilvipalveluiden kehittymiselle, koska luotettavuus ja jatkuvuus ovat ulkoistavalle yritykselle elintärkeitä. Pilvipalveluista ja palvelutasosopimuksista löytyy paljon tutkimusta, mutta huomattavaa on, että aiheen uutuu-den vuoksi hyvin pieni osa tutkimuksesta on vielä ehtinyt tieteellisiin journaleihin asti. Kuitenkin kyseessä on hyvin ajankohtainen aihe, josta tarvitaan lisää tutkimusta. Vaikka pilvipalveluita ja palvelutasosopimuksia on tutkittu erikseen, vain pieni osa tutkimuksesta on keskittynyt pilvipalveluihin ja palveluta-

sosopimukseen yhtenä kokonaisuutena. Aiemmin tehdyissä tutkimuksissa on pyritty rakentamaan viitekehystä pilvipalveluiden palvelutasosopimusten tekemiselle, mutta niihin liittyviä riskejä ei ole vielä tutkittu tarpeeksi. Tässä tutkimuksessa pyritään siis löytämään riskejä, joihin pilvipalvelun asiakkaan on kiinnitettävä huomiota sopimusmallista riippumatta.

Tämä tutkimus on kirjallisuuskatsaus, jossa on pyritty käyttämään ajan-kohtaisia ja luotettavia tieteellisiä lähteitä. Tämän tutkimuksen tavoitteena on kartoittaa pilvipalveluiden palvelutasosopimuksiin liittyviä riskejä yritysasiakkaan näkökulmasta. Tutkielmassa vastataan seuraaviin tutkimuskysymyksiin:

- Mikä on pilvipalvelu?
- Mikä on pilvipalvelun palvelutasosopimus?
- Mitkä ovat pilvipalveluiden palvelutasosopimusten riskit asiakkaalle?

Tutkielman rakenne on seuraava. Tutkielman toisessa luvussa määritellään pilvilaskenta ja pilvipalvelut ja käydään läpi erilaiset palvelu- ja toteutusmallit. Kolmannessa luvussa taas määritellään palvelutasosopimukset ja niiden erityispiirteet pilvipalveluissa, sekä käsitellään palvelutasosopimusten solmimista ja monitorointia. Neljäs luku keskittyy pilvipalveluiden palvelutasosopimusten riskien käsittelyyn asiakkaan näkökulmasta. Tutkielma päättyy yhteenvetoon.

## 2 PILVIPALVELUT

Pilvipalvelut ovat maailmanlaajuisesti tunnettuja ja laajalti käytettyjä, sekä yritykset että yksityiset käyttäjät hyödyntävät niitä. Suuret kansainväliset organisaatiot kuten Amazon, Google, Microsoft ja IBM ohjaavat myös suuria resursseja pilvipalveluiden tutkimiseen. (Chen ym., 2011.) Monelle yritykselle ja yksityiselle käyttäjälle voi kuitenkin olla epäselvää, mistä pilvipalveluissa todellisuudessa on kyse, eikä siitä löydykään kattavaa määritelmää. Tässä luvussa esitellään pilvipalveluita sekä niihin liittyviä käsitteitä ja ominaispiirteitä. Luvussa käydään läpi myös pilvipalveluiden historiaa, ominaisuuksia, erilaisia palvelutyyppisiä sekä toteutusmalleja. Luvussa pyritään luomaan lukijalle kuva pilvipalveluiden kokonaisuudesta, jotta niiden luomia haasteita palvelutasosopimusten tekoon olisi mielekästä pohtia.

### 2.1 Pilvilaskenta ja pilvipalvelut

Pilvipalvelut on terminä melko uusi, mutta toimintamalli on alkanut hakemaan muotoaan jo aikaisemmin. Pilvipalveluiden konseptin voidaan sanoa syntyneen 1960-luvulla, jolloin Douglas Parkhill julkaisi kirjansa "The Challenge of the Computer utility". Parkhill esitteli kirjassaan ajatuksen, että IT-palvelut voisivat joskus olla julkisten palveluiden kaltaisia, kuten esimerkiksi veden jakelu. (Jadeja & Modi, 2012.) Vedestä maksetaan kulutetun määrän mukaan, sitä voi käyttää niin paljon kuin haluaa ja yksittäisellä käyttäjällä ei ole akuuttia riskiä resurssien loppumisesta. Pilvipalveluiden nopea kasvu lähti käyntiin vuonna 2006, kun Amazon julkaisi "Amazon Web Servicen" (AWS). Tällöin myös monet muut suuret toimijat kuten Google ja IBM aktivoituivat pilvipalveluiden hyödyntämisessä. (Jadeja & Modi, 2012.) Eräs syy siihen, miksi pilvipalveluita on alettu hyödyntää suuressa mittakaavassa vasta hiljattain, on tietysti suurten datakeskusten vaatima teknologinen osaaminen. Kuitenkin myös uusilla liiketoimintamalleilla on ollut merkittävä osuus asiaan. Esimerkiksi ajatus laskutusmallista, jossa asiakas maksaa palvelusta joustavasti käyttönsä mukaisen



määrän ja käyttöajan mukaan on ollut tärkeä oivallus. Kyseiseen malliin kuuluu myös palvelun käytön helppo aloitus ja lopetus. (Armbrust ym., 2009.)

Pilvipalvelut käyttävät toiminnassaan pilvilaskentaa, joka määritellään Dillonin ym. (2010) mukaan mallina, jossa käyttäjät pääsevät jaettuihin laskentaresursseihin, esimerkiksi tietoverkkoihin, palvelimiin ja säilytystilaan, helposti käsiksi verkon yli ja jotka ovat saavutettavissa koko ajan. Resursseja voidaan myös tarjota ja vapauttaa nopeasti, eli resurssien jakautuminen käyttäjältä toiselle tarpeen mukaan ei vaadi juurikaan toimia palveluntarjoajalta. Pilvilaskennan synnyssä Grid Computingilla on ollut suuri rooli. Grid Computingin ideana on resurssien jako ja virtualisointi, jotta pystytään ratkaisemaan laskennallisesti hyvin vaativia ongelmia. (Dillon ym., 2010.)

Yleensä pilvipalveluissa suurin osa vaaditusta laitteistosta on fyysisesti palveluntarjoajan tiloissa. Tiedon säilytys, varmuuskopiointi ja laitteiston laskentateho on siis palveluntarjoajan vastuulla, jolloin asiakas pystyy helpommin käyttämään palvelua yksinkertaisella päätelaitteella internetin välityksellä. Pilvipalvelut terminä liittyy siihen, että käyttäjät eivät voi nähdä ”pilven” sisään. Kun palvelu tarjotaan pilvessä, käyttäjät eivät näe palvelun teknisiä yksityiskohtia eikä heillä ole niihin vaikutusmahdollisuutta. Käyttäjät eivät myöskään usein tiedä missä heidän tallentamansa data fyysisesti sijaitsee. (Dillon, ym., 2010.) Osaan palveluista voi päästä käsiksi esimerkiksi mobiililaitteillakin. Pilvipalvelun asiakkaan ei siis tarvitse maksaa omasta fyysisestä IT-infrastruktuurista, sen ylläpidosta tai ylläpidon vaatimasta henkilöstöstä. Pilvipalveluiden käyttöönotto ei myöskään vaadi niin vahvaa tietoteknistä osaamista kuin perinteinen IT-palveluiden malli, jossa yritys omistaa ja ylläpitää IT-infrastruktuuria itse. (Jedeja & Modi, 2012.) Toisaalta pilvipalvelun asiakas on kuitenkin palveluntarjoajan armoilla palvelukatkosten ja tietoturvan osalta (Armbrust ym., 2009). Asiakas voi pilvipalveluun ulkoistamiensa toimintojen määrästä riippuen olla hyvinkin riippuvainen palveluntarjoajasta. Tämä riski liittyy erityisesti julkisiin pilviin. Muita pilvipalveluiden toteutusmalleja ovat yksityinen pilvi ja hybridi pilvi. (Hu ym., 2011.) Pilvipalveluiden toteutusmalleja käsitellään tarkemmin omassa alaluvussaan.

