TURUN YLIOPISTO
Kauppakorkeakoulu

Riskit ja riskienhallinta ennen SaaS-järjestelmän käyttöönottopäätöstä Suomessa toimivissa suurissa organisaatioissa

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatijat:
Tuomas Kavanti
Niklas Oinonen

Ohjaaja:
KTT Reima Suomi

22.4.2025
Turku

Tietojärjestelmätieteen pro gradu -tutkielma

Oppiaine: Tietojärjestelmätiede
Tekijät: Tuomas Kavanti, Niklas Oinonen
Otsikko: Riskit ja riskienhallinta ennen SaaS-järjestelmän käyttöönottopäätöstä Suomessa toimivissa suurissa organisaatioissa
Ohjaaja: KTT Reima Suomi
Sivumäärä: 98 sivua + liitteet 16 sivua
Päivämäärä: 22.4.2025

SaaS-järjestelmät ovat suuressa suosiossa ja organisaatiot ottavat niitä käyttöön yhä enenevissä määrin. SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat useat erilaiset hyödyt, mutta myös riskit tulee huomioida käyttöönottopäätöstä tehdessä. Aikaisemmassa tutkimuksessa on havaittu, että pilvipalveluiden sekä myös spesifisti SaaS:n kohdalla havaitaan useita erilaisia riskejä ja riskiluokkia, jotka vaikuttavat järjestelmän käyttöönottopäätökseen negatiivisesti. Lisäksi aikaisemman tutkimuksen perusteella on selvää, että riskien tunnistamisen jälkeen on tärkeää arvioida, mitä ja miten riskejä tulisi käsitellä. Tämän tutkimuksen tarkoituksena onkin selvittää, millaisia riskejä Suomessa toimivissa suurissa organisaatioissa huomioidaan käyttöönottopäätökseen vaikuttavina tekijöinä ja millaista riskienhallintaa organisaatioissa tehdään ennen SaaS-järjestelmän käyttöönottopäätöstä.

Tutkimus toteutettiin laadullisena tutkimuksena hyödyntäen puolistrukturoituja haastatteluja. Haastateltavina toimivat organisaatioiden SaaS-järjestelmien käyttöönottopäätöksissä mukana olleet henkilöt, joiden joukkoon valittiin useita pääasiassa suurten organisaatioiden ylimmän tason IT-johtajia, kuten tietohallintojohtajia. Tutkimuksessa haastateltiin 14 henkilöä 12 eri organisaatiosta, joilla on toimintaa Suomessa. Analyysi suoritettiin hyödyntäen laadullista sisällönanalyysiä, jonka tukena käytettiin tutkimuksessa muodostettua teoreettista viitekehystä sekä aikaisempaa tietoa tutkimusaiheesta. Tutkimuksessa pyrittiin tunnistamaan SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat keskeiset riskit sekä selvittämään Suomessa toimivien suurten organisaatioiden riskienhallinnan tasoa ja prosesseja ennen SaaS-järjestelmän käyttöönottopäätöstä.

Tutkimuksen tulokset osoittavat, että Suomessa toimivissa suurissa organisaatioissa havaitaan useita erilaisia riskejä, jotka vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen. Tuloksena nousi keskeisiä riskejä jokaisen tässä tutkimuksessa muodostetun laajennetun havaittujen riskien -viitekehyksen riskikategorian alle. Riskit painottuivat strategisten, taloudellisten sekä tietoturva- ja tietosuojariskien kategorioihin, sillä haastateltavat korostivat erityisesti näiden riskien keskeisyyttä vastauksissaan. Riskienhallinnan osalta tulokset osoittivat, että riskienhallinnalla on vaikutus SaaS-järjestelmän käyttöönottopäätökseen Suomessa toimivissa suurissa organisaatioissa. Riskienhallintaan liittyi useita erilaisia toimenpiteitä, joilla organisaatiot pyrkivät vaikuttamaan havaittujen riskien realisoitumiseen jo ennen SaaS-järjestelmän käyttöönottopäätöstä. Nämä toimenpiteet pystyttiin tutkimuksen tulosten perusteella kiteyttämään viiteen riskienhallinnan kategoriaan. Vaikka organisaatioissa riskienhallintaa toteutetaan laajasti ja haastateltavien mukaan pääasiassa riittävästi suhteessa riskienhallinnan kustannuksiin, kaikkiin riskeihin ei pystytä varautumaan etukäteen. Tämän takia resilienssin kasvattaminen ja ketteryyden kulttuurin edistäminen koetaan tärkeäksi riskienhallinnan ja liiketoiminnan jatkuvuuden näkökulmasta SaaS-järjestelmien käyttöönottopäätösten kontekstissa.

Avainsanat: SaaS, käyttöönottopäätös, havaitut riskit, riskienhallinta, riskisuunnitelmat, pilvipalvelut, käyttöönotto, tietojärjestelmät

SISÄLLYS

1 Johdanto 8

1.1 Tausta ja motivointi 8

1.2 Tutkimuksen tavoite ja rajaukset 9

1.3 Tutkielman rakenne 9

2 Pilvipalvelut ja SaaS-järjestelmät 11

2.1 Pilvipalvelut 11

2.1.1 Pilvipalvelun määritelmä 11

2.1.2 Pilvipalvelumallit 12

2.1.3 Pilvipalveluiden keskeiset piirteet ja pilvipalveluiden käyttö 13

2.1.4 Pilvipalveluiden käyttöönottomallit 15

2.2 SaaS yleisesti 17

2.3 SaaS-järjestelmän käyttöönottoon vaikuttavat tekijät 18

2.3.1 Teknologiset tekijät 18

2.3.2 Organisatoriset tekijät 19

2.3.3 Liiketoimintaympäristölliset tekijät 20

3 SaaS-järjestelmän käyttöönoton riskit 22

3.1 Päätöksentekoprosessi ja riskit käyttöönotossa 22

3.2 Laajennettu havaittujen riskien -viitekehys SaaS-järjestelmän käyttöönottopäätöksessä 24

3.2.1 Viitekehyksen muokkaaminen 24

3.2.2 Suorituskykyriskit 25

3.2.3 Tietoturva- ja tietosuojariskit 26

3.2.4 Strategiset riskit 28

3.2.5 Taloudelliset riskit 28

3.2.6 Psykososiaaliset riskit 30

3.2.7 Projektiriskit 31

3.3 Riskienhallinta 31

4 Metodologia 34

4.1 Tutkimuksen viitekehys 34

4.2 Aineiston kerääminen ja analysointi 35

4.3 Tutkimuksen laadukkuus, luotettavuus ja eettisyys 40

5 Tutkimuksen tulokset 43

5.1 Suorituskykyriskit 43

5.1.1 Käytön skaalautuvuus 43

5.1.2 Palvelun saatavuus ja käytettävyys 44

5.1.3 Järjestelmien integraatio 46

5.2 Tietoturva- ja tietosuojariskit 46

5.2.1 Datan ylläpito ja saavutettavuus 46

5.2.2 Globaali toimintaympäristö 47

5.2.3 Tietosuojaloukkaukset 48

5.2.4 Tietovuoto 49

5.3 Strategiset riskit 50

5.3.1 Liiketoiminnan ketteryys ja kehitys 50

5.3.2 Strateginen dissonanssi 51

5.3.3 Strateginen toimittajaloukku 52

5.3.4 Osaamisen menettäminen 53

5.3.5 Liiketoiminnan jatkuvuus 54

5.4 Taloudelliset riskit 56

5.4.1 Hyötyjen realisointi 56

5.4.2 Piilotetut kustannukset 57

5.4.3 Taloudellinen toimittajaloukku 59

5.5 Psykososiaaliset riskit 59

5.6 Projektiriskit 61

5.7 Riskienhallinta ennen SaaS-järjestelmän käyttöönottopäätöstä 62

5.7.1 Organisaation tarpeen ja vaatimusten määrittely 62

5.7.2 Palvelun vastaavuus ja kyvykkyyskartoitus 63

5.7.3 Sopimustekniset asiat 66

5.7.4 Hankeosaaminen ja resursointi 69

5.7.5 Resilienssi ja liiketoiminnan jatkuvuus 71

6 Johtopäätökset 74

6.1 Keskeiset SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat havaitut riskit Suomessa toimivissa suurissa organisaatioissa 74

6.2 SaaS-järjestelmän käyttöönottopäätöstä edeltävä riskienhallinta 81

7 Yhteenveto 85

7.1 Tutkimuksen yhteenveto 85

7.2 Tutkimuksen kontribuutio 87

7.3 Rajoitukset ja jatkotutkimuskohteet 88

Lähteet 90

Liitteet 99

Liite 1. Haastattelurunko 99

Liite 2. Analyysitaulukko SaaS-järjestelmän käyttöönottopäätökseen vaikuttavista havaituista riskeistä 102

Liite 3. Analyysitaulukko käyttöönottopäätöstä edeltävästä riskienhallinnasta 107

Liite 4. Aineistonhallintasuunnitelma 111

KUVIOT

Kuvio 1 Pilvipalvelumallin määritelmä ja pilvipalveluinfrastruktuuri (mukaellen (M. Ali ym., 2015; Marston ym., 2011)) 12

Kuvio 2 SaaS-järjestelmän käyttöönottoon vaikuttavia keskeisiä tekijöitä TOE-viitekehyksen mukaisesti 18

Kuvio 3 Riskitietoisen päätöksenteon perusrakenne (suomennettu (Aven, 2012, s. 114)) 22

Kuvio 4 Riskinkäsittelyn prosessi (mukaellen (Firoiu, 2015; Wheeler, 2011, s. 53–54)) 32

Kuvio 5 Tutkimuksen viitekehys (mukaellen (Benlian & Hess, 2011)) 34

Kuvio 6 SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat havaitut riskit 74

TAULUKOT

Taulukko 1 Tiedot haastateltavista 36

Taulukko 2 Tiedot organisaatioista 37

Taulukko 3 SaaS-järjestelmän käyttöönottopäätöstä edeltävä riskienhallinta 82

1 Johdanto

1.1 Tausta ja motivointi

Pilvipalvelut (engl. Cloud Computing) ovat tuoneet perustavanlaatuisen muutoksen informaatioteknologiapalveluiden tuottamiseen, kehittämiseen, ylläpitämiseen, skaalaamiseen, käyttöönottoon sekä maksamiseen (Avram, 2014). Nykyaikana organisaatioiden tietojenkäsittely muodostaa paradoksin, jossa yhtäältä tietokoneet ovat eksponentiaalisesti tehokkaampia ja laskentatehon yksikkökustannukset pienempiä, mutta toisaalta informaatioteknologian ollessa yhä keskeisempi osa organisaatioiden toimintaa, laajan IT-infrastruktuurin hallinnan monimutkaisuus tekee tietojenkäsittelystä kalliimpaa kuin koskaan aikaisemmin (Marston ym., 2011). Pilvipalvelut pyrkivätkin tuomaan organisaatioille ratkaisun tähän paradoksiin (Marston ym., 2011).

Verkon yli toimitetut pilvipohjaiset ohjelmistopalvelut (engl. Software as a Service, SaaS) ovat saavuttaneet huomattavaa kiinnostusta niin organisaatioiden johdossa kuin tutkimuskentälläkin (Chou & Chiang, 2013; Shuraida & Titah, 2023). Maailmanlaajuisesti SaaS-järjestelmämarkkinaan liitetyn liikevaihdon ennustetaan kasvavan 19,28 % yhdistetyssä vuotuisessa kasvuvauhdissa (engl. compound annual growth rate, CAGR) mitattuna vuoden 2024–2029 välillä. SaaS-järjestelmämarkkinan ennustetaankin nousevan noin 820 miljardiin Yhdysvaltain dollariin vuonna 2029. (Statista, 2024.)

SaaS voi tuoda organisaatioille monenlaisia hyötyjä niin strategisesta kuin toiminnallisestakin näkökulmasta katsottuna (Benlian & Hess, 2011). Näihin lukeutuvat muun muassa kustannussäästöt, joustavuus, organisaation järjestelmiin kohdistuvien IT-resurssien tarpeen väheneminen sekä suurten alkuinvestointien poistaminen (Benlian & Hess, 2011). Tietohallintoon keskittyvä kirjallisuus mainitseekin usein SaaS-järjestelmät johtavana pilvipalvelumuotona (Wu ym., 2011). SaaS-järjestelmien monenlaiset hyödyt tekevät niistä keskeisiä kilpailijoita perinteisille organisaation omissa tiloissa toteutettaville järjestelmille, eli on-premise -järjestelmille (Shapouri ym., 2024).

SaaS-järjestelmien monien hyötyjen lisäksi, niiden käyttöönotto ja hankinta tuovat mukanaan myös monenlaisia riskejä, minkä takia organisaatioiden tuleekin pyrkiä tunnistamaan ja arvioimaan näitä pilvipohjaisten järjestelmien tuomia riskejä liiketoiminnan näkökulmasta (A. Ali ym., 2017; Schneider & Sunyaev, 2016). Kirjallisuudessa on lisäksi tunnistettu pilvipalveluiden hankintapäätöksiin liittyvän empiirisen tiedon olevan niukkaa (Schneider & Sunyaev, 2016), mihin tässä tutkimuksessa pyritään tuomaan lisätietoa erityisesti riskien ja riskienhallintasuunnitelmien kautta.

Lisäksi aikaisempi kirjallisuus tunnistaa vakiintuneiden viitekehysten käytön vähäisyyden pilvipalveluihin, kuten SaaS:iin, liittyvässä tutkimuksessa (Senyo ym., 2018). Tämä tutkimus pyrkii lisäämään vakiintuneiden viitekehysten käyttöä havaittujen riskien -viitekehyksen avulla. Lisäksi aikaisemmat SaaS-järjestelmien käyttöönottopäätöksiin liittyvät tutkimukset ovat tunnistaneet erilaisia hyötyjä ja riskejä SaaS-järjestelmiin liittyen (Benlian & Hess, 2011; Shuraida & Titah, 2023), mutta riskejä ja organisaatioiden riskienhallintasuunnitelmia kohdistuen SaaS-järjestelmien havaittuihin riskeihin ennen käyttöönottopäätöstä ei ole samassa määrin tutkittu.

1.2 Tutkimuksen tavoite ja rajaukset

Tämän tutkimuksen tavoitteena on kartoittaa Suomessa toimivien suurten organisaatioiden havaitsemia keskeisiä riskejä, jotka vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen. Lisäksi tässä tutkimuksessa pyritään tuomaan uutta näkökulmaa tutkimalla SaaS-järjestelmän käyttöönottopäätöstä edeltävää riskienhallintaa havaittuihin riskeihin liittyen sekä tarkastelemalla riskienhallintasuunnitelmien suhdetta käyttöönottoon.

Tutkimuksen tutkimuskysymyksinä ovat seuraavat:

- Mitkä ovat keskeisiä riskejä, jotka vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen Suomessa toimivissa suurissa organisaatioissa?
- Millaista SaaS-järjestelmän havaittuihin riskeihin liittyvää riskienhallintaa organisaatioissa tehdään ennen käyttöönottopäätöstä?

Tässä tutkimuksessa keskitytään erityisesti organisaatioiden SaaS-järjestelmiin liittyviin riskeihin, jolloin SaaS-järjestelmien hyödyt eivät ole tämän tutkimuksen keskiössä. Tutkimus toteutetaan Suomessa ja kohdistetaan Suomessa toimiviin suuriin yksityisiin sekä julkisiin organisaatioihin. Tämä tutkimus ei rajaudu tiettyyn organisaatioon, vaan tarkoituksena on saada mahdollisimman monipuolinen otos, jotta SaaS-järjestelmän käyttöönottopäätökseen vaikuttavia riskejä ja käyttöönottopäätöstä edeltävää riskienhallintaa voidaan analysoida monipuolisesti.

1.3 Tutkielman rakenne

Tutkielman luvun 2 alussa käydään kirjallisuuskatsauksen muodossa yleisesti läpi eri pilvipalvelumallit sekä -infrastruktuuri, minkä jälkeen luvussa 2.2 keskitytään erityisesti tämän tutkimuksen keskiössä olevaan pilvipalvelumalliin, eli SaaS:iin. Luvussa 2.3 havainnollistetaan SaaS-järjestelmien käyttöönottoon vaikuttavia tekijöitä TOE-viitekehyksen eri osa-aluilla.

Luvussa 3 paneudutaan SaaS-järjestelmiin liittyviin riskeihin. Luvun alussa käydään läpi SaaS-järjestelmien riskeihin ja riskiä sisältävään päätöksentekoon liittyvää kirjallisuutta, minkä jälkeen luvussa 3.2 perehdytään tässä tutkimuksessa käytettävään laajennettuun havaittujen riskien -viitekehykseen SaaS-järjestelmien kontekstissa. Luvussa 3.3 tuodaan esiin riskienhallintaan liittyvää kirjallisuutta SaaS-järjestelmiin ja pilvipalveluihin liittyen.

Luvussa 4 käydään läpi tutkimuksen metodologiaa sekä esitellään tutkimuksen viitekehys ja tutkimusaineisto. Luku 4 sisältää tämän lisäksi tiedot metodeista, luotettavuudesta, tietoturvasta sekä eettisyydestä. Luku 5 keskittyy tutkimuksen tulosten esittämiseen, minkä jälkeen luvussa 6 kerrotaan tuloksista tehdyt johtopäätökset vertailemalla tuloksia aikaisempaan kirjallisuuteen. Luku 7 toimii tutkimuksen yhteenvetona ja sisältää lisäksi tutkimuksen rajoitukset sekä ehdotuksia jatkotutkimuskohteille.

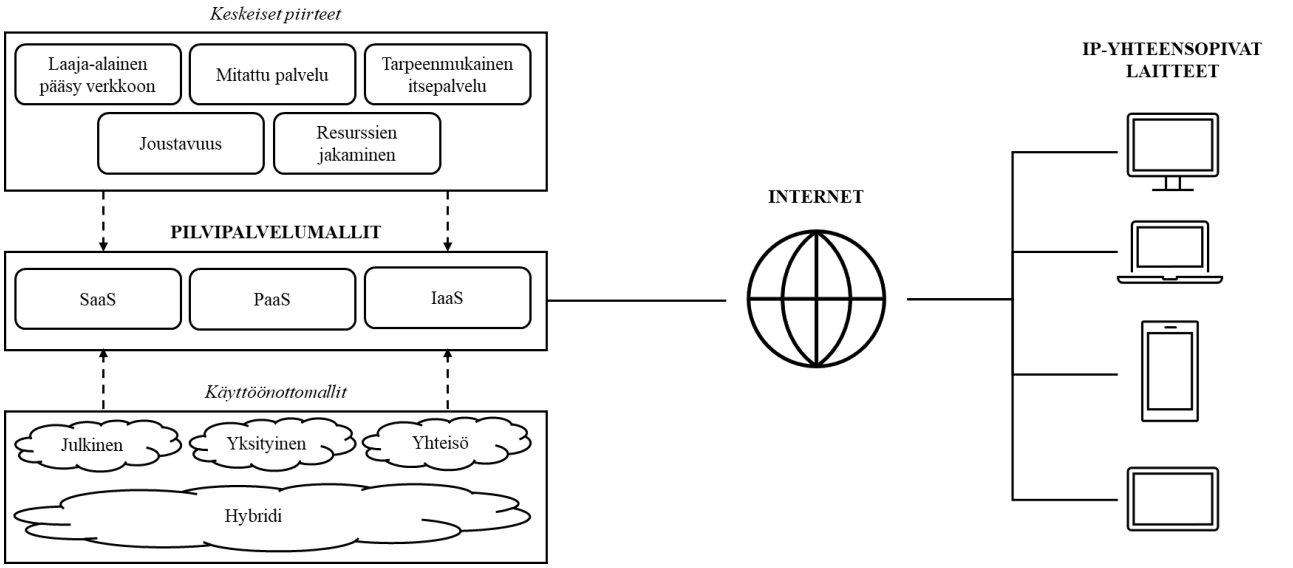
2 Pilvipalvelut ja SaaS-järjestelmät

2.1 Pilvipalvelut

2.1.1 Pilvipalvelun määritelmä

Pilvipalveluille (engl. Cloud Computing) on olemassa monia hieman toisistaan eriäviä määritelmiä (Gartner, 2024 -a; Marston ym., 2011; Mell & Grance, 2011), eikä mikään niistä onnistu yksinään huomioimaan kaikkia keskeisiä pilvipalveluiden piirteitä (Marston ym., 2011). Yhdysvaltain kansallisen standardien ja teknologioiden instituutin (engl. National Institute of Starndards and Technology, NIST) yli 800 sanan pituisen määritelmän mukaan pilvipalvelu on malli, joka mahdollistaa kätevän ja tarpeenmukaisen pääsyn jaettujen konfiguroitavien tietoresurssien verkkoon. Tämä verkko on jalkautettavissa nopeasti ja tehokkaasti, minkä takia mallissa korostuu erityisesti palveluiden saatavuus. (Mell & Grance, 2011.) Gartnerin määritelmän mukaan pilvipalvelu on tietojenkäsittelymalli, jossa skaalautuvia sekä joustavia IT-resursseja toimitetaan palveluna internetin välityksellä (Gartner, 2024 -a).

Marston ym. (2011) pyrkivät määritelmässään tuomaan esiin pilvipalveluiden pääasiallisia hyötyjä liiketoiminnan näkökulmasta sekä esittelemään pilvipalveluiden keskeisimpiä teknologisia erityispiirteitä. Marstonin ym. (2011) määritelmässä painotetaan pilvipalveluiden yhdistävän kahta keskeistä informaatioteknologian trendiä, jotka ovat tehokkuus ja ketteryys. Määritelmässä pilvipalveluiden kuvataan olevan luonteeltaan itsepalvelullisia. Pilvipalveluna tarjottavat resurssit ovat myös jaettuja, dynaamisesti skaalautuvia sekä virtualisoituja, minkä lisäksi palvelusta maksetaan yleisesti käyttökustannuksena, jolloin alkuinvestointien määrä on minimaalinen. (Marston ym., 2011.)



Kuvio 1 Pilvipalvelumallin määritelmä ja pilvipalveluinfrastruktuuri (mukaellen (M. Ali ym., 2015; Marston ym., 2011))

Kuviossa 1 on yhdistetty Alin ym. (2015) pilvipalvelumallin kuvaaja sekä Marstonin ym. (2011) pilvipalveluinfrastruktuurin kuvaaja. Kuvion 1 sisältöä avataan tarkemmin seuraavissa alaluvuissa 2.1.2–2.1.4.

2.1.2 Pilvipalvelumallit

Kuvion 1 vasemmasta laidasta havaitaan, että pilvipalvelumallit voidaan jakaa kolmeen eri kategoriaan, joissa verkon välityksellä tarjotaan joko IT-infrastruktuuria (engl. Infrastructure as a Service, IaaS), alustoja (engl. Platform as a Service, PaaS) tai ohjelmistoja (engl. Software as a Service, SaaS) (M. Ali ym., 2015; Bibi ym., 2012; Kim ym., 2017; Zissis & Lekkas, 2012). IaaS-mallissa organisaatiot voivat ulkoistaa IT-infrastruktuurin, kuten tallennustilan tai laskentatehon. PaaS-mallissa organisaatioiden on puolestaan mahdollista ulkoistaa IT-alustoja, kuten tietokannat tai liiketoimintatiedon hallintajärjestelmän. SaaS-mallissa organisaatiot voivat ulkoistaa erilaisia yleisiä ohjelmistoja, kuten sähköpostin tai toimisto-ohjelmistopaketin, sekä tarkemmin liiketoimintaan tarkoitettuja ohjelmistoja, kuten toiminnanohjausjärjestelmän tai asiakkuudenhallintajärjestelmän. (Yang ym., 2015; Zissis & Lekkas, 2012.) Näistä kolmesta SaaS:ia voidaan pitää lupaavimpana, sillä se tarjoaa asiakasorganisaatioille monenlaisia konkreettisia hyötyjä (Yang ym., 2015). Tässä tutkielmassa keskitytään erityisesti ohjelmistoihin palveluina eli SaaS:iin.

Kirjallisuudesta sekä liiketoimintakentältä voidaan havaita, että palvelullistamisesta on tullut keskeinen osa monien perinteisesti tuotteita valmistavien ja myyvien yritysten strategiaa ja toimintaa (Khanra ym., 2021; Nudurupati ym., 2016). Lähes kaikkea voidaan nykyään palvelullistaa lisäarvon

saavuttamiseksi, minkä takia kirjallisuudessa puhutaan myös XaaS:sta (engl. anything/everything as a service, XaaS), joka viittaa ”kaikki palveluna” -malliin. Termi XaaS ei ole kaikessa kirjallisuudessa sidottu pelkästään pilvipalveluihin, sillä kirjain X voidaan korvata termillä, joka kuvaa tarjottavaa palvelua erilaisilla toimialoilla. (Singh ym., 2022; Taleb ym., 2016.) Näihin voivat kuulua esimerkiksi joustavuus, mukavuus tai vaihdanta palveluna (Singh ym., 2022). XaaS ei ole esillä monissa pilvipalveluiden määritelmissä SaaS:n, PaaS:n ja IaaS:n rinnalla, eikä se liity pelkkiin pilvipalveluihin. Tässä tutkielmassa XaaS:ia ei tutkita tarkemmin, mutta palvelullistaminen tunnistetaan kuitenkin keskeiseksi teemaksi tutkimus- sekä liiketoimintakentällä.

2.1.3 Pilvipalveluiden keskeiset piirteet ja pilvipalveluiden käyttö

Kuvion 1 vasemmassa laidassa oleviin pilvipalvelumalleihin on yhdistetty katkoviivallisin nuolin pilvipalvelumallien keskeiset piirteet ja käyttöönottomallit NIST-määritelmää (Mell & Grance, 2011) sekä Alin ym. (2015) kuviota mukaillen. Pilvipalvelumallien keskeiset piirteet voidaan jakaa viiteen eri kategoriaan. Ensimmäisenä keskeisenä pilvipalvelumallien piirteenä voidaan pitää laaja-alaista pääsyä verkkoon (M. Ali ym., 2015; Mell & Grance, 2011). Tällä tarkoitetaan sitä, että pilvipalveluiden toiminnot ovat saavutettavissa standardimekanismein kevyillä asiakaspäätteillä (engl. Thin Client) sekä raskailla asiakaspäätteillä (engl. Thick Client) (Mell & Grance, 2011). Käyttäjä muodostaa yhteyden pilvipalvelimeen IP-verkkoprotokollaa tukevalla laitteella, kuten kannettavalla tietokoneella, pöytäkoneella tai älypuhelimella, minkä jälkeen hän pystyy käyttämään pilvessä olevia ohjelmistoja, infrastruktuuria tai alustoja (Marston ym., 2011). Tämä pilvipalveluiden käyttöprosessi on havainnollistettu kuviossa 1.

Toisena pilvipalvelun keskeisenä piirteenä voidaan pitää mitattua palvelua. Tällä tarkoitetaan sitä, että pilvipalveluiden käyttöä voidaan seurata mittaamalla esimerkiksi aktiivisten käyttäjien määrää, tallennustilan käyttöä tai prosessointitehoa. Tämä mahdollistaa resurssien seurannan ja raportoinnin, mikä lisää läpinäkyvyyttä niin asiakkaan, kuin palveluntarjoajankin näkökulmasta (Mell & Grance, 2011). Mitatun palvelun hyvänä puolena voidaan pitää myös sen mahdollistamaa automaattista resurssien optimointia, sillä käyttäjiä laskutetaan käyttökohtaisesti (M. Ali ym., 2015). Käyttökohtainen laskutus vähentää myös merkittävästi järjestelmiin tarvittavia alkupääomakustannuksia (Benlian & Hess, 2011; Marston ym., 2011).

Asiakasorganisaation IT-infrastruktuurin hallinta ja suunnittelu, joiden avulla pyritään ennustamaan tarvittavien IT-resurssien määrää sekä saavuttamaan stabiili ja kontrolloitu infrastruktuuri palvelutason laadun varmistamiseksi, siirtyy SaaS:n kontekstissa pääasiassa pilvipalveluntarjoajalle (Candeia ym., 2015). Pilvipalvelut ovat tehneet IT-infrastruktuurin kapasiteetin ennustamisesta ja

suunnittelusta haastavaa (Candeia ym., 2015; Furman & Diamant, 2025). Palveluntarjoajien näkökulmasta SaaS-järjestelmän käyttöä on usein vaikea ennustaa pitkällä aikavälillä, sillä yksittäisten käyttäjien todellista käyttömäärää on hankala arvioida etukäteen. Käyttäjät voivat tämän lisäksi lopettaa palvelun käytön joustavasti lähes milloin tahansa. (Candeia ym., 2015.)

SaaS-järjestelmiä tarjoavat yritykset voivat oman IT-infrastruktuurin omistamisen sijasta hankkia järjestelmään tarvittavan IT-infrastruktuurin palveluna toiselta palveluntarjoajalta. IaaS-ratkaisuja tarjoavat yritykset myyvät useimmiten useampia erilaisia instansseja, joissa käyttömuistin, tallennustilan ja laskentatehon määrät vaihtelevat. Virtuaalisia instansseja tarjotaan usein myös erilaisilla maksumalleilla sekä erilaisilla lupauksilla palvelutason laadun varmistamisesta. Yhdessä yleisessä tavassa infrastruktuuria voi hankkia pilvestä käyttöperusteisesti haluamallaan hetkellä maksamalla esimerkiksi tuntimaksua. Tässä tapauksessa IaaS-tarjoaja ei kuitenkaan takaa halutun infrastruktuurin tason, kuten laskentatehon, olevan vapaana kyseisenä hetkenä, mikä voi johtaa alikapasiteettiin. Toisena vaihtoehtona on usein varausperusteinen malli, jossa IaaS-tarjoaja takaa halutun infrastruktuuritason olevan vapaana silloin, kun asiakas sitä tarvitsee. Tässä tapauksessa IT-infrastruktuurin varauksesta peritään varausmaksua, minkä lisäksi myös todellisesta käytöstä maksetaan hieman alhaisempaa käyttömaksua, kuten alennettua tuntimaksua. (Candeia ym., 2015.)

Yritykset voivat myös itse hankkia oman fyysisen IT-infrastruktuurinsa, mutta tällöin infrastruktuurin kokoa ei ole yhtä joustavaa, eikä välttämättä myöskään yhtä kustannustehokasta, muuttaa kapasiteettitarpeen muuttuessa. Liian suuren infrastruktuurin omaaminen ei ole taloudellisesta eikä myöskään ympäristöllisestä näkökulmasta katsottuna optimaalista, mutta myös liian pienikokoinen IT-infrastruktuuri aiheuttaa vaikeuksia (Furman & Diamant, 2025). SaaS-palveluntarjoajan liian pieni IT-infrastruktuurin kapasiteetti saattaa johtaa palvelutasosopimuksien (engl. Service Level Agreement, SLA) rikkomuksiin, mikä voi puolestaan johtaa sakkoihin ja huonoon maineeseen (Candeia ym., 2015). Jopa 40 % pilvipalveluita tarjoavista yrityksistä maksaa käyttöasteeseen verrattuna tarpeettoman suuresta IT-infrastruktuurista, mikä johtaa ylimääräisiin kustannuksiin ja ympäristöä kuormittaviin ratkaisuihin muun muassa turhan energiakulutuksen myötä. On todettu, että pilvipalveluntarjoajien grafiikkaprosessorien (engl. Graphics Processing Unit, GPU) keskimääräinen käyttöaste on ainoastaan noin 5 % kokonaiskapasiteetista, mikä muiden kapasiteettihuolien ohella kasvattaa tarvetta tehokkaampaan IT-infrastruktuurin hallintaan ja suunnitteluun pilvipalveluiden kontekstissa. (Furman & Diamant, 2025.)

Kolmantena keskeisenä pilvipalveluiden piirteenä on, että ne toimivat tarpeenmukaisina itsepalvelumalleina. Käyttäjät voivat tarvittaessa pyytää enemmän tai laajempia käyttöoikeuksia sekä

hallita olemassa olevia palveluita pilvessä ilman ihmistenvälistä vuorovaikutusta. Neljäntenä keskeisenä piirteenä on se, että pilvipalvelumallit ovat käytön suhteen joustavia ja mahdollistavat nopean skaalautuvuuden asiakkaan muuttuvien tarpeiden mukaan ajankohdasta riippumatta (Ali ym., 2015; P. Mell & Grance, 2011.) Pilvipalvelumallilla on täten mahdollista saavuttaa taloudellista joustavuutta, prosessijoustavuutta, toiminnallista joustavuutta sekä markkinajoustavuutta, joihin kaikkiin liittyy potentiaalisia hyötyjä organisaatioille (Lal & Bharadwaj, 2016).

Viidentenä pilvipalveluiden erityispiirteenä voidaan pitää resurssien jakamista moniasiakasarkkitehtuurin (engl. multi-tenant architecture) avulla. Moniasiakasarkkitehtuurissa palveluntarjoajan resurssit, kuten tallennustila tai prosessointiteho, jaetaan asiakkaille omina instansseinaan, jotka ovat erillään toisten asiakkaiden käytössä olevista resursseista (M. Ali ym., 2015; Mell & Grance, 2011). Kirjallisuudessa on jonkin verran eriäväisyyttä siitä, miten läpinäkyvästi asiakkaat pystyvät määrittämään ja valitsemaan palveluntarjoajan jakamien resurssien sijainnin. Alin ym. (2015) mukaan asiakkailla on näkyvyys resurssien sijaintiin, kun taas Mell ja Grance (2011) kirjoittavat NIST-määritelmässä, että asiakkailla ei ole kontrollia tai tietoa resurssien tarkasta sijainnista, mutta he pystyvät mahdollisesti selvittämään resurssien korkean tason sijainnin esimerkiksi maan, maakunnan tai datakeskuksen tasolla.

Palveluntarjoajan resurssien sijaintiriippumattomuus noudattaa vihreän IT:n periaatteita siinä mielessä, että resursseja voidaan käyttää tehokkaammin ja ne voidaan sijoittaa paikkoihin, joissa on tarjolla halpaa sähköä (Marston ym., 2011). Pilvipalvelut tarjoavat paremman mahdollisuuden vihreän IT:n mukaiseen toimintaan verrattaessa on-premise -järjestelmiin, sillä pilvipalveluiden resurssien ei tarvitse sijaita asiakasorganisaation omissa tiloissa, vaikka niitä siellä käytettäisiinkin. Kirjallisuudessa puhutaan enenevin määrin myös vihreästä pilvestä (engl. green cloud). Tätä termiä käytettäessä korostetaan pilvipalveluiden suotuisia ympäristövaikutuksia. Pilvipalvelut tuovat parhaimmillaan huomattavia energiasäästöjä niin asiakasorganisaatioille, kuin palveluntarjoajillekin. Entistä ympäristötietoisemmassa ja säännellymmässä maailmassa pilvipalveluntarjoajan vihreys saattaa nousta olennaiseksi osaksi palveluntarjoajan valintaa. (Park ym., 2023.)

2.1.4 Pilvipalveluiden käyttöönottomallit

Pilvipalvelut voivat toimia joko yksityisessä pilvessä (engl. private cloud), julkisessa pilvessä (engl. public cloud), yhteisön pilvessä (engl. community cloud) tai hybridipilvessä (engl. hybrid cloud). Yksityisessä pilvessä pilvipalvelun infrastruktuuri on ainoastaan yhden organisaation käytössä, eikä se täten ole laajemman yleisön saavutettavissa (M. Ali ym., 2015; Mell & Grance, 2011; Schneider & Sunyaev, 2016). Yksityistä pilveä hallinnoi joko asiakasyritys itse, kolmas osapuoli tai yhdistelmä

näitä molempia (M. Ali ym., 2015; Mell & Grance, 2011). Yksityinen pilvi saattaa sijaita yrityksen omissa tiloissa tai sen ulkopuolella (M. Ali ym., 2015; Mell & Grance, 2011). Vaikka yksityinen pilvi tarjoaa julkiseen pilveen nähden vähemmän hyötyjä esimerkiksi skaalautuvuudessa tai taloudellisuudessa tarkasteltuna, yksityinen pilvi on usein helpompi yhdistää organisaation tietoturva- ja sääntelyvaatimuksiin (Schneider & Sunyaev, 2016). Yksityinen pilvi soveltuu erityisesti suurille organisaatioille (P. Gupta ym., 2013)

Pilvipalvelun käyttöönottomallin ollessa julkinen pilvi, on pilvipalvelu tällöin suuremman yleisön saavutettavissa ja käytössä (M. Ali ym., 2015; Mell & Grance, 2011; Schneider & Sunyaev, 2016). Julkisessa pilvessä palveluntarjoajan resurssit ovat jaettu asiakkaiden kesken (M. Ali ym., 2015). Infrastruktuuri sijaitsee palveluntarjoajan tiloissa ja sen omistaa palvelua tarjoava julkinen tai yksityinen toimija sekä mahdollisesti myös näiden yhdistelmä (Mell & Grance, 2011). Julkisen pilven omistajia voivat olla esimerkiksi yritykset tai valtio (Mell & Grance, 2011). Vaikka kyseinen malli tarjoaa enemmän taloudellisia hyötyjä yksityiseen pilveen verrattuna, julkiseen pilveen liitetyistä tietoturvariskeistä on tullut keskeinen puheenaihe tutkimuskentällä (Schneider & Sunyaev, 2016). Julkinen pilvi tarjoaa kustannustehokkaan ratkaisun muun muassa pienille ja keskisuurille yrityksille ottaa käyttöön IT-ratkaisuja, kuten esimerkiksi Googlen tarjoamat sovellukset (P. Gupta ym., 2013).

Yhteisön pilvessä pilvi-infrastruktuuri palvelee tiettyä asiakasryhmää, joka koostuu sellaisista organisaatioista, joilla on yhteisiä tavoitteita tai tarpeita (P. Gupta ym., 2013; Marston ym., 2011), kuten missio, tietoturvavaatimukset tai yrityspolitiikka (Marston ym., 2011). Tässä tapauksessa pilven omistaa ja sitä hallinnoi yksi tai useampi yhteisössä oleva organisaatio, kolmas osapuoli tai jokin edellä mainittujen yhdistelmä. Yhteisön pilvi voi sijaita organisaation tiloissa tai sen ulkopuolella. (M. Ali ym., 2015; Mell & Grance, 2011.)

Neljäntenä käyttöönottomallina on hybridipilvi, jossa pilvi-infrastruktuuri on yhdistelmä useampaa edellä mainittua käyttöönottomallia (P. Gupta ym., 2013; Marston ym., 2011; Mell & Grance, 2011). Eri pilvet toimivat omina entiteetteinään, mutta ovat yhdistettyinä toisiinsa teknologioin, jotka mahdollistavat datan ja sovellusten siirrettävyyden (Mell & Grance, 2011). Hybridipilvissä organisaation ei-kriittinen informaatio on ulkoistettu julkiseen pilveen, mutta kriittinen tieto pysyy edelleen organisaation omassa kontrollissa (Marston ym., 2011). Julkisen pilven ja yksityisen pilven yhdistelmällä pyritään yhdistämään molempien käyttöönottomallien parhaat puolet hyötyjen saavuttamiseksi (Schneider & Sunyaev, 2016).

2.2 SaaS yleisesti

Pilvipalveluiden uskotaan saaneen alkunsa SaaS-järjestelmistä (Senyo ym., 2018). Kirjallisuudessa SaaS:sta on tehty useita erilaisia määritelmiä, jotka kuvaavat kyseistä pilvipalvelumallia hieman eri näkökulmista. NIST-määritelmän mukaan SaaS on pilvipalvelumalli, jossa ohjelmia tarjotaan palveluna loppukäyttäjille verkon välityksellä (Mell & Grance, 2011). SaaS-mallissa on olennaista, että ohjelmaa ylläpidetään ja hallitaan asiakasorganisaation ulkopuolella (Cho & Chan, 2015). SaaS:in pääasiallisena ajatuksena on poistaa käytäntö, jossa sovellukset sijaitsevat paikallisesti käyttäjien omilla laitteilla, sillä yksittäisten laitteiden laskentatehoa ei voida hyödyntää korkean suorituskyvyn tarjoamiseksi koko käyttäjäkunnalle (Senyo ym., 2018).

Gartnerin määritelmän mukaan SaaS on ohjelmisto, jonka omistaa, toimittaa ja ylläpitää yksi tai useampi palveluntarjoaja etäyhteyttä hyödyntäen. Palveluntarjoaja toimittaa ohjelmiston, joka perustuu yhteen yhteiseen koodi- ja tietomääritelmään, ja jota kaikki sopimusasiakkaat käyttävät milloin ja missä tahansa yksi-moneen -mallin mukaisesti. Käytöstä maksetaan joko käyttömaksuna tai käyttömetriikkaan perustuvana tilauksena. (Gartner, 2024.) Tämän lisäksi SaaS-järjestelmät ovat useimmiten palveluorientoituneita, jolloin palveluntarjoajat pyrkivät tehostamaan SaaS-ohjelmistojen integroitavuutta toistensa kanssa (S. Yau & An, 2011).