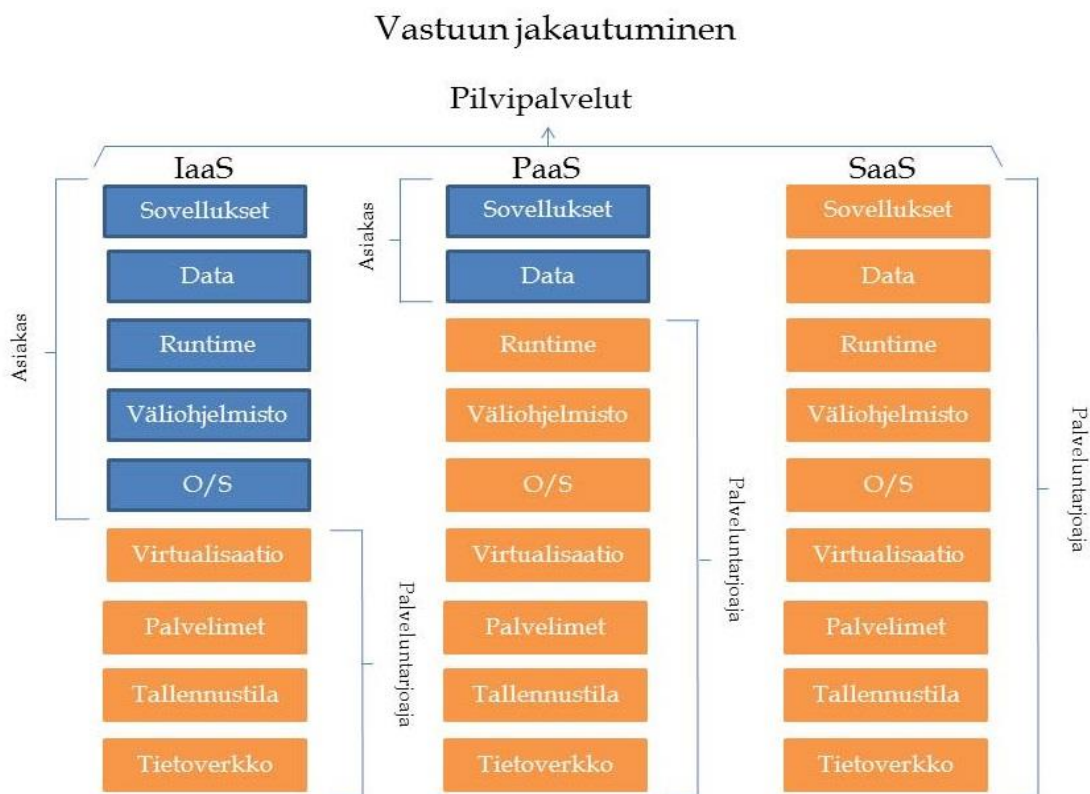
Pilvipalveluiden kehitykseen liittyy myös liiketoimintamalli, jossa asiakas maksaa vain palvelun käytöstä. Aloituskustannukset ovat pienet ja tietoteknisiä resursseja voidaan kasvattaa tai vähentää helposti asiakkaan tarpeen mukaan. Resursseja voidaan kasvattaa myös hetkellisten tarpeiden ajaksi, kuten sesonkiaikojen, jolloin käyttäjien määrän tiedetään olevan erityisen suuri. (Armbrust ym., 2009.) Palveluntarjoajat pystyvät seuraamaan tarkasti kuinka paljon resursseja kukin asiakas käyttää (Dillon ym., 2010). Monitorointi on hyödyllistä asiakkaankin näkökulmasta. Resurssien skaalaus on helppoa, kun pystytään seuraamaan tarpeita. Monitoroimalla voidaan myös luoda tilastoa asiakkaan kuormitustasoista. (Jedeja & Modi, 2012.)

Pilvipalveluissa resurssit jaetaan monen toimijan kesken. Tässäkin pilvipalvelut eroavat perinteisestä IT-palveluiden tuotantomallista, jossa resursseja käyttää vain yksi toimija, niiden omistaja, joka omistaa ohjelmistolisenssit ja IT-infrastruktuurin itse. Monen toimijan ympäristön ominaisuuksiin kuuluu esi-

merkiksi laitteiston käytön optimointi ja sen kapasiteetin jakaminen, helposti jaettavat ohjelmistot ja halvemmat kokonaiskulut kuin perinteisessä mallissa. (Velkoski & Simjanoska, 2013.) Varsinaisia fyysisiä resursseja käyttäjät eivät pilvipalveluissa näe. Yleensä käyttäjillä ei ole tietoa resurssien fyysisestä sijainnista tai niiden koostumuksesta. Käyttäjä ei siis voi tietää tarkkaan mihin hänen pilveen tallentamansa data menee. (Dillon, ym., 2010.) Jaetussa ympäristössä on myös omat ongelmansa. Jaetut fyysiset resurssit luovat mahdollisuuksia haitalliselle toiminnalle toista resurssien käyttäjää kohtaan. Riskinä on myös maineen tahrautuminen, jos samojen resurssien käyttäjä toimii rikollisesti. Asiallisesti toimivalla käyttäjällä voi olla rikollisen kanssa sama verkko-osoite, jolloin huono maine voi kohdistua myös asialliseen käyttäjään. (Dillon, ym., 2010.)

## 2.2 Pilvipalveluiden kolme palvelumallia

Tällä hetkellä pilvipalveluiden tuottamisessa on kolme vallitsevaa mallia: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) sekä Software as a Service (SaaS) (Gibson, Rondeau, Eveleigh & Tan, 2012), joita kuvataan tarkemmin alaluvuissa. Seuraavassa kuviossa 1 on pyritty selkeyttämään eri palvelumallien eroja. Kuviossa on merkitty sinisellä asiakkaan vastuut eri malleissa ja oranssilla palveluntarjoajan vastuut.



KUVIO 1 Vastuun jakautuminen pilvipalveluiden eri päätyypeissä (Chou, 2010. Alkuperäisen pohjalta suomennettu kuvio Ahveninen.)

### 2.2.1 Infrastructure as a Service (IaaS)

Infrastructure as a Service (IaaS) eli infrastruktuuri palveluna mallissa asiakas vuokraa pelkän IT-infrastruktuurin, eli laskentatehoa, tallennustilaa ja muita perusominaisuuksia joita fyysiseenkin IT-infrastruktuuriin liittyisi (Peng ym., 2009). IaaSissa asiakas saa optimoitua resurssien kustannukset verrattuna perinteisen IT-infrastruktuurin rakentamiseen, koska hän maksaa vain käyttämistään resursseista. Asiakkaalla ei siis ole hukkaan menevää laitteistotehoa. Tehoa kuitenkin saa palveluntarjoajalta nopeasti lisää tarpeen mukaan (Biocic, Tomic & Ogrizovic, 2011.)

IaaS-asiakas on käytännössä vastuussa kaikesta muusta paitsi fyysisestä infrastruktuurista ja sen ylläpidosta. Asiakkaalla on siis oltava oma sovellusympäristö. Asiakas on itse vastuussa käyttöjärjestelmien ja muiden sovellusten asentamisesta ja ylläpidosta. Palveluntarjoaja ei myöskään vuokraa tässä palvelumallissa lisenssejä, vaan asiakkaalla on oltava omat lisenssinsä ohjelmistoihin. (Biocic ym., 2011.)

IaaS:ia harkitsevan on kuitenkin mietittävä muitakin kuin suoraan taloudellisia tai laskentatehoon liittyviä seikkoja. Näistä tärkeimpiä ovat turvallisuusnäkökulmat, esimerkiksi minkälainen turvallisuuspolitiikka palveluntarjoajalla on, missä data fyysisesti sijaitsee, ja ketkä siihen pääsevät käsiksi. (Gibson ym., 2012.) Palveluntarjoajan järjestelmänvalvojilla on usein ainakin teoreettinen mahdollisuus päästä käsiksi asiakkaiden dataan ja tietoliikenteeseen, mikä luo riskejä asiakkaan yksityisyydelle (Gibson ym., 2012).

### 2.2.2 Platform as a Service (PaaS)

Platform as a Service (PaaS) eli kehitysalusta palveluna -mallissa palveluntarjoaja tarjoaa asiakkaalle ympäristön jossa on mahdollista kehittää sovelluksia. Alusta on kokonaisvaltainen, eli siihen kuuluu kaikki tarvittava kuten ohjelmointikielet, väliohjelmistot ja ohjelmointirajapinnat. PaaSissa asiakkaan ei siis tarvitse itse kantaa huolta sovelluskehitysohjelmistojen asentamisesta, ylläpidosta tai konfiguroinnista. (Gibson ym., 2012.) Asiakas voi myös testata ohjelmistojaan PaaS ympäristössä. Useimmiten PaaS-palvelun tarjoajat huolehtivat myös sovellusten kauppapaikasta, jolloin valmiiden sovellusten levittäminenkin käy helposti. (Jadeja & Modi, 2012.) Palveluntarjoajat voivat veloittaa PaaS:n käytöstä kausittain tai käytön mukaan. Usein palveluntarjoajat myös veloittavat oman osuutensa heidän kauppapaikkansa kautta myydyistä sovelluksista. (Biocic ym., 2011.)

PaaS-palvelut voidaan jakaa kahteen kategoriaan, täyteen ja osittaiseen. Täydessä PaaSissa asiakas saa kokonaan verkkoselainpohjaisen käyttöliittymän, eikä hänen tarvitse asentaa mitään kehitystyökaluja lokaalisti. Huono puoli täydessä PaaSissa on asiakkaan suuri riippuvuus palveluntarjoajan kanavista. Siirtyminen pois palveluntarjoajan ympäristöstä sovellusten kanssa voi olla vaikeaa yhteensopivuusongelmien takia. Osittaisessa PaaSissa asiakas taas saa

palveluntarjoajalta osan sovelluskehityksen ja sovellusten levittämisen vaatimista palveluista, mutta joutuu kuitenkin asentamaan myös omia kehitysohjelmistoja lokaalisti. (Gibson ym., 2012.)

PaaS-mallissa asiakkaan on myös mahdollista jäädä jälkeen uusimmista teknologioista ja kehitystyökaluista. Ohjelmointirajapinnat ja alustat kehittyvät ja muuttuvat niin nopeasti, että palveluntarjoajalle ei ole mielekäästä tarttua kiinni mihinkään ratkaisuun, ennen kuin se on vakautunut ja kerännyt suuren määrän yleistä kannatusta. (Gibson ym., 2012.)

### 2.2.3 Software as a Service (SaaS)

Software as a Service (SaaS) eli sovellus palveluna -mallissa asiakas käyttää palveluntarjoajan yksittäistä sovellusta, yleensä internet-selaimen kautta. Sovellus ja sen käyttöön liittyvät toiminnallisuudet ovat keskitetysti palveluntarjoajalla, kuten myös vastuu sovelluksen ylläpidosta ja päivittämisestä. Asiakkaalta vaaditaan sovelluksen käyttöön useimmiten vain kevyttä asiakaspäätettä, jossa on internet-yhteys. (Gibson ym., 2012.) SaaS-mallissa asiakkaan ei tarvitse omistaa ohjelmistolisenssejä, sillä niiden vuokraus kuuluu palvelun hintaan. Tämä laskee kustannuksia senkin takia, että suuri palvelua tarjoava organisaatio on usein paremmassa neuvotteluasemassa lisenssien myyjän kanssa kuin esimerkiksi yksittäinen keskikokoinen yritys. (Biocic ym., 2011.)

Pilvipalveluiden yleisenä ongelmana nähdään turvallisuus. SaaS-malli voi kuitenkin jopa parantaa yrityksen tietoturvaa, koska data säilytetään keskitetysti pilvessä. Toisin sanoen vaikka SaaSia hyödyntävän yrityksen työntekijä hukkasi päätelaitteen, siinä ei välttämättä olisi löytäjälle hyödynnettävissä olevaa arkaluontoista tietoa, koska kaikki tieto on pilvessä. (Gibson ym., 2012.)

## 2.3 Pilvipalveluiden toteutusmallit

Pilvipalveluiden päätoteutusmalleja on kolme: julkinen pilvi, yksityinen pilvi ja hybridi pilvi (Jadeja & Modi, 2012), joita käsitellään tarkemmin alaluvuissa. On olemassa myös neljäs malli, yhteisöpilvi, jossa useampi organisaatio jakaa infrastruktuurin pilvessä. Yhteisöpilvessä on myös jaetut säännöt ja toimintamenetelmät. (Dillon ym., 2010.) Yhteisöpilvessä voidaan saavuttaa pilvipalveluiden hyviä puolia ottamatta mukaan varsinaista pilvipalvelun tarjoajaa. Yhteisöpilveä voi ajatella useamman toimijan yksityisenä pilvenä, koska yhteisön jäsenet hallitsevat infrastruktuuria. Tästä syystä yhteisöpilveä ei käsitellä erillisessä alaluvussa. (Briscoe & Marinos, 2009.)

### 2.3.1 Julkinen pilvi

Julkinen pilvi on yleisin nykyisistä toteutusmalleista. Julkinen pilvi palvelee monia asiakkaita ja palveluntarjoaja omistaa palveluun liittyvän infrastruktuu-

rin, vastaa sen ylläpidosta ja määrittää itse hinnoittelu- ja sääntöpolitiikan. (Dillon ym., 2010.)

Julkista pilvää käyttämällä asiakkaan on mahdollista säästää IT-kuluissa verrattuna perinteiseen omistamismalliin, koska julkisen pilven käyttö vaatii asiakkaan osalta vähiten omaa laitteistoa (Jadeja & Modi, 2012). Tämän takia julkisella pilvellä on myös pienimmät aloituskustannukset. Kuitenkin pitkällä aikavälillä julkinen pilvi tulee muita pilvipalveluiden toteutusmalleja kalliimmaksi, koska käyttömaksuja on maksettava jatkuvasti niin kauan kuin palvelua käyttää, toisin kuin esimerkiksi yksityisessä pilvessä. (Hu ym., 2011.)

Julkinen pilvi on asiakkaan tietoturvan kannalta kaikkein riskialttein, koska kaikki tieto liikkuu internetin yli ja on säilössä keskitetyssä ympäristössä johon useampi toimija voi päästä käsiksi, toisin kuin perinteisessä organisaation tietojärjestelmässä. Asiakkaalla ei myöskään ole sananvaltaa siihen, missä hänen tietonsa maantieteellisesti sijaitsevat. (Gibson ym., 2012.) Esimerkiksi Google ja Amazon tarjoavat julkisessa pilvessä toimivia palveluita (Jadeja & Modi, 2012).

### 2.3.2 Yksityinen pilvi

Yksityinen pilvi toimii käyttäjäorganisaation omassa verkossa, johon liittyvän infrastruktuurin organisaatio omistaa itse ja siihen pääsee käsiksi vain organisaatioon kuuluvat henkilöt (Hu ym., 2011). Yksityisellä pilvellä on siis monia samoja piirteitä intranetin kanssa (Jadeja & Modi, 2012).

Yksityinen pilvi vaatii suuria alkuinvestointeja infrastruktuurin rakentamisen takia. Infrastruktuuri vaatii tietysti myös fyysistä tilaa. Pitkällä aikavälillä kustannukset ovat kohtuulliset, koska organisaatiolla on omat laitteet, joista ei makseta vuokraa. Yksityisessä pilvessä resursseja menee myös hukkaan, koska infrastruktuurin on pystyttävä käsittelemään suurta hetkellistä kuormitusta. Suurimman osan ajasta laitteistossa on siis käyttämätöntä tehoa. (Hu ym., 2011.)

Yksityinen pilvi on kuitenkin houkutteleva, koska kriittinen data pysyy organisaation piirissä ja organisaatiolla itsellään on vastuu järjestelmän turvallisuudesta. Organisaatiolla ei myöskään ole pelkoa kriittisten toimintojen keskeytymisestä jonkin muun tahon takia, kun järjestelmät ovat organisaation sisällä. Tietoliikennemaksut, joita julkisen pilven käyttöön liittyy, kun dataa siirretään organisaation piiristä pilveen ovat myös huomionarvoiset. Yksityisessä pilvessä näissäkin säästetään. (Dillon ym., 2010.)

### 2.3.3 Hybridi pilvi

Hybridi pilvi on julkisen ja yksityisen pilven yhdistelmä. Hybridissä pilvessä yksityinen pilvi on yhdistettynä myös ulkoisiin, julkisiin pilvipalveluihin. (Jadeja & Modi, 2012.) Erilliset pilvet pysyvät omina entiteetteinään, mutta ovat yhdistettynä järjestelmillä jotka mahdollistavat yhteistoiminnan (Dillon ym.,

2010). Hybridi pilvi vaatii siis käyttäjältä myös omia laitteistoja, mutta oleellisesti vähemmän kuin yksityisen pilven toteutusmallissa. Eräs hybridin pilven vaikeuksista on juuri näiden erilaisten ympäristöjen yhdistäminen. (Hu ym., 2011.)