SaaS sisältää monenlaisia eri ohjelmistotyyppejä yksinkertaisista toimisto-ohjelmistoista suurempiin ja monimutkaisempiin ohjelmistoihin, kuten toiminnanohjausjärjestelmiin ja asiakkuudenhallintajärjestelmiin (Loukis ym., 2019). SaaS voidaan nähdä sovelluspalveluiden tarjontamallin evoluutiona, sillä SaaS antaa pilvipalveluntarjoajille mahdollisuuden tarjota pääsy useaan ohjelmistoon samanaikaisesti moniasiakasarkkitehtuurissa (Benlian & Hess, 2011). SaaS on tunnistettu tietojärjestelmätieteen kirjallisuudessa teknologiaksi, jolla on mahdollista saavuttaa sekä toiminnallisia, että taloudellisia hyötyjä (Subashini & Kavitha, 2011), minkä lisäksi SaaS on nousemassa johtavaksi palvelumalliksi ohjelmistopalveluiden tarjonnassa (Statista, 2024; Subashini & Kavitha, 2011).

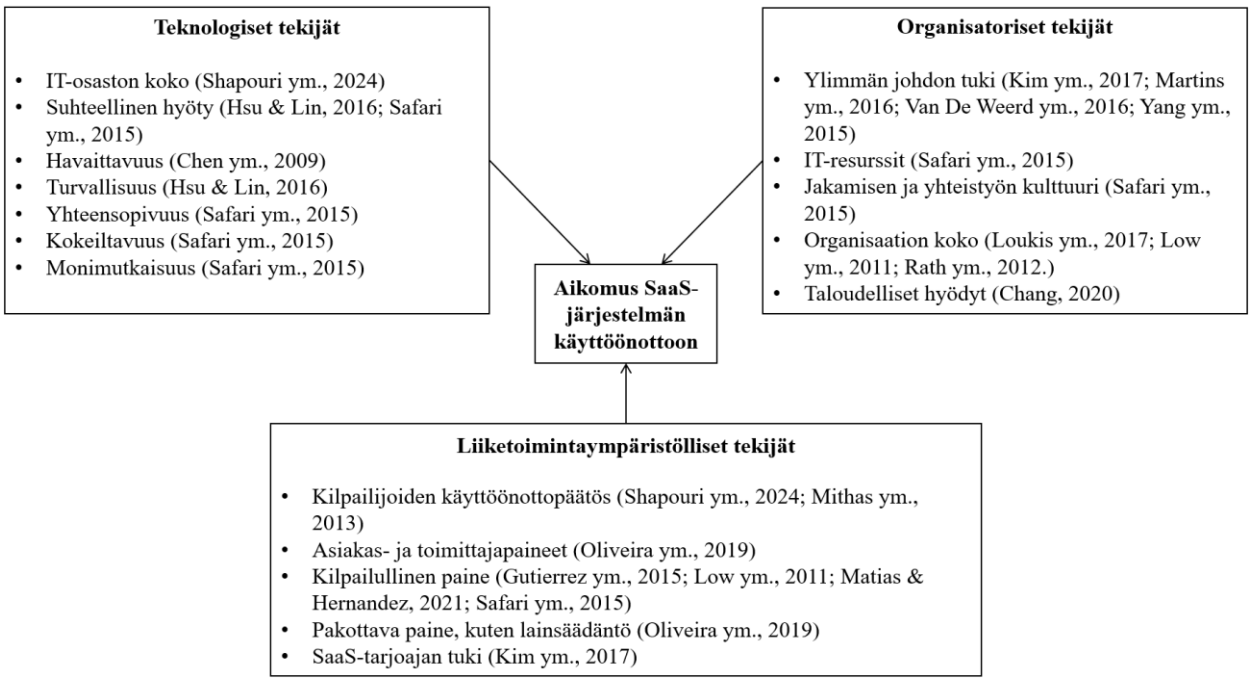
Tietojärjestelmätieteen kirjallisuudessa on tunnistettu useita hyötyjä SaaS-järjestelmiin liittyen. SaaS-järjestelmien yksi olennainen hyöty on niistä saatavat taloudelliset hyödyt, kuten esimerkiksi käyttöperusteisen maksumallin mahdollistamat säästöt (Armbrust ym., 2010) sekä vähentyneet sovelluspohjaisen rakentamisen ja ylläpidon korjauskustannukset (S. Lee ym., 2013). SaaS-järjestelmiin liittyy myös paljon operationaalisia hyötyjä, kuten esimerkiksi asiakasorganisaatioiden helpottunut skaalautuvuus (Marston ym., 2011) ja palvelun tarjoama joustavuus (Sultan, 2010). Tämän lisäksi SaaS-järjestelmistä voi saada muitakin sekalaisia hyötyjä, kuten esimerkiksi alentuneet

esteet IT:n sekä liiketoiminnan innovaatioille (A. Ali ym., 2017; Marston ym., 2011). Tässä tutkimuksessa perehdytään erityisesti SaaS-järjestelmien riskeihin, eikä hyötyihin paneuduta syvällisemmin. Monenlaiset hyödyt tunnistetaan tässä työssä osaksi SaaS:ia sekä vaikuttaviksi tekijöiksi organisaatioiden päätökselle ottaa käyttöön SaaS-järjestelmiä.

2.3 SaaS-järjestelmän käyttöönottoon vaikuttavat tekijät

2.3.1 Teknologiset tekijät

Aikaisempi tutkimus on suurelta osin keskittynyt SaaS-järjestelmän käyttöönottoon vaikuttavien tekijöiden tutkimiseen Tornatzkyn ym. (1990) luomaa teknologia-organisaatio-liiketoimintaympäristö (engl. technology-organization-environment, TOE) -viitekehystä hyödyntäen (Kim ym., 2017; Martins ym., 2016; Oliveira ym., 2019; Safari ym., 2015; Shapouri ym., 2024; Yang ym., 2015). SaaS-järjestelmän käyttöönottoon liittyy samanlaisia käyttöönottoon vaikuttavia tekijöitä kuin IT-ulkoistamiseen liittyvässä tutkimuksessa, mutta jotkin SaaS:n ominaisuudet, kuten sijaintiriippumattomat resurssit ja skaalautuvuus erottavat SaaS:n IT:n ulkoistamisesta (Burkon, 2013). Käyttöönottoon liittyy monia erilaisia vaikuttavia tekijöitä, jotka ovat yhdistettävissä aspekteihin, kuten teknologiaan, organisaatioon ja ulkoisiin tekijöihin. Tämän takia tässä tutkielmassa SaaS-järjestelmän käyttöönottoon vaikuttavia tekijöitä luokitellaan TOE-viitekehyksen mukaisesti teknologiseen, organisatoriseen ja liiketoimintaympäristölliseen osa-alueeseen kuvion 2 osoittamalla tavalla.



Kuvio 2 SaaS-järjestelmän käyttöönottoon vaikuttavia keskeisiä tekijöitä TOE-viitekehyksen mukaisesti

TOE-viitekehyksessä teknologisella kontekstilla tarkoitetaan organisaatiolle relevantteja laitteita ja prosesseja, sekä niihin liittyviä sisäisiä ja ulkoisia teknologioita (Sun ym., 2018). Teknologiset tekijät sisältävät muun muassa tämänhetkiset teknologiset käytännöt, teknologiset taidot sekä organisaatiolle relevantit saatavilla olevat teknologiat (Shapouri ym., 2024). Teknologinen konteksti sisältää kokonaisuudessaan teknisen arkkitehtuurin sekä inhimilliset tiedot, jotka voivat vaikuttaa innovaatioiden omaksumiseen yrityksissä (Zhu ym., 2006).

SaaS-järjestelmien käyttöönottoon vaikuttavia teknologisia tekijöitä on havaittu aikaisemmassa kirjallisuudessa useita. Yksi vaikuttavista tekijöistä on aikaisemmassa tutkimuksessa havaittu olevan IT-osaston koko, jonka on huomattu vaikuttavan SaaS:n hankintapäätökseen. Tästä on kuitenkin myös ristiriitaista tutkimusta, sillä IT-osaston koon vaikutuksista on tutkimusta IT:n ulkoistamistilanteissa, joissa IT-osaston koko on havaittu sekä vaikuttavana, että vaikuttamattomana tekijänä käyttöönottopäätöksissä. (Shapouri ym., 2024.) Tämän lisäksi yritysten saavutettavissa oleva suhteellinen hyöty on havaittu aikaisemmassa tutkimuksessa yhdeksi teknologisista vaikuttavista tekijöistä (Hsu & Lin, 2016; Safari ym., 2015). Suhteellinen hyöty tarkoittaa uuden pilvipalvelujärjestelmän tarjoamaa suhteellista hyötyä verrattuna nykyiseen järjestelmään.

Muita teknologisia vaikuttavia tekijöitä ovat myös havaittavuus ja turvallisuus. (Hsu & Lin, 2016; Safari ym., 2015.) Havaittavuus viittaa vaikeuteen havaita tai kuvailla järjestelmästä saavutettavia hyötyjä (Chen ym., 2009). Turvallisuus viittaa taas järjestelmän koettuun riskimäärään (Hsu & Lin, 2016), jonka on myös havaittu vaikuttavan SaaS:n ja pilvipalveluiden käyttöönottopäätökseen useammassa tutkimuksessa (Barnard & Van Der Lingen, 2022; P. Gupta ym., 2013; Hsu & Lin, 2016; Safari ym., 2015). Käyttöönottopäätökseen voivat vaikuttaa myös SaaS-järjestelmän yhteensopivuus, kokeiltavuus sekä monimutkaisuus. Yhteensopivuudella viitataan uuden järjestelmän kyvykkyyteen olla yhteensopiva nykyisten teknologioiden, arvojen, aikaisempien kokemusten ja yrityksen potentiaalisten tarpeiden kanssa. Kokeiltavuus viittaa puolestaan siihen, missä määrin järjestelmä on kokeiltavissa ja testattavissa ennen järjestelmän käyttöönottoa, kun taas monimutkaisuudella viitataan siihen, kuinka vaikeasti järjestelmä on ymmärrettävissä käyttäjien toimesta. (Safari ym., 2015.)

2.3.2 Organisatoriset tekijät

TOE-viitekehyksessä organisatorisella kontekstilla tarkoitetaan organisaation piirteitä, kuten esimerkiksi yrityksen kokoa, johdon rakennetta tai sisäisten resurssien käyttöastetta. Organisatoriset tekijät keskittyvät prosesseihin ja rakenteisiin, jotka edistävät tai estävät innovaatioiden käyttöönottoa. (Chau & Tam, 1997.) Yksi useammassa artikkelissa havaittu käyttöönottoon vaikuttava tekijä on ylimmän johdon tuki (Kim ym., 2017; Martins ym., 2016; Van De Weerd ym.,

2016; Yang ym., 2015). Ylimmän johdon tuki on tärkeää organisaatioille, sillä se voi luoda käyttöönottoa tukevan ympäristön sekä mahdollistaa riittävät resurssit uusien teknologioiden käyttöönottotilanteissa (Low ym., 2011).

Organisatorisia vaikuttavia tekijöitä ovat lisäksi organisaation jakamisen ja yhteistyön kulttuuri sekä IT-resurssit. Useimmat SaaS-järjestelmät mahdollistavat yhteistyön ja jakamisen verkkoyhteyden kautta lähes sijaintiriippumattomasti, mistä saatavaa etua yritysten tulisikin hyödyntää SaaS-järjestelmissä. IT-resursseilla viitataan puolestaan organisaation olemassa olevaan IT-infrastruktuuriin ja teknologiseen kyvykkyyteen. (Safari ym., 2015.) Aikaisempi tutkimus on osoittanut, että tilanteissa, joissa organisaatio on investoinut laadukkaaseen IT-infrastruktuuriin ja teknologiseen kyvykkyyteen, on mahdollista, että pilvipalvelujärjestelmät eivät ole taloudellisesti kannattava investointi (Misra & Mondal, 2011).

Näiden tekijöiden lisäksi aikaisemmassa tutkimuksessa on tutkittu organisaation koon vaikutusta pilvipalvelujärjestelmien, kuten SaaS-järjestelmien, käyttöönottopäätökseen erilaisissa konteksteissa. Näiden tutkimusten perusteella organisaation koon vaikutus vaihtelee erilaisissa tilanteissa ja yleistettäessä voidaan sanoa, että tutkimusten tulokset ovat sekalaisia vaikutuksen suhteen. (Loukis ym., 2017; Low ym., 2011; Rath ym., 2012.) Esimerkiksi korkean teknologian yrityksissä on havaittu, että organisaation koko on pilvipalvelun käyttöönottoon vaikuttava tekijä. Suurten korkean teknologian yritysten on havaittu käyttöönottavan pilvipalveluita todennäköisemmin, sillä näillä yrityksillä on paremmat resurssit ja kyvykkyydet hallinnoida siirtymää vanhasta järjestelmästä uuteen. (Low ym., 2011.) Toisaalta, eurooppalaisten teollisuusyritysten tapauksessa organisaation koon on havaittu olevan mitätön tekijä pilvipalvelujen käyttöönottopäätöksessä (Loukis ym., 2017). Yhdeksi vaikuttavaksi tekijäksi on myös esitetty koettuja taloudellisia hyötyjä, jotka vaikuttavat yleisesti koettuihin hyötyihin ja tätä kautta lopulta käyttöönottopäätökseen pilvipalveluina toimivien toiminnanohjausjärjestelmien kontekstissa (Chang, 2020).

2.3.3 Liiketoimintaympäristölliset tekijät

SaaS-järjestelmien käyttöönottoon liittyy myös liiketoimintaympäristöllisiä tekijöitä. TOE-viitekehyksessä liiketoimintaympäristöllisillä tekijöillä tarkoitetaan ulkoisia piirteitä, jotka vaikuttavat organisaation päätökseen ottaa käyttöön uusia teknologioita (Oliveira ym., 2019). Organisaatiot eivät toimi eristyksissä ympäristöstään, minkä takia liiketoimintaympäristön piirteet, kuten kilpailijat, yhteistyökumppanit, regulaatio ja julkishallinto tuovat mukanaan rajoitteita ja mahdollisuuksia uusien teknologioiden käyttöönottoon. Yksi näistä tekijöistä on kilpailijoiden päätös käyttöönottaa SaaS-järjestelmiä. Kilpailijoiden käyttöönottopäätöksellä on kirjallisuudessa havaittu

olevan positiivinen vaikutus organisaatioiden omaan käyttöönottopäätökseen. (Shapouri ym., 2024.) Epävarmoissa liiketoimintaympäristöissä yritykset saattavat jäljitellä kilpailijoiden tekemiä päätöksiä vähentääkseen tätä epävarmuutta (Mithas ym., 2013).

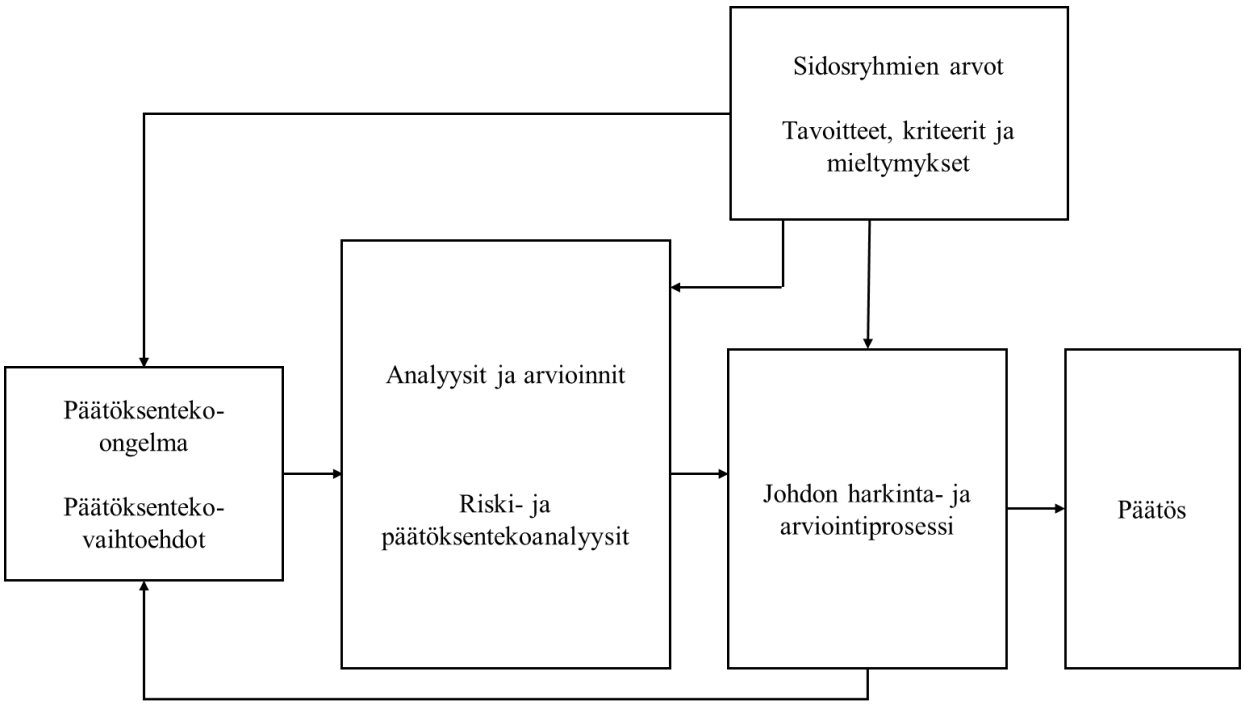
Organisaatioihin kohdistuvat paineet vaikuttavat organisaatioiden SaaS-järjestelmien käyttöönottopäätöksiin. Nämä paineet voidaan jakaa normatiivisiin, jäljitteleviin ja pakotettuihin paineisiin. (Oliveira ym., 2019.) Normatiiviset paineet viittaavat ammattimaisten standardien ja yhteisöjen aiheuttamaan paineeseen käyttöönottaa järjestelmiä ollakseen pätevä olennaisten sidosryhmien keskuudessa (Kung ym., 2015). Tähän ryhmään kuuluvat muun muassa asiakkaat sekä toimittajat (Oliveira ym., 2019). Jäljittelevät paineet viittaavat organisaation paineeseen jäljitellä toimintaansa samankaltaisten yritysten mukaisiksi (Teo ym., 2003). Jäljittelevät paineet liittyvät kilpailijoiden saavuttamiin etuihin, joita organisaatiot pyrkivät saavuttamaan kopioimalla kilpailijoiden toimia (Oliveira ym., 2019). Organisaatioiden kokeman kilpailullinen paineen, eli organisaation kilpailijoista johtuvan paineen, on huomattu vaikuttavan positiivisesti organisaatioiden pilvipalveluiden käyttöönottopäätöksiin useamassa tutkimuksessa (Gutierrez ym., 2015; Low ym., 2011; Matias & Hernandez, 2021; Safari ym., 2015). Kilpailullinen paine käyttöönottopäätöksessä viittaa siihen, kun organisaatio implementoi pilvipalveluteknologiaa kilpailullisena työkaluna, muut yritykset kokevat kilpailullista painetta, joka ajaa näitä organisaatioita käyttöönottamaan pilvipalveluteknologiaa kilpailullisen edun menettämisen pelossa (Gangwar ym., 2015). Pakottavat paineet puolestaan viittaavat organisaatioiden kohtaamiin pakollisiin paineisiin, jotka ovat peräisin tahoilta, kuten valtioilta, sääntelyelimiltä ja yhdistyksiltä (Oliveira ym., 2019). Paineiden lisäksi myös SaaS-järjestelmien palveluntarjoajien tarjoaman tuen on havaittu vaikuttavan käyttöönottopäätökseen. Tähän tukeen sisältyy palveluntarjoajien tarjoama tekninen ja koulutuksellinen tuki, sekä SaaS-järjestelmien palveluntarjoajien kohdentamat markkinointipanokset tarjoamiinsa järjestelmiin. (Kim ym., 2017.)

3 SaaS-järjestelmän käyttöönoton riskit

3.1 Päätöksentekoprosessi ja riskit käyttöönotossa

Se pitäisikö IT-järjestelmät tuottaa itse vai ulkoistaa on keskeinen kysymys niin organisaatioissa, kuin tutkimuskentälläkin (Bibi ym., 2012; Lacity ym., 2010). IT-hankintapäätökset tuovat mukanaan huomattavia taloudellisia, operationaalisia ja strategisia riskejä (Benlian & Hess, 2011; Islam ym., 2017), minkä takia organisaation johdon tuleekin harkita käyttöönottopäätöstä tarkasti (Aubert ym., 2012). Johdon tulisi ottaa päätöksessä huomioon organisaation rakenne, prosessit, keskinäiset riippuvuudet sekä tottumukset ymmärtääkseen erilaisia päätösvaihtoehtoja ja niihin liittyviä rakenteellisia valintoja (Aubert ym., 2012; Moses & Åhlström, 2008).

Kuviossa 3 on esitetty Avenin (2012) riskitietoisen päätöksenteon perusrakenne. Kuvio 3 on muodostettu käyttäen päätöksentekomallia, jossa päätöksenteko nähdään prosessina, joka sisältää päätöksentekoa tukevia muodollisia riski- ja päätöksentekoanalyysejä. Näitä analyysejä seuraa epämuodollinen johdon harkinta- ja arviointiprosessi, joka johtaa lopulta päätökseen. (Aven, 2012 s. 112–114.)



Kuvio 3 Riskitietoisen päätöksenteon perusrakenne (suomennettu (Aven, 2012, s. 114))

Kuvion 3 vasemmasta laidasta nähdään, miten päätöksenteko-ongelmaan ja -vaihtoehtoihin vaikuttavat sidosryhmien arvot sekä organisaatioiden tavoitteet, kriteerit ja mieltymykset. Myös

johdon arvio itse päätöksenteko-ongelmaan sekä -vaihtoehtoihin liittyen vaikuttaa niiden muodostumiseen. Seuraavassa vaiheessa päätöksentekoprosessissa valitut päätöksentekovaihtoehdot otetaan tarkempaan tarkasteluun, jolloin niihin liittyen suoritetaan muodollisia riski- ja päätöksentekoanalyysejä, sekä muita analyysejä ja arviointeja. Näitä seuraa johdon epämuodollinen harkinta- ja arviointiprosessi päätöksentekovaihtoehdoista. Johdon harkinta- ja arviointiprosessiin vaikuttaa edeltävän vaiheen analyysit, kuten riski- ja päätöksentekoanalyysit, sidosryhmien arvot sekä organisaation tavoitteet, kriteerit ja mieltymykset. Kuvion 3 oikeassa laidassa on päätöksentekoprosessin viimeinen vaihe, joka on päätös.

Tässä tutkimuksessa kuviossa 3 olevan päätöksentekomallin nähdään sopivan SaaS-järjestelmän käyttöönottopäätöksen kontekstiin, sillä useammasta sidosryhmästä riippuvaa ja dynaamisessa toimintaympäristössä tapahtuvaa käyttöönottopäätöstä, sekä siihen liitettyä lopputulosta, voi olla hankala optimoida käyttäen pelkkiä optimointimalleja, joita Avenin (2012) mukaan voidaan kuitenkin käyttää joissain päätöksenteon erikoistapauksessa. IT-investointeihin saattaa liittyä myös strategisia tavoitteita, joita on usein hankala määrällistää mittarien avulla (Clemons & Weber, 1990). Järjestelmän käyttöönottopäätös on lopulta ainakin osittain johdon subjektiivisesta arviosta ja harkinnasta johdettu päätös, jossa heidän tulisi kuitenkin ottaa huomioon päätöksen moniulotteisuus (Aubert ym., 2012; Moses & Åhlström, 2008). Avenin (2012, s. 113) mukaan kuviossa 3 esiintyvässä riskitietoisen päätöksenteon perusrakenteessa, muodolliset päätöksentekoanalyysit nähdään päätöksentekoa tukevina toimina, eivätkä ne suoraan johda päätöksentekovaihtoehdon valintaan tai hylkäykseen ennen johdon arviota ja päätöstä. Avenin (2012, s. 114) riskitietoisen päätöksenteon perusrakenne tukee myös tämän tutkimuksen suorittamista siten, että riskitietoisessa päätöksenteossa riskejä tulisi analysoida ja harkita jo ennen päätöksentekoa. Täten tässä tutkimuksessa riskien tunnistamisen ja riskienhallinnan voidaan ajatella tapahtuvan ainakin osittain jo ennen SaaS-järjestelmän käyttöönottopäätöstä ja vaikuttavan myös lopulliseen käyttöönottopäätökseen.

Riskitekijöiden tunnistaminen IT-ulkoistamisessa toimii koko riskienhallinnan perustana. Riskitekijöiden tunnistaminen auttaa päätöksentekijöitä ymmärtämään riskien lähteitä. (Fan ym., 2012.) Vaikka pilvipalveluiden hankinta ja käyttöönottopäätös voidaan periaatteessa ajatella IT-ulkoistamisena, SaaS eroaa kuitenkin perinteisestä IT-ulkoistamisesta pilvipalveluiden sekä SaaS-järjestelmien omien erityispiirteiden myötä (Burkon, 2013; Islam ym., 2017). Riskienhallintaa pidetään yhtenä keskeisimpänä asiana pilvipalveluissa. Riskit voivat ylittää pilven mahdollistamat hyödyt liiketoiminnalle, ja tämän takia toimiva riskienhallinta on tärkeää yritysten toiminnan jatkuvuudelle ja kilpailuedulle. (Islam ym., 2017). Vaikka SaaS-järjestelmät kasvattavatkin suosiotaan organisaatioissa, erityisesti yritysten toiminnalle keskeiset ydinjärjestelmät eivät ole

siirtyneet pilveen samalla tahdilla kuin muut järjestelmät, mikä johtuu osittain juuri pilvipalveluiden riskeistä liiketoiminnalle (Shuraida & Titah, 2023).

Tämän lisäksi empiirisen tiedon pilvipalveluiden hankintapäätöksiin liittyen on tunnistettu olevan kirjallisuudessa niukkaa (Schneider & Sunyaev, 2016). Tarkastellessa erityisesti SaaS:ia, pääasiallisena asiakkaana toimii usein jokin organisaation liiketoimintayksikkö. Täten SaaS eroaa muista pilvipalvelumalleista, kuten IaaS:sta ja PaaS:sta, joiden pääasiallisena asiakkaana toimii IT-osasto. (Schneider & Sunyaev, 2016.)

Voidaan myös todeta, että pilvipalveluihin liittyvän riskienhallintasuunnitelman luominen saattaa olla haastavaa, vaikka riskityypit muistuttaisivatkin muilla laskenta-alustoilla tavattuja riskejä. Pilvipalveluissa riskienhallintasuunnitelmat tulee laatia data-, infrastruktuuri- ja palvelutasoilla. Haasteet ja riskienhallintasuunnitelmien monitasoisuus johtuvat usein siitä, että pilvipalveluiden käyttäjillä ei ole päätäntävaltaa tai tarkempaa tietoa datastaan sen jälkeen, kun data on siirretty palveluntarjoajan pilvi-infrastruktuuriin. (Islam ym., 2017.) Kirjallisuudessa on lisäksi huomattu, että perinteiset tavat arvioida riskejä eivät sellaisenaan sovellu pilvipalveluiden kontekstiin (Akinrolabu ym., 2019; Islam ym., 2017).

3.2 Laajennettu havaittujen riskien -viitekehys SaaS-järjestelmän käyttöönottopäätöksessä

3.2.1 Viitekehyksen muokkaaminen

Havaitut riskit ovat perinteisesti määritelty markkinointitutkimuksessa ostoon liitetyiksi oletetuiksi tappioiksi, jotka toimivat estävinä tekijöinä hankintapäätökselle (Peter & Ryan, 1976). Havaitut riskit ajatellaan usein epävarmuuden tunteeksi, joka liittyy mahdollisiin negatiivisiin seurauksiin omaksuessa tai ottaessa käyttöön tuotetta tai palvelua (Benlian & Hess, 2011). Bettmanin (1973) mukaan havaitut riskit ovat keskeisiä sellaisissa valintapäätöksissä, joissa päätöksentekoon liittyy epävarmuutta, epämukavuutta, ahdistusta tai ristiriitaa.

Benlian ja Hess (2011) määrittävät havaitut riskit SaaS-järjestelmien hankintaan liittyvässä tutkimuksessaan mahdollisiksi tappioiksi halutun lopputuloksen tavoittelussa silloin, kun hankitaan SaaS-järjestelmää. Tässä tutkielmassa käytetään Benlianin ja Hessin (2011) määritelmää havaituista riskeistä keskittyen organisaation SaaS-järjestelmän käyttöönottopäätökseen. SaaS-järjestelmän käyttöönottopäätöksellä tarkoitetaan tässä tutkimuksessa organisaation päätöstä SaaS-järjestelmän käyttöönottamisesta osaksi organisaation toimintaa.

Benlian ja Hess (2011) muodostavat aikaisemmassa tutkimuksessaan havaittujen riskien -viitekehyksen SaaS-järjestelmien käyttöönottoon liittyen. Kyseinen viitekehys pohjautuu Cunninghamin (1967) laatimaan, ja laajasti tutkimuskentällä hyväksyttyyn, havaittujen riskien -viitekehykseen, joka sisältää kuusi riskien osa-aluetta: suorituskyky, taloudellisuus, mahdollisuus/aika, turvallisuus, sosiaaliset tekijät sekä psykologiset tekijät. Benlian ja Hess (2011) tiivistävät viitekehyksen SaaS-järjestelmien kontekstissa viiteen osa-alueeseen: suorituskyky, taloudellisuus, strategiset tekijät, tietoturva ja johdon/psykososiaaliset tekijät.

Tässä tutkimuksessa käytetään edellä mainittuja Benlianin ja Hessin (2011) SaaS-järjestelmien kontekstiin kohdistettuja riskikategorioita, muokaten ja laajentaen viitekehystä kuitenkin aikaisemmasta tutkimuksesta. Ensinnäkin tässä tutkimuksessa Benlianin ja Hessin (2011) viitekehykseen lisätään kuudes riskikategoria, joka on *projektiriskit.* Projektiriskit on tunnistettu keskeiseksi riskikategoriaksi organisaatioiden IT-hankintoihin keskittyvässä tutkimuksessa (Clemons & Weber, 1990) ja täten tässä tutkimuksessa näiden riskien ajatellaan olevan läsnä myös SaaS-järjestelmän käyttöönottopäätöksen yhteydessä. Lisäksi tässä tutkimuksessa Benlianin ja Hessin (2011) psykososiaalisten riskien käsitettä laajennetaan koskemaan organisaation kaikkia työntekijöitä, eikä ainoastaan johtajia, joihin Benlian ja Hess (2011) tutkimuksessaan rajaavat kyseisen riskikategorian. Tässä tutkimuksessa laajennetun psykososiaalisten riskien käsitteen ajatellaan tuovan esiin monipuolisemmin riskejä myös johdon henkilökohtaisten riskien ulkopuolelta, sillä SaaS-järjestelmän käyttöönottamisen ajatellaan vaikuttavan laajemmin myös koko henkilöstön psykososiaalisiin tekijöihin.

Benlian ja Hess (2011) mainitsevat tutkimuksessaan uusien keskeisten riskien tarkastelun osana viitekehystä, sillä uudet mahdolliset riksikategoriat, kuten vaatimuksenmukaisuuteen ja lainsäädäntöön liittyvät riskit, saattavat kasvattaa tärkeyttään tulevaisuudessa. Tämän takia tässä tutkimuksessa Benlianin ja Hessin (2011) viitekehyksen tietoturvariskien kategoriaa laajennetaan koskemaan myös tietosuojaa. Alla olevissa alaluvuissa 3.2.2–3.2.7 avataan tarkemmin tämän tutkimuksen laajennetun havaittujen riskien -viitekehyksen eri osa-alueita SaaS-järjestelmiin ja IT-ulkoistamiseen liittyvän riskikirjallisuuden avulla.

3.2.2 Suorituskykyriskit

Suorituskykyriskit viittaavat riskeihin, jotka liittyvät mahdollisuuteen siitä, että SaaS-palveluntarjoaja ei onnistu toimittamaan odotetun tason palvelua. Tähän liittyy muun muassa riski siitä, että palveluntarjoaja ei pystykään tarjoamaan tarvittavaa saatavuutta tai kaistanleveyttä, jonka tarjoaja on luvannut asiakasorganisaatiolle. (Benlian & Hess, 2011.) Pilvipalveluiden kohdalla

havaittuja suorituskykyriskejä ovat myös tärkeiden taitojen menettäminen, väärien taitojen kehittyminen, työntekijöiden kokemattomuus pilvipalveluiden kanssa toimimisesta sekä organisatorisen oppimisen olemattomuus. Suorituskykyyn liittyvät vaarat ovat erittäin merkityksellisiä pilvipalveluiden käyttöönottopäätöksissä, sillä pilvipalveluiden toiminta määräytyy internet-yhteyden laadun ja saatavuuden mukaan. Tämä synnyttää useita huolia saatavuudesta, palveluongelmista sekä liiketoiminnan jatkuvuudesta. (Gupta ym., 2023.) Pilvipalveluiden käyttöönoton esteitä tutkiessa on myös havaittu, että pilvipalvelun integroitavuus, jossa integroitavuus viittaa pilvipalvelun kykyyn olla yhteensopiva asiakasorganisaation olemassa olevien järjestelmien kanssa, on merkittävä riskitekijä käyttöönottopäätöksessä (Phaphoom ym., 2015).

3.2.3 Tietoturva- ja tietosuojariskit

Tietoturvariskeillä viitataan asiakkaan epävarmuuteen oman datansa ja organisaationsa turvallisuudesta (Benlian & Hess, 2011). SaaS-järjestelmien turvallisuuden kohdalla käyttäjät joutuvat asettamaan luottonsa palveluntarjoajaan, sillä palveluntarjoajat pitävät huolta siitä, että useat eri käyttäjät tai yritykset eivät näe toistensa tietoja luvattomasti. Tämän lisäksi palveluntarjoajat ovat vastuussa infrastruktuurin suojaamisesta hyökkäyksiltä. Samalla myös todennus- sekä salausprosessit ovat palveluntarjoajan vastuulla. (Viega, 2009.) Tietoturvariskejä pidetään kirjallisuudessa yhtenä keskeisimpänä pilvipalveluiden haasteena (Bibi ym., 2012). Tästä syystä ne toimivat edelleen keskeisenä pilvipalveluiden, kuten SaaS-järjestelmien, käyttöönottopäätöksen estävä tekijänä organisaatioissa (Georgiopoulou ym., 2020).

Tietojen häviämistä pidetään ongelmatekijänä organisaation pohtiessa SaaS-järjestelmän käyttöönottoa (Bibi ym., 2012). Asiakkaan käyttäessä SaaS:ia, osa tai jopa kaikki asiakkaan data tallennetaan palveluntarjoajan datakeskukseen. Tällöin palveluntarjoaja hallitsee asiakkaan dataa ilman, että asiakas itse täysin tietää, miten SaaS-tarjoaja turvaa datan ja millaisia varmuuskopioita tai palautuskäytäntöjä tarjoaja käyttää mahdollisten ongelmien sattuessa. (Benlian & Hess, 2011.) Palvelutasosopimusten (engl. Service Level Agreement, SLA) avulla organisaatiot voivat määritellä toivotut tietoturvatasot datallensa, mutta samalla epäselvyydet ja porsaanreiät sopimuksissa saattavat antaa palveluntarjoajille mahdollisuuden monitulkinnaisuuteen tai opportunistiseen käyttäytymiseen. Teknologia kehittyy nopeasti, minkä takia asiakkaiden on vaikea pysyä joustavien sopimusten tuomien tietoturvariskien perässä. (Benlian & Hess, 2011.)

Aikaisemmassa tutkimuksessa on huomattu, että havaittu laillinen epävarmuus sekä havaittu palveluntarjoajan opportunismi ovat vaikuttaneet havaittuun tietoturvariskiin ja tätä kautta myös pilvipalveluiden käyttöönottopäätökseen. Tässä laillinen epävarmuus viittaa asiakasorganisaation

tietämättömyyteen lain antamasta suojasta tietoturvaloukkaustilanteissa, kun taas palveluntarjoajan opportunismi viittaa palveluntarjoajan mahdolliseen opportunistiseen käyttäytymiseen, kuten esimerkiksi tahalliseen alisuoriutumiseen. (Yigitbasioglu, 2014.)

Pilvipalveluiden tietoturvassa on olennaista, että hyökkäykset pilvipalveluiden mihin tahansa kerrokseen voivat vaarantaa muutkin pilvipalveluiden kerrokset. Tämä johtuu siitä, että IaaS toimii usein isännöintialustana sekä PaaS:lle että SaaS:lle, jolloin hyökkäykset IaaS:iin saattavat vaarantaa myös muut kerrokset. Tämän lisäksi PaaS tarjoaa alustan, jolla voidaan toteuttaa SaaS-palveluita, mikä vahvistaa eri kerrosten riippuvuutta toisistaan myös turvallisuuden näkökulmasta (Hashizume ym., 2013.)

Sen lisäksi, että tietoturvariskit toimivat keskeisinä riskeinä SaaS-järjestelmien käyttöönottopäätöksissä (Benlian & Hess, 2011; Bibi ym., 2012; Georgiopoulou ym., 2020), organisaatioiden tulee noudattaa myös tietosuojaan liittyviä vaatimuksia, kuten vuonna 2018 voimaan astunutta Euroopan Unionin yleistä tietosuoja-asetusta (engl. General Data Protection Regulation, GDPR) (Georgiopoulou ym., 2020). GDPR:ssä asetetaan organisaatioille henkilötietojen keräämistä, säilytystä ja hallinnointia koskevat tarkat vaatimukset, joita sekä eurooppalaisten, että Euroopan ulkopuolisten organisaatioiden tulee noudattaa, jos henkilötietoja käsitellään EU:n sisällä tai tietojen käsittely kohdistuu EU-alueen asukkaisiin (EU, 2025). GDPR on keskeinen SaaS-järjestelmien kohdalla niin asiakasorganisaation, kuin palveluntarjoajankin näkökulmasta, sillä sen noudattaminen koskee kaikkia yrityksiä, jotka hallitsevat tai prosessoivat EU-kansalaisten dataa (Georgiopoulou ym., 2020). Ohjelmistopalveluihin liittyvässä vaatimuksenmukaisuudessa tulee lisäksi varmistua siitä, että palvelu vastaa sääntelyä, yksityisyyteen liittyviä standardeja, turvallisuusprotokollia, sekä toimialakohtaisia erityisvaatimuksia (S. S. Yau ym., 2024). Tietosuojavaatimusten noudattamisessa on tärkeää huomioida lisäksi se, millaista dataa hallinnoidaan ja prosessoidaan, sillä esimerkiksi GDPR:ssä sensitiiviseen henkilökohtaiseen dataan, kuten terveysdataan, liittyy erityisvaatimuksia (Georgiopoulou ym., 2020).

Vaatimusten noudattaminen aiheuttaa huolta asiakasorganisaatioissa sekä palveluntarjoajissa, ja niiden noudattamisen epäonnistuminen voi johtaa asiakkaiden tai paikallisten tietosuojavaltuutettujen langettamiin sanktioihin (Georgiopoulou ym., 2020) sekä mainehaittaan muun muassa luottamuksen menettämisen kautta (S. S. Yau ym., 2024). SaaS-järjestelmien tietosuojan keskeisyyden takia tässä tutkimuksessa tietoturvariskien kategoriaa laajennetaan koskemaan sekä tietoturva- että tietosuojariskejä.

3.2.4 Strategiset riskit

Strategiset riskit ovat sellaisia, joihin liittyy kriittisiä resursseja tai kyvykkyyksiä, jotka organisaatio saattaa menettää ulkoistaessaan sovelluksia SaaS-pilvipalvelumallia käyttäen. Strategiset riskit ovat erityisen olennaisia, jos ulkoistetaan liiketoiminnalle kriittisiä sovelluksia sekä sellaisia sovelluksia, jotka ylittävät organisaatioiden funktioiden rajoja. Näihin lukeutuvat muun muassa toiminnanohjausjärjestelmät, asiakkuudenhallintajärjestelmät sekä toimitusketjujen hallintajärjestelmät. SaaS-järjestelmien tapauksessa asiakkaan ja palveluntarjoajan välillä on paljon keskinäisiä riippuvuuksia, mikä saattaa hidastaa organisaation reaktionopeutta sisäisiin strategisiin muutoksiin, kuten liiketoiminnan strategiamuutoksiin, sekä ulkoisiin strategisiin muutostavoitteisiin, kuten uusien markkina-alueiden tavoitteluun. (Benlian & Hess, 2011.)