Hybridillä pilvellä on mahdollista saavuttaa kaikkein paras kustannustehokkuus, kun hyödynnetään sekä julkista että yksityistä pilveä. Käyttäjän ei tarvitse hankkia niin tehokasta infrastruktuuria kuin yksityisen pilven tapauksessa, koska julkisesta pilvestä saadaan lisää resursseja tarpeen vaatiessa. Kuitenkaan julkisen pilven omistajalle ei jouduta maksamaan niin suuria kiinteitä kustannuksia kuin täyden julkisen pilven mallissa, koska suurin osa toiminnasta tapahtuu organisaation omassa infrastruktuurissa. (Hu ym., 2011.)

Hybridi pilvi on houkutteleva ratkaisu myös turvallisuuden näkökulmasta. Käyttäjä pystyy pitämään itselleen tärkeimmät toiminnot ja datan organisaation sisällä, joten ongelmilla julkisessa pilvessä ei ole pysäyttävää vaikutusta organisaation toimintaan. Hyödyt kuten skaalautuvuus saavutetaan silti. (Dillon ym., 2010.)

### 2.3.4 Erilaisten toteutusmallien edut ja haitat

Taulukoissa 1 ja 2 esitellään yhteenvetona erilaisten pilvipalveluiden toteutusmallien edut ja haitat. Lähdetaulukko on suomennettu ja jaettu kahtia kirjoittajan toimesta.

TAULUKKO 1 Yhteenveto erilaisten toteutusmallien eduista (Hu ym., 2011.)

<b>Julkinen pilvi</b>	<b>Yksityinen pilvi</b>	<b>Hybridi pilvi</b>
Yksinkertaisin käyttää ja ottaa käyttöön	Täysi hallinta omista ohjelmisto- ja palvelinpäivityksistä	Paras kustannustehokkuus hyödyntämällä julkisen- ja yksityisen pilven joustavuudet
Pienet aloituskustannukset	Pienet kustannukset pitkällä aikavälillä	Vähemmän altis pitkille palvelukatkoille
Hyötysuhteen nousu palvelimien virtualisoinnin ansiosta	Hyötysuhteen nousu palvelimien virtualisoinnin ansiosta	Hyötysuhteen nousu palvelimien virtualisoinnin ansiosta
Laaja saavutettavuus		Kestää suuret kuormituspiikit
Ei tarvetta fyysiselle konesalille		
Kestää suuret kuormituspiikit		

TAULUKKO 2 Yhteenveto erilaisten toteutusmallien haitoista (Hu ym., 2011.)

<b>Julkinen pilvi</b>	<b>Yksityinen pilvi</b>	<b>Hybridi pilvi</b>
Kallein pitkällä aikavälillä	Suuret aloituskustannukset	Vaikea implementoida heterogeenisen toimitusmallin monimutkaisuuden takia
Altis pitkille palvelukatkoille	Altis pitkille palvelukatkoille Rajallinen saavutettavuus Vaatii eniten fyysistä tilaa konesalin takia Ei sovellu suurien kuormituspiikkien käsittelyyn	Vaatii jonkin verran fyysistä tilaa konesalille

Pilvipalveluiden palvelutasosopimusten tutkimisen kannalta merkittävin toteutusmalli on julkinen pilvi, koska julkisen pilven asiakkaat käyttävät palveluita, joiden vaatima infrastruktuuri on kokonaan jonkin toisen osapuolen omistama. Tällöin korostuu tarve hyvälle sopimuksille ja neuvottelulle.

### 3 PILVIPALVELUIDEN PALVELUTASOSOPIMUKSET

Pilvipalveluiden asiakkaiden ei tarvitse tietää mitä pilvessä on, mutta heidän on kuitenkin oltava varmoja palvelun laadusta. Jos asiakas ulkoistaa ydintoimintonsa pilvipalveluun, hänellä on oltava takeet palvelun toimivuudesta. (Dillon ym., 2010.) Palvelutasosopimukset (Service level agreement, SLA) ovat keino antaa takeita ja rakentaa luottamusta asiakkaan ja palveluntarjoajan välille. Tässä luvussa käydään läpi palvelutasosopimuksen perusmäärittely, erityyppisten pilvipalveluiden palvelutasosopimuksille asettamia haasteita ja sitä min-kälaisia pilvipalveluiden palvelutasosopimukset ovat.

#### 3.1 Palvelutasosopimukset

Palvelutasosopimus on palveluun liittyvä sopimus asiakkaan ja palveluntarjoajan välillä (Dillon ym., 2010). Yksinkertaisimmillaan se on dokumentti, joka sisältää kuvauksen palvelusta, parametreista joiden mukaan palvelun tasoa mitataan, palveluntarjoajan takuista sekä siitä kuinka sopimusrikkomustilanteissa toimitaan (Alhamad, Dillon & Chang, 2010). Yleensä palveluntarjoaja joutuu maksamaan rahallista korvausta asiakkaalle sopimusrikkomuksen tapahtuessa (Jantti & Suhonen, 2012). Palvelutasosopimus antaa asiakkaalle selvän kuvan palvelutasosta, jota hän voi palveluntarjoajalta odottaa. Palveluntarjoajalle sopimus toimii taas määritelmänä siitä, kuinka laadukasta palvelua hänen on tarjottava asiakkaalle. Palvelutasosopimus rakentaa siis luottamusta asiakkaan ja palveluntarjoajan välille. (Rak, Liccardo & Aversa, 2011.) Kaksi yleisintä tapaa tehdä palvelutasosopimus ovat (1) yhden osapuolen, useimmiten palveluntarjoajan, suoraan antama sopimus ja (2) palveluntarjoajan ja asiakkaan edustajien keskenään neuvottelema sopimus (Wieder, Butler, Theilmann & Yahyapour, 2012).

Palvelutasosopimus on tärkeä myös tietämyksen hallinnan kannalta. Sen pohjalta asiakkaan IT-osasto tietää, mitkä asiat ovat palveluntarjoajan vas-



tuulla ja mistä asioista heidän on itse huolehdittava (Jantti & Suhonen, 2012). Tarkemmin palvelutasosopimuksessa sovitaan:

- Teknisistä vaatimuksista, kuten laitteistoista, tietoverkoista, niiden kapasiteetista ja saavutettavuudesta sekä tietoturvasta (Alhamad ym., 2010).
- Asiakaspalveluun liittyvistä vaatimuksista, kuten palveluntarjoajan nopeudesta vastata palvelupyyntöihin ja palveluntarjoajan toiminnasta virhetilanteissa (Jantti & Suhonen, 2012).

Useat palveluntarjoajat priorisoivat palvelupyyntöjä asiakkaan palvelutasosopimuksen mukaan. Siksi asiakkaan on tärkeää saada hyvä sopimus ja olla tietoinen sopimuksessaan määritellystä palvelun tasosta (Jantti & Suhonen, 2012). Seuraavaksi käsitellään palvelutasosopimusten neuvottelua ja monitorointia.

### **3.1.1 Palvelutasosopimusten neuvottelu**

Perinteisin muoto solmia palvelutasosopimus on bilateraalin neuvottelu asiakkaan ja palveluntarjoajan välillä (Keller & Ludwig, 2003). Kummallakin osapuolella on halu suorittaa neuvotteluprosessi nopeasti resurssien säästämiseksi, mutta toisaalta sekä asiakas että palveluntarjoaja tahtovat itsensä kannalta parhaan mahdollisen sopimuksen (Tripathy & Patra, 2011).

Bilateraalisesta neuvottelusta puhuttaessa on muistettava, että yleensä sopimusta ei pystytä luomaan pelkästään kahden neuvottelijan voimin. Useimmiten neuvotteluja hoitaa liiketoiminta-analyttikko. Liiketoiminta-analyttikolla ei kuitenkaan yleensä ole tarpeeksi teknistä osaamista parhaan lopputuloksen aikaansaamiseksi, jolloin neuvotteluun tarvitaan myös henkilöitä joilla on teknistä tietotaitoa. (Tripathy & Patra, 2011.)

### **3.1.2 Palvelutasosopimusten monitorointi**

Palvelutasosopimukseen liittyvien ehtojen aktiivinen monitorointi on tärkeää sekä asiakkaan että palveluntarjoajan näkökulmasta. Asiakkaan on seurattava, että saatava palvelu on sovitulla tasolla, jotta erilaiset rikkomukset pystytään tunnistamaan ja niihin voidaan vaatia sovittua reagointia palveluntarjoajan puolelta. Palveluntarjoajan taas on tärkeää monitoroida palvelua virheiden tunnistamiseksi, jotta niihin voidaan reagoida ennen sopimusrikkomusta. Palveluntarjoajalle on hyötyä monitorointitiedoista myös epäselvässä kiistatilanteessa asiakkaan kanssa. Palveluntarjoaja pystyy omilla monitorointitiedoilla esittämään oman näkemyksensä. (Tripathy & Patra, 2011.) Monitorointidatan kerääminen on tärkeää palveluntarjoajalle myös siksi, että pystytään osoittamaan potentiaalisille asiakkaille palvelun toimivuus ja taso verrattuna kilpailijoihin (Liu & Xu, 2013).

Palvelutasosopimukseen liittyvien laatuparametrien on oltava helposti mitattavia ja niitä tulisi olla paljon. Kun parametrit ovat selkeitä, palveluntarjoajan ja asiakkaan on helpompi löytää yhteisymmärrys niistä saatavista tuloksista. Hyvistä parametreista saadaan myös hyödyllistä tietoa, jota voidaan tilastoida ja tulkita liiketoiminnan kehittämiseksi. (Liu & Xu, 2013.)

Monitoroinnissa voidaan käyttää myös kolmatta osapuolta. Monitoroinnin ulkoistaminen on tarpeellista, jos esimerkiksi asiakas tai palveluntarjoaja eivät kykene tai ole halukkaita toteuttamaan monitorointia itse. Asiakas ja palveluntarjoaja voivat käyttää kolmatta osapuolta monitoroinnissa myös, jos heidän keskinäinen luottamuksensa on huono. Kun monitorointi siirretään ulkoiselle kumppanille, rahoituksesta huolehtii asiakas, palveluntarjoaja tai molemmat. (Keller & Ludwig, 2003.)

### 3.2 Palvelutasosopimukset pilvipalveluissa

Pilvipalveluiden suosion kasvun myötä myös markkinoilla olevien palveluntarjoajien määrä on kasvanut. Kun toimijoita on paljon ja kilpailu kovenee, palvelutasosopimukset, monitorointi sekä testidatan kerääminen muodostuvat tärkeiksi palveluntarjoajalle liiketoiminnan kannalta. Pilvipalveluiden yleistyessä myös asiakkaiden valvettavuus laatuun liittyvistä tekijöistä on noussut, jolloin on tärkeää pystyä pitävästi osoittamaan oman palvelunsa paremmuus kilpailijoihin verrattuna testidatalla ja paremmilla takeilla. Palvelutasosopimukset ja testidata antavat palveluntarjoajille myös hyödyllistä tietoa asiakkaiden mieltymyksistä, joka taas auttaa palveluiden optimoinnissa. (Liu & Xu, 2013.)

Palveluntarjoajien on tärkeää pyrkiä olemaan rikkomatta tekemiään sopimuksia. Mahdollisen sakkomaksun lisäksi 57% Forrester Consultingin tutkimukseen osallistuneista pilvipalveluiden tarjoajista huomasivat laskun liikevaihdossa ja asiakastyytyväisyydessä palvelutasosopimusrikkomuksen jälkeen. (Sun ym., 2012.) Palveluntarjoajan näkökulmasta palvelutasosopimuksen on oltava asiakkaiden tarpeiden mukainen, mutta samalla kilpailukykyinen, koska korkean tason luotettavuuden ylläpito vaatii paljon resursseja. Käyttämättömän puskurin tarve palveluntarjoajan järjestelmässä kasvaa parempien laatuasteiden lupaamisen myötä. Varajärjestelmiä tarvitaan kompensoimaan pääjärjestelmän virheitä, jotta voidaan välttää sopimusrikkomukset. (Gonzalez & Helvik, 2012.)

Pilvipalveluiden eri toteutusmallien palvelutasosopimuksissa on monia yhteisiä piirteitä, kuten turvallisuus, yksityisyys, monitorointi, tukipyyntöihin vastaaminen ja laskutus (Alhamad ym., 2010). Taulukossa 3 esitellään Alhamadin ym. (2010) näkemys erilaisten toteutusmallien palvelutasosopimuksien yhteisistä sopimusehdoista. Taulukko tehty alkuperäisen pohjalta uudelleen suomeksi.

TAULUKKO 3 Erilaisten toteutusmallien yhteiset sopimusehdot (Alhamad ym., 2010. Alkuperäisen pohjalta suomennettu taulukko Ahveninen.)

Sopimusehto	Kuvaus
Monitorointi	Kuka monitoroi ja millä menetelmällä
Laskutus	Palvelun hinta ja kuinka se lasketaan
Turvallisuus	Kryptaus, autentikointi ja autorisointi
Tietoverkot	IP osoitteiden määrä ja verkon läpisyöttö
Yksityisyys	Kuinka dataa säilytetään ja siirretään
Tukipalvelut	Kuinka palveluntarjoajalta saa tukea
Paikalliset ja kansainväliset	Toimintaperiaatteet, joiden mukaan palveluntarjoaja toimii toimintaperiaatteet

Erilaiset toteutusmallit ovat kuitenkin keskittyneitä erilaisten palveluiden tuottamiseen, joten eri palvelut luovat erilaisia vaatimuksia palvelutasosopimusten parametreille (Liu & Xu, 2013). Näihin erityispiirteisiin perehdytään seuraavissa alaluvuissa.

### 3.2.1 IaaS-sopimusten erityispiirteet

Infrastruktuuri palveluna -palvelutasosopimuksissa on keskityttävä infrastruktuurin suorituskykyä ja saavutettavuutta mittaaviin parametreihin, esimerkiksi virtuaalikoneiden suorituskykyyn, infrastruktuurin verkko-ominaisuuksiin, vasteaikaan ja tallennustilan määrään (Liu & Xu, 2013).

Yhtenä infrastruktuuri palveluna -mallin ensimmäisessä luvussa mainituista hyödyistä on sen helppo skaalattavuus asiakkaan tarpeiden mukaan. On siis myös tärkeää sopia skaalattavuudesta palvelutasosopimuksessakin. Alhamad ym. (2010) ehdottavat parametreiksi skaalauksen määrää, kestoa ja automaattiskaalaus-toimintoa.

### 3.2.2 PaaS-sopimusten erityispiirteet

Kehitysalusta palveluna -palvelutasosopimuksissa huomioon on otettava erityisesti kehitysalusta ja sen tarjoamat sovelluskehitysmahdollisuudet. Sopimuksessa parametreinä voi olla esimerkiksi integraatio muiden palveluiden kanssa, skaalaus, käyttöalustat ja kehitysalustaa käyttävien kehittäjien määrä (Alhamad ym., 2010).

Kehitysalustassa palveluna on otettava huomioon myös sillä kehitettyjen sovellusten käyttö ja elinkaari. Eli sopimuksessa on huomioitava myös millä alustalla sovellusta voi käyttää, kuinka paljon sovellus voi käyttää palveluntarjoajan resursseja ja missä palveluissa sovelluksen voi julkaista (Liu & Xu, 2013).

### 3.2.3 SaaS-sopimusten erityispiirteet

Sovellus palveluna -palvelutasosopimuksissa päärooliin nousee sovelluksen käytettävyys ja luotettavuus. Tärkeitä parametrejä ovat esimerkiksi käyttöliit-

tymän taso, ohjelman vasteaika sekä alustat joilla ohjelmaa voi käyttää (Liu & Xu, 2013).

Alhamad ym. (2010) nostavat esiin myös sovelluksen kustomoitavuuden. Kohdaksi palvelutasosopimukseen voisi siis ottaa myös sen, kuinka hyvin sovellusta voidaan muokata erilaisten käyttäjien tarpeisiin.