Asiakasorganisaation luoton palveluntarjoajaa kohtaan sekä havaitun kontrollin on tunnistettu vaikuttavan havaittuihin riskeihin pilvipalveluiden käyttöönottopäätöksissä, sillä niiden molempien on huomattu vähentävän havaittuja riskejä asiakasorganisaatioissa. Havaitulla kontrollilla viitataan tässä tapauksessa asiakasorganisaatioiden näkemykseen mahdollisuudestaan hallinnoida organisaation informaation vapauttamista ja levittämistä. (Chang & Hsu, 2019.)

IT-järjestelmien ulkoistamisessa, IT-investoinnin hylkäämisen riskit nousevat keskeisiksi erityisesti silloin, kun hankittavalla järjestelmällä on strategista vaikuttavuutta. Investoimatta jättäminen saattaa riskeerata muun muassa yrityksen markkinaosuuden, liiketoiminnan kasvun tai uusien markkina-alueiden saavutettavuuden tulevaisuudessa. Investoimatta jättäminen saattaa johtaa myös kilpailuedun heikentymiseen ja tulevaisuuden pakollisiin investointeihin, jotta organisaatio saa pysyttyä markkinakilpailun mukana. (Clemons & Weber, 1990.)

Aikaisemmassa tutkimuksessa on mainittu myös toimittajaloukku (engl. Vendor lock-in), joka on merkittävä pilvipalvelujärjestelmien käyttöönottoa estävä tekijä (Opara-Martins ym., 2016). Toimittajaloukku on tilanne, jossa asiakasorganisaatio on riippuvainen yhdestä pilvipalveluntarjoajan ratkaisusta, eikä täten pysty siirtymään muihin vaihtoehtoisiin järjestelmäratkaisuihin ilman suuria kuluja, laillisia rajoitteita tai teknisiä ongelmia (Armbrust ym., 2010). Tässä tutkimuksessa tällaiseen tilanteeseen joutuminen voidaan nähdä riskinä SaaS-järjestelmän käyttöönottopäätöksessä.

3.2.5 Taloudelliset riskit

Vaikka SaaS-järjestelmien yksi olennaisemmista hyödyistä onkin sen suomat taloudelliset hyödyt (Armbrust ym., 2010), liittyy SaaS:iin myös taloudellisia riskejä. Taloudellisiin riskeihin lukeutuu

muun muassa se, että asiakas voi joutua maksamaan oletettua enemmän saavuttaakseen halutun toiminnan tason. Taloudellisiin kustannuksiin kuuluvat myös niin sanotut piilotetut kustannukset, joita SaaS-järjestelmiin saattaa liittyä. Palveluntarjoajan omistaessa ydinsovelluksen, sillä saattaa olla myös enemmän neuvotteluvoimaa, kun puhutaan hinnankorotuksista tai sovelluksiin tehtävistä muutoksista. (Benlian & Hess, 2011.)

Pilvipalveluiden kohdalla riskiksi on nostettu myös operationaalisten kustannusten yllättävä ja odottamaton kasvu. Tällaiset operationaaliset kustannukset voivat kasvaa muun muassa pilvipalvelujärjestelmän monimutkaisuuden tai pilvipalveluiden ja olemassa olevien järjestelmien heikon yhteensopivuuden takia. (Brender & Markov, 2013.)

IT-ulkoistamiseen liittyvässä aikaisemmassa tutkimuksessa on nostettu esiin piilotettuja kustannuksia, jotka voidaan nähdä riskeiksi myös tässä tutkimuksessa, kun ajatellaan SaaS-järjestelmiä ja niiden käyttöönottopäätöksiä. Barthelemy (2001) jaottelee IT-ulkoistamisen piilotetut kustannukset neljään osa-alueeseen: palveluntarjoajan etsintä ja sopimukset, siirtyminen palveluntarjoajalle, ulkoistamisen hallinta sekä uudelleen siirtyminen ulkoistamisen jälkeen.

Palveluntarjoajan etsintään ja sopimuksiin kuluu usein enemmän aikaa ja rahaa kuin organisaatiot etukäteen olettavat. IT-järjestelmien ja infrastruktuurin siirtäminen palvelutarjoajalle on myös resurssi-intensiivinen prosessi, eikä se usein tapahdu yhtä yksinkertaisesti kuin organisaatiot saattavat etukäteen olettaa. Ulkoistamisen jälkeisten hallintakustannusten voidaan nähdä kattavan suurimman osan piilotetuista kustannuksista perinteisessä IT-ulkoistamisessa, sillä ne kattavat palveluntarjoajan monitoroinnin, palveluntarjoajan kanssa neuvottelun ja mahdolliset sanktiot sekä sopimusmuutoksiin liittyvät neuvottelut.

Yhtenä piilotettujen kulujen kategoriana voidaan lisäksi pitää uudelleensiirtymistä ulkoistamisen jälkeen. Tähän osa-alueeseen sisältyy palveluntarjoajan vaihtaminen tulevaisuudessa sekä IT:n siirtäminen takaisin sisäiseksi toiminnoksi. Monien johtajien on usein vaikea ajatella uudelleensiirtymiseen liittyviä kustannuksia, sillä ulkoistamisen tuomaa muutosta ja siitä saatavia hyötyjä pidetään usein pysyvinä silloin, kun ajatellaan ulkoistamispäätöstä. (Barthelemy, 2001.) Tässä tutkimuksessa edellä mainittujen piilotettuihin kustannuksiin liittyvien riskien voidaan nähdä vaikuttavan myös SaaS-järjestelmien kontekstissa osana käyttöönottopäätöstä.

Toiminnallisuusriskin on lisäksi tunnistettu olevan yksi strategisiin IT-investointeihin liittyvä riski. Vaikka organisaatio onnistuisikin järjestelmän käyttöönotossa tai mallinnuksessa, se ei välttämättä kuitenkaan onnistu realisoimaan järjestelmästä odotettuja hyötyjä. Tällainen toiminnallisuusriski voi

realisoitua muun muassa silloin, jos suunnitteluvaiheessa ei oteta huomioon käyttäjien tarpeita tai organisaatioin tavoitteet muuttuvat, jolloin järjestelmä ei tuekaan organisaation uusia tavoitteita. (Clemons & Weber, 1990.) Tässä tutkimuksessa toiminnallisuusriski nähdään osana taloudellisten riskien kategoriaa, sillä tässä tutkimuksessa ajatellaan, että SaaS-järjestelmästä saatavien hyötyjen tulisi ylittää järjestelmän hyötyihin suhteutetut kustannukset, jotta käyttöönottopäätös voidaan nähdä organisaatiolle kannattavana.

3.2.6 Psykososiaaliset riskit

Aikaisemmassa tutkimuksessa psykososiaalisilla riskeillä viitataan riskeihin, jotka saattavat vaikuttaa liiketoimintaprosessista vastuussa olevan johtajan henkilökohtaiseen maineeseen tai uraan, mikä johtuu muun muassa väitteistä ulkoistamisen vaikutuksesta työpaikkojen vähentymiseen (Gewald & Dibbern, 2009). Psykososiaalisten riskien vaikutusta on tarkasteltu myös vaikuttavana tekijänä SaaS-järjestelmien käyttöönottopäätöksissä (Benlian & Hess, 2011), mutta tutkimus psykososiaalisista tekijöistä ja niiden vaikutuksesta SaaS-järjestelmien kontekstissa on vähäistä. Ulkoistamisen on kuitenkin havaittu vaikuttavan psykososiaalisiin aspekteihin pelkän johtajien näkökulman sijasta myös koko organisaation työntekijöiden näkökulmasta, sillä on havaittu, että ulkoistaminen voi vaikuttaa joissakin tilanteissa organisaation työntekijöiden työtyytyväisyyteen negatiivisesti (G. R. Lee & Lee, 2020). Tässä tutkimuksessa ajatellaan, että tällaiset vaikutukset voidaan nähdä riskeinä, ja täten psykososiaalisiin riskeihin sisällytetään mahdolliset yrityksen henkilöstöön liittyvät riskit, jotka eivät asetu muiden riskikategorioiden alle.

Clemons ja Weber (1990) mainitsevat sisäiset poliittiset riskit osaksi strategisten IT-investointien mukanaan tuomia riskejä. Sisäisillä poliittisilla riskeillä tarkoitetaan organisaation jäsenten intressien ja etujen ristiriitaa. Tämä ristiriita saattaa johtaa tilanteeseen, jossa organisaation henkilöstö tai jotkin osastot eivät suostu yhteistyöhön tai ovat hitaita hyväksymään uutta järjestelmää työtehtäviin liittyvien uhkien takia. (Clemons & Weber, 1990.) Tässä tutkimuksessa sisäiset poliittiset riskit voidaan nähdä osana psykososiaalisten riskien laajennettua käsitettä, jossa psykososiaalisten riskien ajatellaan koskevan SaaS-järjestelmään ja sen käyttöönottopäätökseen liittyviä riskejä, niin päätöksiä tekevän johtohenkilöstön, kuin organisaation muunkin henkilöstön näkökulmasta. Tämän tutkimuksen psykososiaalisten riskien käsite on täten monipuolisempi ja laajentaa Benlianin ja Hessin (2011) käsitettä, joka kohdistuu johtajiin.

3.2.7 Projektiriskit

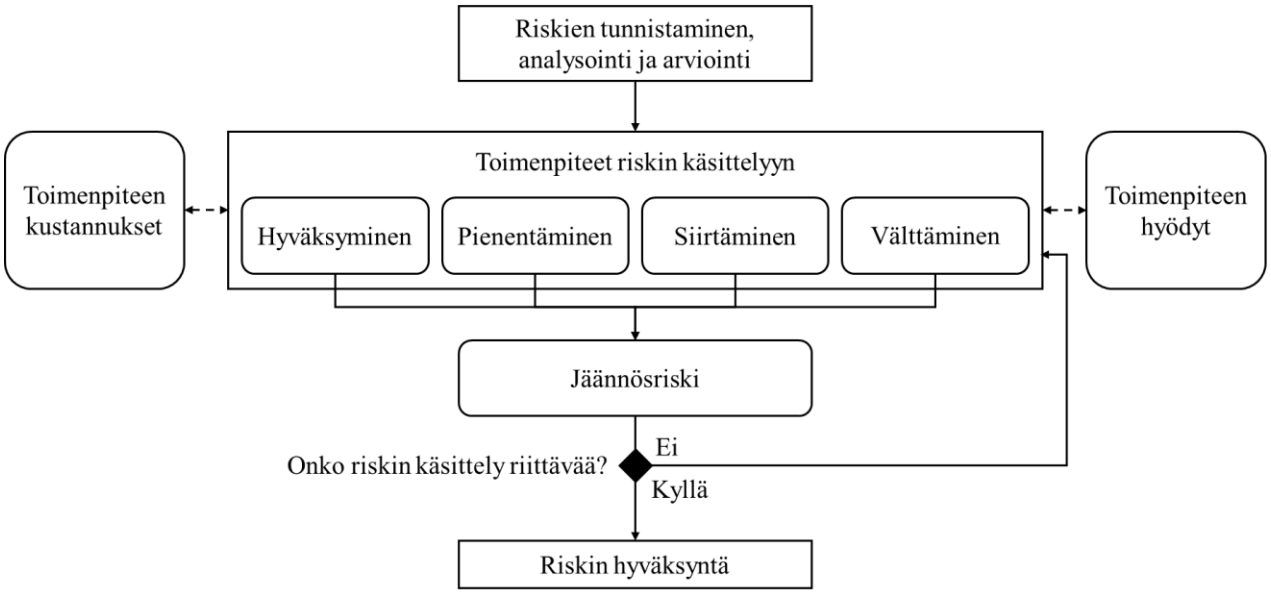
Cunninghamin (1967) alkuperäinen havaittujen riskien -viitekehys on luotu markkinointitutkimukseen, ja Benlianin ja Hessin (2011) SaaS-järjestelmiin kohdistettu havaittujen riskien -viitekehys soveltaa tätä alkuperäistä viitekehystä. Benlian ja Hess (2011) eivät kuitenkaan SaaS-järjestelmien kontekstiin muokatussa riskiluokituksessaan ota huomioon SaaS-järjestelmien käyttöönottoon liittyviä projektiriskejä, joista puolestaan Clemons ja Weber (1990) puhuvat strategisten IT-järjestelmien ulkoistamiseen liittyvässä tutkimuksessaan. Projektiriskeillä tarkoitetaan projektin laajuudesta, monimutkaisuudesta tai henkilökunnan taitojen ylittymisestä johtuvia riskejä. Näitä riskejä voidaan pyrkiä pienentämään muun muassa palkkaamalla organisaation ulkopuolista apua, kuten konsultteja (Clemons & Weber, 1990).

Vaikka SaaS-järjestelmät eroavat perinteisesti IT-ulkoistamisesta (Burkon, 2013; Islam ym., 2017), tässä tutkimuksessa myös SaaS-järjestelmien käyttöönottoprojekteihin uskotaan liittyvän erilaisia projektiriskejä, joita tulisi huomioida käyttöönottopäätöksessä. Tämän takia tässä tutkimuksessa Benlianin ja Hessin (2011) viitekehystä laajennetaan myös kuudennella riskikategorialla, joka on projektiriskit.

3.3 Riskienhallinta

Sen jälkeen, kun riskit on tunnistettu, tulee ne arvioida sekä pohtia mitä ja miten riskejä tulee käsitellä (Wheeler, 2011, s. 53). Tehdessä riskejä sisältäviä päätöksiä on hyvä pohtia lopputulosta, sillä se auttaa ymmärtämään haluttuja tavoitteita ja päätökseen liittyviä preferenssejä. On kuitenkin tärkeää muistaa, että päätökset tehdään ennen kuin pystytään analysoimaan lopputulosta, joten päätöksiin liittyy aina epävarmuutta. (Aven, 2012, s. 113.) Riskienhallinnan keskeisimpänä sääntönä toimiikin se, että kaikkea riskiä ei ole mahdollista, eikä tarvitsekaan, poistaa kokonaan (Wheeler, 2011, s. 53).

Riskienhallintaan liittyvässä kirjallisuudessa on neljä yleistä tapaa riskien käsittelyyn: hyväksyminen, pienentäminen, välttäminen ja siirtäminen (Firoiu, 2015; Wheeler, 2011, s. 53-54). Kuviossa 4 on kuvattuna edellä mainitut riskin käsittelyn neljä tapaa sekä riskinkäsittelyn prosessi yhdistämällä Firoiun (2015) sekä Wheelerin (2011, s. 53-54) teoksia.



Kuvio 4 Riskinkäsittelyn prosessi (mukaellen (Firoiu, 2015; Wheeler, 2011, s. 53–54))

Kuten kuviosta 4 nähdään, riskit tulee ensin tunnistaa, analysoida ja arvioida, minkä jälkeen olennaiset riskit voidaan ottaa tarkempaan käsittelyyn (Firoiu, 2015; Wheeler, 2011, s. 53). Riskien käsittelyyn on yleisesti neljä erilaista tapaa, joita organisaatiot voivat käyttää riskienhallinnassa (Firoiu, 2015; Wheeler, 2011, s. 54). Yhtenä tapana on riskin hyväksyminen, jolla tarkoitetaan tilannetta, jossa tietty riski hyväksytään (Firoiu, 2015; Wheeler, 2011, s. 54), sillä se on organisaation määrittelemän riskinsietokyvyn rajojen sisällä (Firoiu, 2015). Jos riski puolestaan ylittää organisaation riskinsietokyvyn, voidaan riskiä pyrkiä pienentämään (Firoiu, 2015). Riskin pienentäminen tapahtuu käyttämällä sopivia metodeja riskin ja sen vaikutuksen pienentämiseksi organisaation riskinsietokyvyn hyväksymälle tasolle (Firoiu, 2015; Wheeler, 2011, s. 56).

Riskiä voidaan myös siirtää (Firoiu, 2015; Wheeler, 2011, s. 54). Tällä tarkoitetaan vastuun tai velvollisuuden siirtämistä toiselle osapuolelle (Firoiu, 2015; Wheeler, 2011, s. 54), tai riskin jakamista jonkun toisen kanssa (Firoiu, 2015). Riskien jakaminen tuo kuitenkin usein mukanaan uusia riskejä, ja kyseinen toiminta saattaa muokata myös jo aiemmin tunnistettuja riskejä (Firoiu, 2015). Neljäntenä on riskin välttäminen, jolla tarkoitetaan tietyn osa-alueen tai prosessin poistamista (Firoiu, 2015; Wheeler, 2011, s. 54), tai jopa koko riskiä tuottavan toiminnan välttämistä (Wheeler, 2011, s. 54). Esimerkiksi luonnonkatastrofien aiheuttamien riskien takia, datakeskukset voitaisiin sijoittaa kokonaan vähäriskisemmälle tai paremmin kontrolloidulle alueelle (Firoiu, 2015). Jos tunnistettua riskiä ei voida muilla keinoin järkevästi hallita, voidaan välttää koko riskiä tuottavaa toimintaa (Wheeler, 2011, s. 53–54).

Riskisuunnitelmia tehdessä ja riskien käsittelystä päätettäessä on tärkeää ymmärtää riskienhallinnan toimenpiteiden kustannuksia. Näitä kustannuksia voivat olla muun muassa rahalliset kustannukset, tukiresurssit, koulutukset tai toiminnan tehokkuuden pieneneminen monimutkaisuuden lisääntymisen tai suorituskyvyn pienenemisen myötä. Riskienhallinnan vaihtoehtoiskustannusten takia ei ole kannattavaa lähteä pienentämään kaikkia riskejä, tai ainakaan yrittää poistaa niitä kokonaan. Riskienhallinnan toimenpiteiden kustannukset saattavat jopa ylittää toimenpiteistä saatavat hyödyt tai riskin kohteena olevan asian kustannukset. (Wheeler, 2011 s 53–54.) Kuviossa 4 on katkoviivallisin nuolin yhdistetty riskin käsittelyn toimenpiteisiin liittyvät riskien kustannukset ja hyödyt, sillä ne vaikuttavat riskienhallinnan toimenpiteisiin.

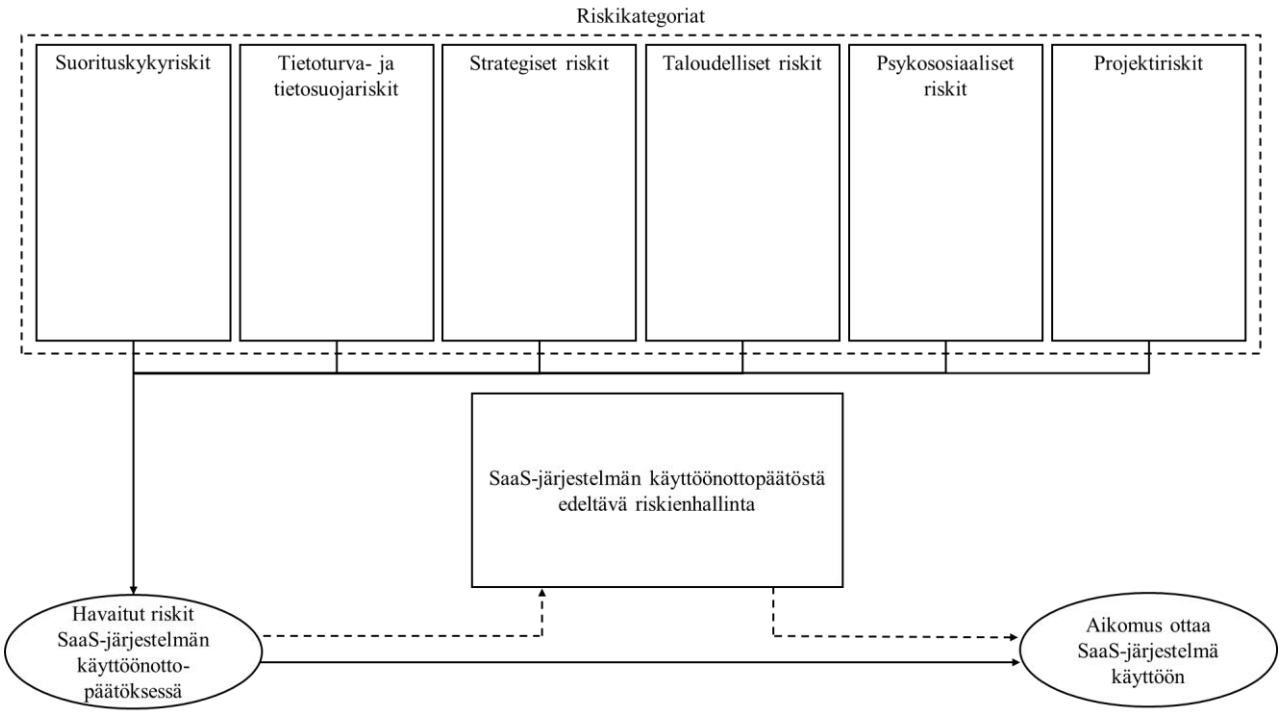
Riskin käsittelyn jälkeen tulee arvioida jäljelle jäävän jäännösriskin määrää ja verrata sitä organisaation riskinsietokyvyn tasoon. Jos riskin käsittely on organisaation mielestä riittävää, voidaan riski hyväksyä. Muussa tapauksessa voidaan pyrkiä tekemään muita toimenpiteitä, tai päättää välttää koko riskiä. (Firoiu, 2015; Wheeler, 2011, s. 53–54.)

Lisäksi järjestelmäinvestoinnin hylkäämisen riskiä pohdittaessa, johdon tulisi valita jokin selkeä mittari investoinnin lopulliselle arvolle (Clemons & Weber, 1990). Mittarin valitseminen on kuitenkin haastavaa erityisesti silloin, kun järjestelmillä on myös strategista vaikuttavuutta (Clemons & Weber, 1990). Strategisina mittareina voidaan käyttää esimerkiksi markkinaosuutta, alentuneita kustannuksia, uusia markkina-alueita tai liiketoiminnan kasvua. Investointiriskiä ei tulisi verrata vallitsevaan tilanteeseen, vaan tulevaisuuden liiketoimintaympäristöön, jossa kilpailijat ottavat uuden teknologian käyttöön onnistuneesti. Investointipäätös silloinkin, vaikka investoinnilla olisikin laskennallisesti negatiivinen nettonykyarvo, voi olla parempi vaihtoehto kuin organisaation tulevaisuus, jossa investointia ei tehty ollenkaan. (Clemons & Weber, 1990.)

4 Metodologia

4.1 Tutkimuksen viitekehys

Tutkimuksessa käytetään projektiriskeillä, tietosuojariskeillä ja monipuolisemmilla psykososiaalisilla riskeillä laajennettua Benlianin ja Hessin (2011) SaaS-järjestelmän käyttöönottopäätökseen liittyvää havaittujen riskien -viitekehystä. Tämän lisäksi viitekehykseen yhdistetään riskienhallintasuunnitelmat. Riskienhallintasuunnitelmien suhdetta käyttöönottoon ei tarkkaan tiedetä ennen empirian keräystä, minkä takia riskienhallintasuunnitelmat yhdistyvät riskeihin katkoviivallisin nuolin kuviossa 5. Tutkimuksen tavoitteena on selvittää, millaisia SaaS-järjestelmien käyttöönottopäätöksiin vaikuttavia riskejä Suomessa toimivissa suurissa organisaatioissa havaitaan ja asettaa ne tämän tutkimuksen teoreettisen viitekehyksen riskikategorioiden alle. Tämän lisäksi tavoitteena on selvittää, millaista riskienhallintaa Suomessa toimivat suuret organisaatiot tekevät ennen SaaS-järjestelmän käyttöönottopäätöstä, ja koetaanko käyttöönottopäätöstä edeltävällä riskienhallinnalla olevan vaikutusta SaaS-järjestelmän käyttöönottopäätökseen.



Kuvio 5 Tutkimuksen viitekehys (mukaellen (Benlian & Hess, 2011))

Pilvipalvelujen hankintaan liittyvän tutkimuksen on kirjallisuudessa tunnistettu olevan melko niukkaa (Schneider & Sunyaev, 2016), minkä takia tässä tutkimuksessa SaaS-järjestelmän

käyttöönottopäätökseen liittyvistä riskeistä sekä käyttöönottopäätöstä edeltävästä riskienhallinnasta pyritään tuomaan uudenlaista ymmärrystä käyttäen laajennuttua ja muokattua viitekehystä. Tämä tutkimus toteutetaan laadullisena puolistrukturoituna haastattelututkimuksena ymmärryksen lisäämiseksi, ja empiirinen aineisto kohdistetaan Suomessa toimiviin suuriin organisaatioihin. Laadullinen tutkimusote sopii erityisesti tutkimuksiin, joissa tutkittavasta kohteesta on verrattain vähän aikaisempaa tutkimusta (Eriksson & Kovalainen, 2008, s. 5). Laadullinen liiketoimintatutkimus tuottaa tietoa siitä, miten ja miksi ihmiset ja asiat toimivat oikeassa elämässä jollakin tietyllä tavalla, ja miten tämän asian voi ymmärtää muuttaakseen asiaa parempaan suuntaan (Eriksson & Kovalainen, 2016, s. 3).

4.2 Aineiston kerääminen ja analysointi

Aineisto kerättiin käyttäen puolistrukturoituja haastatteluita. Haastattelut suoritettiin helmikuun ja maaliskuun aikana vuonna 2025. Puolistrukturoidut haastattelut mahdollistavat kohdistettujen haastatteluiden pitämisen, joissa on kuitenkin mahdollista tutkia myös vapaamuotoisempia olennaisia seikkoja tutkittavaan asiaan liittyen (Adeoye-Olatunde & Olenik, 2021). Puolistrukturoiduista haastatteluista saadaan systemaattista ja ymmärrettävää materiaalia pitäen samalla haastattelutilanteen keskustelunomaisena ja epävirallisena (Eriksson & Kovalainen, 2016, s. 94). Haastattelujen etuna voidaan pitää myös sitä, että haastateltaviksi voidaan tietoisesti valita henkilöt, joilla on kokemusta tutkimusaiheesta tai ilmiöstä (Tuomi & Sarajärvi, 2018, s. 86). Puolistrukturoiduissa haastatteluissa pyritään löytämään merkityksellisiä vastauksia käyttäen etukäteen valittuja haastatteluteemoja, jotka perustuvat tutkimuksen viitekehykseen, eli aikaisempaan tutkimustietoon tutkittavasta ilmiöstä (Tuomi & Sarajärvi, 2018, s. 88). Tässäkin tutkimuksessa haastattelurungon ja -teemojen pohjana toimi tutkimuksen viitekehys.

Haastateltavina toimivat organisaatioiden SaaS-järjestelmien käyttöönottopäätöksissä mukana olleet henkilöt, joihin valittiin useita Suomessa toimivien suurten organisaatioiden ylimmän tason IT-johtajia, kuten tietohallintojohtajia. Haastatteluihin valittiin myös joitain toiminnanomistajia, liiketoiminnan edustajia sekä tietoturva-asiantuntijoita, jotta saataisiin laajempi kuva ilmiöstä, sekä nähtäisiin asiaa myös korkeimman tason IT-johdon ulkopuolelta. Haastateltavat valittiin tietoisesti olemalla heihin suoraan yhteydessä sähköpostitse tai LinkedIn-alustan kautta. Tämän lisäksi tässä työssä käytettiin lumipallo-otantaa haastateltavien valikoinnissa. Lumipallo-otannalla tarkoitetaan sitä, että tutkija tietää jonkin avainhenkilön, joka johdattaa hänet toisen tiedonantajan luokse (Tuomi & Sarajärvi, 2018, s. 99). Avainhenkilö toimii täten linkkinä tutkijoiden ja uusien tiedonantajien välillä (Tuomi & Sarajärvi, 2018, s. 99). Tässä tutkimuksessa osa haastateltavista valikoitui

lumipallo-otannan avulla, sillä haastattelutilanteen päätteeksi haastateltavalta, eli avainhenkilöltä, tiedusteltiin muita henkilöitä, joilla on tietoa tutkimusaiheesta.

Haastattelut toteutettiin, joko paikan päällä kasvotusten tai etänä käyttäen Microsoftin Teams-alustaa. Lähes kaikki haastattelut olivat yksilöhaastatteluita lukuun ottamatta yhtä haastattelua, johon osallistui kaksi henkilöä samanaikaisesti. Tämän lisäksi yksi haastattelijoista vastasi haastatteluun kirjallisesti sähköpostilla hänen omasta pyynnöstään. Kaikilta haastateltavilta pyydettiin suostumus haastattelujen tallentamiseen, haastattelusisällön anonyymiin käsittelyyn ja vastausten julkaisemiseen osana tätä tutkimusta. Haastattelun vapaaehtoisuudesta, tallentamisesta sekä anonymiteetista kerrottiin haastateltaville alustavan kirjallisen kutsun lisäksi myös haastattelutilanteessa ennen tallentamisen aloittamista. Tällä varmistuttiin siitä, että jokainen haastateltava oli tietoinen tutkimuseettisyydestä ja sen toteutumisesta osana tätä tutkimusta.

Taulukko 1 Tiedot haastateltavista

Haastateltava	Haastattelun päivämäärä	Toimiala	Tehtävänimike	Rooli päätöksenteossa	Haastattelun kesto
H1	4.2.2025	Terveys- ja hyvinvointiala	Tietohallinto-johtaja	Päättävä	58min
H2	12.2.2025	Elintarvikeala	IT-johtaja	Päättävä	35min
H3	13.2.2025	Perintä- ja luottotieto-palvelut	IT-johtaja	Päättävä	60min
H4	13.2.2025	Terveys- ja hyvinvointiala	Ohjelmajohtaja	Tukeva	1h 14min
H5	14.2.2025	Lääketeollisuus	Digitalisaatio-portfolion johtaja	Päättävä	46min
H6	18.2.2025	Konsultointi	Projektijohtaja	Tukeva	45min
H7	18.2.2025	Valmistus/ logistiikka	Tietohallinnon muutosjohtaja	Tukeva	38min
H8	21.2.2025	Terveys- ja hyvinvointiala	Tietohallinto-johtaja	Päättävä / Tukeva	59min
H9	24.2.2025	Teknologia-teollisuus	Tietohallinto-johtaja	Päättävä	(Kirjallinen)
H10	24.2.2025	Bioteknologia	Globaali IT-johtaja	Päättävä / Tukeva	51min

H11	24.2.2025	Bioteknologia	IT Compliance -johtaja	Tukeva	51min
H12	24.2.2025	Valmistava teollisuus	Tietohallinto-johtaja	Tukeva	1h 9min
H13	27.2.2025	Elintarvikeala	Digijohtaja	Tukeva	51min
H14	5.3.2025	Finanssi	Kokonaisarkki-tehtuurijohtaja	Tukeva	59min

Tässä tutkimuksessa haastateltiin 14 henkilöä keskittyen pääasiassa tietohallinnon sekä IT-toiminnon johtohenkilöihin. Kaikilla haastateltavilla oli kokemusta useammasta SaaS-järjestelmän käyttöönotosta ja monet haastateltavista olivat toimineet pitkään vastaavanlaisissa tehtävissä, mikä lisää heidän asiantuntemustaan vastaajina. Kun puhutaan aineiston riittävyydestä, puhutaan usein aineiston saturaatiosta, eli kyllääntymisestä (Tuomi & Sarajärvi, 2018, s. 99). Kyllääntymisellä tarkoitetaan tilannetta, jossa aineisto alkaa toistaa itseään, eivätkä tiedonantajat tuota enää tutkimuskysymysten kannalta olennaista uutta tietoa. Voidaan ajatella, että aineiston määrä täten riittää tuomaan esiin teoreettisen peruskuvion tutkimuskohteesta. (Tuomi & Sarajärvi, 2018, s. 99.) Vaikka kokemukset kyllääntymispisteestä ovat vaihtelevia, aikaisemman tutkimuksen perusteella kyllääntymispiste voidaan saavuttaa usein noin 15 vastauksella (Tuomi & Sarajärvi, 2018, s. 99), minkä takia tässäkin tutkimuksessa pyrittiin seuraamaan saturaatiopisteen saavuttamista sekä haastattelemaan noin 15 asiantuntevaa henkilöä.

Haastateltavien organisaatioissa IT-osaston johtajaa saatettiin kutsua joko tietohallintojohtajaksi tai IT-johtajaksi. Haastateltavaksi valittiin useampi lopullisen käyttöönottopäätöksen tekijä sekä myös päätöstä tukevia henkilöitä, joilla kaikilla oli selkeä kuva käyttöönottopäätösprosessista ja käyttöönottopäätöstä edeltävästä riskienhallinnasta. Useammalla haastateltavalla oli myös kokemusta useammasta eri päätöksentekoroolista SaaS-järjestelmien käyttöönottopäätöksien kontekstissa.

Taulukko 2 Tiedot organisaatioista

Organisaatio	Haastateltavien määrä	Toimiala	Henkilöstömäärä	Koko	Yksityinen / Julkinen
O1	1	Elintarvikeala	250–1 000	Suuri	Yksityinen
O2	1	Perintä- ja luottotietopalvelut	250–1 000	Suuri	Yksityinen
O3	1	Lääketeollisuus	1 000–5 000	Suuri	Yksityinen

O4	1	Valmistus /logistiikka	Yli 10 000	Suuri	Yksityinen
O5	1	Teknologiateollisuus	250–1 000	Suuri	Yksityinen
O6	2	Bioteknologia	Yli 10 000	Suuri	Yksityinen
O7	1	Valmistava teollisuus	250–1 000	Suuri	Yksityinen
O8	1	Elintarvikeala	5 000–10 000	Suuri	Yksityinen
O9	1	Finanssi	Yli 10 000	Suuri	Yksityinen
O10	1	Konsultointi	0–250	Pieni	Yksityinen
O11	2	Hyvinvointiala	Yli 10 000	Suuri	Julkinen
O12	1	Hyvinvointiala	Yli 10 000	Suuri	Julkinen

Haastateltavia oli useammalta eri toimialalta ja heitä tarkoituksenmukaisesti valikoitiin sekä julkisista organisaatioista, että yksityisistä yrityksistä, jotta saataisiin parempi kokonaiskuva tutkittavasta aiheesta. Kokonaisuudessaan haastateltiin henkilöitä 12 eri organisaatiosta. Suurimmassa osassa organisaatioita haastateltavina toimi yksi henkilö, lukuun ottamatta organisaatioita O6 ja O11, joissa haastateltavina oli kaksi henkilöä. Tämän lisäksi kaikki organisaatiot olivat suuria organisaatioita, lukuun ottamatta organisaatiota O10, joka oli konsulttiyritys. Konsulttiyrityksen O10 asiakkaina toimivat usein kuitenkin suuret organisaatiot, joten haastateltavalla oli hyvää kokemusta monesta suuresta organisaatiosta, joiden asiakasprojekteissa hän oli ollut mukana. H6, joka työskentelee organisaatiossa O10 mainitseekin mittaavansa organisaation kokoa enemmänkin asiakasorganisaation koon perusteella:

> ”Konsulttiyritys on semmoinen vajaa [x-kymmentä] ihmistä. Käytännössähän mä teen asiakasprojekteja koko aika, niin mä yleensä mittaan sitä mikä on se organisaatio, missä mä nyt oon. Sanotaan, että mä katson, että mä saan palkkani hieman eri kautta kuin muut siinä asiakasorganisaatiossa tekevät työntekijät. Mut mä olen yksi työntekijä heidän muiden osalla. Heillä on palkollisia ja heillä on konsultteja sun muita siellä sitten tekemässä samoja projekteja. Ja asiakasorganisaatio on iso pörssiyhtiö, niin siinä puhutaan sitten hyvin monista tuhansista [henkilöistä]. ” – H6

Haastattelut tallennettiin haastattelutilanteessa, joko käyttäen älypuhelinta tai Microsoft Teams-alustan ”Tallenna”-toimintoa. Haastattelut tallennettiin suojattuun tietokantaan, joka tässä tutkimuksessa oli Microsoft OneDrive. Haastatteluiden jälkeen haastattelut tarkastettiin virheiden varalta ja litteroitiin käyttäen apuna Turun Yliopiston UTU Transcribe -palvelua sekä Microsoft Wordin litterointityökalua.

Tämän tutkimuksen empiirisen aineiston analysointiin käytetään laadullista deduktiivis-induktiivista sisällönanalyysiä, sillä koodaamisessa hyödynnetään tutkimuksessa luotua teoreettista viitekehystä. Havaittujen riskien analysoinnissa keskeiset nostot haastateltavien vastauksista jaotellaan teoreettisen viitekehyksen sisältämiin riskikategorioihin, minkä jälkeen analyysissä edetään pelkistettyjen ilmausten muodostamisen jälkeen uusien alaluokkien laatimiseen. Täten tässä tutkimuksessa pystytään vastaamaan ensimmäiseen tutkimuskysymykseen keskeisistä havaituista riskeistä. SaaS-järjestelmien käyttöönottopäätöstä edeltävän riskienhallinnan kohdalla hyödynnetään puolestaan aineistolähtöistä, eli induktiivista, lähestymistapaa, sillä käyttöönottopäätöstä edeltävästä riskienhallinnasta on tehty verrattain vähän tutkimusta tässä kontekstissa, eikä teoriapohja ole riittävän laaja deduktiivisen lähestymistavan tehokkaaseen käyttöön.

Sisällönanalyysi koostuu kolmesta vaiheesta, jotka ovat valmistelu-, analyysi- ja raportointivaihe (Elo ym., 2022). Valmisteluvaiheessa valitaan ensin analyysiyksikkö, jonka perusteella aineistoa analysoidaan (Graneheim & Lundman, 2004). Tämän jälkeen aineistoon tulee perehtyä huolellisesti. Analyysivaiheessa deduktiivisen analyysin kohdalla muodostetaan analyysimatriisi, joka perustuu aikaisempaan tutkimukseen, malliin tai tietoon. Tämän lisäksi haastattelut pelkistetään ja koodataan, minkä jälkeen matriisiin poimitaan aineistosta poimitut pelkistetyt ilmaukset, jotka kuuluvat analyysimatriisin luokkiin. (Elo ym., 2022.)

Tässä tutkimuksessa analyysimatriisin muodostamiseen hyödynnetään tutkimuksessa aiemmin muodostettua teoreettista viitekehystä, ja täten analyysimatriisin luokittelu muodostetaan viitekehyksen riskikategorioiden avulla. Jos jokin asia ei liity suoraan mihinkään analyysimatriisin luokkaan, mutta vastaa tutkimuskysymykseen, kerätään ne omaksi listakseen ja tehdään niille luokittelu aineistolähtöisesti (Elo ym., 2022). Laadullisen sisällönanalyysin raportointivaiheessa löydökset raportoidaan kategorialuokittelun mukaisesti. Analyysin etenemisen kuvaamiseksi tutkimukseen sisällytetään usein myös taulukko tai kuvio, jossa luokittelu esitetään (Elo & Kyngäs, 2008). Tämä vahvistaa analyysin luotettavuutta osoittamalla lukijalle, että tuloksiin on päästy analyysin, eikä tekijöiden omien sattumanvaraisten tulkintojen perusteella (Elo ym., 2014). Tässä tutkimuksessa analyysien etenemisestä ja muodostamisesta luodaan prosessia havainnollistavat taulukot, jotka liitetään tutkimukseen liitetiedostoina.

Laadullisen sisällönanalyysin raportoinnissa tulosten yhteys alkuperäisaineistoon esitetään käyttäen autenttisia lainauksia. Näiden alkuperäisten lainausten esittäminen lisää tutkimuksen luotettavuutta sekä tulkinnan uskottavuutta. (Elo ym., 2014; Kyngäs ym., 2011.) Tämän lisäksi saavutettuja tuloksia verrataan aikaisempien tutkimusten tuloksiin (Elo ym., 2022).