## 4 PILVIPALVELUIDEN PALVELUTASOSOPIMUSTEN RISKIT ASIAKKAALLE

Palvelutasosopimus on tärkeä työkalu niin asiakkaalle kuin palveluntarjoajallekin pilvipalveluissa. Kuitenkaan edes palvelutasosopimus ei ole täysin varma keino suojautua kaikilta ongelmilta, vaan pitää sisällään omat riskinsä. Tässä luvussa esitellään kyseisiä riskejä pilvipalveluiden asiakkaiden näkökulmasta. Luku aloitetaan esittelemällä neuvotteluun liittyviä riskejä, jonka jälkeen siirrytään turvallisuuteen liittyviin riskeihin. Riskille on monta määritelmä, mutta tässä luvussa riskillä tarkoitetaan tilannetta, jolla voi mahdollisesti olla negatiiviset seuraukset (Hansson, 2012).

### 4.1 Neuvottelun riskit

Bilateraalinen neuvottelu on aina riskialtista. Tämä perustuu siihen, että molemmat osapuolet tahtovat omalta kannaltaan parhaan mahdollisen lopputuloksen. Palvelutasosopimuksen neuvotteluvaiheessa molemmat osapuolet käyttävät kaiken tietämyksensä maksimoidakseen voittonsa ja palvelutasosopimuksen arvon omasta näkökulmastaan (Tripathy & Patra, 2011). Molemmat osapuolet pyrkivät saamaan mahdollisimman paljon hyötyä sopimuksesta, mutta tekemään samalla mahdollisimman vähän myönnytyksiä (Rak ym., 2011). Tästä seuraa, että asiakkaan huonompi tietämys voi johtaa asiakkaan kannalta huonompaan sopimukseen.

Neuvottelun riskeistä osa on tyypillisiä monenlaisille tilanteille, jossa eri toimijat pyrkivät luomaan keskinäisen sopimuksen. Seuraavaksi listataan neuvottelun riskin tekijöitä:

1. *Neuvottelijan riittämättömät tekniset taidot.* Palvelutasosopimuksen neuvottelijana toimii usein liiketoiminta-analyttikko. Liiketoiminta-analyttikolla on usein myös jonkinlaista teknistä taitopohjaa, mutta ei riittävästi hyvän sopimuksen solmimista varten. Neuvottelija tarvitsee tukea erilaisilta teknisiltä asiantuntijoilta. (Tripathy & Patra, 2011.) Neuvotteluasetelmaan syntyy

siis selvä epätasapaino palveluntarjoajan hyväksi, jos asiakkaalla ei ole käytössään tarpeeksi teknistä tietotaitoa (Tafti, 2005). Sen lisäksi koko asetelmaan vaikuttaa se, että toimivan palvelutasosopimuksen tekeminen on jo lähtökohtaisesti vaikea tehtävä (Sun ym., 2012). Neuvotteluasetelman epätasapainoisuudesta voi siis koitua asiakkaalle suurta haittaa.

2. *Tilastollisten tietojen harhaanjohtavuus.* Liiallinen luottamus keskimääräisiin arvoihin palveluntarjoajan kyvykkyydestä voi johtaa vääriin johtopäätöksiin. Päätelmien tukena on hyvä käyttää myös vaihteluvälejä keskiarvojen tukena. Palveluntarjoaja pystyy naamioimaan ongelmiaan tilastotiedolla keskimääräisestä kyvykkyydestä. Keskimääräisyydet piilottavat pahimmat ongelmatapaukset, niistä ei esimerkiksi näe, jos palveluntarjoajalla on kestänyt todella pitkään hoitaa joitakin yksittäisiä ongelmia. (Tafti, 2005.)
3. *Sovitut korvaukset eivät vastaa tappiota.* Palvelutasosopimuksessa sovitaan sopimusrikkomukseen liittyvistä korvauksista, mutta vastaan voi kuitenkin tulla tilanteita, joissa korvaus on asiakkaan mielestä haittaaan verrattuna liian pieni. Kiistat palveluntarjoajan ja asiakkaan välillä voidaan ehkäistä sopimalla kolmannen osapuolen käytöstä tilanteissa, joissa korvauksista tulee epäselvyyksiä. (Tafti, 2005.)

## 4.2 Turvallisuusriskit

Huono tietoturva on Subashinin ja Kavithan (2011) mukaan suurin yksittäinen seikka, joka aiheuttaa yrityksissä vastahakoisuutta siirtyä käyttämään pilvipalveluita. Palveluntarjoajat eivät vieläkään pysty ylläpitämään asiakkaidensa tietoturvaa ongelmitta. Ainoa keino varmistaa turvallisuus on käyttää yksityistä pilveä. Julkisessa pilvessä taas turvallisuutta voidaan parantaa palvelutasosopimuksilla. (Subashin & Kavitha, 2011.) Palvelutasosopimuksetkin toimivat kuitenkin vain vakuutteluna, eivätkä täysin varmana turvajärjestelynä. Palvelutasosopimusten turvallisuusnäkökulmien kehittyminen on tärkeää asiakkaan kannalta (Kandukuri, Ramakrishna & Rakshit, 2009).

Turvallisuusriskeistä monet ovat tyypillisiä juuri pilvipalveluille. Ne eivät ole varsinaisesti mitattavia parametreja, mutta ne on silti otettava huomioon palvelutasosopimusta tehtäessä. Seuraavaksi esitellään pilvipalveluiden palvelutasosopimusten turvallisuusriskejä:

1. *Asiakkaan tietojen fyysinen sijainti.* Kuten aikaisemmassa luvussa mainittiin, pilvipalveluiden asiakas ei näe pilven taakse. Tämän seurauksena asiakas ei myöskään tiedä palveluntarjoajan infrastruktuurin fyysistä sijaintia. Asiakkaan tietojen sijainti jää siis epäselväksi, ellei siitä erikseen sovita. Tästä syntyy Subashinin ja Kavithan (2011) mukaan erityisesti lakiin liittyviä riskejä, koska esimerkiksi useassa EU-maassa arkaluontoiset tiedot eivät saa lain mukaan poistua rajojen ulkopuolelle. Ongelmaksi muodostuu myös se, minkä valtion toimivallan alueelle tieto kuuluu, mikäli tiedoista joudutaan tekemään tutkintaa (Subashini & Kavitha, 2011). Palvelutasosopimuksessa on siis tärkeää sopia fyysisestä alueesta, jossa data sijaitsee, sekä siitä, suos-

tuuko palveluntarjoaja asiakkaan tietoja käsiteltäessä noudattamaan samoja tietosuojasääntöjä, joita asiakkaan on lain mukaan noudatettava (Kandukuri ym., 2009).

2. *Eri asiakkaiden tietojen erottelu.* Julkisissa pilvissä toimitaan monen toimijan ympäristöissä, joten on tärkeää saada palveluntarjoajalta takeet palvelutasosopimukseen yksittäisen asiakkaan tietojen riittävästä salauksesta (Kandukuri ym., 2009). Muuten asiakkaat pystyvät käyttämään järjestelmän heikkouksia hyödykseen ja tarkastelemaan toisten asiakkaiden arkaluontoisia tietoja esimerkiksi hyödyntämällä SQL-injektiota. Eri asiakkaiden tiedot pitäisi pystyä erottamaan sekä fyysisellä- että ohjelmistotasolla. Palvelun on pystyttävä erottamaan eri käyttäjien tallentamat ja käyttämät tiedot. (Subashin & Kavitha, 2011.)
3. *Jatkuvuus ja palautuminen.* Palveluntarjoaja voi joutua tilanteeseen, jossa jatkuvuus on uhattuna esimerkiksi luonnonkatastrofin, konkurssin tai yritysoston takia. Kandukurin ym. (2009) mukaan asiakkaan onkin saatava palvelutasosopimukseen palveluntarjoajan kyky ja edellytykset reagoida katastrofeihin. Palvelutasosopimuksessa kannattaa myös sopia, mitä tiedoille tapahtuu, jos palveluntarjoaja myydään toiselle yritykselle (Kandukuri ym., 2009). Subashini ja Kavitha (2011) ovat sitä mieltä, että palvelutasosopimuksessa kannattaa sopia myös siitä, mitä asiakkaan datalle tapahtuu tilanteessa, jossa tämä vaihtaa palveluntarjoajaa tai ei kykene enää maksamaan palvelusta sovittua hintaa. Jos asiakas ei huolehdi näistä asioista, hän saattaa menettää palveluun tallentamansa tiedot tai oikeus asiakkaan tallentamiin tietoihin saattaa siirtyä palveluntarjoajalle.
4. *Palveluntarjoajan työntekijöiden pääsy tietoihin.* Palveluntarjoajan turvallisuuskäytännöistä on myös oltava selvitys, koska ne voivat poiketa hyvinkin paljon yrityksen omista vaatimuksista. Asioihin, joista on saatava virallista tietoa kuuluvat esimerkiksi henkilöstön, erityisesti järjestelmänvalvojien mahdollisuudet nähdä asiakkaiden tietoja, palkkausprosessi ja siihen liittyvät turvallisuusselvitykset sekä palveluntarjoajan yleiset turvallisuuskäytännöt. (Kandukuri ym., 2009.) Subashin ja Kavitha (2011) ovat sitä mieltä, että myös jokainen palveluntarjoajan työntekijän kirjautuminen asiakkaan tietoihin on hyvä tallentaa ja auditoida palveluntarjoajan toimesta.