Siinä, missä tämän tutkimuksen teorialähtöisessä laadullisessa sisällönanalyysissä teoreettisen viitekehyksen riskikategorioista edetään uusien alaluokkien muodostamiseen, aineistolähtöisessä analyysissa analyysimatriisin luokittelu tehdään täysin empirialähtöisesti. Aineistolähtöisessä laadullisessa sisällönanalyysissä aineisto ensin redusoidaan, eli pelkistetään, minkä jälkeen edetään aineiston klusterointiin, eli ryhmittelyyn (Tuomi & Sarajärvi, 2018, s. 122). Viimeisenä analyysin vaiheena on aineiston abstrahointi, eli teoreettisten käsitteiden muodostaminen (Tuomi & Sarajärvi, 2018, s. 122). Abstrahointia jatketaan yhdistelemällä luokituksia niin kauan, kuin se on sisällön kannalta mahdollista ja olennaista (Tuomi & Sarajärvi, 2018, s. 125). Täten tässä tutkimuksessa saadaan muodostettua SaaS-järjestelmän käyttöönottopäätöstä edeltävän riskienhallinnan analyysitaulukon yläkäsitteet, sekä pystytään vastaamaan tutkimuksen toiseen tutkimuskysymykseen käyttöönottopäätöstä edeltävästä riskienhallinnasta.

Toisin sanoen voidaan todeta, että tämä tutkimus tehdään käyttäen abduktiivista lähestymistapaa. Abduktiivisella lähestymistavalla tarkoitetaan teoriaohjaavaa lähestymistapaa, jossa yhdistetään teoria- ja aineistolähtöisiä lähestymistapoja. Analyysissä tunnistetaan aikaisemman tiedon merkitys ja sen vaikutus tutkimukseen, mutta analyysin tehtävä ei ole ainoastaan testata teoriaa, vaan syventää teoriaa avaamalla siihen uusia ulottuvuuksia. (Tuomi & Sarajärvi, 2018, s. 109.) Tämän tutkimuksen tukena käytetään aikaisemman kirjallisuuden pohjalta luotua laajennettua viitekehystä, joka ohjaa tutkimuksen analyysiä ja haastatteluja. Tutkimuksen analyysissä yhdistyy kuitenkin sekä teoria- että aineistolähtöiset lähestymistavat. Teorian syventämiseksi ja ymmärryksen lisäämiseksi haastateltavien oma ääni on keskeisessä osassa. Aineistolähtöinen analyysi johtaa tässä työssä myös uuden kirjallisuuden lukemiseen, jotta ilmiötä voidaan ymmärtää paremmin.

4.3 Tutkimuksen laadukkuus, luotettavuus ja eettisyys

Tutkimuksen luotettavuutta mitataan yleisesti reliabiliteetin ja validiteetin kautta (Hirsjärvi ym., 2007, s. 226-228), minkä takia tässäkin tutkimuksessa pyritään pitämään nämä molemmat korkealla tasolla luotettavuuden maksimoimiseksi. Käsitteet reliabiliteetti ja validiteetti ovat kuitenkin saaneet osakseen kritiikkiä laadullisen tutkimuksen piirissä, sillä ne ovat syntyneet määrällisessä tutkimuksessa ja vastaavat erityisesti sen tarpeisiin (Tuomi & Sarajärvi, 2018, s. 160).

Laadullisen tutkimuksen luotettavuuden kriteereiksi on ehdotettu uskottavuutta (engl. credibility), siirrettävyyttä (engl. transferability), riippuvuutta (engl. dependability) ja vahvistettavuutta (engl. confirmability) (Tuomi & Sarajärvi, 2018, s. 162). Uskottavuudella tarkoitetaan sitä, vastaavatko tutkijan tulkinnat vastaajien näkemyksiä (Nowell ym., 2017). Yksi tapa kasvattaa uskottavuutta ja validiteettia laadullisessa tutkimuksessa on triangulaatio (Nowell ym., 2017; Tuomi & Sarajärvi,

2018, s. 167), jolla tarkoitetaan yksinkertaisimmillaan usean tutkimusmetodin, teorian, tiedonlähteen tai tutkijoiden yhdistämistä tutkimuksessa (Tuomi & Sarajärvi, 2018, s. 167). Tässä tutkimuksessa voidaan sanoa, että validiteettia pyritään kasvattamaan usean tutkijan triangulaatiolla, sillä tutkijoita on kaksi, mikä mahdollistaa useamman kuin yhden näkökulman, tulkinnan sekä ajatusmaailman yhdistämisen. Tämän lisäksi luotettavuutta pyritään korostamaan sisällyttämällä tutkimuksen väitteiden tueksi useita laadukkaita lähteitä, joiden laadukkuus on tarkistettu käyttäen hyödyksi Cabells Journalytics -tietokantaa sekä Julkaisufoorumin tietokantaa. Lisäksi tutkimuksen haastattelutilanteissa pyrittiin olemaan mahdollisimman objektiivisia, ja johdattelutilanteita vältettiin laadukkailla haastattelukysymyksillä, ylläpitäen kuitenkin puolistrukturoidun rakenteen.

Tutkimuksen siirrettävyydellä tarkoitetaan tutkimustulosten siirrettävyyttä toiseen tutkimuskontekstin ulkopuoliseen vastaavaan kontekstiin (Tuomi & Sarajärvi, 2018, s. 162). Tutkijat eivät voi etukäteen tietää, mihin konteksteihin tuloksia halutaan myöhemmin siirtää, minkä takia tuloksia tulee kuvata riittävän ymmärrettävästi, jotta toiset pystyvät arvioimaan tulosten siirrettävyyttä omiin konteksteihinsa (Nowell ym., 2017). Tutkimuksen riippuvuudella tarkoitetaan sitä, että tutkimus on toteutettu loogisesti, jäljiteltävästi sekä dokumentoitu selkeästi (Nowell ym., 2017). Toisin sanoen riippuvuudella tarkoitetaan sitä, että tutkimus on toteutettu tieteellisen tutkimuksen toteuttamista ohjaavin periaattein (Tuomi & Sarajärvi, 2018, s. 162). Tässä tutkimuksessa tutkimuksen toteuttamisen vaiheet sekä tutkijoiden valinnat pyritään dokumentoimaan ja perustelemaan selkeästi, jotta tutkimuksen toteuttamisen vaiheet voidaan loogisesti jäljittää. Tämä mahdollistaa lisäksi tulosten siirrettävyyden arvioinnin vastaavanlaisissa prosesseissa ja konteksteissa.

Tutkimuksen vahvistettavuus ilmenee siten, että tutkimuksessa osoitetaan tutkimustulosten yhteys todelliseen aineistoon. Tämä edellyttää sitä, että tutkijat demonstroivat, miten johtopäätöksiin ja tulkintoihin on päädytty. Tämän lisäksi tutkijoiden tulee perustella metodologisten, teoreettisten sekä analyyttisten valintojen syitä läpi tutkimuksen, jotta muut ymmärtävät miten ja miksi valintoihin on päädytty. Tutkijoiden tulee olla refleksiivisiä, eli itsekriittisiä omaa tutkimustaan kohtaan, jotta he ymmärtävät omiin päätöksiinsä vaikuttavat arvot ja muut taustalla piilevät tekijät. (Nowell ym., 2017.) Tässä tutkimuksessa tutkimusaineisto ja tutkimustulokset esitellään selkeästi, minkä lisäksi tutkimustulosten muodostumisen prosessi visualisoidaan analyysitaulukoiksi, jotka liitetään tutkimukseen liitetiedostoina. Lisäksi tulosten ja johtopäätösten muodostumista tuetaan autenttisin lainauksin haastateltavien vastauksista.

Tutkimuksessa kiinnitetään huomiota myös tutkimuksen eettisyyteen. Tutkimuksen eettiset säännöt eivät ole tärkeitä pelkästään oikean ja väärän ymmärtämiseksi, vaan myös siksi, että lähes kaikki tutkimuskysymykset sisältävät joko suoria tai epäsuoria eettisiä aspekteja (Eriksson & Kovalainen, 2016, s. 64). Eettisyys otettiin tässä tutkimuksessa huomioon muun muassa siten, että haastattelut toteutettiin anonyymeinä, jolloin haastateltavien identiteettiä ei voida tunnistaa tutkimuksessa. Haastateltavat osallistuivat tutkimukseen vapaaehtoisesti ja heillä oli halutessaan mahdollisuus jättäytyä pois tutkimuksesta myös alustavan hyväksynnän jälkeen, haastattelutilanteessa tai haastattelutilanteen jälkeen ennen tutkimuksen julkaisua. Haastateltaville kerrottiin tutkimuksen tarkoitus ja heiltä pyydettiin suostumukset haastattelun tallentamiseen sekä haastattelusisällön oikeaoppiseen ja anonyymiin käsittelyyn. Tämän lisäksi haastattelutilanteet ja tutkimus kokonaisuudessaan pyrittiin pitämään mahdollisimman objektiivisena. Myös tutkimuksen sponsoroinnilla voi olla eettisesti negatiivisia seurauksia, jos sponsorointisuhde vaikuttaa tutkimuksen rajaukseen, vääristymien tai ennakkoasenteiden määrään negatiivisesti (Eriksson & Kovalainen, 2016, s. 68). Tässä tutkimuksessa ei ole mukana sponsoria tai muuta rahallista tukea, jolloin tutkimus on myös tältä osin eettinen.

Tekoälyn, eli AI:n kehittymisellä ja yleistymisellä on ollut suuret vaikutukset akateemiseen tutkimukseen, ja sitä on käytetty hyödyksi laadullisessa tutkimuspiirissä monella eri tavalla. Tekoälyn hyödyntäminen tutkimuksessa on nostanut esiin myös useita eettisiä huolia, muun muassa tekoälyn mahdollisiin vääristymiin ja ennakkoasenteisiin liittyen. (Christou, 2023.) Tässä tutkimuksessa on hyödynnetty tekoälyä maltillisesti, sillä sitä on käytetty apuna ainoastaan tutkimusideoiden muodostamiseen ja erilaisten teoreettisten viitekehysten tarkasteluun. Tekoälyn käytössä on huomioitu mahdolliset vääristymät, eikä sitä käytetty tutkimuksen tekstin luomiseen. Tutkimuksen osana on hyödynnetty OpenAI:n ChatGPT:tä sekä Microsoftin CoPilot:ia.

5 Tutkimuksen tulokset

5.1 Suorituskykyriskit

5.1.1 Käytön skaalautuvuus

Useissa haastatteluissa nousee esiin suorituskykyriskinä käytön skaalautuvuus. Haastateltavat mainitsevat muun muassa liiketoimintaan liittyvien kuormitushuippujen aiheuttavan mahdollisia ongelmatilanteita käytettävyydessä. H3 mainitsee loppukäyttäjäpiikkeihin liittyvästä skaalauksesta seuraavaa:

> "Keskeisimmät riskit ovat tietoliikenteen määrässä, eli pystyykö se toimittaja oikeasti skaalaamaan, jos tulee suuria loppukäyttäjäpiikkejä siihen palveluun." – H3

H4 mainitsee riskistä käytön skaalautuvuudessa silloin, kun liiketoiminnassa on päiväkohtaisia tai viikkokohtaisia kuormitushuippuja:

> "Onko semmoista päiväkohtaista tai viikkokohtaista jotain kuormitushuippua. Esimerkiksi nyt meillä täällä meidän alalla maanantaiaamupäivät on kuormitushuippuja. Ihmisiä tulee puhelimessa ja chatissa paljon enemmän sisään, kun mitä perjantai-iltapäivällä. Ihmiset ilmoittavat sairastavansa maanantaiaamusta paljon. Eli onko tämä tämmöistä ajan yli heiluvaa kuormitusta." – H4

Tilanteissa, joissa toiminnan volyymi on odotettua suurempi, saattaa nousta riski siitä, että palveluntarjoajan kapasiteetti ei riitä liiketoiminnan tarpeisiin. H8 ja H9 mainitsevat asiasta seuraavaa:

> ”Joo minun mielestäni voisi ajatella, että ainakin kapasiteettiriski on sellainen, että ei riitä järjestelmän paukut pyörittämään sitä niillä käyttäjämäärillä tai sen toiminnan määrillä mitä on. Jos on sellaisia yhtäaikaisten käyttäjien määrään perustuvia lisenssejä, missä sitten onkin se käytön tarve suurempi, kuin on arvioitu. Tällaisia voi tietenkin olla. Se, että järjestelmän tekninen kapasiteetti ei riitä meidän toimintamme volyymiin on ihan oleellinen riski. Minun mielestäni meidän aikaisemmassa järjestelmässämme laukesi se riski, että järjestelmän kapasiteetti ei sinänsä riittänyt sen meidän volyymimme pyörittämiseen. Tämän tyyppisiä on tunnistettu. Ehkä ne ovat tärkeimmät.” – H8

> ”Palvelun skaalautuvuus; SaaS-järjestelmät toteutetaan lähes poikkeuksetta nykyään teknologioilla, joissa tietoja lähetetään ja sitten odotetaan vastauksia. Asiakkaalla ei välttämättä ole mahdollisuuksia vaikuttaa myöskään palveluiden mitoituksiin.” – H9

Haastateltavien vastauksissa skaalautuvuuteen liitetään riski, sillä liiketoiminnan volyymien vaihtelut saattavat johtaa tilanteeseen, jossa palveluntarjoaja ei pysty skaalaamaan palvelua sopivalla tavalla. Tämä aiheuttaa usean haastateltavan mukaan riskiä suorituskyvyssä, mikä puolestaan saattaa johtaa ongelmatilanteisiin organisaation toiminnassa.

5.1.2 Palvelun saatavuus ja käytettävyys

Usea haastateltava mainitsee verkon nopeuden ja latenssin aiheuttavan mahdollisia ongelmia käytettävyyteen. H2 ja H14 mainitsevat asiasta seuraavaa:

> "No kyllä se on se käytön hitaus varmasti ollut. Ehkä sitten kokonaan se saatavuuskin, että jos se on pois päältä emmekä me voi tehdä asialle mitään. Kyllä se aika pitkälle kulminoituu siihen, että on hidas käyttää." – H2

> ”…mutta olen kyllä nähnyt siis sellaisia, mihin nämä on realisoitunutkin tämän tyyppiset riskit. Vaikkapa vasteaika ei ole halutunlainen tai muuta. Ja sitten se näkyy siinä toiminnassa ja tietysti aiheuttaa erilaisia haasteita.” – H14

Vaikka usea haastateltava tunnistaa verkon nopeuden ja latenssin olevan keskeisiä suorituskykyyn liittyviä riskejä, lähes jokainen riskin tunnistaneista mainitsee verkon nopeuteen ja latenssiin liittyvän riskin pienentyneen ajan saatossa, jolloin ne eivät ole nykypäivänä samassa määrin ongelma kuin ennen. Verkon nopeuteen ja latenssiin liittyviä asioita on pystytty tunnistamaan ja hallitsemaan paremmin. Osa haastateltavista mainitsee verkon nopeuden kasvun sekä suurten datakeskusten perustamisen Suomeen vaikuttaneen suorituskykyriskien pienentymiseen. H6 ja H2 mainitsevat asiasta seuraavaa:

> "Niin onko esimerkiksi verkon nopeus riittävä, jotta pystytään toimimaan sen kanssa? Kun aikaisemmin on ollut paikallisia sovelluksia ja serverit on esimerkiksi samalla mantereella tai samassa maassa. Niin on ihan tästä nykyisestä hankkeesta ja itse asiassa muutamasta aikaisemmastakin. Niin mikä on siis sanotaan latenssi, jos meillä pyörii ”pannut” vaikka Dublinissa, mutta käyttäjät ovat vaikka Australiassa. Niitä on joutunut sitten perkaamaan. Loppujen lopuksi ne on sitten aika hyvin pystytty ”mitigoimaan”, koska puhutaan kuitenkin tällaisista globaaleista ratkaisuista." – H6

> ”Aikaisemmin suorituskykyriski oli aika merkittävä, kun hankittiin SaaS-sovelluksia, mutta kun konesalit tuodaan Suomeen ja meillä on täällä isojen toimittajien ja pienempienkin toimittajien konesaleja, niin suorituskykyriski on laskenut ihan viime vuosien aikana merkittävästi, kun on tullut tänne Suomeen konesaleja ja muuta. Se on ehkä huomionarvoinen asia liittyen noihin, että se oli aikaisemmin enemmän ainakin mulla huolenaiheena.” – H2

H1 mainitsee julkiverkkojen toimivan joissain tilanteissa jopa paremmin kuin omien sisäverkkojen:

> ”Yllättävän hyvin julkiverkon yli jopa ajetaan SaaS-palveluita, että latenssi, suorituskyky ja verkon nopeus ei tunnu meillä olevan se ongelma. Meillä saattaa jopa oma sisäverkko olla välillä hitaampi tietyissä paikoissa, että suorituskyky verkon nopeuden kannalta harvoin on tänä päivänä enää ongelma.” – H1

Verkon nopeuden ja latenssin tunnistetaan olevan keskeisiä asioita käytettävyydessä, vaikkakin usea haastattelija mainitsee niiden aiheuttavan nykypäivänä melko vähän huolta. H4 mainitsee, ettei suorituskykyriskit hänen mukaansa eroa nykypäivänä on-premisen ja SaaS:in välillä:

> ”Nykyäänhän kuitenkin käytännössä katsoen kaikki asiat tapahtuu internetissä tai internet-protokollalla. On se SaaS tai on-premise, mutta ei oikein kellään enää ole edes semmoista on-premisea. Harvalla on omaa konesalia. Vaikka se olisi periaatteessa on-premise, niin se on sitten kuitenkin jonkun toisen salissa ja sinne mennään internetin yli. Tietysti ihan pienet yritykset, joilla voi olla oma palvelin jossain siivouskaapissa siellä moppien joukossa, niin sitäkin nähdään edelleen. Niin heillä voi semmoista on-premisea olla. Suorituskykyriskeissä tietysti ne ei täten kovasti eroa toisistaan.” – H4

Toisena palvelun saatavuuteen ja käytettävyyteen liittyvänä tekijänä haastateltavat kokivat palvelun lokaation ja koon. H1 mainitsee lokaation ja koon olevan tärkeitä, sillä on tärkeää ymmärtää, pystyykö palveluntarjoaja pitämään palvelun toiminnassa:

> "Se datan sijainti on meille ehkä tärkeämpää ja sitten se, että pystyykö ne pitämään sen pystyssä. Meillä on niitä pieniä hallinnonsovelluksia, että ne saattavat olla teoriassa ainakin jossain melkein sen firman omassa konesalissa, jossain komerossa, ja me halutaan yleensä aina ymmärtää, että missä se on. Tämä liittyy sitten just siihen, että pystyykö ne pitämään sen pystyssä" – H1

Samoin H5 mainitsee palveluntarjoajan koon vaikuttavan palvelun saatavuuteen ja käytettävyyteen siten, että mieluummin valitaan isompi palveluntarjoaja riskien pienentämiseksi:

> ”Jos muistatte muutamia vuosia sitten Ranskassa paloi yksi konesali ja siinähän kävi niin, että niillä ei edes ”synkka” toiminut oikein, eli ne ”backupit” ei ollutkaan siellä heidän "secondary” lokaatiossa ja asiakkaalta ruvettiin kysymään "backuppeja". En kuolemaksenikaan muista, että mikä sen putiikin nimi oli, mutta ”anyways” se oli semmoinen toimija, joka olisi nimenomaan juuri täällä konesalissa. Me todettiin, että ”kiitos vaan, mutta tää ei näytä hyvältä”. Meidän tässä alkuvaiheessa tehdään niin paljon sitä valmistelevaa työtä, että … se meidän valintamme tapahtuu siellä valintavaiheessa eikä sitten enää käyttöönottoaikana. Eli siinä kohtaa, kun me lähdetään siihen projektiin, niin meillä on aina niin hyvät taustatiedot ja edellytykset, että meillä ei käyttöönottoajalla ole mitään riskiä, jota me ruvettaisiin miettimään. Me siis vuosia sitten opittiin, että meidän kannattaa valita, mikäli se on vain muuten järkevää, toimittaja, joka toimii näissä isoissa pilvipalveluissa. Koska sitten kun mennään jonnekin AWS:ään ja Microsoftiin, niin niillä ei ole varaa ”sössiä” sitä hommaa. Se on ”too big to fail”.” – H5

H12 mainitsee lisäksi, että vaikka verkon nopeudesta ja latenssiasioista puhutaan usein suorituskykyriskien kohdalla, tärkeintä on kuitenkin, että palvelu on käytettävissä ja saatavilla:

> ”…aika usein sitten, kun saadaan tämmöinen pilvikonsultti, niin se alkaa aina höpöttelemään latenssista: “Katsokaas pojat, että tämä latenssi ja latenssi”. Mutta se tärkein asia on se, että hitaallakin yhteydellä vielä pärjää, mutta jos ei se toimi ollenkaan, niin se on rankka juttu. Ja tämä on ehkä sellainen, minkä halusin nostaa, että suorituskyky ja toiminnan jatkuvuus. Lisäksi nimenomaan ehkä sellainen, mikä on yksi tärkeimpiä, eli

> miten varmistetaan, että karrikoiden sanottuna se viimeisinkin käyttäjä saa sen palvelun sieltä, voisiko käyttää termiä ”riittävällä tasolla”.” – H12

5.1.3 Järjestelmien integraatio

Haastateltavien vastauksista nousee esiin suorituskykyriski liittyen järjestelmien integraatioon. Vastauksista käy ilmi, että SaaS-järjestelmien integraatio organisaation olemassa oleviin järjestelmiin sekä osaksi organisaation kokonaisarkkitehtuuria saattaa aiheuttaa ongelmia ja monimutkaisuutta organisaation toiminnassa. Haastateltavat H2 ja H14 mainitsevat asiasta seuraavaa:

> "Ja yksi varmaan semmoinen mikä tuli niin noi integraatiot on aina semmoinen ikuinen juttu, että kun SaaS-järjestelmien käyttöönottoa ja riskejä mietitään niin varmasti se, että saadaanko ne SaaS-järjestelmät integroitua meidän olemassa oleviin SaaS-järjestelmiin taikka meidän on-premise -järjestelmiin. Se on ehkä semmoinen mikä on nyt tullut tapetille näitten SaaSien myötä, että onko siellä näitä API:ja ja muita riittävästi." – H2

> "Sitten otetaan toinen ääripää, otetaan joku liiketoimintaprosessin osaa tai kokonaista prosessia tuottava SaaS-järjestelmäkokonaisuus, joka pitää integroida vaikkapa meidän organisaation kanaviin. No sitten alkaakin olla vähän erilaiset tekniset vaatimukset, joiden osalta sitten kukin voi tietysti olla riski, jos ei sitä saada sovitettua. Nythän puhutaan siitä, että kun SaaS-järjestelmää tai SaaS-palvelua hankitaan, niin mulla varsinkin tai meidän porukalla on erityisenä intona katsoa, että miten se sopii tähän kokonaisarkkitehtuuriin, mikä tällä alueella on. Kun puhutaan liiketoiminnan kyvykkyyksistä, prosesseista ja sitten niitä toteuttavista IT-järjestelmistä, niin miten tämä palanen istuu tähän ja mitä asioita pitää huomioida. Totta kai integraatiot on yksi tärkeä kulma, että okei, no millä standardilla ja tavoilla sitä voi integroida. Yleensä halutaan, varsinkin kun ollaan tällä toimialalla, millä ollaan ja olemme vahvasti reguloitu, niin asiat täytyy tapahtua tietyllä tapaa ja sitten täytyy tiettyjä asioita huomioida. Ei niin sanotusti voi ihan kaikkia tehdä, mitä tapoja on esimerkiksi integraatioiden suhteen, vaan täytyy olla aika hallittuja standardeja ja mekanismeja." – H14

Vastauksista käy ilmi, että integraatiot aiheuttavat riskiä sekä järjestelmätasolla, että kokonaisarkkitehtuurin tasolla. Vaikka SaaS-järjestelmä saataisiin teknisesti integroitua osaksi muita järjestelmiä, voi kuitenkin olla, että haluttu SaaS-järjestelmä ei integroidu sujuvasti esimerkiksi liiketoimintaprosessien kanssa. Epäedulliset integraatiot saattavat aiheuttaa suorituskykyriskejä organisaatioille.

5.2 Tietoturva- ja tietosuojariskit

5.2.1 Datan ylläpito ja saavutettavuus

Useampi haastateltava mainitsee datan ylläpidon ja saavutettavuuden olevan SaaS-järjestelmien käyttöönottopäätöksiin vaikuttava tietoturvariski. Yksi näihin riskeihin vaikuttava tekijänä on datan palauttamisen vaikeus. Sekä H1 että H5 mainitsevat asiasta näin:

> ”Toinen näkökulma on sitten tässä se, että miten me saadaan omat tiedot takaisin, jos meillä tapahtuu jotain tai meillä tulee sopimuksellisesti haasteita tai me ei haluta jatkaa sitä käyttöä. Miten me saadaan ne omat tietomme sieltä takaisin? Ikään kuin kotiutettua ja mahdollisesti vietyä uuteen järjestelmään. Niissä on tavallaan paljon enemmän riskejä, kun siinä on-premisessä, joka on se perinteinen malli, koska silloinhan ne ”pörrää” jossain meidän tai jonkun meidän infratoimittajan kellarissa ne ”pöntöt” ja se tietohan on siellä.” – H5

> ”…voi olla ne vendor-riskit, että jos se firma ei pysy pystyssä niin sitten taas, missä se meidän data on? Saadaanko se data turvaan, jos käy huonosti?” – H1

Useampi haastateltava mainitsee myös datan eheyden menettämisen olevan datan ylläpitoon ja saavutettavuuteen vaikuttava riskitekijä. H1, H8 sekä H9 mainitsevat asiasta seuraavaa:

> ”datat on niin kuin koherentisti jossain, että jos joku pieni firma sijaitsee jossain eksoottisessa Euroopassa, niin onko se varma, että kriisitilanteissa tai sitten jos se firma menee konkkaan niin ne datat saadaan sieltä pois ja mihin ”backupit” tehdään. SaaS:ssa on usein se ongelma, että se unohtuu, että mihin ne datat sitten ”backupataan” eikä välttämättä minnekään. Tämän tyylisiä ongelmia siinä tulee.” – H1

> ”Nämähän on sellaisia SaaS-järjestelmässä olevia ihan oleellisia riskejä, että miten me voidaan vakuuttua siitä, että meidän tieto on aina saatavilla ja se eheys, että se tieto on koskematonta ja siihen ei ole kajottu. Esimerkiksi nyt geopoliittisen tilanteenkin ollessa sellainen, kun se on, niin miten voidaan varmistua siitä, että SaaS-järjestelmän kohdalla, jota käytetään internet-yhteyksillä, meillä on pääsy siihen meidän järjestelmään? Miten esimerkiksi, jos tulee tällaisia tilanteita, että tietoon ei voida enää luottaa tai siihen joku pääsee koskemaan, niin miten sitten palaudutaan niistä?” – H8

> ”Tietojen menetys; Tietojen varmistamiseen on käytettävissä vain palveluntarjoajan ratkaisut. Omat hyväksi havaitut käytännöt eivät välttämättä siis ole käytettävissä.” – H9

Haastattelujen perusteella datan on oltava saatavilla ja eheää. Datan eheyteen ja saatavuuteen liittyy epävarmuutta, joka on yksi merkittävä tietoturva- ja tietosuojariski.

5.2.2 Globaali toimintaympäristö

Globaali toimintaympäristö nähdään useamman haastateltavan toimesta SaaS-järjestelmän käyttöönottopäätökseen vaikuttavana riskinä, johon liittyy useita asioita, kuten geopoliittiset muuttujat ja mahdolliset alueelliset muutokset. Haastateltavat mainitsevat datakeskuksen sijainnin olevan merkittävä riskitekijä, johon liittyy asioita, kuten geopoliittinen tilanne ja maakohtainen lainsäädäntö. H6 ja H14 mainitsevat asiasta seuraavaa:

> ”Sitten tulee näitä toisennäköisiä. Se, mikä on kanssa aika konkreettinen asia, eikä välttämättä päätöksenteossa ole aina, liittyy erinäköisiin maakohtaisiin lainsäädäntöihin. Ja se on sitten estänyt tämän SaaS-palvelun käyttöönoton, tai sitten vaatinut jotain extra-kommervenkkeja, jotta sen pystyy käyttämään hyväksi. Kiina esimerkiksi on hirveän hankala, ja käytännössä usein tapaukset ovat sellaisia, että siinä esimerkiksi Kiina on

> kokonaan “scoupattu” ulos. Kiinassa tehdään, mitä Kiinassa tehdään. Ei voida lähteä siitä, että pystyttäisiin sitä bisnesprosessia pyörittämään missään muualla. Jos se toimiikin hetken aikaa, niin siinä voi olla riskejä, että katkeaa.” – H6

> ”Yhden tällaisen hyvän voisi nostaa tässä, mikä mulla nyt viime aikoina erään palvelun ulkoistuksessa tuli esiin on se, että jos geopoliittinen tilanne muuttuu tietyllä tapaa, niin pitääkö meidän vetää palvelu takaisin sisään. Eli tavallaan exit-suunnitelma ja exit-kriteeristön ymmärtäminen. Taisi olla silloin, että palvelu tuotettiin tai tuotetaan EU ja ETA-alueen ulkopuolelta, jos siihen sitten liittyy riski, että esimerkiksi EU-tasolla tai jopa kansallisella tasolla sitten haluttaisiin irtautua, vaikka kyseisen maan palvelusta ja muista, niin se tarkoittaisi sitten irtautumista siitä ulkoistuksesta. Tämähän on sen tyyppinen riski.” – H14

H1 mainitsee vastauksessaan globaaliin toimintaympäristöön ja sen muutokseen liittyvän riskin siitä, että alueelliset olot tai alueiden väliset suhteet saattavat muuttua, jolloin alueella voi puhjeta esimerkiksi konflikti:

> ”Voiko se [SaaS-järjestelmä] sijaita sellaisella alueella, että tulee alueellinen konflikti?” – H1

Yleisesti globaalin toimintaympäristön muutos saattaa aiheuttaa epävarmuutta ja uhkakuvia organisaatioissa. Nämä havaitaan SaaS-järjestelmien käyttöönottopäätöksiin vaikuttavina riskeinä. Geopoliittinen tilanne sekä muut aluekohtaiset muuttujat, kuten lainsäädäntö ja mahdolliset uhkatilanteet alueella, jossa SaaS-järjestelmän tietovarastot tai ylläpito sijaitsevat, voivat aiheuttaa epävarmuutta. Haastatteluiden perusteella nämä huomioidaan osassa organisaatioita SaaS-järjestelmän käyttöönottopäätökseen vaikuttavina riskitekijöinä.

5.2.3 Tietosuojaloukkaukset

Useampi haastateltava mainitsee tietosuojaloukkaukset tietoturva- ja tietosuojariskinä, johon vaikuttaa muun muassa se, millä tahoilla on pääsy dataan ja miten datan käyttöä hallitaan. Lisäksi lainsäädännöllisten velvoitteiden noudattaminen sekä lainsäädännölliset muutokset vaikuttavat riskin muodostumiseen. H13 mainitsee lainsäädännöllisten velvoitteiden noudattamisesta ja muutoksesta seuraavaa:

> "Tietenkin se, että se regulaatio muuttuu ja kaikkien pitäisi pysyä sitten kärryillä niistä muutoksista. Nyt jos puhutaan vaikka GDPR:stä, niin sekin muuttuu ja vaikka tästä EU AI actista. Se on itse asiassa hyvä esimerkki siitä. Ne muuttuvat ja kaikkien pitää pysyä kärryillä. Toinen on se myös, että tulkintoja on erilaisia. Eli jos ajatellaan, että me ollaan asiakas ja meillä on hyvin tiukka tulkinta ja sitten se emo-firma, jolta me ostetaan se itse ”platta” [alusta], niin heillä voi olla tietynlainen tulkinta ja sitten heidän aliketjutus-vendoreillaan, sovelluksien kehittäjällä, voi olla aivan omanlainen tulkinta. Se on se haaste siinä, että mikä tulkinta on oikea." – H13

Lainsäädännön noudattaminen ja seuraaminen nähdään riskinä, sillä lainsäädäntö saattaa muuttua nopeasti. Jos muutoksissa ei pysytä perässä, voidaan joutua ongelmiin ja tehdä tietosuojaloukkauksia jopa tietämättään. Samalla SaaS-järjestelmissä palvelun toimitusketjun pituuden huomataan vaikuttavan lainsäädännön oikeaoppiseen noudattamiseen, sillä tulkitsevia tahoja saattaa olla toimitusketjussa useita.

Muutama haastateltavista mainitsee myös identiteetinhallinnan vaikuttavan tietosuojaan ja tietoturvaan. H10 mainitsee, että identiteetinhallinnan on oltava keskitettyä, sillä SaaS-järjestelmien määrän kasvaessa hallinta vaikenee ja monimutkaistuu, jolloin myös riski tietosuojaloukkauksista saattaa kasvaa. H10 mainitsee identiteetinhallinnasta ja dataan pääsystä seuraavasti:

> ”Ja mä sanoisin, että identiteetinhallinta pitää olla keskitetty. Eli sehän pitää pystyä sitouttamaan sen yrityksen, ostavan yrityksen identiteetinhallintaan. Se on mun mielestä kaikkein kriittisin. Eli mitä mä yritän sanoa, että jos te ostatte SaaS-palvelun, niin sinne ei jaeta staattisia tunnuksia jokaiselle, koska sen jälkeen se hallittavuus on täysin nolla. Eli sen täytyy olla keskitetty. Siinä vaiheessa, kun X lähtee talosta ulos ja me suljemme X:n tilin, niin kaikki SaaS-palvelut sammuu sille samalla hetkellä. ... koska sen jälkeen, kun X on todella katkera siitä, että hänet irtisanottiin ja sen jälkeen hän pääsee sinne edelleen ja sitten on maailma auki.” – H10

5.2.4 Tietovuoto

Useampi haastateltava mainitsee tietovuotojen olevan merkittävä riski, joka vaikuttaa SaaS-järjestelmän käyttöönottopäätökseen. Tietovuotoon riskitekijänä vaikuttavat haastateltavien mukaan toimitusketjun kompleksisuus, kontrollin menetys, dataan käsiksi pääsy sekä datan sijainti. Datan sijainnista H1 mainitsee seuraavaa:

> ”Se missä se sijaitsee, että onko se sen palveluntuottajan komerossa tai vaatehuoneessa, vai onko se jossain isossa konesalissa, niin se on päivänselvää, että joku Googlen Haminan datakeskus on aika hyvin suojattu, että sinne ei kukaan pääse. Käytännössä joku ammattimainen terroristi korkeintaan, mutta siihen työasemalle tai vaatehuoneen komeroon saattaa päästä helpostikin.” – H1

Datan sijainnin lisäksi useampi haastateltava mainitsee toimitusketjun kompleksisuuden tietovuotoriskiin vaikuttavana tekijänä. H4, H9 ja H12 mainitsevat asiasta seuraavaa:

> "Mut ne toimitusketjut on niin pitkiä. Tässäkään ei tavallaan korkattu [X:n] järjestelmistä mitään. Vaan oli korkattu [X:n] palvelutuottajan järjestelmä, josta oli sitten saatu käyttäjätunnus ja salasana, millä oli päästy tunkeutumaan [X:n] järjestelmiin." – H4

> "Datan vuotaminen: Ulkopuolinen voi päästä yrityksen tietoihin käsiksi, sillä tietoturvakäytännöt ovat SaaS-tarjoajan vastuulla eikä omissa käsissä. Käyttäjiä voi olla paljon ja palvelu näkyvissä monille yrityksille. Yksittäisen yrityksen tiedot eivät ole yhtä

> houkuttelevia kuin ympäristöt, joissa on enemmän tietoja varastettavaksi tai väärinkäytettäväksi." – H9
>
> "Ja sitten jos ajatellaan tietoturvamielessä, niin taas uhka ja epävarmuus, niin sovellustasolla yksi suuri kysymys on se, että miten sitä sovellusta ylläpidetään, minkälaiseen teknologiaan se perustuu, miten sitä ylläpidetään. Jos siellä on tarkoitus tehdä erilaisia korjauksia tai muita, esimerkiksi tietoturvauhkien takia, niin miten tämä on hoidettu. Ja sitten ehkä alimpana on arkkitehtuurinen [taso], niin kuin tavallaan tämä infrastruktuuri ja muu, niin siinä tullaan taas siihen, että miten siellä on huolehdittu tämmöiset tekniset ylläpidot ja versiohallinnat. Ja tietysti se, että ei käytetä semmoisia versioita tai tekniikkaa, joka on vanhaa tai ennen kaikkea, että on haavoittuvaista." – H12

Toimitusketjun laajuus havaitaan tekijänä, joka lisää toimitusketjun kompleksisuutta ja täten myös tietovuotoriskiä. Toimitusketjun laajentuessa ja toimijoiden määrän kasvaessa myös riskin havaitaan kasvavan. Tämä johtuu siitä, että usean organisaation dataa käsitellään samassa tietovarastossa. Tällaisia ympäristöjä voidaan pitää houkuttelevimpina kohteina kyberhyökkäyksille. Toimitusketjun kompleksisuuteen liittyy osaltaan myös kontrollin menettäminen, sillä vastuu ja ymmärrys tietovuotojen estämisestä ei ole omissa käsissä.

5.3 Strategiset riskit

5.3.1 Liiketoiminnan ketteryys ja kehitys

Yhtenä SaaS-järjestelmän käyttöönottopäätökseen vaikuttavana strategisena riskinä nähdään mahdollinen negatiivinen vaikutus liiketoiminnan ketteryyteen ja kehitykseen. Tähän asiaan vaikuttavana tekijänä mainitaan usean haastateltavan toimesta negatiivinen vaikutus liiketoiminnan mahdollisuuteen reagoida muutoksiin sekä oman toiminnan muokkaamiseen dynaamisesti. H6 ja H12 mainitsevat asiasta seuraavaa:

> "Ne keskeisimmät strategiset riskit ovat nimenomaan siinä, että miten varmistetaan, että se SaaS-palvelu tukee liiketoiminnan muutoksia, joita tulee tulevaisuudessa koko ajan. Jos mä katson nyt tästä 10 vuotta taaksepäin niin me ollaan heitetty voltti muutaman kerran vuodessa. Toisinaan on vaikutuksia näihin keskeisiin liiketoimintajärjestelmiin toisinaan ei. Eli jos keskeisen liiketoimintajärjestelmän heittää SaaS:iin niin se riski on tietyssä mielessä, että sun kyvykkyys reagoida muutoksiin heikkenee." – H6
>
> "SaaS-palvelun luonne-ero tavallaan tämmöiseen, voisiko sanoa dedikoituun omaan sovellukseen tai järjestelmään. Siinä tavallaan se riski tai epävarmuus tulee siinä, että ollaanko valmiita, koska tämähän on se liiketoiminnan kyky enemmän ehkä kuin tietohallinnon. Kyllähän tietohallinto varmaan SaaS-palvelun kanssa vielä pystyy elämään, vaikka vähän huonommankin kanssa, mutta jos se ei tue tai auta liiketoiminnan kehitystä. Jos se SaaS kehittyy hitaammin kuin se, mitä liiketoiminta haluaisi sen kehittyvään, niin sehän tulee jarruksi tai hidasteeksi. Eli tavallaan tämmöinen bisneksen, ei nyt hidastuminen, mutta tavallaan sen ketteryyden saaminen, niin voi olla, että se menetetään siinä, kun ollaankin tavallaan keskitetyn SaaS-palvelun piirissä." – H12

H6 mainitsee SaaS-järjestelmien sisältävän riskin, jossa liiketoiminnan ketteryys heikkenee sellaisissa dynaamisissa olosuhteissa, joissa liiketoiminnan tarpeet muuttuvat. H12 puolestaan mainitsee riskin siitä, että SaaS-järjestelmä ei kehity samaa tahtia oman liiketoiminnan kanssa, ja tästä syytä liiketoiminnan ketteryys sekä kehitys kärsii. Toisena riskitekijänä mainitaan SaaS-järjestelmän kyvykkyyksien riittämättömyys tulevaisuudessa. H4 mainitsee asiasta seuraavaa:

> "Onko jotain riskejä joidenkin asiakkaiden kanssa materialisoitunut ja pitääkö itse reagoida niihin jotenkin. Koska niissä aina sitten joudutaan pohtimaan vaihtokustannuksia. Jos ajat jotain isoa ERP:iä SaaS:ina ja sit sanotaan, että alkaisi osoittautua, että se ei kehity tai se alkaa degeneroitua, niin sitten sun vaihtoehdot on aloittaa jonkun toisen SaaS-järjestelmän käyttöönottoprojekti." – H4

H4 mainitsee riskitekijänä sen, että SaaS-järjestelmän kyvykkyydet eivät kehity tai ne huononevat ajan kuluessa. Tämä on osittain päällekkäinen huomio ketteryyden ja kehityksen heikentymisen kanssa, sillä SaaS-järjestelmä saattaa vaikuttaa heikentyessään myös liiketoiminnan kehitykseen negatiivisesti.

5.3.2 Strateginen dissonanssi

Yhtenä keskeisimpänä strategisena riskinä, joka vaikuttaa SaaS-järjestelmän käyttöönottopäätökseen, on strateginen dissonanssi. Tähän liittyen useat haastateltavat nostavat esiin mahdolliset ongelmat liiketoiminnan sovittamisessa SaaS-järjestelmäympäristöön. Keskeisenä asiana haastateltavat näkevät liiketoimintaprosessien ja järjestelmälogiikan mahdollisen ristiriitaisuuden. H7 ja H8 mainitsevat asiasta seuraavaa:

> "Ehkä se suurin semmoinen riski on aina se, että se järjestelmä pureutuu johonkin tiettyyn bisnesprosessiin. Ja sitten jos se bisnesprosessi ja järjestelmän logiikka ei kohtaa, niin siinä meillä tulee niitä haasteita. Ja sitten siinä on aina tämä ”muna-kana -tilanne”, että pitäisikö mennä niin, että järjestelmän ”standardisetuppi” on joku, ja sitten muokataan prosessia sen mukaan, vai olisiko meillä pitänyt olla prosessialusta, joka sitten muodostaa sen, tai koetetaan mahdollisimman paljon mukailla sitten siellä järjestelmämaailmassa. Ja tuntuu, että tämä on aina se kohta, missä se suurin “clash” syntyy" – H7

> "Tämä toiminnan muutos on se, mikä pitää ottaa huomioon siinä käyttöönottopäätöksessä. Se pitää ymmärtää, että mitkä ovat nyt toiminnan ydinprosessit ja miten ne menevät sitten sen uuden järjestelmän kanssa. Jos se toiminnan muutos on niin suuri, että me emme kykene sitä viemään läpi, niin sehän on selkeä asia, mikä pitäisi tämän käyttöönoton yhteydessä tunnistaa ja sen varmasti pitäisi vaikuttaa siihen käyttöönottopäätökseen. Jos vaihtoehtona on kaksi järjestelmää, joista toinen on sellainen, että toiminnan luonne tai toiminta ei muutu niin paljon nykyiseen verrattuna tai vaihtoehtoisesti, että syntyy merkittävä muutos toiminnalle, että työnteko, vaikka työnjako ammattilaisten välillä tai se järjestys, jossa asioita tehdään, muuttuu merkittävästi tai jos se vaarantuu se prosessi ja se toiminnan jatkuvuus kärsii siitä, niin kyllähän tommoiset asiat pitäisi tunnistaa siinä käyttöönottopäätöksenteossa." – H8

Toisena riskitekijänä useammat haastateltavat mainitsevat strategisten tavoitteiden eroavaisuuden tai intressien ristiriitaisuuden palveluntarjoajan ja asiakasorganisaation välillä. H12 ja H14 mainitsevat asiasta seuraavaa:

> "Olenpa senkin nähnyt, että on tehty joskus tavallaan iso muutos siinä, että yksi vähittäiskauppa totesi, että se haluaa irti Amazonin palvelusta, kun Amazon ilmoitti, että niillä on tulossa Suomessa vähittäiskauppoja Pohjoismaihin. Niin tämmöisiäkin strategisia kuvioita. SaaS-toimittaja tuleekin sun bisnesalueelle. ... ne [strategiset tavoitteet] voi olla samanlaisia, että se alkaakin tulla sun bisnesalueelle ja sitten sehän on vähän hupaisaa. Se on vähän sama kuin voisi ajatella näin, että Silmäasema käyttäisi Nissenin tietojärjestelmiä. Eikö se kuulosta vähän erikoiselle?" – H12

> "Kyllähän sen täytyy olla, että jos puhutaan strategisesta tasosta, niin kuin SaaS, jos oletetaan, että se SaaS-ulkoistus tai se SaaS-hankinta on strategisesti merkittävä. Silloin se toimittaja on myös hyvin tärkeä strategisesti, että pitäisi puhua varmaan jo kumppanista siinä kohdassa, eikä pelkästään toimittajasta. Silloinhan se [strategia] täytyy olla kyllä ”aligned”. Sitten pitää kyllä puhua pitkästä, jos ei ole avioliitosta, niin jonkinlaisesta kumppanuudesta siinä mielessä." – H14

H12 nostaa esiin riskin strategisten intressien ristiriitaisuudesta tai tavoitteiden liiallisesta samankaltaisuudesta. H14 nostaa puolestaan esiin riskin siitä, että strategiset tavoitteet eivät ole linjassa asiakasorganisaation ja palveluntarjoajan välillä.

5.3.3 Strateginen toimittajaloukku

Useampi haastateltava näkee strategisen toimittajaloukun SaaS-järjestelmän käyttöönottopäätökseen vaikuttavana riskinä. H4 ja H6 mainitsivat strategisesta toimittajaloukusta seuraavaa:

> ”Että sen jälkeen, kun sä oot laittanut sun kahden miljardin bisneksen siihen ja kolmetuhatta käyttäjää, niin kyllä sä oot naimisissa sen palveluntarjoajan kanssa. Sä et joka kolmas vuosi halua aloittaa puolentoista vuoden ja viiden miljoonan projektia, jossa sä vaihdat järjestelmää. Kyllä niiden kanssa aina sitten on enemmän tai vähemmän naimisissa.” – H4

> "Todennäköisesti siinä on yksi organisaatio, joka hoitaa sen käyttöönoton siellä, niin kuin tavallaan projektipuoli. Niin jos on niin, että joku konsulttifirma tulee sen tekemään, niin he hoitaa sen käyttöönottoprojektin. Sitten tekee ”handoverin” usein saman firman jollekin tämmöiselle ”ongoing services” -pumpulle. Silloin tavallaan me ollaan naimisissa sen kyseisen firman kanssa, toki myöskin sen SaaS-palvelun. Mutta siinä on niin kuin useampia kehyksiä. ... Mutta nimenomaan se tavallaan, kuka ylläpitää sitä palvelua sille firmalle ja tukee sitä firman varsinaista bisnestä, niin se on ehkä se isoin riskikohta." – H6

Palveluntarjoajan ja asiakasorganisaation välille saattaa syntyä toimittajaloukku, jolloin siirtyminen toiseen järjestelmään voi olla vaikeaa ja työlästä. Tällöin tilanne, jossa syystä tai toisesta halutaan

vaihtaa järjestelmää, saatetaan nähdä ongelmallisena. Strateginen toimittajaloukku nähdään täten käyttöönottopäätökseen vaikuttavana strategisena riskinä.

5.3.4 Osaamisen menettäminen

Osa haastateltavista näkee osaamisen menettämisen riskinä, joka vaikuttaa SaaS-järjestelmän käyttöönottopäätökseen. H3, H9 ja H14 mainitsevat asiasta seuraavaa:

> ”Kun se hyppäys tehdään sinne, niin yleensä se tarkoittaa myös sitä, että sen vanhan järjestelmän ympärillä oleva henkilöstö ja osaaminen vähenee aika radikaalisti. Jos sulla on ollut 15 ihmistä kolvaamassa jotain vanhaa järjestelmää, niin tämän jälkeen sulla ei ole enää viittätoista ihmistä ja se tarkoittaisi myöskin sitä, että se ymmärrys lähtee pikkuhiljaa hämärtymään. Miten se SaaS-järjestelmä nyt ihan oikeasti toimii tai mitä siellä on alla? Jos sitä lähdetään jossain vaiheessa vaihtamaan niin voi alkaa kivulias seikkailu. Mutta tää täytyy nyt rinnastaa sitten siihen, että jos ”inhouse-järjestelmää” lähdetään vaihtamaan, niin ei se yhtään vähemmän kivuliasta ole. Se on erilaista.” – H3

> "Oma osaaminen menetetään. Kun siirrytään SaaS palveluun, omaa osaamista ei enää vastaavasti tarvita. Näin ollen mahdollinen paluu takaisin, on erittäin hankalaa eikä aitoa vertailua enää pystytä tekemään eri vaihtoehdoista." – H9

> ”Sittenhän meidän pitäisi varautua siihen, että sitä osaamista otetaan takaisin tai uudelleen organisoidaan muuten. Tämän tyyppinen on sellainen, mitä me arvioidaan aika lailla jokaisen SaaS-hankinnan kanssa.” – H14

Haastateltavat nostavat osaamisen menettämisen riskinä, johon liittyy SaaS-järjestelmästä pois siirtymiseen liittyviä epävarmuuksia sekä hankaluuksia. Jos SaaS-järjestelmä ei ole sopiva tai halutaan siirtyä muihin järjestelmäratkaisuihin, voi siirtyminen olla hankalaa osaamisen puutteen takia. H3 mainitsee, että vaikka tämä havaitaan riskinä, siinä ei ole suuria eroja verrattuna on-premise-ratkaisuihin. Toisaalta useampi haastateltavista mainitsee, että osaamisen menettäminen ei ole välttämättä riski, vaan hyöty. H6, H10 ja H14 mainitsevat asiasta seuraavaa:

> ”Ei niinkään ole, että osaamista tai kyvykkyyksiä sillä lailla pistetään [riskiksi], koska pikemminkin nämä toiminnot, varsinkin jos henkilöistä puhutaan, niin ne on yleensä tukiorganisaatioita, mitkä ulkoistetaan. Silloin se ei ole normaalille yritykselle mikään ongelma, päinvastoin. Yritykset ehkä pyrkivät siihen, että tämmöistä tavallaan “kiinteää läskiä” saadaan pois, jolloin se tukee enemmän strategiaa.” – H6

> ”Onko se riski, jos me siirrytään SaaS-palveluun ja menetetään joku on-premise-talentti? Koska toihan just, että hyvä syy siirtyä SaaS-palveluun on se, että sinä et ole enää riippuvainen yhdestä tai kahdesta sankarista talossa. Mä näkisin sen ihan päinvastoin just.” – H10

> ”Se on meidän organisaatiossamme hyvinkin selvää, että se on selvästi sanottu, että millä alueilla ja minkä kyvykkyyksien osalta me haluamme hyödyntää SaaS-tyyppisiä

> palveluita. Ja sen kautta sitten ehkä riski siitä, että menetetään osaamista tai tämän tyyppistä, niin aina välillä voi kääntää toisinkin päin.” – H14

Osaamisen menettäminen tai sen siirtyminen pois voidaan nähdä myös organisaatiota hyödyttävänä asiana. Haastattelujen perusteella tämä riskitekijä jakaa mielipiteitä ja se voidaan nähdä sekä riskinä, että hyötynä organisaatiolle.

5.3.5 Liiketoiminnan jatkuvuus

Keskeisinä strategisina riskeinä haastateltavien vastauksista nousee liiketoiminnan jatkuvuuteen liittyvät riskit. Usea haastateltava nostaa esiin riskin siitä, että SaaS-järjestelmän käytettävyys saatetaan menettää kokonaan, mikä on keskeinen riski liiketoiminnan jatkuvuudelle. SaaS-järjestelmän käytettävyyden menettäminen voi johtaa erilaisiin ongelmiin, joista muun muassa H9 mainitsee:

> "Liiketoiminta voi häiriintyä, mikäli palveluntarjoajalla on ongelmia tai vaikka huoltokatkoja. Mainehaitta voi olla välitön, mikäli ongelmat näkyvät arvoketjussa muille osapuolille" - "miten aiotaan varmistaa liiketoiminnan jatkuvuus ongelmatilanteissa sekä siinä, että asiakkaan oma henkilö tekee merkittävän virheen. Mikäli palveluntarjoajalla ei ole näihin ratkaisuja, ei niitä synny projektinkaan aikana" – H9

Myös H12 mainitsee, että SaaS-järjestelmän käytettävyys on joissain tilanteissa niin kriittistä liiketoiminnalle, että jatkuvuus tulee varmistaa myös ongelmatilanteiden sattuessa:

> "Mehän voidaan tietohallinnossa esimerkiksi mennä arvaamaan, mikä liiketoiminnan mielestä on kriittistä. Mutta kyllähän sen liiketoiminnan pitää pystyä itsekin sanomaan, että voiko tämä SaaS-palvelu olla pois käytöstä esimerkiksi päivän, taikka viikon, vai onko se niin, että tuntikin on jo liian pitkä aika. Ja tähän tietoturvamielessä jatkuvuuteenhan sitten tullaan siinä, että jos me saadaan se viesti, että puoli päivää tai neljä tuntia on pisin aika, kun se voi olla alhaalla, niin sittenhän meidän täytyy alkaa miettimään, tämä liittyy siihen hankintapäätökseenkin tai käyttöönottopäätökseen, että millä tavalla me varmistetaan, että SaaS-järjestelmä on käytettävissä. Elikkä, mitkä on meidän varajärjestelmät. Mennäänkö varajärjestelmään niin, että jos tämä ei ole käytössä, niin sitten otetaan kynä ja paperi, ja sillä pitää sitten hoitaa? Tai sitten se, että me haetaan siihen sitten vaikka muita tietoliikenneratkaisuja taustalle, siis varajärjestelmiä. Tai sitten täytyy selvittää, että onko sillä SaaS-toimittajalla riittävät kyvyt huolehtia siitä, että se ei ole pidempää kuin sen neljä tuntia alhaalla." – H12

Liiketoiminnan jatkuvuusriskiin liittyen useampi haastateltavista mainitsee, että palveluntarjoajan toiminnan laajuus ja tulevaisuusnäkymät vaikuttavat asiakasorganisaation saamaan palvelutasoon. Useampi haastateltavista mainitsee suurten palveluntarjoajien olevan luotettavampia kuin pienempien palveluntarjoajien. Tähän liittyy haastateltavien mukaan ajatus siitä, että suuret palveluntarjoajat pysyvät todennäköisemmin pystyssä pitkällä aikavälillä, jolloin niiden toiminta ei

tule päätökseen asiakkuussuhteen aikana. Haastateltavien vastauksista nousee esiin riski liiketoiminnan jatkuvuudesta oman liiketoiminnan, kuin myös palveluntarjoajan kohdalla. Suurien palveluntarjoajien uskotaan pystyvän ylläpitämään ja kehittämään toimintaa paremmin kuin pienten palveluntarjoajien. Haastateltava H4 mainitsi asiasta seuraavaa:

> "Tietysti, jos tietoturvan ja kapasiteetin, ehkä muidenkin asioiden näkövinkkelistä, niin sitten on tietysti se SaaS-palvelutuottajan liiketoiminnan jatkuvuus. Miten siihen varaudutaan, että jos se yritys, joka sitä SaaS-palvelua tuottaa, niin jos liiketoiminta lähtee alamäkeen ja siellä on vähemmän asiantuntijoita paikalla, ne yrittävät olla kustannustehokkaita, että minkälaisia muutoksia siellä tulee? Onko se SaaS-palvelun tuottajana uskottava ja luotettava siihen, että ne pystyvät tuottamaan seuraavat 15–20 vuotta sitä palvelua niin, että se kehittyy jatkuvasti. Siitä tulee [muuten] semmoinen ”dead end”, että jäätiin 2010-luvulle." – H4

Haastateltava H12 mainitsee palveluntarjoajan koolla olevan vaikutusta liiketoiminnan jatkuvuuteen, mutta tuo esille myös pienten ja suurten palveluntarjoajien eroja asiakasorganisaation tukemisessa:

> "Yksi on se, että onko se liian pieni vai voiko se olla liian iso. Ja tällä tarkoitan sitä, että jos se on liian iso, niin esimerkiksi tietyissä asioissa, jos tarvitaan apua tai tukea, niin se voi olla, että oma bisnes on niin pientä, että se ei tämmöistä isoa toimittajaa oikeasti kiinnosta. Se pistää suurin piirtein vaan sähköpostitukea ja se ei välttämättä taas auta. Liian pieni toimija, niin kuin tiedätte, niin se riski voi olla jopa se, että se IT-toimittaja tai SaaS-toimittaja ei pysy hengissä, jolloin tavallaan se kumppanuus häviää tämmöisen kautta." – H12

Osa haastateltavista mainitsee palveluntarjoajan koon ja tulevaisuudennäkymien vaikuttavan palvelun jatkuvuusriskiin, sillä suuret yritykset saattavat ostaa pienemmät palveluntarjoajat tulevaisuudessa. H4 ja H6 mainitsevat asiasta seuraavaa:

> ”Yrityskauppoja tapahtuu jatkuvasti, että jos otat jonkun vähän pienemmän SaaS-palvelun ja siitä tulee sitten vähän menestyneempi ”business”, niin sitten joku isompi ostaa sen. Ja sitten, kun se siirtyy toiseen omistukseen tai toiseen portfolioon, niin sen tuottavan yrityksen näkövinkkelistä se on vaan joku palikka portfoliossa. Saattaa olla, että tulevaisuuden linjaukset ja muut muuttuu. Hinnoittelun tosi usein pyrkivät muuttamaan tämmöisessä tilanteessa, koska niistä vanhoista asiakkaista pitää saada enemmän liikevaihtoa ja tuottoa kuin mitä ennen sitä yrityskauppaa tehtiin.” – H4

> ”Sitten sanotaan, että joissain vastaavissa kilpailutuksissa on pitänyt oikeasti katsoa myöskin sitä, että mikä tämän firman todennäköinen positio on 5–10 vuoden jälkeen. Tämä on taloudellinen riski toki, mutta onko se esimerkiksi semmoinen, että todennäköisesti toi on sen kokoinen, että joku toinen firma kiinnostuu siitä ja ostaa sen pois. Joissain näissä tapauksissa mennään sinne itse asiassa johonkin 10–15 vuotta taaksepäin. Silloin mä olin [suomalaisessa kansainvälisessä yrityksessä] vielä tekemässä kilpailutuksia, niin meillä oli yksi tämmöinen. Se oli joku master dataan liittyvä keskikokoinen puolitoistatuhatta ihmistä. Nouseva kyky, joka oli meidänkin arvostuksessamme teknisesti siellä kärkipäässä. Mietin jo siinä kohtaa, että jos mä olisin joku investori, niin mä ostaisin tuon pois vähän ajan päästä. Se oli juuri ”venture

> capitalin” kautta firma lähtenyt käyntiin. Silloinhan siinä tavallaan [on kyseessä] kasvuyritys, niin lähdetään siitä, että jostakin se raha saadaan sitten pois, mitä siihen kasvuyritykseen laitetaan. Siinä meni sitten vuoden verran, niin [yritys x] oli ostanut sen. Tämän tyylisiä juttuja. Mutta sitten sä tiedät, että jos se on mahdollista, niin mitä sitten. Koska [yritys y] oli silloin yksi kilpailija kanssa, ja heillä oli huonompi tuote, niin mitä se sitten tarkoittaa? Haluatko sä sitten ottaa sen riskin, että sulle tulee joku toinen, eikä tämä jonka kanssa sä nyt neuvottelet?” – H6

Yrityskaupat voivat johtaa epävarmuuteen jatkosta. Yrityskaupan jälkeen uusi omistajayritys saattaa tehdä suuria muutoksia palveluihinsa, eikä uuden tarjoajan kanssa ole alun perin muodostettu, eikä välttämättä saadakaan muodostettua, läheistä suhdetta. Haastatteluiden perusteella tämän riskin kohdalla olennaisia ovat muutokset hinnoittelussa, luottamussuhteessa sekä tavoitteiden linjautumisessa.

5.4 Taloudelliset riskit

5.4.1 Hyötyjen realisointi

Yhdeksi keskeiseksi taloudellisten riskien kategoriaksi nousee hyötyjen realisointiin liittyvä riski. Haastateltavat nostavat vastauksissaan esiin SaaS-järjestelmän käyttöönottopäätökseen liittyvän riskin siitä, että SaaS-järjestelmästä ei välttämättä saada riittävästi hyötyjä suhteessa kustannuksiin. Haastateltava H4 mainitsee asiasta seuraavaa:

> "Kyllä mä oon nähnyt paljon semmoisia projekteja, mitkä on toteutettu ajallaan ja budjetissa ja toteuttanut niille asetetut laatukriteerit, mutta kuitenkaan ei oo sit tuottanut sitä, mitä niiden piti. Eli periaatteessa joku asia on jäänyt huomioimatta. Itekin tehnyt pari sellaista." – H4

Osa haastateltavista mainitsee siitä, että olisi tärkeää hahmotella hyötyolettama, joka valitusta järjestelmästä tultaisiin saamaan ja suhteuttaa se kustannuksiin. Osassa vastauksia mainitaan myös, että mitä kokonaisvaltaisemmin SaaS-järjestelmä saadaan integroitua osaksi organisaation toimintaa, sitä enemmän siitä todennäköisesti voidaan myös hyötyä. Haastateltavat H4 ja H6 kertovat aiheesta seuraavaa:

> ”Toinen taloudellinen riski, joka periaatteessa aina liittyy projektityöhön, on se, että se panostus, mikä tehdään, koska SaaS-palvelut täytyy kuitenkin ottaa silleen käyttöön. Täytyy konfiguroida, ihmiset kouluttaa ja rajapinnat rakentaa ja kaikkea muuta. Ja hyvin harva pystyy ottamaan laajoista SaaS-palveluista aivan kaikkea käyttöön. Niistä otetaan aina vain joku osa. Niin saavutetaanko sillä, mitä on suunniteltu otettavan käyttöön, ne liiketoimintahyödyt, mitä kuvitellaan saavuttavan. Koska se, että mitä otetaan käyttöön, siihen sitoutuu käyttöönottokustannus ja käyttökustannus, tavalla tai toisella. Ja sitten, kun ajatuksena on ollut, että kun tämän verran panostetaan, niin sit saadaan tuollaisia hyötyjä. Niin toteutuuko se hyötyolettama. Se on ehkä se määräävin riskitekijä.

> Saadaanko sillä panoksella se, mitä tavoiteltiin. Se, että maksaako se x euroa vai 1,2 kertaa x euroa, niin on kuitenkin vielä jossain määrin siedettävä riski verrattuna siihen, saavutetaanko me sillä se liiketoimintahyöty, mitä lähdettiin hakemaan. Se on se riski, mitä pitää ”manageerata”. Se hyöty, tavallaan hyötyjen ja saavuttamisen taso.” – H4

> ”Ehkä se isoin asia toki on siinä, että silloin kun tämmöistä isompaa SaaS:ia otetaan käyttöön, niin siinä täytyy aika tarkkaan laskea se, että sä saat sen hyödyn sieltä irti myös, koska ne eivät ole mitään halpoja. Ja silloin se tarkoittaa sitä, että jos ottaa nyt vaikka, käytetään nyt taas tätä Salesforcea esimerkkinä, sieltä vaikka jonkun ”service-cloudin” käyttöön. Niin jos sä sieltä ”service-cloudista” käytät jonkun pienen nurkan, niin todennäköisesti sä et saa sieltä niin isoa hyötyä, kuin että sä pystyisit kokonaisvaltaisesti sen käyttämään hyödyksi. Tai sitten jos ottaa isomman osuuden. Silloin kun sen pystyy täydellisemmin integroimaan ja hyödyntämään sen firman toiminnoissa, niin silloin todennäköisyys, että siitä saadaan taloudellisestikin kannattava, niin se on suuri.” – H6

Haastateltava H13 mainitsee lisäksi SaaS-järjestelmän hyötyolettamaan liittyvän riskin siitä, että asiakasorganisaatio ei itse omista käyttöönotettavaa SaaS-järjestelmää. Tästä syystä SaaS-järjestelmästä tulisi saada ulos riittävästi hyötyjä ennen kuin siitä päätetään luopua:

> ”Ja käytännössä sä otat käyttöön sen SaaS-teknologian, mutta sä et kuitenkaan itse ikinä omista sitä. Eli joku päivä, jos sä päätät siitä lähteä ja vielä ennen sen takaisinmaksun aikaa, niin sehän on menetettyä rahaa niin sanotusti. Ja se ei tule sun mukana. Eli se ei ole jotain fyysistä, joka sitten siirtyy sun kanssa.” – H13

Vaikka hyötyjen realisointi voi haastateltavien vastausten mukaan tarkoittaa muutakin, kuin suoria taloudellisia hyötyjä, ovat ne kuitenkin sidottuna kustannuksiin, jotka siirtymään sekä SaaS-järjestelmän elinkaareen on investoitu. Tämän takia SaaS-järjestelmän kustannus-hyötyolettaman tulisi kallistua siihen suuntaan, että investointi nähdään organisaation toiminnan kannalta positiivisena. Useat haastateltavat näkevät hyötyjen realisoinnin yhtenä keskeisenä SaaS-järjestelmän käyttöönottopäätökseen vaikuttavana riskinä.

5.4.2 Piilotetut kustannukset

Useat haastateltavista tunnistavat käyttöönottopäätökseen liittyvän riskin piilotetuista kustannuksista. Yhtenä tekijänä vastauksista esiin nousee SaaS-järjestelmien kulurakenteen kompleksisuus, joka saattaa johtaa odotettua suurempiin kustannuksiin tulevaisuudessa. Jos kulurakennetta ei ymmärretä tai osata ennustaa kunnolla etukäteen, voivat todelliset kustannukset olla huomattavasti oletettua suuremmat. Haastateltavat H7 ja H12 kertovat vastauksissaan seuraavaa:

> ”Liian usein me tuijotetaan siinä, kun tehdään uusien järjestelmien käyttöönottopäätöksiä, niin pelkästään sitä lisenssikulua ja me unohdetaan, että kaikkiin järjestelmiin liittyy myöskin muita kuluja. Siellä on aina joku, no joku hosting-kulu nyt on yleensä aika pieni, mutta se vaatii aina jonkun [vastuussa olevan]. Vaikka me ei oltais tehty kustomointia, niin se vaatii yleensä aina jonkun, joka omistaa sen järjestelmän ja omistaa esimerkiksi

> sen konfiguroinnin. Omistaa sen, että sille seurataan tulevia päivityksiä, ja hoitaa testaukset päivitykseen ja näihin konfiguraatioihin liittyen. Varmistaa, että kun tulee lakivaatimuksia, jotka pitää viedä ja muuttaa sinne järjestelmään, niin ne otetaan huomioon. Kaikki tämän tyyppiset asiat. Aika usein siihen, etenkin jos puhutaan vähänkään merkittävämmästä järjestelmästä, niin siihen liittyy sitten kuitenkin myöskin resurssipainotuksia. Meillä saattaa olla meidän isoissa ”platformeissa” kolmekin ihmistä, jotka tekee täyspäiväisesti niiden kanssa töitä. Ja sitten tietysti pienkehitystä tai sitten laajennettuja käyttöönottoja. Ehkä se on myös semmoinen, mikä on tullut tässä matkan varrella [huomattua].” – H7

> "Asiakkaat katsoi sitä hankintahintaa, mutta ei oikeasti katsonut, että mitä se maksaa, kun sulla on se käytössä. Se on vähän sama, kun joku hankkii vaikka veneen ja toteaa, että ”no eihän tämä maksanut kuin 50 tonnia”. Mutta sitten niin kuin voin sanoa, itse olen omistanut joskus tommoisen ehkä vähän kalliimmankin veneen, niin voin sanoa, että helkkaristi sitä rahaa meni sitten sen saakelin vehkeen ylläpitoon. Enkä puhu pelkästään polttoaineesta. Ja tämä on tavallaan sitten se, mikä mun mielestä on yksi tärkeä asia myös. Hankintapäätöksessä yksi haaste on se, että jos ei tunnisteta, mitkä ovat sen järjestämän jatkuvat palvelut, eli tavallaan puhun siitä tuotantovaiheesta, niin se voi olla, että sieltä syntyy suuria kustannuseriä ja sitä kautta taloudellisista haastetta tai vähintään epävarmuutta. Ehkä jos oikeasti ruvetaan laskemaan, niin voidaan alkaa huomaamaan, että siihen liittyy aika kalliita asioita, vaikka sen jatkuvuuden tai muun varmistamiseksi." – H12

Piilotettujen kustannusten riskiin liittyen vastauksissa esiin nousee myös muutoskustannusten suuruus siirryttäessä järjestelmästä toiseen. Haastateltava H8 mainitsee muutosprojektien olevan mahdollisesti oletettua monimutkaisempia ja suurempikustanteisia kuin etukäteen on arvioitu:

> "Riippuu vähän tapauksesta, mutta voi olla aika isoja koulutustarpeita, joita ei ole osattu ottaa huomioon. Uusien järjestelmien käyttöönottoon liittyy aina yleensä migraatioita vanhoista järjestelmistä ja siellä voi olla aika isoja ja haastaviakin tekemisiä, joita ei välttämättä osata ottaa huomioon, jolloin se taloudellinen puoli voi tulla sielläkin aika mittavaksi, kun joudutaan tekemään erilaista konversiota ja migraatiota, että saadaan tiedot mukaan vanhoista järjestelmistä. Tämän tyyppisiä, että monessa kohdissa voi olla vaikea arvioida etukäteen. Se vaatii aika tarkkaa määrittelyä." – H8

H6 mainitsee suuret muutoskustannukset, jotka voidaan nähdä riskinä. Jos liiketoimintaa muutetaan oleellisesti tulevaisuudessa, saattaa se johtaa muutoksiin myös järjestelmätasolla. Tällaiset muutokset puolestaan aiheuttavat kustannuksia asiakasorganisaatiolle:

> ”Ehkä riski tulee siinä kohdassa, jos firman toimintoja oleellisesti muutetaan. Niin kauan, kun jatketaan sitä bisnestä niin kuin se on, niin “nou hätä”. Mutta sitten jos tulee joku isompi muutos, niin sellaisessa kohdasta sitten voi tulla yllättävän isokin kustannus muutosprojektina. Toki sopii toivoa, että edelleenkin pystytään käyttämään SaaS-järjestelmää täyspainoisesti. Se, että kuinka iso se ikään kuin uudelleenkonfigurointi esimerkiksi on, niin se on aina sitten sellainen oma lukunsa. Toki se on kaikissa järjestelmissä sitä, mutta SaaS-järjestelmät, kun on alun perin tavallaan kyseinen järjestelmä hankittu, niin on katsottu, että se sopii sen hetkiseen toimintamalliin hyvin. ”Custom-järjestelmät” on tavallaan sitä, kun sä teet sen ”custom-järjestelmän”, niin sitten

> sä “konffaat” siitä toisen ”custom-järjestelmän”. Mutta SaaS:issa ei välttämättä toimi ihan näin.” – H6

5.4.3 Taloudellinen toimittajaloukku

Haastateltavien vastauksissa toistuu toimittajaloukku, eli vendor lock-in, taloudellisten riskien kohdalla. Toimittajaloukun nähdään taloudellisten riskien lisäksi liittyvän myös muihin kategorioihin, joista yhtenä oleellisimpana on strategiset riskit. Taloudellisten riskien kohdalla toimittajaloukun nähdään liittyvän erityisesti siihen, että palveluntarjoaja saattaa nostaa palvelun hintoja silloin, kun asiakasorganisaatio on ajautunut toimittajaloukku-tilanteeseen. Irtautuminen toimittajaloukusta voi olla haastavaa, joten hinnankorotuksia on vaikea vastustaa. Esimerkiksi H1 mainitsee, että hinnannousut saattavat karata käsistä:

> ”Toki siinä voi olla sitten vendor lock-in tyyppisiä asioita, että ollaan jumissa jonkun ison toimittajan kanssa ja vaikea irtautua ja sitten hinnannousut karkaavat käsistä" – H1

Haastateltavat H2 ja H9 mainitsevat myös hinnannousujen olevan mahdollinen riski toimittajaloukkuun ajautuessa:

> "No kyllä aika merkittäviäkin taloudellisia riskejä siinä mielessä, että nyt ollaan jo nähty se, että hinnat on pompannut ihan merkittävästi siitä mitä ne olivat alunperin. Kun saadaan tavallaan tuntumaan siltä asiakkaalta, että nyt ollaan vendor lock-in -tilanteessa, niin sitten nostetaan helposti hintoja ja taloudellinen riski on aika merkittävä siinä tapauksessa." – H2

> ”Lisenssien tai käyttöoikeuksien korotukset, sillä järjestelmien vaihtaminen voi olla todella suuri investointi. Mikäli sopimuksellisesti ei hintoja lyödä lukkoon riittävän pitkäksi aikaa, on jopa todennäköistä, että hinnat nousevat merkittävästi." – H9

Hintojen nousu koetaan riskiksi varsinkin toimittajaloukkuun jouduttaessa. Toimittajaloukussa hinnankorotukset joudutaan usein hyväksymään, vaikka asiakas kokisi ne kohtuuttoman suuriksi. Tämä johtuu siitä, että SaaS-järjestelmän vaihtoon liitetyt vaihtoehtoiskustannukset koetaan hinnankorotuksia suurempina. Merkittävänä tekijänä nousee haastateltavien aikaisemmat kokemukset hintojen noususta, sillä kyseisen riskin tiedetään realisoituneen aiemmin.

5.5 Psykososiaaliset riskit

Psykososiaaliset riskit ovat haastatteluiden perusteella riskikategoria, jossa merkittävimpänä riskitekijänä nähdään SaaS-järjestelmään kohdistuva muutosvastarinta. Useampi haastateltava mainitsee merkittäväksi psykososiaaliseksi riskiksi muutosvastarinnan sen eri muodoissa. H11 mainitsee muutosvastarinnan riskitekijäksi seuraavasti:

> ”Mun puolelta mä tunnistan kyllä tuon ”change resistance”, joka on yksi, koska kyllähän se tietyssä mielessä, että sä vähennät sitä oman hallinnan mahdollisuutta, kun siirtyy on-premisesta pilveen, joka voidaan kokea uhkana tai riskinä tässä tapauksessa.” – H11

Tämän tyyppiset nostot korostavat muutosvastarinnan merkitystä vaikuttavana psykososiaalisena riskinä. Muutosvastarintaan mainitaan vaikuttavan useita erilaisia asioita, jotka kuitenkin kiteytyvät muuttuvien prosessien tai toimintatapojen tuottamaan ahdistukseen sekä muuhun stressiin, jota organisaatiossa pelätään. Useat haastateltavat mainitsevat tunnistavansa joitakin psykososiaalisia riskejä liittyen SaaS-järjestelmien käyttöönottopäätöksiin, mutta mainitsevat myös, että nämä riskit eivät vaikuta kaikissa tapauksissa lopulliseen käyttöönottopäätökseen. Esimerkiksi H13 havaitsee muutosvastarinnan tietynlaisena psykososiaalisena riskinä seuraavasti:

> ”Joo, itse asiassa tunnistan kyllä. Tästä on vuosia aikaa. Muistan, kun me otettiin meidän verkkokauppa-alustamme käyttöön ja se oli SaaS, niin meillä oli vastustusta IT:stä kyllä siihen. Koska se oli vähän niin kuin, että bisnes halusi ottaa sen käyttöön, koska se oli helppoa, nopeaa ja bisnes pystyi itse hyvin pitkälti käyttämään sitä tuotetta, niin kuin ”admin” puolella. Ja sitten se toi niin kuin IT:lle vastustusta, koska ei ole totuttu ensinnäkään ostaa semmoista, että ei ole totuttu siihen, että bisnes haluaa itse operoida. Eli siinä tuli tällainen identiteettikriisi sitten ICT:ssä” – H13

H13 tunnistaa muutosvastarinnan psykososiaaliseksi riskiksi, mutta mainitsee muutosvastarinnan vaikuttavuudesta käyttöönottopäätökseen seuraavaa:

> ”Ei ne kyllä enää ole. Se aika on ainakin meidän firmastamme eletty. Ja mä luulen, että siihen liittyy paljon se, että on tullut niin paljon uutta teknologiaa ja niiden käytettävyydet on kehittynyt huomattavasti. Niin ei tarvitse enää ikään kuin olla IT-velho pystyäkseen käyttämään. Ja se on tapahtunut ”all across”, niin mä luulen, että se on edesauttanut siinä muutoksessa.” – H13

H13 ja useampi muu haastateltava tunnistaa muutosvastarinnan riskiksi, joka ei kuitenkaan ole SaaS-järjestelmän käyttöönottopäätökseen vaikuttava tekijä, vaan asia, joka huomioidaan, mutta ei laskelmoida käyttöönottopäätöstä tehdessä. Muutosvastarintaan liittyvinä riskeinä haastateltavat nostavat myös henkilöstön tyytyväisyyden, koetun sosiaalisen oikeudenmukaisuuden sekä koetun prosessien monimutkaisuuden. Näistä H8 sanoo seuraavaa:

> ”Esimerkiksi sen uuden järjestelmän vaikeakäyttöisyys tai se, että se vaatii merkittävästi koulutusta, on riski. Tavallaan voisi ajatella myös niin, että työntekijät voivat kokea, että sen järjestelmän prosessi, mitä siinä otetaan käyttöön, niin siinä voi olla sellaisia piirteitä, jotka koetaan lainvastaisiksi tai jollain muulla tavalla haastaa sitä sosiaalista oikeudenmukaisuutta tai sen kokemusta. Tämän tyyppisiä asioita saattaa ilmentyä.” – H8

Henkilöstön tyytyväisyys, koettu sosiaalinen oikeudenmukaisuus sekä prosessien koettu vaikeakäyttöisyys nousevat erillisinä riskeinä kuitenkin vain kerran. Tämän lisäksi, nämä ilmentymät

voidaan luokitella myös muutosvastarinnan alle, sillä muutosvastarinnassa voidaan havaita tämänkaltaisia asioita.

5.6 Projektiriskit

Projektiriskit ovat haastatteluiden perusteella riskikategoria, jossa keskeisenä riskitekijänä esiintyy hankeosaamisen puute. Hankeosaamisen puutteeseen liittyvät asiat, kuten projektin kompleksisuus, resurssien riittämättömyys sekä osaamiseen liittyvät ongelmat. Usea haastateltava tunnistaa projektiriskien vaikuttavan SaaS-järjestelmän käyttöönottopäätökseen. Hankeosaamisen puutteeseen liittyvinä asioina nähdään käyttöönottoprojektin kompleksisuus sekä odotettua suurempi resurssitarve, joista muun muassa H8 mainitsee:

> ”Esimerkiksi tämä monimutkaisuus ja henkilökunnan taitojen ylittyminen. Mietin, että miten nämä asiat osataan huomioida käyttöönottopäätöstä tehdessä? Se monimutkaisuus monesti tulee siitä, että taloudelliset ja resurssiasiat ja projektin laajuus yllättää. Monesti on niin, että se työmäärä mikä sitten oikeasti vaaditaan sen käyttöönottoon, onkin moninkertainen, vaikka siihen mitä on osattu arvioida ja sitten siinä ylittyy sen takia jokin aikataulu tai sitten tämä budjetti, että näin minä itse ajattelen sitä.” – H8

H8 kuvaa projektin käyttöönottovaiheen monimutkaisuutta ja yllätyksellisyyttä riskitekijänä, minkä lisäksi hän mainitsee myös osaamisen ylittymisen SaaS-järjestelmän käyttöönottopäätökseen vaikuttavana tekijänä. Projektin monimutkaisuus saattaa vaikuttaa muun muassa budjetin ylittymiseen tai resurssien riittämättömyyteen. Monimutkaisuus nousee puheenaiheeksi myös H14 kohdalla:

> ”Täytyyhän sitä, kun SaaS-palvelua ollaan hankkimassa, niin arvioida, että miten helppo se on sitten integroida taloon, ottaa niin sanotusti käyttöön. Hyvin paljon, missä mä oon nyt ollut, nyt tulee mieleen oikeastaan enemmän näitä liiketoiminnan isompia hankkeita, niin erityisesti, kun puhutaan sen SaaS-palvelun hankinnasta, ja kun sillä oletettavasti meidän kontekstissa haetaan sitten myös prosessien kehittämistä. Halutaan standardoida jotain liiketoimintaprosessin osaa sellaiselle tasolle, mitä markkinoilla yleensä tehdään, ja yleensä siihen liittyy se SaaS sitten. Me halutaan sitten matuuria palvelua, joka kestää tarkastelua, eikä siihen tarvitse itse panostaa, kun se ei ole se lisäarvo, vaan hyödyntää enemmänkin sitä. Silloin tulee se, että kun tullaan siihen käyttöönottoon, että sitten pitäisi [olla] olemassa olevaa henkilökuntaa, jotka tuottavat ja osallistuvat sen prosessin omistamiseen, tai sen prosessin suorittamiseen. Tämän orkestrointi on tyypillisesti aika hankalaa riippuen laajuudesta, koska on niin monta osaa.” – H14

Aika, raha ja osaaminen mainitaan tärkeinä resurssitekijöinä, jotka vaikuttavat havaittuun projektiriskiin. Ajasta mainitsee myös H10:

> ”Mutta sitten jos me rupeamme katsomaan esimerkiksi jotain siirtymää SaaS:iin. Jos sä viet jotain, sanotaan, että sulla on ollut joku, mistä sä siirryt tähän SaaS-palveluun. Niin kuinka kauan tämä siirtymä esimerkiksi kestää? Mulla on itseasiassa nyt semmoinen

> projekti menossa, missä mä oon siirtymässä palvelusta toiseen. Ja tavallaan se siirtymä kestää aivan luokattoman kauan. Ja se on ihan täysin tavallaan, no en mä olisi voinut ikinä kuvitellakaan, että se kestää niin kauan, mutta se on myös tavallaan mun osaamattomuuttani, koska mä en osannut sitä ottaa huomioon riskinä.” – H10

Monimutkaisuus ja resurssien riittämättömyys ovat merkittäviä riskitekijöitä, joka vaikuttavat havaittuun projektiriskiin ja täten myös SaaS-järjestelmien käyttöönottopäätökseen.