### 4.3 Yhteenveto pilvipalveluiden palvelutasosopimusten riskeistä asiakkaalle

Seuraavassa taulukossa 4 esitetään yhteenveto edellä mainituista riskeistä. Taulukossa kerrataan myös niiden kuvaukset ja luokitukset sekä esitellään niitä tukevia lähteitä.

TAULUKKO 4 Kooste pilvipalveluiden asiakkaiden palvelutasosopimuksiin liittyvistä riskeistä.

Riski	Luokitus	Kuvaus	Lähteet
Neuvottelijan riittämätön tekninen osaaminen	Neuvotteluriski	Neuvottelija ei tunne palvelua tarpeeksi hyvin kattavaa sopimusta varten	Tripathy & Patra (2011), Rakym. (2011), Tafti (2005)
Tilastollisen tietojen harhaanjohtavuus	Neuvotteluriski	Sopimusta tehtäessä keskiarvot piilottavat ääritapaukset	Tafti (2005)
Sovitut korvaukset eivät vastaa asiakkaan kokemaa tappiota	Neuvotteluriski	Sopimusrikkomuksesta saadut korvaukset ovat liian pieniä haittaan nähden	Tafti (2005)
Tietojen fyysinen sijainti	Turvallisuusriski	Tietojen tuntematon sijainti voi aiheuttaa lakiin ja tietoturvaan liittyviä ongelmia	Subashini & Kavitha (2011), Kandukuri ym. (2009)
Eri asiakkaiden tietojen erottelu	Turvallisuusriski	Tietojen huono erottelu voi avata takaportteja muille asiakkaille	Subashini & Kavitha (2011), Kandukuri ym. (2009)
Jatkuvuus ja palautuminen	Turvallisuusriski	Palautuminen ja tietojen säilyminen ongelmatilanteissa	Subashini & Kavitha (2011), Kandukuri ym. (2009)
Palveluntarjoajan työntekijöiden pääsy asiakkaan tietoihin	Turvallisuusriski	Palveluntarjoajan työntekijöiden mahdollisuus nähdä asiakkaan tietoja	Subashini & Kavitha (2011), Kandukuri ym. (2009)

Palvelutasosopimuksiin liittyy monia riskejä, mutta on huomattava, että useat näistä riskeistä voidaan välttää oikealla varautumisella, asiantuntemuksella, riittävällä teknisellä tuella neuvottelijalle ja hyvällä sopimuksen teolla.



## 5 YHTEENVETO

Pilvipalveluissa on kyse merkittävästä ilmiöstä, niin taloudellisen kuin teknologisen kehityksen kannalta. Pilvipalveluita käyttämällä yritykset voivat saavuttaa suuria hyötyjä, kuten pienempiä kustannuksia, kilpailukykyistä teknologiaa ja helposti skaalattavaa laskentatehoa. Kuitenkin tämä kehitys tarvitsee tuekseen takeita palvelutasosopimusten muodossa, koska riskit ovat muuten niin suuret, että yritykset eivät kykene siirtymään pilvipalveluiden käyttäjiksi. Riskit turvallisuudelle ovat suurin yksittäinen yritysten pilvipalveluihin siirtymistä hidastava tekijä. Yritys ei voi vaarantaa liiketoiminnan jatkuvuutta. Palvelutasosopimukset auttavat asiakkaita saavuttamaan turvallisuuden tunteen palvelun käyttäjinä ja palveluntarjoajille ne ovat tärkeä työkalu positiivisen imagon rakentamiseen ja kilpailijoista erottumiseen. Palvelutasosopimuksillakaan ei voida saavuttaa molemmille osapuolille optimaalista ratkaisua, koska molemmat pyrkivät maksimoimaan oman hyötynsä, jolloin se osapuoli, joka on kykenevämpi sopimusten tekoon, saa omalta kannaltaan aikaan paremman sopimuksen. Palvelutasosopimukset ovat kuitenkin tärkeä työkalu pilvipalveluiden käyttäjille ja palveluntarjoajille ja niitä tulisikin tutkia ja kehittää lisää. Erittäin tärkeää on tietää minkälaisia ongelmia pilvipalveluiden palvelutasosopimuksiin voi liittyä, jotta on mahdollista solmia hyviä sopimuksia ja ottaa oikeat asiat huomioon sopimuksentekovaiheessa.

Tutkimuksen tavoitteena oli tunnistaa pilvipalveluiden palvelutasosopimusten riskejä asiakkaan näkökulmasta, sekä löytää määritelmä pilvipalveluille ja pilvipalveluiden palvelutasosopimuksille. Tutkimuksessa ei pyritty löytämään viitekehystä palvelutasosopimusten teolle, vaan määrittelemään sopimusten mahdolliset riskit. Riskien vaikutuksiin niiden toteutuessa ei tutkimuksessa myöskään otettu kantaa. Tutkimus toteutettiin kirjallisuuskatsauksena.

Pilvipalvelu on internetin välityksellä toteutettava palvelu, joka hyödynää toiminnassaan pilvilaskentaa. Pilvipalvelussa datan painopiste siirtyy asiakkaiden päätelaitteilta keskitettyihin palveluntarjoajan keskuksiin, joiden fyysistä infrastruktuuria tai toimintaa käyttäjän ei ole mahdollista nähdä, eikä hänellä ole myöskään mahdollisuutta vaikuttaa siihen. Siitä tuleekin pilvi terminä, käyttäjä ei näe pilven taakse. Pilvipalveluihin liittyy myös helppo skaalattavuus,

käyttäjän on helppo pyytää lisää laskentatehoa ja palveluntarjoaja pystyy hoitamaan sen jakamisen automaattisesti. Pilvipalveluissa on myös käyttäjälle pienet aloituskustannukset ja palvelusta maksetaan käytön mukaan. Pilvipalvelulla havaittiin kolme yleistä palvelumallia, sovellus palveluna, kehitysalusta palveluna ja infrastruktuuri palveluna. Toteutusmalleja havaittiin myös olevan kolme, julkinen pilvi, yksityinen pilvi sekä näiden yhdistelmä, hybridi pilvi. Yhteisöpilveä ei käsitelty erillisenä mallina, koska kyse on oikeastaan useamman toimijan yksityisestä pilvestä.

Pilvipalveluiden palvelutasosopimuksessa sovitaan palvelusta, parametreista joilla sen tasoa mitataan, palveluntarjoajan takeista palvelun tasolle ja korvauksista sekä toiminnasta virhetilanteissa. Sopimuksen monitorointi sen tekemisen jälkeen on tärkeää sekä asiakkaan että palveluntarjoajan näkökulmasta. Asiakkaan on hyvä tunnistaa erilaiset virhetilanteet ja palveluntarjoaja saa monitoroinnilla aikaan hyödyllistä tilastoa palvelustaan ja mahdollisuuden reagoida virheisiin ennen niiden tapahtumista. Pilvipalveluiden eri toteutusmallien palvelutasosopimuksissa on monia yhteisiä piirteitä, kuten turvallisuus, yksityisyys, monitorointi, tukipyyntöihin vastaaminen ja laskutus. Toisaalta erilaiset palvelumallit keskittyvät erilaisten palveluiden tuottamiseen, jolloin tarvitaan sopimuksia, joissa otetaan huomioon palvelumallien erityispiirteet. Esimerkiksi IaaSissa on tärkeää mitata infrastruktuurin suorituskykyä, kun taas PaaSissa tärkeäksi nousee esimerkiksi integraatio ja käyttöalustat. SaaSissa taas palvelutasosopimus liittyy vahvemmin itse sovelluksen ominaisuuksiin.