5.7 Riskienhallinta ennen SaaS-järjestelmän käyttöönottopäätöstä

5.7.1 Organisaation tarpeen ja vaatimusten määrittely

Usea haastateltava nostaa organisaation tarpeen ja vaatimusten määrittelyn tärkeäksi havaittuja riskejä pienentäväksi tekijäksi, joka otetaan huomioon ennen SaaS-järjestelmän käyttöönottopäätöstä. Haastateltavien vastauksissa korostuu liiketoiminnan tarpeen ymmärtäminen osana SaaS-järjestelmän käyttöönottopäätöstä sekä riskien pienentämistä ja kartoittamista. Tarpeen määrittelyssä korostuu ymmärrys järjestelmän todellisesta käytöstä osana liiketoiminnan ja koko organisaation prosesseja. H1, H12 ja H14 mainitsevat asiasta seuraavaa:

> ”Mutta ne tulee meillä siinä, kun ne on julkisia kilpailutuksia ja hankintoja, niin meillä on tosiaan siellä vaatimusmäärittelyssä ja siinä hankintavaatimuksissa jo määritelty ne tietyt peruskriteerit.” – H1

> ”Ja sun pitää tavallaan sitä omaa liiketoimintaa ehkä jossain asioissa enemmän sovittaa siihen ympäristöön, mitä siellä on, kuin se, että sitä tietojärjestelmää sovitettaisiin siihen sun bisnekseen. … Ja tämähän tarkoittaa just sitä, että strategisessa riskissä yksi tärkeä asia on se, että silloin kun liiketoiminta tietää, mitä se haluaa, tai sulla on jollain tavalla määritetty niitä asioita, niin silloin se strateginen puoli on jo paljon helpompi. Eli sinä tiedät tavallaan, mitä se liiketoiminta on hakemassa tai ainakin toivoo saavansa. Toisaalta, jos tavallaan tämä puoli on epävarmaa, niin se ei tarkoita, että se asia menisi huonommaksi, mutta se vastuu siirtyy hurjan paljon tietohallinnon puolelle. Ja sitten taas ollaankin jo enemmän semmoisissa asioissa, missä bisnes saattaa olla sitten jo vähän jälkijättöisesti mukana, jos tehdään hankintapäätökset ensin ja sitten ruvetaan katsomaan, että “ai niin, mitä sillä muuten piti tehdä sillä SaaS-työkalulla” – H12

> ”Mun vinkkelistä, miten mä näen tätä, niin kun ollaan SaaS-järjestelmää hankkimassa, niin ensin kiinnostaa se, onko se talon strategian mukaista, ja miten se istuu tavoitearkkitehtuuriin. Nyt puhutaan arkkitehtuurista, kokonaisarkkitehtuurista, eli se pitää sisällään kaiken, ei pelkästään IT:n, vaan myös liiketoiminta-arkkitehtuurin. Miten se istuu siihen? Jos ei se istu strategiaan ja siihen kokonaistavoitearkkitehtuuriin, niin sitten tuhlataan aikaa. Sitten ollaan sovittamassa jotain, jonka motiivi on jotain, joka ei ole huomioitu jostain syystä strategiassa, eikä kokonaisarkkitehtuurissa. Ja jos näin on, niin sitten on joku rikki jossain. Se voi olla, että se on tarpeellinen, mutta sitten vaan tarkoittaa, että jotain ei ole huomioitu tai ymmärretty. Mutta jos tuosta pääsee läpi, niin silloinhan se on enemmän sitten ”executeemista” ja sen sovittamista sitten. – H14

Vastausten perusteella organisaatioiden olisi kannattavaa kiinnittää huomiota liiketoiminnan tarpeiden määrittämiseen ja kokonaisarkkitehtuurin yhteensopivuuteen SaaS-järjestelmän kanssa jo ennen SaaS-järjestelmän käyttöönottopäätöstä. Tähän liittyy vaatimusten ja kriteerien asettaminen liiketoiminnan tarpeiden mukaisesti, jotta ei jouduta tilanteeseen, jossa valittu järjestelmä on alkujaan sopimaton. Sopimaton järjestelmä johtaa siihen, että toivottuja hyötyjä ei saavuteta.

5.7.2 Palvelun vastaavuus ja kyvykkyyskartoitus

Useampi haastateltava mainitsee palvelun vastaavuuden ja kyvykkyyskartoitukset tärkeäksi osaksi riskienhallintaa ennen SaaS-järjestelmän käyttöönottopäätöstä. Palvelun vastaavuuden ja soveltuvuuden varmistamiseksi tehdään erilaisia asioita, kuten SaaS-ratkaisun testaamista ja SaaS-järjestelmän soveltuvuusarviointia, jossa järjestelmää verrataan olemassa olevaan kokonaisarkkitehtuuriin ja liiketoiminnan tarpeisiin. H5, H6 ja H7 mainitsevat näistä asioista seuraavaa:

> ”Käyttäjävaatimukset on meillä todella iso ja tärkeä kokonaisuus jo sen validisuusvaatimuksen takia. Eli itse asiassa joka ikinen käyttäjävaatimus pitää validoinnissa testata ja käyttäjävaatimusta kohtaan pitää olla testi.” – H5

> ”No kyllä siis sanotaan, että SaaS-järjestelmissä yleensäkin on se yhteensopivuus firman prosessien kanssa, että sen varmistaminen tavalla tai toisella. Jos sitä ei tee kunnolla ja tulee yllätyksenä, niin siinä kohtaa voi mennä monessakin suunnassa aika pahasti pieleen. Jos tiivistyksen tiivistystä täytyy ottaa, niin nimenomaan katso, että se sun SaaS-järjestelmä ”mätsää” sun prosesseihin ja täyttää sen tarpeen kunnolla.” – H6

> ”No ehkä paremmin hahmottaa tosiaan sitä kokonaisuutta sekä se, että miten se järjestelmä istuu sen yrityksen IT-arkkitehtuuriin. Miten se järjestelmä istuu nykyiseen yritykseen tai siihen, miten se vastaa prosessin tarvetta ja loppukäyttäjien tai bisnesomistajan todellista tarvetta. Ja sitten myöskin kustannusten näkökulmasta, että mikä se todellinen lisäkustannus on, mitä se järjestelmä ja sen kaikki vaaditut palvelut kautta resurssit tarvitsevat.” – H7

H5 painottaa käyttäjävaatimusten merkitystä ja järjestelmän testausmahdollisuutta, eli kokeiltavuutta, joka on myös yksi aikaisemmassa tutkimuksessa löydetty SaaS-järjestelmän käyttöönottopäätökseen vaikuttava tekijä (Safari ym., 2015). H6 ja H7 puolestaan painottavat prosessien ja SaaS-järjestelmän linjautumista ja vastaavuutta. Liiketoimintaprosessien ja SaaS-järjestelmän tulee olla yhteensopivat. Yhteensopivuus on aikaisemmassa tutkimuksessa havaittu olevan SaaS-käyttöönottopäätökseen vaikuttava tekijä (Safari ym., 2015).

Useampi haastateltava mainitsee kyvykkyyskartoitukseen liittyen palvelun arvioinnin ja analysoinnin tärkeänä toimena ennen SaaS-järjestelmän käyttöönottopäätöstä. Haastateltavat

mainitsevat, että palveluntarjoajan kyvykkyyttä on tärkeä analysoida. Palveluntarjoajan on myös varmistettava riittävä panostus halutun palvelutason toimittamiseksi. Tämän lisäksi palveluntarjoajan liiketoiminnan tulevaisuusnäkymien arviointi sekä referensseihin nojautuminen ovat esillä vastauksissa. Palveluntarjoajan analysoinnista ja panostuksesta halutun palvelutason toimittamiseksi mainitaan seuraavaa:

> ”Heidän pitää täyttää ne vendor-riskiin liittyvät asiat, riittävän kokoinen firma ja heidän pitää taata tietty osaaminen esimerkiksi omalta henkilöstöltään.” – H1

> ”Useimmat markkinatoimittajat ovat olleet tässä bisneksessä jo jonkin aikaa ja siellä on taustalla Microsoftia, Azurea, Googlea tai AWS:ää ja siellä on aika hyviä teknologioita skaalata sitä suorituskykyä. Yleisesti ottaen, kun arvioidaan toimittajan kyvykkyyttä, me haluamme jotain todisteita siitä, miten he esimerkiksi seuraavat kapasiteettia siinä palvelussa ja miten he pystyvät raportoimaan meille sitä palveluntasoa.” – H3

> ”No silloin, kun lähdetään ihan siitä, että tehdään näitä, niin ihan sieltä alusta asti RFI-prosessista alkaa, niin silloinhan ne on totta kai mukana siellä. Mä tein itse esimerkiksi energiapuolelle kilpailutuksen tuossa noin muutama vuosi sitten, niin se oli yksi tämmöinen merkittävä asia itse asiassa siellä arvostuksessa. Tämä on nyt tämän kokoinen firma. Ja tavallaan periaatteessa sen firman kyvykkyys, mikä tulee koon ja tuotevalikoiman ja tämmöisten kautta. Eli pystyykö se ikään kuin sitä kautta vastaamaan.” – H6

Haastateltavien mukaan palveluntarjoajaa arvioidaan, ja pyritään täten varmistamaan palveluntarjoajan kyvykkyys. Palveluntarjoajan koko mainitaan useamman kerran. Palveluntarjoajan suuruuden nähdään vaikuttavan organisaatioiden näkemyksiin palveluntarjoajan kyvykkyydestä positiivisesti. Palveluntarjoajan analysointi sekä selkeät viitteet suorituskyvyn riittävyydestä ovat useamman haastateltavan mukaan merkittäviä tekijöitä riskienhallinnassa ennen SaaS-järjestelmän käyttöönottopäätöstä. H1 ja H6 mainitsevat kyvykkyyden varmistamisen sekä tulevaisuudennäkymien analysoinnin tärkeänä osana kyvykkyyskartoitusta:

> ”Onko se toimittaja uskottava ja että onko se semmoinen firma, että ne osaajat pysyvät siellä, että onko meillä luottoa siihen, että se on viiden vuoden päästäkin pystyssä …” – H1

> ”Joissain vastaavissa kilpailutuksissa on pitänyt oikeasti katsoa myös sitä, että mikä tämän firman [palveluntarjoajan] todennäköinen positio on 5–10 vuoden jälkeen. Tämä on taloudellinen riski toki, mutta onko se esimerkiksi semmoinen, että todennäköisesti toi on sen kokoinen, että joku toinen firma kiinnostuu siitä ja ostaa sen pois. Joissain näissä tapauksissa meni sinne itse asiassa johonkin 10–15 vuotta taaksepäin. Silloin mä olin [suuressa suomalaisessa kansainvälisessä yrityksessä] vielä tekemässä kilpailutuksia, niin meillä oli yksi tämmöinen. Se oli joku master dataan liittyvä keskikokoinen nouseva kyky, joka oli meidänkin arvostuksessa teknisesti siellä kärkipäässä. Mietin jo siinä kohtaa, että jos mä olisin joku investori, niin mä ostaisin tuon pois vähän ajan päässä. ... Tuossa [toisessa] jutussakin siinä oli tällaisia nousevia tähtiä jonkun verran mukana, ja se

> oli ihan selkeästi yksi asia, mitä mä siellä vertailin. Eli että onko tämä todennäköisesti osa toista firmaa hetken päästä?”

Tulevaisuudennäkymät ja palveluntarjoajan positio markkinoilla on haastateltavan mukaan tarkastettava ja analysoitava, jotta voidaan varmistua tarjoajan kyvykkyydestä pidemmällä aikavälillä. Useampi haastateltava mainitsee referenssit, joilla pyritään varmentamaan palveluntarjoajan luotettavuutta ja kyvykkyyttä. H3 ja H5 mainitsevat asiasta seuraavaa:

> ”No tärkeimmät vaikuttaa, sillä lailla että ei pääse edes tarjoamaan, jos ei täytä niitä pakollisia vaatimuksia. Joku sanoo vaikka, että se ei halua täyttää meidän tietosuojan ja tietoturvan vaatimuksia niin se ei pääse tarjoamaan. Tai se ei täytä, vaikka jotain referenssivaatimuksia, että ne on niin kuin niin pieniä tai ei ole käytössä missään, niin se ei pääse edes tarjoamaan.” – H1

> … ”yleensä on sitten referenssit, että ne pyritään aina jollain tavalla varmentamaan, että se ei ole ihan huuhaata mitä siellä on.” – H3

> ” Että se on kyvykäs toimittaja. Sitä selvitetään eri tavoin. On näitä referenssejä …” – H5

Haastateltavien perusteella myös referensseillä tai referenssivaatimuksilla on merkitystä ennen SaaS-järjestelmän käyttöönottopäätöstä. Referensseillä pyritään varmentamaan palveluntarjoajan kyvykkyys ja referenssivaatimuksilla voidaan pienentää joidenkin riskien realisoitumisen todennäköisyyttä. Tämän lisäksi vaatimuksilla ja selvityksillä pyritään vaikuttamaan tietoturvariskien pienentämiseen. H11 ja H14 mainitsevat asiasta seuraavaa:

> "No taas mä käännyn, että se riippuu siitä, minkälainen ”framework” toimittajalla on käytössä. Jos sieltä saadaan kaikki sertit ja SOC 2, niin kyllä mä kuittaan aika pitkälle mahdolliset tietoturvariskit niillä katetuiksi, tai ainakin mitigoiviksi." – H11

> "Ja se on tavallaan meillä SaaS-palveluihin, kun niitä hankitaan, niin aika usein tai käytännössä aina sisällytetään siihen se auditointimahdollisuus eli mahdollisuus auditoida palvelu eri näkökulmista. Yksi tyypillisin on nimenomaan tietoturvan kulmalta, tai kyberin kulmalta ... Tämä on se kulma, millä yleensä varmistetaan, että palvelu tuotetaan oikein. Ja niissä yleensä me käytämme kolmansia osapuolia tuottamaan sen arvio palvelun soveltuvuudesta meidän vaatimuksiin, mitä meillä on tietoturvan osalta. Ja sitten, jos sieltä nousee poikkeamia ja nousee havaintoja, niin joko niitä pystytään jollain mitigoimaan tai hallitsemaan ja jäännösriski jää pieneksi, hallittavaksi ja hyväksyttäväksi …” – H14

Tietoturvavaatimuksilla ja -selvityksillä voidaan hallita tietoturvariskejä, jotka ovat haastateltavien perusteella yksi merkittävimmistä riskeistä. Tietoturvavaatimuksilla ja -selvityksillä voidaan haastateltavien mukaan varmistua siitä, että palveluntarjoaja tuottaa palvelua asiakasorganisaation näkökulmasta toivotulla ja tarpeeksi tietoturvallisella tavalla.

5.7.3 Sopimustekniset asiat

Usea haastateltava mainitsee sopimusteknisiä asioita riskienhallinnassa ennen SaaS-järjestelmän käyttöönottopäätöstä. Osa haastateltavista mainitsee etukäteen määritellyt hinnat sekä sopimuskauden pituuden olevan asioita, jotka tulee ottaa huomioon jo ennen SaaS-järjestelmän käyttöönottopäätöstä. H2 ja H5 mainitsevat seuraavaa:

> ”Kyllä ehdottomasti on ja sen takia niissä sopimuksissa täytyy olla erityisen tarkka, että varmistetaan se ”exit” siellä. Jos lähtee ihan niin kuin käsistä sen hinnoittelu. Mutta että meilläkin on esimerkkejä, että hinnat ovat nousseet 30 prosenttiakin. Eli ”exitin” suunnittelu ja ehkä sitten pidemmät sopimuskaudet, jos se katsotaan järkeväksi, jossa lyödään se hinta kiinni 3–5 vuodelle.” – H2

> ”Tyypillisesti käyttäjämäärät joustavat iloisesti ylöspäin, mutta surullisesti alaspäin. Me saadaan neuvoteltua hinta jollekin tietylle käyttäjämäärälle. Siinä voi olla jotain volyymiportaita tai mitä vaan, kun puhutaan isosta organisaatiosta, mutta tyypillisesti se hankintasitoumus on sille jollekin minimimäärälle. Jos me tavallaan hypoteettisesti sanotaan, että me tarvitsemme 1500 lisenssiä niin 1500 lisenssillä hinta on jotain. Jos me halutaankin varmistua, että meillä ei jää käyttämättömiä lisenssejä missään vaiheessa, että ne hankitaankin tavallaan 1000 lisenssiä per seuraavat kolme vuotta ja sitten siihen 500 päälle heittolisensseinä, että me voidaan joustavasti sitten niitä vähentää tai lisätä, niin tyypillisesti 1000 lisenssin hinta on jotain x ja 500 lisenssin hinta on 1,5 kertaa x.” – H5

H8 mainitsee, että SaaS-järjestelmän käyttökustannusten tulisi seurata liiketoiminnan volyymien vaihtelua, jolloin hiljaisempina aikoina kustannusten tulisi olla pienempiä:

> ”Tämmöistä ei nykyään ole niinkään, mutta kun meillä voi olla jo tilanteita missä on tällaisia piikkipaikkoja, missä johonkin aikaan vuodesta syntyy merkittävä kuormaa tuohon järjestelmään ja sitten voi olla toisaalta niitä hiljaisempia aikoja. Tämä tulee huomioida siinä sopimuksessa, että se kustannus skaalautuu myöskin. Laskutuksen pitää seurata tavallaan sitä, että se skaalautuu se järjestelmä. Laskutuksen pitää seurata sitä, ettei makseta kapasiteetista silloin, kun sitä ei käytetä. Tämän tyyppisiä asioita voisi tuohon lisätä.” – H8

Haastateltavat mainitsevat vastauksissaan myös exit-strategian, eli strategian, jolla irtaudutaan tietystä SaaS-järjestelmästä. Tämän lisäksi haastateltavat mainitsevat turvatakuiden sopimisen tärkeyden käyttöönottopäätöstä edeltävässä riskienhallinnassa. Haastateltavat mainitsevat SaaS-järjestelmään siirtymisen muodostavan kumppanuuden palveluntarjoajan ja asiakasorganisaation välille, josta irtaumista täytyy suunnitella etukäteen. Tähän liittyy sopimukselliset määritykset siitä, miten toimitaan yhteistyön loppuessa ja uuteen järjestelmään siirryttäessä. H3 mainitsee asiasta seuraavaa:

> ”Tottakai nämä kysymykset liittyy myös siihen, että me tehdään myös siinä hankintavaiheessa sitä pohdintaa exitistä, koska kaikki sopimukset päättyy jonain päivänä

> jollain tavalla. Että se tapa millä me kävellään tästä jos tulee ryppy rakkauteen tai jotain muutoksia. Kyllä me mietitään tämä irtautuminen kaikissa sopimuksissa." – H3

Myös muun muassa H2 mainitsee exit-strategian sopimisen tärkeydestä ja sen yhteydestä esimerkiksi toimittajaloukkuriskin toteutumiseen. H2 mainitsee lisäksi, miten palveluntarjoajaa voidaan velvoittaa tukemaan asiakasorganisaatiota siirtymässä uuteen järjestelmään:

> "Se vendor lock-in, kun jotain viedään SaaS:iin, niin exit-suunnitelma, eli se miten siitä päästään irti pitää miettiä siinä kohtaa. Siihenkin otetaan usein sopimuksissa kantaa, että me omistetaan data ja meillä on mahdollisuus saada tavalla tai toisella se data sitten itsellemme siinä kohtaa, kun lähdetään eri teille. Yleensä vielä sellainen klausuuli, että se SaaS-palveluntarjoaja velvoitetaan tukemaan meitä siinä siirtymässä toiseen SaaS-palveluun." – H2

Lisäksi H14 mainitsee exit-suunnitelman sekä kriteeristön ymmärtämisen tärkeyden, minkä lisäksi exit-suunnitelman todennäköisyys ja siihen liittyvä jäännösriski tulisi huomioida riskienhallinnassa ennen käyttöönottopäätöstä:

> ”Yhden tällaisen hyvän voisi nostaa tässä, mikä mulla nyt viime aikoina erään palvelun ulkoistuksessa tuli esiin on se, että jos geopoliittinen tilanne muuttuu tietyllä tapaa, niin pitääkö meidän vetää palvelu takaisin sisään. Eli tavallaan exit-suunnitelma ja exit-kriteeristön ymmärtäminen. Taisi olla silloin, että palvelu tuotettiin tai tuotetaan EU ja ETA-alueen ulkopuolelta, jos siihen sitten liittyy riski, että esimerkiksi EU-tasolla tai jopa kansallisella tasolla sitten haluttaisiin irtautua, vaikka kyseisen maan palvelusta ja muista, niin se tarkoittaisi sitten irtautumista siitä ulkoistuksesta. … Sittenhän meidän pitäisi varautua siihen, että sitä osaamista otetaan takaisin tai uudelleen organisoidaan muuten. Tämän tyyppinen on sellainen, mitä me arvioimme aika lailla jokaisen SaaS-hankinnan kanssa. Ehkä semmoisena keskeisenä strategisena riskinä mä näen sen, että kuinka kestävä se valinta on ja minkälainen jäännösriski liittyy siihen exit-suunnitelmaan sitten, että kuinka todennäköisesti siihen joudutaan menemään. Syystä tai toisesta.” – H14

Osa haastateltavista mainitsee vastauksissaan turvatakuut. Turvatakuilla voidaan varmistua siitä, että oman liiketoiminnan jatkuvuus säilytetään myös silloin, kun palveluntarjoajan liiketoiminta loppuu, palvelusta tulee siirtyä toiseen tai tapahtuu jokin muu ongelmatilanne, joka muutoin aiheuttaisi hankaluuksia. Osa haastateltavista puhuu sopimuksen tuomasta turvasta, johon exit-strategiakin voidaan liittää. H1 ja H3 mainitsevat sopimukset, joiden avulla voidaan varmistua siitä, että oma data saadaan palautettua ja varmistettua myös ongelmatilanteissa:

> "Entä jos se firma menee tosiaan konkkaan tai se häviää missä se koodi on, että siihen on tietysti ratkaisuja niin sanottuja escrow-sopimuksia, että se ”source-koodi” viedään talteen jonnekin ja meillä on mahdollisuus se saada," – H1

> ”Eli miten sä pystyt varmistamaan, että sun liiketoiminnalle tärkeät datat ovat suojassa, että ne pystytään aina palauttamaan, tapahtui mitä tahansa. Siinä on paljon kompleksisuutta. Me pyritään se tänä päivänä hanskaamaan sopimusten kautta…” – H3

Useat haastateltavista mainitsevat sopimusteknisenä asiana tietoturvan- ja tietosuojan sopimusmääritykset. Nämä tulee määritellä sopimuksissa, jotta palveluntarjoaja tiedostaa, millaista tietoturva- ja tietosuojatasoa asiakasorganisaatio vaatii noudatettavan. Muun muassa H1 ja H2 mainitsevat näistä sopimusteknisistä asioista seuraavaa:

> "No jos mä ajattelen, että kun valitaan SaaS-palvelutarjoajaa niin meillä on omat tietysti tämmöiset tietosuoja- ja tietoturvaehdot. Jos kiinnostaa ne voi lähettää perästä päin mailissakin. On tämmöinen oma ”planketti”, mihin sen toimittajan pitää sitoutua ja siinä on oikeastaan kerrottu niitä käytännön juttuja ja vähän valvontaankin liittyviä asioita. Sopimusehdoissa meillä on just nämä tämmöiset perusklausuulit, että meidän pitää tietää missä se data on ja kuka alihankkija käsittelee sitä dataa ja sitä järjestelmää. Nämä ovat siis perushygieniafaktoreita, jotka me haluamme tietää." – H1

> ”Tietoturva on osana SaaS-sopimuksia yleensä. SLA, GDPR ja DPA eli datankäsittelysopimukset on aina niitten toimittajien kanssa, jossa määritellään se datan sijainti.” – H2

Haastateltavien vastauksista nousee esiin palveluntarjoajan sekä asiakasorganisaation vastuiden ja velvoitteiden määrittäminen sopimuksissa. Muun muassa H1 ja H2 mainitsevat siitä, miten sopimuksissa voidaan vaatia, että palveluntarjoaja suhtautuu vakavuudella palvelun tuottamiseen:

> ”Sitten täytyy olla tietty määrä tietyn tason osaajia tukemassa ja kehittämässä sitä järjestelmää niin sillä ei oikeastaan ole merkitystä onko se SaaS tai joku muu tekniikka, mutta ne koskee niitä kaikkia ja sillä sitä riskiä sitten vähennetään.” – H1

> "No ei niissä ole noussut, että me otetaan sopimuksissa aina kantaa sitten siihen, että koitetaan suojata sopimusteknisesti meidän mainetta ja sitä, että toimittaja suhtautuisi vakavuudella, kun ne tuottaa meille palvelua..." – H2

Tämän lisäksi H8 puhuu vastuiden ja velvoitteiden määrittelyn tärkeydestä siinä, että kaikki osapuolet tietävät tehtävänsä, minkä lisäksi ongelmatilanteissa pystytään myös vetoamaan kyseisiin sopimusmäärityksiin:

> "Nämähän on sellaisia SaaS-järjestelmässä olevia ihan oleellisia riskejä, että miten me voidaan vakuuttua siitä, että meidän tieto on aina saatavilla ja eheys, että se tieto on koskematonta ja siihen ei ole kajottu. Esimerkiksi nyt geopoliittisen tilanteenkin ollessa sellainen, kun se on, niin miten voidaan varmistua siitä, että SaaS-järjestelmän kohdalla, jota käytetään internet-yhteyksillä, meillä on pääsy siihen meidän järjestelmään? Miten esimerkiksi, jos tulee tällaisia tilanteita, että tietoon ei voida enää luottaa tai siihen joku pääsee koskemaan niin miten sitten palaudutaan niistä? Tän tyyppisiä asioita varmaan nyt tulee mieleen. Ja nämä ovat sitten sopimusasioita, koska SaaS-järjestelmässä oleellista on se, että sitä johdetaan sen sopimuksen kautta, että siinä on oltava sitten sopimuksissa hyvinkin tarkkaan ne vastuut ja velvollisuudet jokaisella osapuolella. Jos ei ole riittävän hyvin vastuita kuvattu, niin sitten on aika vaikea niihin vedota, jos jotain tapahtuu. Eli sopimuspuolella se riski on aika merkittävä ja sopimuksilla pyritään sitä riskiä taklaamaan, että ne asiat olisivat sovittu ja hallinnassa." – H8

5.7.4 Hankeosaaminen ja resursointi

Osan haastateltavien perusteella riskienhallintaan ennen SaaS-järjestelmän käyttöönottopäätöstä liittyy myös hankeosaaminen ja resursointi. Haastateltavien vastaukissa nousee esiin tarve osallistaa ja sitouttaa henkilöstö ja sidosryhmät muutokseen, sekä varmistaa laadukas ja monimuotoinen osaaminen muutosprojektin läpiviemiseksi. H12 ja H14 mainitsevat asiasta seuraavaa:

> ”… sen oman organisaation pitää myös alkaa sitten jo muodostamaan sitä projektiorganisaatiota. Eli me pystytään myös sitten tarvittaessa ihmisiä sitouttamaan siihen mukaan … Että jos ihmiset eivät ole tietoisia, että esimerkiksi joku tämmöinen hankintakuvio, tai muu on tulossa, tai ollaan järjestelmää uudistamassa, ja eivät pääse siihen mukaan. Niin ei se tarkoita sitä, etteikö ihmiset tekisi hommiaan. Mutta kyllä yleensä se työn laatu ja ennen kaikkea se, että kun tulee ensimmäiset ongelmat. Niin se kyvykkyys, ja halu tavallaan selvittää niitä asioita, ja viedä se niin sanotusti positiivisesti eteenpäin on aina parempi.” – H12

> ”Ja silloin, kun otetaan omaa porukkaa mukaan, niin sen pitää olla osaavaa, pitää olla monelta eri näkökantilta. Ja se hankeosaaminen on todellakin oltava aika vahvaa. Koska muuten siinä, niin kuin mä olen nähnyt, että sitten vaan vaihtuu se bändiä pyörittävä tahtipuikonheiluttaja, kun mikään ei toimi, jos se ei ymmärrä. Ja siinä pitäisi ymmärtää tosi laajasti sitä kontekstia, ketkä siellä laajuudessa on. Siinä ei ole pelkästään se toimittaja, vaan siinä on tosi paljon eri sidosryhmiä siitä omasta organisaatiosta myös, riippuen SaaS:in laajuudesta. … Mutta mä itse pidän, että kun on vahva hankeosaaminen, niin osaa ymmärtää näitä riskejä, mitä liittyy muutosvastarintaan tai viestintään, joka epäonnistuu ”by the way” aina. … Mutta jos on kova hankeosaaminen, niin pystyy taklaamaan näitä ja ymmärtää, että näihin pitää panostaa.” – H14

Hankeosaamisen varmistaminen sekä henkilöstön sitouttaminen on haastateltavien mukaan tärkeää. Tämän lisäksi haastateltavat mainitsevat projektin toteuttamisen suunnittelun ja resurssitarpeen varmistamisen tärkeinä tekijöinä riskienhallinnassa jo ennen SaaS-järjestelmän käyttöönottopäätöstä. H6 ja H14 mainitsevat projektitoimitusmallin hahmottamisesta ja vastuumäärittelystä seuraavaa:

> ”Joo, kyllä näissä kaikissa hankkeissa, missä olen ollut, niin on noudatettu ihan tällaista, sanotaan hyvää projektihallintamenetelmää. Eli riskisuunnitelma on siellä mukana. Toki se on sitten aina, että kuinka kokenut manageri on, niin kuinka perusteellisesti tehdään. Mutta kyllä niissä käytännössä on ne samat praktiikat olleet käytössä. Ja riskit kirjataan hyvinkin tarkkaan, kirjataan mikä se sisältö on, riippuvuudet, mahdolliset taloudelliset vaikutukset, mitigaatiotavat, ketkä ovat vastuussa ja niin edelleen. Eli ihan siis sanotaan, että otat ihan minkä tahansa projektin ”management-templaten”, niin vastaavia seurataan. – H6

> ”Jos SaaS-järjestelmää joku mulle myy, eli tässä nyt oli taas joku järjestelmä, mitä me ollaan hankkimassa, niin mähän tapasin sen IT-toimittajan, kun ”bisnes” oli käynyt jo pitkään keskustelua. Niin mähän pyysin heiltä projektitoimitusmallin. Miten he toimittavat ja mikä on se heidän sapluunansa? … Ja tässähän nimenomaan puhutaan näistä riskisuunnitelmista. Eli tavallaan tämmöisestä vastuumatriisista. Koska yksi iso osahan on tavallaan tämmöisissä riskiasioissa myös se, että kuka tekee ja mitä tekee. Eli

> olette varmaan kuulleet tällaisesta RACI-matriisista. … Niin tämä on mun mielestä semmoinen, minkä ehkä voisi ajatella, mikä sitten just korostuu siinä, kun lähdetään sitä käyttöönottoon kuuluvaa riskisuunnitelmaa [pohtimaan]. Ja yleensä mä pyydän aina jonkun alustavan projektisuunnitelman, koska sitten pystytään myös katsomaan, että mitä meiltä odotetaan asiakkaan roolissa, ja mitä sitten toimittaja tekee, ja ottaa oletettavasti silloin myös vastuuta siitä.” – H14

Osan vastausten perusteella projektitoimitusmalli tulisi ymmärtää ja hahmottaa etukäteen, minkä lisäksi myös vastuuasiat tulisi määrittää niin sopimusteknisesti, kuin myös yleistasollakin ennen käyttöönottopäätöstä. Vastuuasiat palveluntarjoajan ja asiakasorganisaation kesken tulisi selvittää ennen SaaS-järjestelmän käyttöönottopäätöstä, jotta näihin liittyvät riskit voidaan minimoida. Resurssitarpeen varmistaminen, jolloin ymmärretään tarvittava resurssimäärä ja varmistetaan, että organisaatiolla on riittävästi erilaisia resursseja muutoksen läpivientiin, nousee keskeisenä toimenpiteenä vastauksissa. H6 ja H8 sanovat asiasta seuraavaa:

> ”Mutta sanotaan, että nämä osaamiset ja henkilöiden saatavuus, että on tarpeeksi resursseja, ne valitettavasti yleensä huomataan vasta liian myöhään. Elikkä se tulee sitten, kun projekti on jo liikkeellä, että nyt tätä ei saatu tehtyäkään. Ne on sellaisia asioita, joita ei välttämättä pysty mittaamaan niin helposti, kun tehdään jotain sopimuksia vaikka.” – H6

> ”… jos lähdetään projektia tekemään ja meillä on projektisuunnitelma, missä se raha ja resurssit elikkä se henkilötyö on sitä, mitä me ostetaan palveluna ja siitä me maksetaan palkkoja sekä sitten se muu, mihin käytetään rahaa siinä projektissa. Sitten on se projektin laajuus, mikä on tärkeää, että se on arvioitu, että se on oikein eli tietysti se, että mikä on se sisältö mitä saadaan. … Yleensä projektissa jokin näistä ei jousta, että jos nyt ajatellaan, että halutaan tietty järjestelmä, mikä tekee tietyt temput, jolloin me emme voi vähempää hyväksyä, niin silloin joku asia joustaa. Jos se tekemisen laajuus yllättää meidät, että nyt loppuu joko rahat tai sitten tarvittaisiin lisää aikaa, että keretään kaikki tämä tekemään … Meillä aika usein on, että sen käyttöönoton pitää tapahtua tiettyyn päivään mennessä, kun meidän vanhat sopimuksemme päättyy tai joku lainsäädäntö muuttuu. Meidän on pakko saada se uusi järjestelmä käyttöön juuri silloin. Silloin meillä käyttöönottopäivä ei jousta ja sitten pitää miettiä, että millä kapasiteetilla tai volyymilla me teemme, että jos alkuperäinen budjetti ei meinaa riittää. … Mitä jätetään pois alkuperäisestä laajuudesta?” – H8

Osan haastateltavien mukaan resurssitarpeen varmistaminen sekä resurssijoustavuuden ylläpitäminen ovat tärkeitä asioita riskienhallinnan näkökulmasta ennen SaaS-järjestelmän käyttöönottopäätöstä. Organisaatiolla tulee olla selkeä käsitys vaadittavista resursseista sekä toimenpiteistä, jotta vaaditut resurssit eivät ylittyisi projektin aikana. H12 ja H14 mainitsivat resursseista seuraavaa:

> ”Kyllä se hankintapäätös on se, että jos me päätetään hankkia, niin kyllähän muun muassa se tarkoittaa sitä, että onko meillä riittävästi ihmisiä tekemään se työ, että me otetaan se käyttöön. Konsultteja varmaan aina riittää, mutta kun siihen tarvittaisiin aina, niitä omiakin ihmisiä mukaan. Kyllä nämä niin kuin silleen on tämmöistä resursointia ja raha-asiaa. Onko rahaa sitten tehdä sitä ja tosiaan, onko meillä aikaa? Tämä on semmoinen

> pahin, että pistetään projekteja johdon puolta tai jostain liikkeelle, mutta sitten esimerkiksi tietohallinnossa tai liiketoimissa ei riitä ihmisiä tekemään niitä. Ja sitten tuosta siirrosta tuotantoon, mä sen takia näen sen tärkeänä, just siihen hankintapäätökseen, että sitä ei tarvitse yksityiskohtaisesti, mutta projektiriskinä, että kun se maksaa nimittäin ne jatkuvat palvelut. Jos meillä ei ole sitä, niin mä voin sanoa, että se projekti, joka on puolitoista vuotta pyörinyt siellä tuotannossa, mutta edelleen projekti on käynnissä, niin se on konsulttien kultamaata, mutta se ei ole välttämättä sille asiakasorganisaatiolle mitään muuta kuin rahareikä.” – H12

> ”Kyllä se mun mielestä vaikuttaa siihen vähintään, koska yleensä pitää ainakin sellaisessa kohdassa, missä mä olen ollut mukana täällä meillä, niin pitää arvioida, kuinka realistinen sitten esimerkiksi se käyttöönotto, aikataulut ja muut ovat. Yleensä, kun puhutaan näistä hankinnoista ja tämän tyyppisistä SaaS:sta, niin totta kai siellä meidän liiketoimintajohtomme odottaa, että no koska pääsee lunastamaan sitä lisäarvoa. Alkaa tulla deadline, aikataulu ja milloin. Ja sitten pitää olla tarkkana, että ei luvata mitään sellaista, mikä ei onnistu. Tai jos luvataan, niin silloin täytyy ymmärtää, että millä kriteeristöllä ja mitä asioita pitää olla. Pitääkö olla hanketoimisto, pitääkö olla minkälaista erilaista resursointia ja erilaista kompetenssia siinä? Ja tämä on tyypillisesti mun kokemuksen mukaan asia, missä mennään vikaan aika pahasti. Kun saadaan aikatauluodotusta, niin siihen ei osata mitoittaa, mitä siihen aikatauluun pääseminen vaatii. Se vähätellään mun mielestä usein eri organisaatioissa. Meilläkin on käynyt sitä. On vähätelty se, että mitä tarvitaan tähän aikatauluun pääsemiseksi.” – H14

Henkilöresurssien ja osaamisen riittäminen on haastateltavien mukaan tärkeää huomioida jo ennen SaaS-järjestelmän käyttöönottopäätöstä. Osaamisen puuttuminen tai riittämättömyys voi johtaa taloudelliseen tappioon ja SaaS-järjestelmästä saataviin kokonaishyötyihin. Resursoinnissa on otettava huomioon riittävä osaaminen, ihmiset, raha ja aika riskienhallinnan näkökulmasta, sillä resurssien riittävyydellä voidaan hallita muun muassa projektiriskejä sekä taloudellisia riskejä.

5.7.5 Resilienssi ja liiketoiminnan jatkuvuus

Useamman haastateltavan mukaan riskienhallintaan ennen SaaS-järjestelmän käyttöönottopäätöstä liittyy resilienssi sekä liiketoiminnan jatkuvuus. Liiketoiminnan jatkuvuudesta mainitaan haastatteluissa usean kerran. Liiketoiminnan jatkuvuuteen liittyy varajärjestelmät sekä liiketoiminnan jatkuvuuden varmistaminen muilla sopivilla tavoilla. H2, H3 ja H12 mainitsivat asiasta seuraavaa:

> ”… sitten mahdolliset korvaustoimenpiteet, että jos meillä on joku korvaava järjestelmä sitten tarvittaessa helposti otettavissa käyttöön.” – H2

> ”Ensimmäinen kysymys, miten kriittinen se on liiketoiminnalle? Se asettaa raamit sille keskustelulle ja se on ensimmäinen. Sen jälkeen se meneekin sitten oikeastaan tietosuojaan ja tietoturvaan liittyviin riskeihin ja miten sun liiketoimintasi kestää, jos tämä palvelu on alhaalla pidempiä aikoja. Mikä se sun "operational resilience". En tiedä onko sille hyvää suomen kielistä vaihtoehtoa, mutta siitä puhutaan paljon. Sekin on suhteessa siihen kriittisyyteen, että miten sä pystyt varmistamaan, että sun liiketoimintasi jatkuu, jos toimittaja onkin yhtäkkiä pois pelistä. Se ei ole aina kauhean helppo kysymys ja se on

> myös se syy, miksi mä sanoisin, että silti tänä päivänä valtaosan yrityksistä ydinliiketoimintajärjestelmistä on on-premise-tyyppisiä tai hybridivirityksiä.” – H3

> ”Mehän voidaan tietohallinnossa mennä arvaamaan, mikä liiketoiminnan mielestä on kriittistä. Mutta kyllähän sen liiketoiminnan pitää pystyä itsekin sanomaan, että voiko tämä SaaS-palvelu olla pois käytöstä esimerkiksi päivän, taikka viikon, vai onko se niin, että tuntikin on jo liian pitkä aika. Ja tähän tietoturvamielessä jatkuvuuteenhan sitten tullaan siinä, että jos me saamme sen viestin, että puoli päivää tai neljä tunti on pisin aika, kun se voi olla alhaalla, niin sittenhän meidän täytyy alkaa miettimään... tämä liittyy siihen hankintapäätökseenkin tai käyttöönottopäätökseen...että no millä tavalla me varmistamme, että SaaS-järjestelmä on käytettävissä. Mitkä on meidän varajärjestelmämme? Mennäänkö varajärjestelmään niin, että jos tämä ei ole käytössä, niin sitten otetaan kynä ja paperi? Sillä pitää sitten hoitaa. Tai sitten se, että me haemme siihen sitten vaikka muita tietoliikenneratkaisuja taustalle, siis varajärjestelmiä. Tai sitten täytyy selvittää se, että onko sillä SaaS-toimittajalla riittävät kyvyt huolehtia siitä, että se ei ole pidempää kuin neljä tuntia alhaalla.” – H12

Liiketoiminnan jatkuvuuteen on osan haastateltavien mukaan kiinnitettävä huomiota. Tähän voidaan vaikuttaa muun muassa varajärjestelmillä, joihin voidaan nojautua tilanteissa, joissa SaaS-järjestelmä ei toimi tai ole käytettävissä. Varajärjestelmät ja liiketoiminnan jatkuvuus ovat kytköksissä organisaation resilienssiin, eli siihen, miten organisaatio pystyy varmistamaan, että toiminta jatkuu mahdollisissa ja odottamattomissakin ongelmatilanteissa. Liiketoiminnan jatkuvuuden huomioiminen, varajärjestelmät ja resilienssin edistäminen ovat haastateltavien mukaan tärkeä osa riskienhallintaa.

Liiketoiminnan jatkuvuuteen liittyy osan haastateltavien mukaan myös kriittisen tiedon varmuuskopiointi. H2 ja H5 mainitsivat varmuuskopioinnista seuraavaa:

> ”Ne mitkä ovat kriittisiä [järjestelmiä], niin me ollaan usein sitten varmistettu tavalla tai toisella meidän on-premise -järjestelmiin, että ollaan ne datat esimerkiksi "backupattu" meidän omaan konesaliin, jos on koettu se tarpeelliseksi.” – H2

> ”Jos muistatte muutamia vuosia sitten Ranskassa paloi yksi konesali ja siinähän kävi niin, että niillä ei edes synkka toiminut oikein, eli ne ”backupit” ei ollutkaan siellä heidän "secondary lokaatiossa" ja asiakkaalta ruvettiin kysymään "backuppeja". – H5

Varmuuskopiointi on osan haastateltavien mukaan tapa pienentää riskiä uhkatilanteissa. H2 mainitsee varmuuskopioinnin olevan merkityksellistä varsinkin kriittisen tiedon kohdalla. H5 antaa esimerkin, jossa varmuuskopiointi ei toiminut, mikä johti tilanteeseen, jossa tiedot katosivat. Kriittisen tiedon lisäksi liiketoiminnan kannalta tärkeät järjestelmät tulee osan haastateltavien mukaan tunnistaa, jotta voidaan varautua ongelmatilanteista palautumiseen sekä mahdollisesti välttää ongelmatilanteiden syntyminen etukäteen. H12 mainitsee kriittisten järjestelmien tunnistamisesta seuraavaa:

> ”… parhaimmillaan organisaatiossahan on olemassa tämmöinen liiketoiminnan jatkuvuuteen liittyvä suunnitelma. … Että mikäs täällä nyt on kriittisiä, tai mikä voi olla niin huonolla tekniikalla, että sitä on pakko miettiä, että jos se sitten kuitenkin kohta taas kaatuu. Niin siinä mielessä tavallaan tämän tyyppisiä riskisuunnitelmia ja kartoituksia varmasti on tai pitäisi olla. Ja nimenomaan tämmöisten toiminnan jatkuvuuteen tai ”disaster recovery plan”, DRP-tyyppisissä asioissa. Ja ne yleensä ei varmaan suoraan tavallaan tämmöisiin käyttöönottopäätöksiin tai hankintapäätöksiin vaikuta, paitsi jos esimerkiksi just nimenomaan sieltä on joku heijastuma, että meidän on ihan oikeasti pakko tehdä jotain tälle ja uudistaa ja korjata. …” – H12

H12 mainitsee, että kriittisten järjestelmien tunnistaminen ja ymmärtäminen on tärkeää, mutta ei välttämättä suoraan vaikuta käyttöönottopäätökseen vaan käyttöönottopäätöstä edeltäviin riskisuunnitelmiin. Liiketoiminnan jatkuvuuden lisäksi H3:n aikaisemmin mainitsema resilienssi on merkittävä tekijä riskienhallinnassa ennen SaaS-järjestelmän käyttöönottopäätöstä. Organisaation resilienssiin voidaan vaikuttaa osan haastateltavien mukaan liiketoiminnan ketteryyden kulttuuria edistämällä, tunnistamalla liiketoiminnan kannalta kriittiset järjestelmät ja varautumalla ongelmatilanteista palautumiseen. H4 mainitsi ketteryydestä seuraavaa:

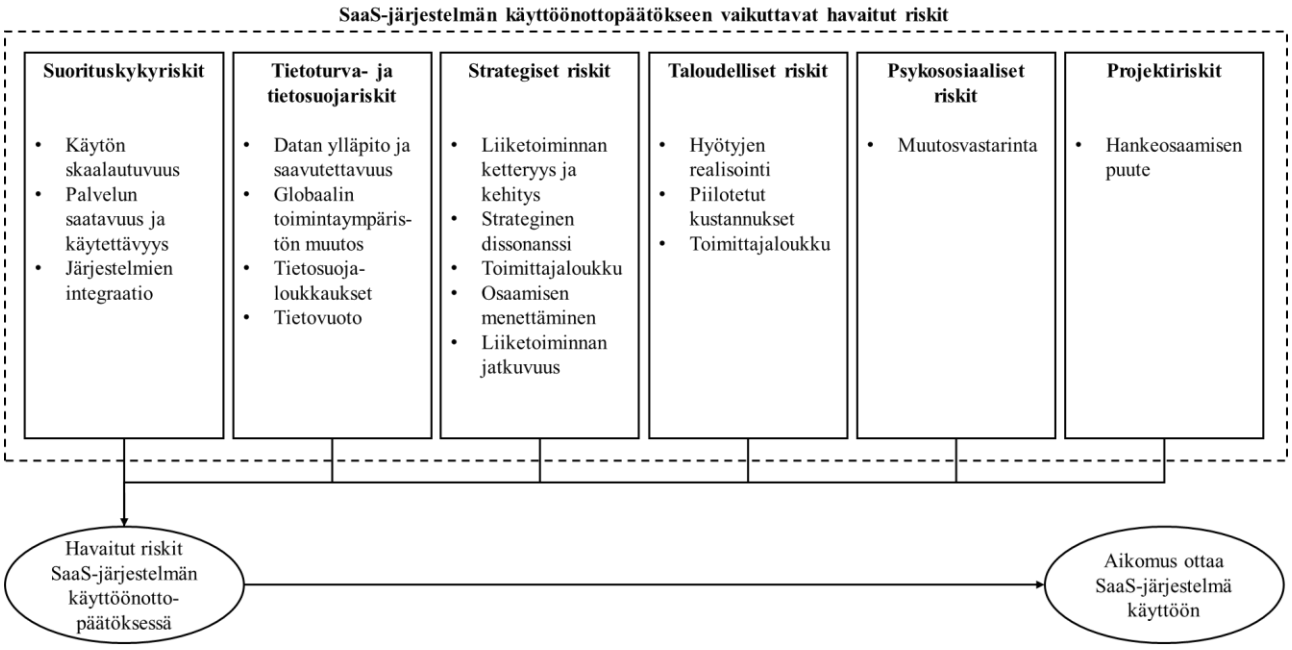
> ”No se vähän riippuu organisaatiokypsyydestä. Tavallaan laatukulttuurista, että kuinka laaja se riskianalyysi pitää olla. Jossain isossa globaalissa yrityksessä, missä voi tapahtua kaiken näköistä. Mä vedin [suuressa globaalissa yrityksessä] yhtä tuotetiedonhallintajärjestelmän uudistusprojektia, mikä oli globaali projekti, ja siinä oli tiimiä kaikkialta maailmassa. Sitten tullut joku SARS-epidemia, ei ollut kuitenkaan yhtä vakava kuin COVID, mutta asetti aikamoisia matkustusrajoituksia. Niin nimettiin ihan taho, joka seurasi sitä, että miten se mahdollisesti tulee vaikuttamaan. Sitten on sellaisia, että vedin yhden globaalin yrityksen ERP-projektia, kun Islannissa poksahti joku tulivuori ja lentoliikenne Euroopassa päättyi viikoksi. Ensinnäkin, miten me saimme edes ne saksalaiset konsultit kotiin Suomesta, kun lennot peruutettiin, ja muuta. Voi myös tapahtua sellaisia merkittäviä asioita, joita sulla ei ollut mitään mahdollisuutta laittaa sinne riskilokiin, ja sitten yhtäkkiä ne vaan tapahtuvat. Et sitä voi keksiä kaiken näköisiä pieniä riskejä, ja täyttää sen lokinsa, ja kaikki menee hyvin, tai sitten on joku sellainen ulkoinen tapahtuma, mille ei vaan voi vaikuttaa mitään. Periaatteessa koska kaikkea ei voi ennakoida, niin tavallaan organisaatioista pitää rakentaa sellainen, että se pystyy toipumaan melkein mistä tahansa. Sitten täytyy miettiä, et mitä voidaan tehdä. Se, että pitää luoda semmoinen ketteryyden kulttuuri, et tapahtuu mitä tapahtuu, niin mukautetaan se oma toiminta siihen ilmiöön tai muutokseen, mikä on tapahtunut.” – H4

H4 mainitsee ketteryyden kulttuurin edistämisen tärkeäksi tekijäksi riskienhallinnassa. Riskeihin ei voida aina täysin varautua etukäteen, jolloin vastoinkäymisiin tulee varautua luomalla ketteryyden kulttuuria. Resilienssin avulla pystytään palautumaan ongelmatilanteista dynaamisella liiketoimintakentällä.

6 Johtopäätökset

6.1 Keskeiset SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat havaitut riskit Suomessa toimivissa suurissa organisaatioissa

Tutkimuksen ensimmäinen tutkimuskysymys pyrki selvittämään keskeisiä SaaS-järjestelmän käyttöönottopäätökseen vaikuttavia riskejä, joita Suomessa toimivissa suurissa organisaatioissa havaitaan. Haastattelukysymykset ja havaittujen riskien analyysi pohjautui tämän tutkimuksen laajennettuun SaaS-järjestelmän havaittujen riskien -viitekehykseen, jota oli laajennettu Benlianin ja Hessin (2011) aikaisemmasta tutkimuksesta. Kuviossa 6 nähdään tämän tutkimuksen tuloksina nousseet keskeiset SaaS-järjestelmien käyttöönottopäätökseen vaikuttavat riskit, joita havaitaan Suomessa toimivissa suurissa organisaatioissa.



Kuvio 6 SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat havaitut riskit

Tulosten perusteella Suomessa toimivissa suurissa organisaatioissa havaitaan paljon erilaisia riskejä, jotka vaikuttavat SaaS-järjestelmien käyttöönottopäätöksiin. Riskit otetaan organisaatioissa huomioon johdonmukaisesti. Kaikilla haastateltavilla oli selkeä käsitys havaituista riskeistä ja niiden vaikutuksesta organisaation toimintaan sekä SaaS-järjestelmän käyttöönoton onnistumiseen. Jokaisen tutkimuksen viitekehyksen muodostaman riskikategorian alle nousi haastattelujen perusteella riskejä. Havaitut riskit painottuivat tutkimuksen viitekehyksen mukaisesti jaoteltuna strategisiin, taloudellisiin sekä tietoturva- ja tietosuojariskeihin. Näiden riskikategorioiden kohdalla

esiintyi eniten havaintoja haastateltavien keskuudessa, minkä lisäksi haastateltavat myös painottivat näiden kategorioiden tärkeyttä vastauksissaan.

Haastateltavat tunnistivat myös useita suorituskykyriskejä SaaS-järjestelmien käyttöönottopäätökseen vaikuttavina tekijöinä. Useat haastateltavat mainitsivat kuitenkin suorituskykyriskien painoarvon pienentyneen vuosien saatossa, minkä takia ne eivät ole nykypäivänä yhtä keskeisiä riskejä kuin aikaisemmin. Tulosten perusteella suorituskykyriskien keskeisyyden muutos johtuu ainakin osittain teknologian kehittymisestä sekä suurten datakeskusten siirtymisestä Suomeen lähemmäs loppukäyttäjiä. Suomessa toimivissa suurissa organisaatioissa verkon nopeuden kasvun sekä julkiverkkojen ja suurten palveluntarjoajien luotettavuuden lisääntymisen nähdään pienentävän suorituskykyriskiä. SaaS-järjestelmien integroitavuus nähtiin kuitenkin yhtenä keskeisenä suorituskykyriskinä, mikä tukee aikaisempaa tutkimusta (Phaphoom ym., 2015).

Tutkimuksen tulosten perusteella myös palvelun skaalautuvuus nähdään yhtenä SaaS-järjestelmän käyttöönottopäätökseen vaikuttava suorituskykyriskinä, mikä on osittain ristiriidassa aikaisemman tutkimuksen kanssa, jossa SaaS-järjestelmien skaalautuvuus nähdään yhtenä SaaS-järjestelmien keskeisenä piirteenä ja vahvuutena (Marston ym., 2011; Mell & Grance, 2011). Organisaatioissa, joiden toiminnassa on yli ajan tapahtuvaa volyymien vaihtelua, kuten käyttäjäpiikkejä, saattaa realisoitua riski siitä, että järjestelmän käytettävyys heikkenee tai saavutettavuus menetetään jopa kokonaan, jos palvelu ei skaalaudu organisaation tarpeisiin. Palvelun skaalautuvuuteen liittyvä riski tukee kuitenkin aikaisempaa kirjallisuutta siitä, että SaaS-järjestelmät ovat tehneet IT-infrastruktuurin kapasiteetin ennustamisesta ja suunnittelusta haastavaa, jolloin palveluntarjoaja ei aina onnistu varmistamaan haluttua palvelutasoa käytön määrän vaihdellessa yllättäen (Candeia ym., 2015; Furman & Diamant, 2025). Tämän tutkimuksen sekä aiemman kirjallisuuden perusteella (Candeia ym., 2015; Furman & Diamant, 2025) SaaS-järjestelmien kapasiteetinhallintaan ja ennustamiseen tulisi kiinnittää enemmän huomiota, jotta myös käyttöönottopäätökseen vaikuttavia riskejä saataisiin pienennettyä.

Keskeisimpänä suorituskykyriskinä voidaan tulosten perusteella pitää palvelun saatavuutta. Jos SaaS-järjestelmä ei ole saatavilla, se voi aiheuttaa suuria ongelmia organisaation toiminnassa. Palvelun saatavuuteen liittyvä riski on erityisen keskeinen, jos kyseessä on liiketoiminnalle kriittinen SaaS-järjestelmä. Täten tutkimuksen tulokset havaituista riskeistä tukevat aikaisempaa tutkimusta siitä, minkä takia liiketoiminnalle kriittiset järjestelmät eivät ole siirtyneet samalla tahdilla pilveen kuin vähemmän kriittiset järjestelmät (Shuraida & Titah, 2023). Jos tietojärjestelmä on organisaation ydintoiminnalle elintärkeä, eli sen toiminnassa ei ole sallittavaa esiintyä saatavuusongelmia, on SaaS-

järjestelmään siirtymistä pidetty joissain tapauksissa liian riskialttiina. Tulosten perusteella tämänlaisia järjestelmiä olivat joissakin organisaatioissa esimerkiksi toiminnanohjausjärjestelmät, asiakkuudenhallintajärjestelmät sekä potilaiden hoitoon kriittisesti linkitetyt järjestelmät. Haastatteluissa kuitenkin ilmeni useita organisaatioita, jotka olivat jo siirtäneet kriittisiä järjestelmiään SaaS:iin, sekä organisaatioita, joiden kriittisten järjestelmien siirtymä SaaS:iin oli suunnitteilla. Empirian perusteella voidaan todeta, että Suomessa toimivissa suurissa organisaatioissa pilveen sekä SaaS-järjestelmiin siirtyminen nähdään lähes ainoana järkevänä vaihtoehtona tulevaisuudessa. Myös tiukasti säännellyillä toimialoilla, joiden toiminnassa käsitellään sensitiivistä dataa, kuten terveys-, lääke- tai finanssidataa, SaaS-järjestelmät sekä tietojärjestelmien siirtyminen pilveen nähdään olevan arkipäivää tulevaisuudessa.

Tuloksina muodostuneet tietoturva- ja tietosuojariskit, peilaavat vahvasti aikaisempaa tutkimusta. Datan ylläpito ja saavutettavuus sekä tietojen häviäminen nähdään riskeinä, jotka nousivat tietoturvariskeinä myös Bibin ym. (2012) tutkimuksessa. Tietovuodot nousevat tässä tutkimuksessa yhdeksi merkittäväksi tietoturva- ja tietosuojariskiksi. Tietovuotoriskiin vaikuttivat muun muassa kontrollin menettäminen ja datan ylläpidon sekä palauttamisen epävarmuus, mikä osaltaan peilaa Benlianin ja Hessin (2011) aikaisempaa tutkimusta. Benlianin ja Hessin (2011) tutkimuksessa mainitaan riskinä se, että palveluntarjoaja hallitsee asiakkaan dataa ilman, että asiakas itse täysin tietää, miten SaaS-palveluntarjoaja turvaa datan ja millaisia varmuuskopioita tai palautuskäytäntöjä tarjoaja käyttää mahdollisten ongelmien sattuessa. Samoin Chang ja Hsu (2019) mainitsevat kontrollin menettämisen vaikutuksesta käyttöönottopäätökseen. Kontrollin menettämiseen liittyvä epävarmuus on nähtävissä tietoturva- ja tietosuojariskiin vaikuttavana tekijänä myös Suomessa toimivissa suurissa organisaatioissa.

Tutkimuksen tulosten ja aikaisemman kirjallisuuden perusteella datan ylläpitoon sekä vastuuasioihin on syytä kiinnittää huomiota tietoturva- ja tietosuojariskien kohdalla. SaaS-järjestelmät toimivat usein IaaS:in sekä PaaS:in päällä, minkä takia hyökkäykset mihin tahansa kerrokseen saattavat vaarantaa SaaS-järjestelmän (Hashizume ym., 2013). Tämä on yksi syy, minkä takia Suomessa toimivissa suurissa organisaatioissa esiintyy enemmän luottoa suuriin palveluntarjoajiin, kuten Amazoniin, Microsoftiin ja Googleen. Asiakasorganisaation luoton palveluntarjoajaa kohtaan nähdään vähentävän pilvipalveluiden käyttöönottopäätökseen liittyvää riskiä myös aiemmassa tutkimuksessa (Chang & Hsu, 2019). Tietoturvan sekä SaaS-järjestelmän eheyden osalta suuriin palveluntarjoajiin kohdistui haastatteluissa ”too big to fail”-ajattelua. Tulosten perusteella palveluntarjoajan suuruus ja vakiintuneisuus markkinoilla johtaa luoton kasvuun ja asiakasorganisaatiossa ajatukseen siitä, että suuret tarjoajat ovat liian suuria epäonnistuakseen

halutun palvelun tuottamisessa. Kuitenkin myös riskiä suuriin toimijoihin ilmenee. Osan vastausten perusteella suurten toimijoiden ei uskottu tarjoavan riittävän yksilöllistä tukea asiakkaalle, mikä tukee Kimin ym. (2017) löydöksiä SaaS-järjestelmien käyttöönottopäätöksiin vaikuttavista tekijöistä.

Haastateltavat painottavat vastauksissaan tietosuojariskin merkitystä. Tietosuojariskit lisättiin tässä tutkimuksessa Benlianin ja Hessin (2011) aiempaan viitekehykseen uutena kategoriana tietoturvan rinnalle. Tämän tutkimuksen tulosten perusteella tietosuojariskit ovat läheisessä yhteydessä tietoturvariskeihin, minkä takia kyseisten riskiluokkien yhdistäminen yhteisen kategorian alle voidaan nähdä loogisena luokitteluna tässä työssä. Tietosuojan ylläpitämisen ja lainsäädännön noudattamisen nähdään muodostavan riskiä johtuen erityisesti SaaS-järjestelmien toimitusketjujen pituudesta. Toimitusketjun pituuden ja toimijoiden määrän kasvaessa myös monimutkaisuus ja monitulkinnaisuus lisääntyvät. Kuten aiemmassakin kirjallisuudessa, myös tässäkin tutkimuksessa tietosuojaloukkaukset nähtiin riskeinä, joiden realisoituminen voi johtaa sanktioihin (Georgiopoulou ym., 2020) sekä mainehaittaan ja luottamuksen menettämiseen (S. S. Yau ym., 2024). Erityisesti GDPR:n noudattaminen sekä toimialakohtaiset tietosuojan erityisvaatimukset aiheuttavat tämän tutkimusten tulosten perusteella epävarmuutta SaaS-järjestelmän käyttöönottopäätöksen kohdalla. Muun muassa terveystietoja tai finanssialan tietoja käsittelevissä organisaatioissa tietosuojaan liittyy tiukkoja toimialakohtaisia erityisvaatimuksia. Joidenkin toimialakohtaisten erityisvaatimusten takia muun muassa datan sijainti tulee määrittää tarkasti, eikä dataa saa viedä Euroopan, eikä joissain tapauksissa myöskään Suomen rajojen ulkopuolelle.

Tietoturva- ja tietosuojariskien kohdalla toimitusketjun pituuden lisäksi myös geopoliittisten tekijöiden tunnistetaan aiheuttavan riskiä Suomessa toimivissa suurissa organisaatioissa. Tietosuojaa noudattaakseen organisaatioiden tulee olla tarkkoja alueellisesta sekä toimialakohtaisesta lainsäädännöstä. Erityisesti kansainvälisten sekä sensitiivistä dataa käsittelevien organisaatioiden tulee pohtia palvelun sijaintiin ja toimintaympäristöön liittyvää riskiä tietoturvan ja -suojan näkökulmasta. Myös alueelliset konfliktit ja geopoliittinen epävarmuus muun muassa Ukrainaan kohdistuneen hyökkäyssodan sekä Yhdysvaltojen tämänhetkisen geopoliittinen turbulenssin takia, ovat nousseet asioiksi, joita otetaan huomioon SaaS-järjestelmien käyttöönottopäätöksissä. Geopoliittiset tekijät sekä globaali toimintaympäristö ja sen muutos aiheuttavat riskiä niin turvallisuuden, kuin myös esimerkiksi tietosuojan, vaatimusten noudattamisen, mainehaitan sekä palvelun jatkuvuuden näkökulmasta. Tulosten perusteella voidaan sanoa, että organisaatioiden kannattaisi riskejä välttääkseen hahmottaa SaaS-järjestelmän toimintaa makrotasolla, jolloin toimintaympäristöön liittyvät seikat huomioitaisiin laajemmin jo käyttöönottopäätöstä pohtiessa.

Strategiset riskit sisältävät tulosten perusteella useita toisistaan eriäviä riskejä, minkä voidaan ajatella johtuvan riskikategorian laajuudesta, mutta myös sen merkityksestä. Tulosten perusteella palveluntarjoajaa voidaan pitää strategisena kumppanina erityisesti kriittisten järjestelmien kohdalla. Strateginen kumppanuus aiheuttaa riskiä muun muassa strategisen dissonanssin muodossa silloin, jos asiakasorganisaation ja palveluntarjoajan tavoitteet eivät ole linjassa, sekä myös silloin, jos strategiset tavoitteet ovat päällekkäisiä. Liiketoiminnan ketteryys ja kehitys saattaa lisäksi häiriintyä, jos SaaS-järjestelmä ei ole yhteensopiva organisaation kokonaisarkkitehtuurin kanssa, tai jos järjestelmä ei tue liiketoiminnan kehitystä. Tulokset tukevat aikaisempaa tutkimusta siitä, että asiakkaan ja palveluntarjoajan välillä on keskinäisiä riippuvuuksia, jotka saattavat hidastaa organisaation reaktionopeutta strategisissa muutoksissa (Benlian & Hess, 2011).

Toimittajaloukun nähdään vaikuttavan strategisiin riskeihin, sillä SaaS-järjestelmästä irtautuminen saattaa olla hankalaa. Yrityksen liiketoiminnan ketteryys ja kehitys ovat sidottuina SaaS-järjestelmän kehitykseen ja muovautumiseen erityisesti kriittisten järjestelmien kohdalla. Toimittajaloukku tunnistetaan käyttöönottopäätökseen vaikuttavana tekijänä myös aikaisemmassa tutkimuksessa (Armbrust ym., 2010; Opara-Martins ym., 2016). Jos SaaS-järjestelmä alkaa degeneroitua tai palveluntarjoajan liiketoiminta pahimmassa tapauksessa loppuu kokonaan, aiheuttaa se riskiä myös asiakasorganisaation liiketoiminnan jatkuvuuteen ja kehitykseen. SaaS-järjestelmiä tarjoavat yritykset pyrkivät myymään mieluummin valmiita paketteja yksilölliseksi räätälöityjen kokonaisuuksien sijaan, minkä takia asiakasorganisaation tulee usein sopeuttaa prosessejaan ja toimintaansa yhteensopivaksi SaaS-järjestelmän kanssa. Tulosten perusteella valmiit paketit mahdollistavat usein helpomman ylläpidon ja päivitykset kuin pitkälle räätälöidyt ratkaisut. Organisaatiolle saattaa kuitenkin aiheutua strategista riskiä liiketoimintalogiikan yhteensovittamisen ja muokkaamisen takia. Tutkimusten tulosten perusteella voidaan sanoa, että organisaatioiden tulisi SaaS-järjestelmän käyttöönottopäätöstä pohtiessaan analysoida myös palveluntarjoajan liiketoiminnan strategiaa ja tulevaisuudennäkymiä, jotta oma liiketoiminta ei häiriintyisi myöhemmin realisoituvien strategisten riskien myötä.

Osaamisen menettäminen nähdään SaaS-järjestelmien kohdalla sekä riskinä, että hyötynä asiakasorganisaatiolle. Hyödyt ilmenevät haastatteluiden perusteella siten, että organisaatio saa vähennettyä ylimääräistä henkilöstöä ja kohdistettua resurssejaan liiketoiminnalle keskeisten ydintoimintojen pariin tukitoimintojen sijaan. Osaamisen menettäminen nähdään samalla myös riskinä. Kun organisaatiosta lähtee IT-osaamista, organisaation sisäinen ymmärrys IT:stä vähenee, jolloin myös uudelleensiirtyminen pois valitusta SaaS-järjestelmästä voi hankaloitua. Täten osaamisen menettämisen riski tukee osaltaan Benlianin ja Hessin (2011) aiempaa tutkimusta, mutta

on samalla ristiriidassa sen kanssa, sillä IT-osaamisen menettäminen nähtiin tulosten perusteella myös SaaS-järjestelmän käyttöönottopäätökseen liittyvänä hyötynä.

Taloudellisissa riskeissä yhtenä keskeisenä löydöksenä esiintyy hyötyjen realisointi, sillä SaaS-järjestelmän tulisi tuoda asiakasorganisaatiolle riittävästi hyötyjä suhteessa kustannuksiin. Clemons ja Weber (1990) puhuvat tutkimuksessaan toiminnallisista riskeistä, jotka ovat verrattavissa tämän tutkimuksen löydökseen hyötyjen realisoinnin riskistä. Jos tietty SaaS-järjestelmä päätetään ottaa käyttöön organisaatiossa, tulisi järjestelmän kustannukset suhteuttaa hyötyolettamaan. Tuloksissa ilmeni myös hyötyjen realisoinnin riski liittyen siihen, että SaaS-järjestelmää ei omisteta itse. Tällöin SaaS-järjestelmään investoidut resurssit menetetään uudelleensiirtymisen yhteydessä. Tämä on erityisen ongelmallista, jos uudelleensiirtymä tehdään ennen hyötyjen realisoimista. Tulosten perusteella siirtyminen järjestelmästä toiseen koetaan usein hankalaksi ja resurssi-intensiiviseksi prosessiksi. Tämä on yksi syy, minkä takia toimittajaloukun tunnistettiin aiheuttavan taloudellista riskiä Suomessa toimivissa suurissa organisaatioissa. Toimittajaloukku voi aiheuttaa taloudellista riskiä asiakasorganisaatiolle myös käyttökustannusten ja hintojen nousun takia. Kun asiakasorganisaatio on ajautunut toimittajaloukkuun, on palveluntarjoajalla usein enemmän neuvotteluvoimaa hinnankorotuksiin liittyen, mikä tukee myös aiempaa tutkimusta SaaS-järjestelmien toimittajaloukusta (Benlian & Hess, 2011).

Tuloksissa ilmenee lisäksi SaaS-järjestelmiin liittyvät piilotetut kustannukset. Piilotettuja kustannuksia saattaa aiheutua esimerkiksi SaaS-järjestelmän kulurakenteen monimutkaisuuden takia, jos asiakasorganisaatio ei hahmota järjestelmään liittyviä kustannuksia kokonaisuudessaan. Piilotettuja kustannuksia saattaa liittyä myös SaaS-järjestelmän käyttöönottoprosessiin, uudelleensiirtymään tulevaisuudessa, ylläpitokustannuksiin tai SaaS-järjestelmän muokkaamiseen tulevaisuudessa liiketoiminnan prosessien muuttuessa oleellisesti. SaaS-järjestelmien kulurakenteet ovat useamman haastateltavan mielestä monimutkaisia, jolloin todelliset kustannukset koostuvat monimutkaisten lisenssimaksujen lisäksi myös muista käyttöön liitetyistä kuluista. Nämä piilotetut kustannukset aiheuttavat taloudellista riskiä Suomessa toimivissa suurissa organisaatiossa SaaS-järjestelmien käyttöönottopäätöksissä. Löydös piilotettuihin kustannuksiin liittyvästä riskistä tukee myös muun muassa Barthelemyn (2001) aikaisempaa tutkimusta, jonka mukaan IT-ulkoistamiseen liittyy monenlaisia piilotettuja kustannuksia, joiden hahmottaminen etukäteen saattaa olla hankalaa.

Tutkimusten tulosten perusteella yritysten tulisi hahmottaa SaaS-järjestelmään liittyviä kokonaiskustannuksia paremmin jo käyttöönottopäätösvaiheessa, jotta riski piilotetuista kustannuksista ei realisoituisi. Kulurakenteen ymmärtämiseksi voitaisiin palkata esimerkiksi

organisaation ulkopuolista apua, jos organisaation sisällä ei ole riittävästi omaa osaamista tai resursseja.

Psykososiaalisten riskien kohdalla tuloksissa esiintyy eroavaisuuksia. Eroavaisuudet näkökulmissa saattavat johtua siitä, että kaikissa organisaatioissa ei ajatella kyseisiä riskejä kovin tarkasti, sillä ne eivät ole yhtä helposti mitattavia ja seurattavia, kuin esimerkiksi taloudelliset riskit. Toisaalta osa haastateltavista pitää näitä riskejä tärkeinä ja käyttöönottopäätökseen vaikuttavina tekijöinä. Tämän takia organisaatioiden voi olla järkevää miettiä, tulisiko psykososiaalisia riskejä tarkastella enemmän jo käyttöönottopäätösvaiheessa. Organisaatioiden saattaa olla myös hyödyllistä pohtia, miten kyseisiä riskejä voidaan mitata ja seurata, jotta niitä voidaan hallita tehokkaammin.

Psykososiaalisten riskien kategoria kulminoitui pääasiassa riskiin, joka liittyy muutosvastarintaan sen eri muodoissa. Henkilöstö saattaa kokea kontrollin menettämisen tunnetta, pelätä työpaikkansa puolesta, kokea muutoksen epäoikeudenmukaiseksi tai jollain muulla tavalla vääräksi. Muun muassa nämä asiat vaikuttavat henkilöstön muutosvastarintaan, jota voi tulosten perusteella esiintyä käyttöönotossa, käyttöönoton jälkeen sekä jo käyttöönottopäätösvaiheessa. Tulokset tukevat osaltaan Clemonsin ja Weberin (1990) tutkimusta strategisiin IT-investointeihin liittyvistä sisäisistä poliittisista riskeistä, jotka juontuvat organisaation jäsenten intressien ja etujen riskiriidasta, ja saattavat johtaa muutosvastarintaan henkilöstön kokemien uhkien takia.

Muutosvastarinnan nähdään joissain tapauksissa vaikuttavan suoraan käyttöönottopäätökseen, kun taas toisissa tapauksissa muutosvastarinta nähtiin asiana, joka ei vaikuta päätökseen, mutta puolestaan järjestelmän kokonaisvaltaiseen käyttöön ja järjestelmästä saataviin hyötyihin. Psykososiaalisten riskien kohdalla tulokset olivat täten vaihtelevia. Lähes kaikki haastateltavat kuitenkin tunnistivat muutosjohtamisen sekä henkilöstön osallistamisen ja sitouttamisen olevan tärkeää muutosprosessin läpiviennissä. Se, miten paljon psykososiaaliset riskit vaikuttavat käyttöönottopäätökseen oli tutkimustulosten perusteella vaihtelevaa. Tulos psykososiaalisten riskien vaihtelevasta vaikutuksesta käyttöönottopäätökseen on täten osittain linjassa Benlianin ja Hessin (2011) tutkimuksen kanssa, jonka mukaan psykososiaaliset riskit eivät vaikuta merkittävästi käyttöönottopäätökseen. Benlian ja Hess (2011) kuitenkin tutkivat psykososiaalisia riskejä ainoastaan johdon näkökulmasta, minkä takia tässä tutkimuksessa psykososiaalisten riskien kategoriaa laajennettiin vastaamaan koko henkilöstöä. Laajemmin tarkasteltuna psykososiaaliset riskit nähtiin tulosten mukaan tärkeinä SaaS-järjestelmän käyttöönottopäätökseen vaikuttavina tekijöinä osassa vastauksia.

Projektiriskit lisättiin tässä työssä Benlianin ja Hessin (2011) alkuperäiseen viitekehykseen, ja haastateltavat tunnistivat useita erilaisia riskejä projektiriskien kategoriassa. Projektiriskit

keskittyivät suurelta osin SaaS-järjestelmän käyttöönottoprojektin monimutkaisuuteen sekä resurssien riittämättömyyteen, jotka kulminoituvat hankeosaamisen puutteeseen. Tutkimuksen tulokset ovat osaltaan ristiriitaista aikaisemman tutkimuksen kanssa, sillä SaaS-järjestelmiä on yleisesti pidetty yksinkertaisina ratkaisuina, jotka korvaavat monimutkaiset ja resursseja vaativat järjestelmäratkaisut (Marston, 2011). Haastateltavat mainitsivat resursseja, kuten ajan, osaamisen ja rahan, joiden tarve on yllättänyt projektin edetessä. Löydös tukee myös Clemonsin ja Weberin (1990) aikaisempaan tutkimusta projektirikeistä.

Tulosten perusteella organisaatioiden tulisi varmistaa riittävä hankeosaaminen jo käyttöönottopäätösvaiheessa. Tällä tavalla voidaan välttää projektiriskien realisoituminen valitun SaaS-järjestelmän käyttöönottoprojektin aikana. Hankeosaamisen puutteeseen tulisi tulosten perusteella paneutua lisää, sillä SaaS-järjestelmien käyttöönottoprojektien monimutkaisuuden juurisyyt voisi olla hyödyllistä tunnistaa, jotta organisaatiot voisivat välttyä yllätyksiltä ja toteuttaa käyttöönottoprojektit tehokkaammin. Tällä tavalla pystyttäisiin todennäköisesti myös vähentämään projektiriskejä tehokkaammin.

Aikaisemman tutkimuksen tulokset projektiriskien vähentämisestä palkkaamalla ulkoista apua, kuten konsultteja (Clemons & Weber, 1990), ovat osittain linjassa tämän tutkimuksen kanssa. Useat haastateltavista mainitsivat ulkoisen avun olevan hyödyllistä riskien pienentämiseksi, mutta samalla osa haastateltavista mainitsi ulkoiseen apuun liittyvän myös riskiä. Yksi ulkoiseen apuun liittyvä riski juontuu siitä, että pilvikonsultit eivät aina ymmärrä organisaation liiketoimintaa, eivätkä liiketoiminnan osaajat puolestaan ymmärrä SaaS-järjestelmiä, jolloin sidosryhmien sujuvan yhteistyön epäonnistuessa projektin lopputulos jää heikoksi. Konsulttien palkkaamiseen saattaa tulosten perusteella liittyä myös taloudellista riskiä projektin pitkittyessä.

6.2 SaaS-järjestelmän käyttöönottopäätöstä edeltävä riskienhallinta

Tämän tutkimuksen toisen tutkimuskysymyksen avulla pyrittiin selvittämään Suomessa toimivien suurten organisaatioiden SaaS-järjestelmien käyttöönottopäätöksiä edeltävää ja niihin vaikuttavaa riskienhallintaa. Tutkimuksen haastattelukysymyksillä pyrittiin aluksi selvittämään organisaatioiden tekemiä SaaS-järjestelmän käyttöönottopäätökseen vaikuttavia riskisuunnitelmia, mutta vastaukset osoittautuivat laajoiksi, minkä takia SaaS-järjestelmän käyttöönottopäätöstä edeltävään riskienhallintaan pystyttiin vastaamaan tehokkaammin. Taulukosta 3 nähdään tämän tutkimuksen tulokset SaaS-järjestelmän käyttöönottopäätöstä edeltävästä riskienhallinnasta.

Taulukko 3 SaaS-järjestelmän käyttöönottopäätöstä edeltävä riskienhallinta

Organisaation tarpeen ja vaatimusten määrittely	Palvelun vastaavuus ja kyvykkyyskartoitus	Sopimustekniset asiat	Hankeosaaminen ja resursointi	Resilienssi ja liiketoiminnan jatkuvuus
• Vaatimusmäärittely ja järjestelmän kokonaisvaltaisen käytön hahmottaminen	• Palvelun soveltuvuus ja vastaavuus • Palveluntarjoajan kyvykkyys • Tietoturva- ja tietosuoja-selvitykset	• Etukäteen määritellyt hinnat ja sopimuskauden pituus • Exit-strategia ja turvatakuu • Tietoturvan ja tietosuojan sopimusmääritykset • Vastuiden ja velvoitteiden sopiminen	• Henkilöstön osallistaminen ja sitouttaminen • Projektin toteuttamisen suunnittelu ja resurssitarpeen varmistaminen	• Varajärjestelmät ja liiketoiminnan jatkuvuuden varmistaminen • Organisaation resilienssin kasvattaminen

Jokainen haastateltava mainitsee, että organisaation tekemät riskisuunnitelmat vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen. Haastattelujen perusteella on selvää, että organisaatioissa tehdään laajasti riskienhallintaa jo ennen SaaS-järjestelmän käyttöönottopäätöstä, jotta mahdolliset riskit saadaan tunnistettua ja järjestelmän vaatimukset sekä mahdollinen käytönaikainen riskienhallinta selvitettyä ennen käyttöönottopäätöstä. Se, että riskienhallinta ja riskisuunnitelmat vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen on linjassa aikaisemman kirjallisuuden kanssa, jossa päätöksentekoprosessissa riski- ja päätöksentekoanalyysit tehdään ennen lopullista päätöstä (Aven, 2012, s.114). Haastattelujen perusteella voidaan sanoa, että Suomessa toimivissa suurissa organisaatioissa havaittujen riskien lisäksi riskienhallinta ja riskisuunnitelmat vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen.