Pilvipalveluiden palvelutasosopimukseen liittyvien riskien havaittiin jakautuvan kahteen kategoriaan, neuvotteluriskeihin ja turvallisuusriskeihin. Neuvotteluriskinä voidaan pitää esimerkiksi neuvottelijan riittämätöntä teknistä osaamista, jolloin neuvottelija ei tunne palvelua tarpeeksi hyvin kunnollisen sopimuksen tekoa varten. Tilastollisten tietojen harhaanjohtavuus on myös riski joka tulee esille neuvotteluvaiheessa, eli neuvottelussa on varottava tukeutumista pelkkiin tilastollisiin keskiarvoihin palvelun toiminnasta, koska ääripaukset voivat jäädä niissä piiloon. Sopimusrikkomuksesta on myös pystyttävä sopimaan kunnollinen korvaus, jotta se vastaa koettua haittaa mahdollisessa sopimusrikkomustilanteessa. Turvallisuuteen taas liittyy esimerkiksi datan fyysinen sijainti. Datan tuntematon fyysinen sijainti voi aiheuttaa ongelmia tietoturvaan ja säädösten noudattamiseen. Eri asiakkaiden datan huono erottelu taas voi antaa mahdollisuuden muille asiakkaille päästä käsiksi heille kuulumattomaan dataan takaporttien kautta. Jatkuvuus ja palautuminen liittyvät riskeinä odottamattomiin tilanteisiin, joissa keskipisteessä on palveluntarjoajan kyky toipua erilaisista ongelmista. Palveluntarjoajan työntekijöiden pääsy dataan on myös huomattava turvallisuusriski. On tärkeää, että ulkopuoliset eivät pääse tarkkailemaan asiakkaan toimia ja dataa.

Tulosten perusteella voidaan sanoa, että palvelutasosopimuksen neuvotteluun on panostettava tarpeeksi resursseja ja usein liiketoimintataustaiselle neuvottelijalle on myös annettava tarpeeksi teknistä tukea, jotta riskejä pystyttäisiin välttämään alusta asti ja sopimus saadaan vastaamaan yrityksen tarpeita. Sopimukseen on osattava valita juuri kyseiselle yritykselle kyseiseen tarkoituk-

seen sopivat parametrit, joiden tasosta sovitaan ja joita monitoroidaan. Pilvipalveluiden erilaiset palvelumallit asettavat toisistaan paljonkin poikkeavia vaatimuksia palvelutasosopimuksien teolle. On huomattava myös, että turvallisuudenkin liittyviä riskejä voidaan välttää, kun ne otetaan huomioon jo sopimuksen neuvotteluvaiheessa. Siksi onkin tärkeää tuntee riskit etukäteen, antaa neuvottelijalle riittävästi teknistä tukea ja selvittää tarkkaan, mitä sopimuksella halutaan varmistaa.

Tutkimuksessa luotiin tieteellisiä ja ajankohtaisia lähteitä käyttäen mielestäni hyvä yleiskuva pilvipalveluista, palvelutasosopimuksista ja niihin liittyvistä riskeistä. Tutkimus auttaa ymmärtämään, kuinka nämä asiat nivoutuvat toisiinsa, eikä tulosten ymmärtäminen vaadi vahvaa teknistä osaamistaustaa, vaan ne ovat loogisia ja johdonmukaisia. Jatkotutkimuksen aiheina mielenkiintoisia olisivat mielestäni pilvipalveluiden palvelutasosopimusten riskien tutkiminen myös palveluntarjoajan näkökulmasta, yleinen osaaminen ja ymmärrys yrity maailmassa pilvipalveluiden palvelutasosopimukseen liittyen sekä pilvipalveluiden asiakkaiden kokemaa riittävyys saadusta kompensatiosta sopimusrikkomustilanteessa.

## LÄHTEET

- Armbrust, M., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, R., Lee, G., Patterson, D., Rabkin, A. & Stoica, I. (2009). Above the clouds: A Berkeley view of cloud computing. *University of California, Berkeley, Tech. Rep. UCB*, 07-013.
- Alhamad, M., Dillon, T., & Chang, E. (2010). Conceptual SLA framework for cloud computing. *4th IEEE International Conference on Digital Ecosystems and Technologies*, 606-610.
- Biocic, B., Tomic, D., & Ogrizovic, D. (2011). Economics of the cloud computing. *MIPRO, 2011 Proceedings of the 34<sup>th</sup> International Convention*, 1438-1442.
- Briscoe, G., & Marinos, A. (2009). Digital ecosystems in the clouds: Towards community cloud computing. *2009 3rd IEEE International Conference on Digital Ecosystems and Technologies*, 103-108.
- Chen, Y., Li, X., & Chen, F. (2011). Overview and analysis of cloud computing research and application. *2011 International Conference on E-Business and E-Government (ICEE)*, 1-4.
- Chou, Y., (2010). Cloud Computing Primer for IT Pros. TechNet -blogi. <http://blogs.technet.com/b/yungchou/archive/2010/11/15/cloud-computing-primer-for-it-pros.aspx>, haettu 22.11.2013
- Dillon, T., Wu, C., & Chang, E. (2010). Cloud Computing: Issues and Challenges. *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 27-33.
- Gibson, J., Rondeau, R., Eveleigh, D., & Tan, Q. (2012). Benefits and challenges of three cloud computing service models. *2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN)*, 198-205.
- Gonzalez, A. J., & Helvik, B. E. (2012). System management to comply with SLA availability guarantees in cloud computing. *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*, 325-332.
- Hansson, S. O., "Risk", *The Stanford Encyclopedia of Philosophy* (Winter 2012 Edition), Edward N. Zalta (ed.)
- Hu, F., Qiu, M., Li, J., Grant, T., Tylor, D., McCaleb, S., Butler, L., Hamner, R. (2011). A Review on Cloud Computing : Design Challenges in Architecture and Security. *Journal of Computing and Information Technology*, 19, 25-55.
- Jadeja, Y., & Modi, K. (2012). Cloud computing-concepts, architecture and challenges. *2012 International Conference on Computing, Electronics and Electrical technologies [ICCEET]*, 877-880.
- Jantti, M., & Suhonen, A. (2012). Improving Service Level Management Practices: A Case Study in an IT Service Provider Organization. *2012 IIAI International Conference on Advanced Applied Informatics*, 139-144.
- Kandukuri, B. R., Ramakrishna, P. V., & Rakshit, A. (2009). Cloud Security Issues. *2009 IEEE International Conference on Services Computing*, 517-520.

- Keller, A., & Ludwig, H. (2003). The WSLA framework: Specifying and monitoring service level agreements for web services. *Journal of Network and Systems Management*, 11(1), 57-81.
- Liu, X., & Xu, F. (2013). Cloud Service Monitoring System Based on SLA. *2013 12th International Symposium on Distributed Computing and Applications to Business, Engineering & Science*, 137-141.
- Peng, J., Zhang, X., Lei, Z., Zhang, B., Zhang, W., & Li, Q. (2009). Comparison of Several Cloud Computing Platforms. *Information Science and Engineering (ISISE), 2009 Second International Symposium on Information Science and Engineering*.
- Rak, M., Liccardo, L., & Aversa, R. (2011). A SLA-based interface for security management in cloud and GRID integrations. *2011 7th International Conference on Information Assurance and Security (IAS)*, 378-383.
- 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.
- Sun, L., Singh, J., & Hussain, O. (2012). Service level agreement (SLA) assurance for cloud services: a survey from a transactional risk perspective. *Proceedings of the 10<sup>th</sup> International Conference on Advances in Mobile Computing & Multimedia*, 263-266.
- Tafti, M. H. A. (2005). Risks factors associated with offshore IT outsourcing. *Industrial Management & Data Systems*, 105(5), 549-560.
- Tripathy, A. K., & Patra, M. R. (2011). Modeling and monitoring SLA for service based systems. *Proceedings of the 2011 International Conference on Intelligent Semantic Web-Services and Applications - ISWSA '11*, 1-6.
- Velkoski, G., & Simjanoska, M. (2013). CPU utilization in a multitenant cloud. *EUROCON, 2013 1-4, (July)*, 242-249.
- Wieder, P., Butler, J. M., Theilmann, W., Yahyapour, R. (2012). *Service Level Agreements For Cloud Computing*. Springer.