Tulokset osoittavat lisäksi sen, että Suomessa toimivissa suurissa organisaatioissa riskinkäsittelyprosessi on samankaltainen kuin aikaisemmin tässä tutkimuksessa esitetty riskinkäsittelyprosessi (Firoiu, 2015; Wheeler, 2011, s. 53–54). Tutkimuksen tulosten perusteella Suomessa toimivissa suurissa organisaatioissa riskejä analysoidaan, arvioidaan ja tunnistetaan erilaisilla toimenpiteillä. Tulosten perusteella voidaan sanoa, että organisaatioiden toimenpiteillä pyritään ainakin pienentämään, siirtämään sekä välttämään riskejä. Useat tuloksissa esiin nousseet toimenpiteet, kuten organisaation tarpeen kartoittaminen ja palveluntarjoajan kyvykkyyden varmistaminen pyrkivät pienentämään riskejä. Toisaalta toimenpiteillä, kuten erilaisten vaatimusten asettamisella ja sopimusmäärityksillä voidaan pyrkiä välttämään tiettyjen riskien realisoitumista kokonaisuudessaan, sekä siirtämään riskiä muille tahoille. Osassa vastauksia ilmeni jäännösriskin suhteuttaminen organisaation riskinsietokykyyn sekä riskinkäsittelyn kustannusten suhteuttaminen

toimenpiteellä saavutettaviin kokonaishyötyihin. Kustannusten suhde hyötyihin vaikuttaa tulosten perusteella siihen, että jokaista riskiä ei kannata pyrkiä poistamaan kokonaan. Kokonaisuudessaan Suomessa toimivissa suurissa organisaatioissa riskinkäsittelyprosessi vaikuttaa toimivan samankaltaisesti aikaisemmin kuviossa 4 esitetyn riskinkäsittelyprosessin (Firoiu, 2015; Wheeler, 2011, s. 53–54) kanssa.

Tämän tutkimuksen tulosten perusteella organisaation tarpeen sekä SaaS-järjestelmän kokonaisvaltaisen käytön määrittäminen on tärkeää ennen SaaS-järjestelmän käyttöönottopäätöstä. Aikaisemmassa tutkimuksessa SaaS-järjestelmästä saatava suhteellinen hyöty on nostettu SaaS-järjestelmän käyttöönottopäätökseen vaikuttavaksi tekijäksi (Hsu & Lin, 2016; Safari ym., 2015), mikä on osittain linjassa myös tämän tutkimuksen löydösten kanssa. Tämän tutkimuksen tulosten perusteella organisaation tarve on tunnistettava, jotta pystytään selvittämään, saadaanko SaaS-järjestelmästä riittävästi hyötyä verrattuna vanhaan järjestelmään. Jotta suhteellinen hyöty voidaan mitata, täytyy tietää vastaako SaaS-järjestelmä nimenomaan kyseisen organisaation tarpeeseen tai siihen ongelmaan, jota varten uutta järjestelmää ollaan hankkimassa. Yhteensopivuus nostettiin aikaisemmassa tutkimuksessa SaaS-järjestelmän käyttöönottopäätökseen vaikuttavaksi tekijäksi (Safari ym., 2015), mikä on linjassa myös tämän tutkimuksen löydösten kanssa. Kokonaisvaltaisen käytön määrittämisessä haastateltavat korostivat SaaS-järjestelmän hahmottamista osana organisaation prosesseja ja kokonaisarkkitehtuuria. Haastateltavat korostivat sitä, että organisaation tulisi huomioida SaaS-järjestelmän yhteensopivuus omien prosessien ja järjestelmien kanssa jo käyttöönottopäätösvaiheessa.

Tutkimuksen tuloksista käy lisäksi ilmi, että palvelun vastaavuus ja kyvykkyyskartoitukset ovat tärkeä osa riskienhallintaa ennen SaaS-järjestelmän käyttöönottopäätöstä. Varmistamalla, että SaaS-järjestelmä vastaa liiketoiminnan tarpeisiin, organisaatiot voivat pienentää riskejä, joita saattaa syntyä, jos tavoitteet ja prosessit eivät ole linjassa liiketoiminnan vaatimusten kanssa. Myös palveluntarjoajan kyvykkyys nousi esille tuloksissa, sillä useat haastateltavat painottivat kyvykkyyskartoitusten merkitystä riskienhallinnassa ennen SaaS-järjestelmän käyttöönottopäätöstä. Organisaatiot pyrkivät kartoittamaan palveluntarjoajan sekä SaaS-järjestelmän kyvykkyydet ennen käyttöönottopäätöstä, jotta voidaan varmistua, että kyvykkyydet ovat riittävän korkealla tasolla. Täten pyritään estämään kyvykkyyteen liittyvien riskien realisoitumista tulevaisuudessa. Tämä löydös on osittain yhdenmukainen Hsun ja Linin (2016) tutkimuksen kanssa, jossa pilvipalvelujärjestelmän käyttöönottoon havaittiin vaikuttavan järjestelmän havaittavuus, jolla tarkoitetaan sitä, missä määrin järjestelmän hyödyt ovat muiden havaittavissa. SaaS-järjestelmän

kyvykkyyksien tunnistaminen on tärkeää ennen käyttöönottopäätöstä, jotta mahdolliset riskit pystytään ottamaan huomioon jo päätöksentekovaiheessa.

Sopimustekniset asiat nousevat esiin tutkimuksen tuloksissa yhtenä tärkeänä riskienhallinnan osa-alueena ennen SaaS-järjestelmän käyttöönottopäätöstä. Tulosten perusteella Suomessa toimivissa suurissa organisaatioissa on tärkeää ymmärtää sopimuksiin liittyvät asiat sekä niiden merkitys organisaation ja SaaS-järjestelmän toiminnalle. Havaittuihin riskeihin voidaan vaikuttaa sopimusteknisesti usealla eri tavalla. Näihin lukeutuvat etukäteen määritellyt hinnat ja sopimuskauden pituuden määrittäminen, exit-strategian huomioiminen ja turvatakuiden asettaminen, tietoturvan ja tietosuojan sopimusmääritykset sekä vastuiden ja velvoitteiden sopiminen. Havaittuja riskejä voidaan pyrkiä välttämään ja siirtämään määrittämällä sopimuksellisesti muun muassa erilaiset vastuut asiakasorganisaation ja palveluntarjoajan välillä. Kokonaisuudessaan sopimustekniset asiat ovat tulosten perusteella yksi tärkeimmistä riskienhallinnan osa-alueista ennen SaaS-järjestelmän käyttöönottopäätöstä.

Tuloksissa nousevat esiin myös hankeosaamisen varmistamisen ja resursointi osana SaaS-järjestelmän käyttöönottopäätöstä edeltävää riskienhallintaa. Tuloksissa korostui muun muassa henkilöstön sitouttaminen ja osallistaminen hyvissä ajoin ennen projektin alkua. Vaikka kaikki haastateltavat eivät suoraan viitanneet muutosvastarintaan puhuessaan henkilöstön osallistamisesta ja sitouttamisesta, on mahdollista, että osallistamisella ja sitouttamisella voidaan vaikuttaa muutosvastarinnan riskin realisoitumiseen. Henkilöstön sitouttaminen ja osallistaminen edesauttaa tulosten perusteella myös SaaS-järjestelmän vastaavuutta liiketoiminnan tarpeiden sekä tavoitteiden kanssa. Lisäksi on tärkeää, että organisaatiossa ymmärretään SaaS-järjestelmän käyttöönoton resurssitarpeet. Täten voidaan varmistua resurssien riittävyydestä jo ennen SaaS-järjestelmän käyttöönottopäätöstä sekä pienentää tähän liittyvien riskien realisoitumista myöhemmässä vaiheessa.

Yhtenä keskeisenä tekijänä riskienhallinnassa ennen SaaS-järjestelmän käyttöönottopäätöstä on tulosten perusteella resilienssi ja liiketoiminnan jatkuvuus. Liiketoiminnan jatkuvuuteen voidaan vaikuttaa varajärjestelmillä sekä tunnistamalla ja ymmärtämällä liiketoiminnalle kriittiset järjestelmät. SaaS-järjestelmien käyttöönottopäätöksissä on tärkeää ymmärtää, miten käyttöönotto voi vaikuttaa liiketoiminnan jatkuvuuteen. Myös resilienssin kasvattaminen ja ylläpitäminen on tärkeää Suomessa toimivissa suurissa organisaatioissa, sillä kaikkiin riskeihin ei voida varautua, eikä niitä pystytä tunnistamaan etukäteen. On tärkeää, että organisaatio pystyy toimimaan muuttuvissa tilanteissa dynaamisesti ja tehokkaasti, jotta liiketoiminnan jatkuvuus voidaan turvata.

7 Yhteenveto

7.1 Tutkimuksen yhteenveto

Tässä tutkimuksessa pyrittiin selvittämään, mitkä keskeiset riskit vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen Suomessa toimivissa suurissa organisaatioissa sekä millaista riskienhallintaa organisaatioissa toteutetaan ennen käyttöönottopäätöstä. Tutkimuksen teoria perustui aikaisempaan tutkimukseen SaaS-järjestelmistä, SaaS-järjestelmien käyttöönottopäätöksiin vaikuttavista tekijöistä sekä riskienhallinnasta riskitietoisessa päätöksenteossa. Tutkimuksessa haastateltiin 14 henkilöä 12 eri organisaatiosta, joilla on toimintaa Suomessa. Tutkimukseen valittiin sekä suuria yksityisiä, että suuria julkisia organisaatioita erilaisilta toimialoilta tulosten monipuolisuuden lisäämiseksi. Haastateltavat olivat pääasiassa ylimmän tason IT-johtajia, kuten tietohallintojohtajia, sekä muita johtohenkilöitä, joilla oli kokemusta SaaS-järjestelmien käyttöönottopäätöksistä. Empiirisen aineiston analyysi toteutettiin laadullisen sisällönanalyysin mukaisesti.

Tutkimuksen ensimmäisessä tutkimuskysymyksessä pyrittiin vastaamaan seuraavaan kysymykseen:

- Mitkä ovat keskeisiä riskejä, jotka vaikuttavat SaaS-järjestelmän käyttöönottopäätökseen Suomessa toimivissa suurissa organisaatioissa?

Tutkimuksen tuloksena nousi keskeisiä havaittuja riskejä jokaisen tässä tutkimuksessa muodostetun laajennetun havaittujen riskien -viitekehyksen riskikategorian alle. Riskit painottuivat strategisten, taloudellisten sekä tietoturva- ja tietosuojariskien kategorioihin, sillä haastateltavat painottivat erityisesti näiden riskien keskeisyyttä vastauksissaan. Tuloksissa ilmeni se, miten suorituskykyriskien vaikutus käyttöönottopäätökseen on vähentynyt teknologian kehittymisen myötä sekä suurten palveluntarjoajien datakeskusten siirtyessä Suomeen lähemmäs loppukäyttäjiä. Tulosten perusteella suuriin palveluntarjoajiin kohdistuu lisäksi enemmän luottoa kuin pienempiin toimijoihin.

Tähän tutkimukseen uutena riskikategoriana lisätyt tietosuojariskit havaittiin keskeiseksi riskikategoriaksi tietoturvariskien ohella. Tietosuojariskit ovat keskeisiä GDPR:n ja toimialakohtaisten erityisvaatimusten noudattamisen takia globaalissa ja muuttuvassa toimintaympäristössä. Tietoturvaan liittyy puolestaan riskejä erityisesti toimitusketjun laajuuden ja monimutkaisuuden takia, mikä aiheuttaa asiakasorganisaatioissa epävarmuutta ja kontrollin puutteen tunnetta.

Strategiset riskit ilmenivät erityisesti liiketoiminnan ketteryyteen ja kehitykseen sekä palvelun jatkuvuuteen liittyvinä riskeinä, jotka juontuivat siitä, että asiakasorganisaation ja palveluntarjoajan

välille muodostuu keskinäisiä riippuvuuksia SaaS-järjestelmään siirryttäessä. Keskinäisten riippuvuuksien sekä SaaS-järjestelmän vaihtoon liitettyjen korkeiden kustannusten takia strategisen dissonanssin ja toimittajaloukun nähdään aiheuttavan riskiä. Näiden riskien merkitys kasvaa erityisesti kriittisten järjestelmien kohdalla tilanteissa, joissa palveluntarjoajan strategia ei tue asiakasorganisaation toimintaa dynaamisessa toimintaympäristössä.

Taloudelliset riskit keskittyivät tuloksissa hyötyjen realisointiin, piilotettuihin kuluihin sekä toimittajaloukkuun, kun taas viitekehykseen uutena lisätyt projektiriskit kulminoituivat hankeosaamisen puutteeseen. Psykososiaalisten riskien kategoriaa laajennettiin tässä tutkimuksessa vastaamaan koko organisaation henkilöstöä. Tämä laajennus johti tuloksissa siihen, että osa haastateltavista koki psykososiaalisten riskien olevan tärkeitä ja vaikuttavan käyttöönottopäätökseen, kun taas osa piti psykososiaalisten riskien, kuten muutosvastarinnan, vaikutusta SaaS-järjestelmän käyttöönottopäätökseen vaikuttamattomana tekijänä. Tuloksina nousseet SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat keskeiset riskit Suomessa toimivissa suurissa organisaatioissa ovat nähtävissä kuviossa 6.

Tutkimuksen toisessa tutkimuskysymyksessä pyrittiin puolestaan vastaamaan seuraavaan kysymykseen:

- Millaista SaaS-järjestelmän havaittuihin riskeihin liittyvää riskienhallintaa organisaatioissa tehdään ennen käyttöönottopäätöstä?

Jokainen haastateltava mainitsi, että riskien varalle tehdään riskisuunnitelmia ja riskienhallintaa jo ennen SaaS-järjestelmän käyttöönottopäätöstä. Suomessa toimivissa suurissa organisaatioissa käyttöönottopäätöstä edeltävällä riskienhallinnalla koettiin olevan vaikutusta myös lopulliseen käyttöönottopäätökseen. Organisaatioiden SaaS-järjestelmän käyttöönottopäätöstä edeltävä riskienhallinta pystyttiin tutkimuksen tulosten avulla kiteyttämään viiteen kategoriaan: organisaation tarpeen ja vaatimusten määrittely, palvelun vastaavuus ja kyvykkyyskartoitus, sopimustekniset asiat, hankeosaaminen ja resursointi sekä resilienssi ja liiketoiminnan jatkuvuus.

Riskienhallinnan avulla organisaatiot pystyvät vaikuttamaan havaittujen riskien realisoitumiseen jo ennen käyttöönottopäätöstä. Riskienhallintaa tehdään organisaatioissa laajasti, mutta tulosten perusteella kuitenkaan kaikkiin riskeihin ei pystytä varautumaan etukäteen. Tämä takia liiketoiminnan jatkuvuuden, resilienssin sekä ketteryyden kulttuurin korostaminen on tärkeää riskienhallinnan näkökulmasta. Tutkimuksen tulokset SaaS-järjestelmän käyttöönottopäätöstä edeltävästä riskienhallinnasta ovat nähtävissä taulukossa 3.

7.2 Tutkimuksen kontribuutio

Tämän tutkimuksen tulokset vastaavat osittain aikaisempaa tutkimusta, mutta myös uusia tuloksia ilmeni. Aiheesta on tehty aikaisempaa tutkimusta, mutta Suomessa toimivien suurten organisaatioiden näkökulmaa ei ole juurikaan tutkittu. Tämän tutkimuksen tulokset vahvistavat aikaisempaa tutkimusta SaaS-järjestelmien käyttöönottopäätöksiin vaikuttavista riskeistä. Tutkimus luo lisäksi tieteellistä kontribuutiota tuomalla esiin uusia näkökulmia laajentamalla havaittujen riskien -viitekehystä projektiriskeillä, tietosuojariskeillä sekä laajennetulla psykososiaalisten riskien kategorialla. Kaikkiin tämän tutkimuksen viitekehyksen riskikategorioiden alle nousi havaittuja riskejä Suomessa toimivien suurten organisaatioiden näkökulmasta. Tämän lisäksi erityisesti tietosuojariskien kasvu keskeiseksi riskikategoriaksi tietoturvariskien rinnalle voidaan nähdä tutkimuksen kontribuutiona. Tämä yhtäältä vahvistaa aikaisempaa tutkimusta vaatimuksenmukaisuuteen liittyvien riskien tärkeydestä sekä lisää aikaisempaan Benlianin ja Hessin (2011) tutkimukseen, jossa vaatimuksenmukaisuuteen, kuten tietosuojaan, liittyviä riskejä ei huomioitu.

Tutkimuksen avulla luotiin lisäksi ymmärrystä riskienhallinnan tasosta Suomessa toimivissa suurissa organisaatioissa. Tulokset osoittivat, että riskienhallintaa ja havainnointia tehdään laajasti ja systemaattisesti jo ennen SaaS-järjestelmän käyttöönottopäätöstä. Suurten Suomessa toimivien organisaatioiden riskienhallinta ennen SaaS-järjestelmän käyttöönottopäätöstä mukailee riskitietoisen päätöksenteon sekä riskinkäsittelyn prosesseja. Suurin osa haastateltavista koki organisaation suorittaman riskienhallinnan olevan monipuolista ja riittävällä tasolla suhteutettuna riskienhallinnan kustannuksiin.

Tämän tutkimuksen tulokset voivat hyödyttää erityisesti Suomessa toimivia suuria organisaatioita, tarjoamalla käytännön työkaluja, joilla voidaan huomioida keskeisimmät riskit sekä riskienhallinnan tärkeimmät osa-alueet SaaS-järjestelmien käyttöönottopäätöksissä. Organisaatiot voivat hyödyntää tätä tutkimusta myös suunnitellessaan omaa päätöksentekoprosessia sekä vahvistaessaan riskienhallintaa SaaS-järjestelmien ja muiden pilvipalveluiden kontekstissa. Myös pienemmät ja keskisuuret organisaatiot voivat hyötyä tämän tutkimuksen tuloksista suhteuttamalla ne omaan toimintaansa. Tällöin pienemmätkin organisaatiot pystyvät tehostamaan riskienhallintaa ja päätöksentekoa omissa konteksteissaan.

7.3 Rajoitukset ja jatkotutkimuskohteet

Tässä tutkimuksessa, kuten useimmissa tutkimuksissa, on tiettyjä rajoitteita. Vaikka tutkimus tehtiin useamman kuin yhden tutkijan toimesta, puolueellisuutta ja tästä johtuvia vinoumia voi silti esiintyä. Tutkijat omaavat samankaltaiset opintotaustat ja täten diversiteettiä tutkijoiden välillä on rajallisesti. Mahdollisuutta vinoumien muodostumiseen on kuitenkin pyritty minimoimaan esimerkiksi antamalla haastateltavien oman äänen olla analyysien keskiössä, noudattamalla metodologia- ja metodikirjallisuutta sekä yhdistelemällä tutkijoiden ajatuksia. Yhdistämällä tutkijoiden ajatuksia on pystytty jossain määrin haastamaan ja laajentamaan yhden henkilön näkemyksiä tulosten muodostamisessa. Lisäksi tutkimuksessa haastateltiin suurimmaksi osaksi vain IT-ammattilaisia, jolloin tutkimuksen näkökulma saattaa olla rajallinen.

Tutkimuksessa käytetty havaittujen riskien -viitekehys on tutkimuskentällä laajasti hyväksytty, mutta sen käytöstä SaaS-järjestelmien käyttöönottopäätösten kontekstissa on kuitenkin verrattain vähän aikaisempaa tutkimusta. Tämän lisäksi havaittujen riskien -viitekehystä muokattiin ja laajennettiin tätä tutkimusta varten, mikä tuo toisaalta uutta näkökulmaa aiheeseen, mutta toisaalta myös epävarmuutta tulosten validoinnissa, sillä aikaisempaan tutkimukseen ei voida täysin nojautua. Samoin laajan riskin luokittelu ainoastaan yhden riskikategorian alle voidaan nähdä rajoitteena, sillä laajoilla riskeillä saattaa olla vaikutusta pääasiallisen riskikategorian lisäksi myös toisiin riskikategorioihin. Tämän takia jatkossa voidaan pyrkiä muokkaamaan viitekehystä entisestään, jolloin havaittujen riskien -viitekehyksen riskikategorioiden välisiä yhteyksiä pystyttäisiin paremmin selvittämään.

Tutkimuksessa haastateltavat mainitsivat, mitä SaaS-järjestelmän käyttöönottopäätökseen vaikuttavia riskejä organisaatioissa havaitaan ja miksi, mutta riskien yksilökohtaisia vaikutuksia tai vaikutusten painoarvoa ei tutkittu tässä tutkimuksessa. Tämä tulosten määrällistämisen puute voidaan nähdä rajoitteena, sillä yksittäisten riskitekijöiden laskennallista painoarvoa tai niiden lopullista merkitystä osana kokonaisuutta ei voida tarkasti määrittää osana tätä tutkimusta. Osalla havaituista riskeistä saattaa olla toisia riskejä pienempi lopullinen vaikutus SaaS-järjestelmän käyttöönottopäätökseen. Yksittäisten riskien painoarvoa on mahdollista tutkia tulevissa tutkimuksissa, jolloin riskien merkityksestä saataisiin tarkempaa tietoa määrällisessä muodossa laadullisen painotuksen sijaan.

SaaS-järjestelmät tulevat luultavasti muuttumaan tulevaisuudessa sekä teknologisesti että liiketoimintalogiikaltaan, jolloin myös niiden riskit voivat muuttua radikaalisti. Lisäksi toimintaympäristössä, kuten lainsäädännössä, saattaa tapahtua keskeisiä muutoksia, jotka voivat

vaikuttaa suoraan tai välillisesti SaaS-järjestelmiin. Jatkotutkimusta voidaan tehdä myös samasta aiheesta tällaisten keskeisten teknologisten, liiketoimintalogiikallisten tai toimintaympäristöllisten muutosten jälkeen. SaaS-järjestelmän käyttöönottopäätökseen liittyvät riskit saattavat olla erilaisia myös erikokoisissa organisaatioissa, joten samankaltaista tutkimusta voitaisiin tehdä myös pienten ja keskisuurten Suomessa toimivien tai ulkomaisten organisaatioiden näkökulmasta.

Lähteet

Adeoye-Olatunde, O. A., & Olenik, N. L. (2021). Research and scholarly methods: Semi-structured interviews. *JACCP: JOURNAL OF THE AMERICAN COLLEGE OF CLINICAL PHARMACY*, *4*(10), 1358–1367. https://doi.org/10.1002/jac5.1441

Akinrolabu, O., Nurse, J. R. C., Martin, A., & New, S. (2019). Cyber risk assessment in cloud provider environments: Current models and future needs. *Computers & Security*, *87*, 101600. https://doi.org/10.1016/j.cose.2019.101600

Ali, A., Warren, D., & Mathiassen, L. (2017). Cloud-based business services innovation: A risk management model. *International Journal of Information Management*, *37*(6), 639–649. https://doi.org/10.1016/j.ijinfomgt.2017.05.008

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, *305*, 357–383. https://doi.org/10.1016/j.ins.2015.01.025

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. https://doi.org/10.1145/1721654.1721672

Aubert, B. A., Houde, J.-F., Patry, M., & Rivard, S. (2012). A multi-level investigation of information technology outsourcing. *The Journal of Strategic Information Systems*, *21*(3), 233–244. https://doi.org/10.1016/j.jsis.2012.04.004

Aven, T. (2012). *Foundations of Risk Analysis*. John Wiley & Sons, Incorporated. http://ebookcentral.proquest.com/lib/kutu/detail.action?docID=847490

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology*, *12*, 529–534. https://doi.org/10.1016/j.protcy.2013.12.525

Barnard, F. H., & Van Der Lingen, E. (2022). Adoption of software as a service: A FUZZY APPROACH TO RANKING THE DETERMINANTS. *South African Journal of Industrial Engineering*, *33*(4). https://doi.org/10.7166/33-4-2639

Barthelemy, J. (2001). The Hidden Costs of IT Outsourcing. *MIT Sloan Management Review*, *42*(3), 60–69. ProQuest Central.

Benlian, A., & Hess, T. (2011). Opportunities and risks of software-as-a-service: Findings from a survey of IT executives. *Decision Support Systems*, *52*(1), 232–246. https://doi.org/10.1016/j.dss.2011.07.007

Bettman, J. R. (1973). Perceived Risk and Its Components: A Model and Empirical Test. *Journal of Marketing Research*, *10*(2), 184. https://doi.org/10.2307/3149824

Bibi, S., Katsaros, D., & Bozanis, P. (2012). Business Application Acquisition: On-Premise or SaaS-Based Solutions? *IEEE Software*, *29*(3), 86–93. https://doi.org/10.1109/MS.2011.119

Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management*, *33*(5), 726–733. https://doi.org/10.1016/j.ijinfomgt.2013.05.004

Burkon, L. (2013). Quality of Service Attributes for Software as a Service. *Journal of Systems Integration*, *4*(3), 38–47. ProQuest Central; Publicly Available Content Database.

Candeia, D., Santos, R. A., & Lopes, R. (2015). Business-Driven Long-Term Capacity Planning for SaaS Applications. *IEEE Transactions on Cloud Computing*, *3*(3), 290–303. https://doi.org/10.1109/TCC.2015.2424877

Chang, Y.-W. (2020). What drives organizations to switch to cloud ERP systems? The impacts of enablers and inhibitors. *Journal of Enterprise Information Management*, *33*(3), 600–626. https://doi.org/10.1108/JEIM-06-2019-0148

Chang, Y.-W., & Hsu, P.-Y. (2019). An empirical investigation of organizations' switching intention to cloud enterprise resource planning: A cost-benefit perspective. *Information Development*, *35*(2), 290–302. https://doi.org/10.1177/0266666917743287

Chau, P. Y. K., & Tam, K. Y. (1997). Factors Affecting the Adoption of Open Systems: An Exploratory Study. *MIS Quarterly*, *21*(1), 1. https://doi.org/10.2307/249740

Chen, J. V., Yen, D. C., & Chen, K. (2009). The acceptance and diffusion of the innovative smart phone use: A case study of a delivery service company in logistics. *Information & Management*, *46*(4), 241–248. https://doi.org/10.1016/j.im.2009.03.001

Cho, V., & Chan, A. (2015). An integrative framework of comparing SaaS adoption for core and non-core business operations: An empirical study on Hong Kong industries. *Information Systems Frontiers*, *17*(3), 629–644. https://doi.org/10.1007/s10796-013-9450-9

Chou, S.-W., & Chiang, C.-H. (2013). Understanding the formation of software-as-a-service (SaaS) satisfaction from the perspective of service quality. *Decision Support Systems*, *56*, 148–155. https://doi.org/10.1016/j.dss.2013.05.013

Christou, P. (2023). How to Use Artificial Intelligence (AI) as a Resource, Methodological and Analysis Tool in Qualitative Research? *The Qualitative Report*. https://doi.org/10.46743/2160-3715/2023.6406

Clemons, E. K., & Weber, B. W. (1990). Strategic Information Technology Investments: Guidelines for Decision Making. *Journal of Management Information Systems*, *7*(2), 9–28. https://doi.org/10.1080/07421222.1990.11517887

Cunningham, S. (1967). *The major dimensions of perceived risk, D.F. Cox (Ed.), Risk Taking and Information Handling in Consumer Behavior, Harvard University Press, Cambridge, MA, S. 102–108.*

Elo, S., Kajula, O., Tohmola, A., & Kääriäinen, M. (2022). Laadullisen sisällönanalyysin vaiheet ja eteneminen. *Hoitotiede*, *34*(4), 215–225.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Elo, S., Kääriäinen, M., Kanste, O., Pölkki, T., Utriainen, K., & Kyngäs, H. (2014). Qualitative Content Analysis: A Focus on Trustworthiness. *Sage Open*, *4*(1), 2158244014522633. https://doi.org/10.1177/2158244014522633

Eriksson, P., & Kovalainen, A. (2008). *Qualitative Methods in Business Research*. SAGE Publications Ltd. https://doi.org/10.4135/9780857028044

Eriksson, P., & Kovalainen, A. (2016). *Qualitative methods in business research* (2nd edition). Sage.

EU. (2025, maaliskuuta 3). *Yleinen tietosuoja-asetus (GDPR)*. Your Europe. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Fan, Z.-P., Suo, W.-L., & Feng, B. (2012). Identifying risk factors of IT outsourcing using interdependent information: An extended DEMATEL method. *Expert Systems with Applications*, *39*(3), 3832–3840. https://doi.org/10.1016/j.eswa.2011.09.092

Firoiu, M. (2015). General Considerations on Risk Management and Information System Security Assessment According to ISO/IEC 27005:2011 and ISO 31000:2009 Standards: Acces la Success. *Calitatea*, *16*(149), 93–97. ProQuest Central.

Furman, E., & Diamant, A. (2025). Optimal capacity planning for cloud service providers with periodic, time-varying demand. *European Journal of Operational Research*, *322*(1), 133–146. https://doi.org/10.1016/j.ejor.2024.11.017

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated TAM-TOE model. *Journal of Enterprise Information Management*, *28*(1), 107–130. https://doi.org/10.1108/JEIM-08-2013-0065

Gartner. (ei pvm.-a). *Definition of Cloud Computing—Gartner Information Technology Glossary*. Gartner. Noudettu 6. marraskuuta 2024, osoitteesta https://www.gartner.com/en/information-technology/topics/cloud-strategy

Gartner. (ei pvm.-b). *Definition of Software as a Service (SaaS)—Gartner Information Technology Glossary*. Gartner. Noudettu 8. marraskuuta 2024, osoitteesta https://www.gartner.com/en/information-technology/glossary/software-as-a-service-saas

Georgiopoulou, Z., Makri, E.-L., & Lambrinoudakis, C. (2020). GDPR compliance: Proposed technical and organizational measures for cloud provider. *Information & Computer Security*, *28*(5), 665–680. https://doi.org/10.1108/ICS-01-2020-0009

Gewald, H., & Dibbern, J. (2009). Risks and benefits of business process outsourcing: A study of transaction services in the German banking industry. *Information & Management*, *46*(4), 249–257. https://doi.org/10.1016/j.im.2009.03.002

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today*, *24*(2), 105–112. https://doi.org/10.1016/j.nedt.2003.10.001

Gupta, P., Seetharaman, A., & Raj, J. R. (2013). The usage and adoption of cloud computing by small and medium businesses. *International Journal of Information Management*, *33*(5), 861–874. https://doi.org/10.1016/j.ijinfomgt.2013.07.001

Gupta, S., Pani, S. K., Muduli, K., Vaish, A., & Kumar, A. (2023). Risk Managed Cloud Adoption: An ANP Approach. *International Journal of Mathematical, Engineering and Management Sciences*, *8*(1), 78–93. https://doi.org/10.33889/IJMEMS.2023.8.1.005

Gutierrez, A., Boukrami, E., & Lumsden, R. (2015). Technological, organisational and environmental factors influencing managers' decision to adopt cloud computing in the UK. *Journal of Enterprise Information Management*, *28*(6), 788–807. https://doi.org/10.1108/JEIM-01-2015-0001

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications*, *4*(1), 5. https://doi.org/10.1186/1869-0238-4-5

Hirsjärvi, S., Remes, P., Sajavaara, P., Sinivuori, E., & Tammi (yhtiö), kustantaja. (2007). *Tutki ja kirjoita* (13., osin uudistettu painos.). Kustannusosakeyhtiö Tammi.

Hsu, C.-L., & Lin, J. C.-C. (2016). Factors affecting the adoption of cloud services in enterprises. *Information Systems and E-Business Management*, *14*(4), 791–822. https://doi.org/10.1007/s10257-015-0300-9

Islam, S., Fenz, S., Weippl, E., & Mouratidis, H. (2017). A Risk Management Framework for Cloud Migration Decision Support. *Journal of Risk and Financial Management*, *10*(2), 10. https://doi.org/10.3390/jrfm10020010

Khanra, S., Dhir, A., Parida, V., & Kohtamäki, M. (2021). Servitization research: A review and bibliometric analysis of past achievements and future promises. *Journal of Business Research*, *131*, 151–166. https://doi.org/10.1016/j.jbusres.2021.03.056

Kim, S. H., Jang, S. Y., & Yang, K. H. (2017). Analysis of the Determinants of Software-as-a-Service Adoption in Small Businesses: Risks, Benefits, and Organizational and Environmental Factors: JOURNAL OF SMALL BUSINESS MANAGEMENT. *Journal of Small Business Management*, *55*(2), 303–325. https://doi.org/10.1111/jsbm.12304

Kung, L., Cegielski, C. G., & Kung, H.-J. (2015). An Integrated Environmental Perspective on Software as a Service Adoption in Manufacturing and Retail Firms. *Journal of Information Technology*, *30*(4), 352–363. https://doi.org/10.1057/jit.2015.14

Kyngäs, H., Elo, S., Pölkki, T., Kääriäinen, M., & Kanste, O. (2011). Sisällönanalyysi suomalaisessa hoitotieteellisessä tutkimuksessa. *Hoitotiede*, *23*, 138–148.

Lacity, M. C., Khan, S., Yan, A., & Willcocks, L. P. (2010). A Review of the it Outsourcing Empirical Literature and Future Research Directions. *Journal of Information Technology*, *25*(4), 395–433. https://doi.org/10.1057/jit.2010.21

Lal, P., & Bharadwaj, S. S. (2016). Understanding the impact of cloud-based services adoption on organizational flexibility: An exploratory study. *Journal of Enterprise Information Management*, *29*(4), 566–588. https://doi.org/10.1108/JEIM-04-2015-0028

Lee, G. R., & Lee, S. (2020). How Outsourcing May Enhance Job Satisfaction in the U.S. Federal Bureaucracy: Exploring the Role of Knowledge Sharing. *The American Review of Public Administration*, *50*(4–5), 387–400. https://doi.org/10.1177/0275074020913980

Lee, S., Park, S. B., & Lim, G. G. (2013). Using balanced scorecards for the evaluation of "Software-as-a-service". *Information & Management*, *50*(7), 553–561. https://doi.org/10.1016/j.im.2013.07.006

Loukis, E., Arvanitis, S., & Kyriakou, N. (2017). An empirical investigation of the effects of firm characteristics on the propensity to adopt cloud computing. *Information Systems and E-Business Management*, *15*(4), 963–988. https://doi.org/10.1007/s10257-017-0338-y

Loukis, E., Janssen, M., & Mintchev, I. (2019). Determinants of software-as-a-service benefits and impact on firm performance. *Decision Support Systems*, *117*, 38–47. https://doi.org/10.1016/j.dss.2018.12.005

Low, C., Chen, Y., & Wu, M. (2011). Understanding the determinants of cloud computing adoption. *Industrial Management & Data Systems*, *111*(7), 1006–1023. https://doi.org/10.1108/02635571111161262

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems*, *51*(1), 176–189. https://doi.org/10.1016/j.dss.2010.12.006

Martins, R., Oliveira, T., & Thomas, M. A. (2016). An empirical analysis to assess the determinants of SaaS diffusion in firms. *Computers in Human Behavior*, *62*, 19–33. https://doi.org/10.1016/j.chb.2016.03.049

Matias, J. B., & Hernandez, A. A. (2021). Cloud Computing Adoption Intention by MSMEs in the Philippines. *Global Business Review*, *22*(3), 612–633. https://doi.org/10.1177/0972150918818262

Mell, P., & Grance, T. (2011). *The NIST definition of cloud computing* (NIST SP 800-145; 0 p., s. NIST SP 800-145). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-145

Misra, S. C., & Mondal, A. (2011). Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. *Mathematical and Computer Modelling*, *53*(3–4), 504–521. https://doi.org/10.1016/j.mcm.2010.03.037

Mithas, S., Tafti, A., & Mitchell, W. (2013). How a Firm's Competitive Environment and Digital Strategic Posture Influence Digital Business Strategy. *MIS Quarterly*, *37*(2), 511–536. https://doi.org/10.25300/MISQ/2013/37.2.09

Moses, A., & Åhlström, P. (2008). Problems in cross-functional sourcing decision processes. *Journal of Purchasing and Supply Management*, *14*(2), 87–99. https://doi.org/10.1016/j.pursup.2007.11.003

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*(1), 1609406917733847. https://doi.org/10.1177/1609406917733847

Nudurupati, S. S., Lascelles, D., Wright, G., & Yip, N. (2016). Eight challenges of servitisation for the configuration, measurement and management of organisations. *Journal of Service Theory and Practice*, *26*(6), 745–763. https://doi.org/10.1108/JSTP-02-2015-0045

Oliveira, T., Martins, R., Sarker, S., Thomas, M., & Popovič, A. (2019). Understanding SaaS adoption: The moderating impact of the environment context. *International Journal of Information Management*, *49*, 1–12. https://doi.org/10.1016/j.ijinfomgt.2019.02.009

Opara-Martins, J., Sahandi, R., & Tian, F. (2016). Critical analysis of vendor lock-in and its impact on cloud computing migration: A business perspective. *Journal of Cloud Computing*, *5*(1), 4. https://doi.org/10.1186/s13677-016-0054-z

Park, J., Han, K., & Lee, B. (2023). Green Cloud? An Empirical Analysis of Cloud Computing and Energy Efficiency. *Management Science*, *69*(3), 1639–1664. https://doi.org/10.1287/mnsc.2022.4442

Peter, J. P., & Ryan, M. J. (1976). An Investigation of Perceived Risk at the Brand Level. *Journal of Marketing Research*, *13*(2), 184. https://doi.org/10.2307/3150856

Phaphoom, N., Wang, X., Samuel, S., Helmer, S., & Abrahamsson, P. (2015). A survey study on major technical barriers affecting the decision to adopt cloud services. *Journal of Systems and Software*, *103*, 167–181. https://doi.org/10.1016/j.jss.2015.02.002

Rath, A., Mohapatra, S., Kumar, S., & Thakurta, R. (2012). Decision points for adoption cloud computing in small, medium enterprises (SMEs). *ICITST*, 688–691.

Safari, F., Safari, N., & Hasanzadeh, A. (2015). The adoption of software-as-a-service (SaaS): Ranking the determinants. *Journal of Enterprise Information Management*, *28*(3), 400–422. https://doi.org/10.1108/JEIM-02-2014-0017

Schneider, S., & Sunyaev, A. (2016). Determinant Factors of Cloud-Sourcing Decisions: Reflecting on the IT Outsourcing Literature in the Era of Cloud Computing. *Journal of Information Technology*, *31*(1), 1–31. https://doi.org/10.1057/jit.2014.25

Senyo, P. K., Addae, E., & Boateng, R. (2018). Cloud computing research: A review of research themes, frameworks, methods and future research directions. *International Journal of Information Management*, *38*(1), 128–139. https://doi.org/10.1016/j.ijinfomgt.2017.07.007

Shapouri, F., Ward, K., & Setor, T. (2024). Determinants of Software as a Service (SaaS) Adoption. *Journal of Computer Information Systems*, *64*(2), 301–313. https://doi.org/10.1080/08874417.2023.2199270

Shuraida, S., & Titah, R. (2023). An examination of cloud computing adoption decisions: Rational choice or cognitive bias? *Technology in Society*, *74*, 102284. https://doi.org/10.1016/j.techsoc.2023.102284

Singh, M., Jiao, J., Klobasa, M., & Frietsch, R. (2022). Servitization of Energy Sector: Emerging Service Business Models and Startup's Participation. *Energies*, *15*(7), 2705. https://doi.org/10.3390/en15072705

Statista. (2024, heinäkuuta). *Software as a Service: Market data & analysis*. Statista. https://www.statista.com/study/84974/software-as-a-service-report/

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. https://doi.org/10.1016/j.jnca.2010.07.006

Sultan, N. (2010). Cloud computing for education: A new dawn? *International Journal of Information Management*, *30*(2), 109–116. https://doi.org/10.1016/j.ijinfomgt.2009.09.004

Sun, S., Cegielski, C. G., Jia, L., & Hall, D. J. (2018). Understanding the Factors Affecting the Organizational Adoption of Big Data. *Journal of Computer Information Systems*, *58*(3), 193–203. https://doi.org/10.1080/08874417.2016.1222891

Taleb, T., Ksentini, A., & Jantti, R. (2016). "Anything as a Service" for 5G Mobile Systems. *IEEE Network*, *30*(6), 84–91. https://doi.org/10.1109/MNET.2016.1500244RP

Teo, Wei, & Benbasat. (2003). Predicting Intention to Adopt Interorganizational Linkages: An Institutional Perspective. *MIS Quarterly*, *27*(1), 19. https://doi.org/10.2307/30036518

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *The Processes of Technological Innovation*. Lexington Books. https://books.google.fi/books?id=EotRAAAAMAAJ

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Van De Weerd, I., Mangula, I. S., & Brinkkemper, S. (2016). Adoption of software as a service in Indonesia: Examining the influence of organizational factors. *Information & Management*, *53*(7), 915–928. https://doi.org/10.1016/j.im.2016.05.008

Viega, J. (2009). Cloud Computing and the Common Man. *Computer*, *42*(7), 106–108. https://doi.org/10.1109/MC.2009.252

Wheeler, E. (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up*. Elsevier Science & Technology Books. http://ebookcentral.proquest.com/lib/kutu/detail.action?docID=685406

Wu, W.-W., Lan, L. W., & Lee, Y.-T. (2011). Exploring decisive factors affecting an organization's SaaS adoption: A case study. *International Journal of Information Management*, *31*(6), 556–563. https://doi.org/10.1016/j.ijinfomgt.2011.02.007

Yang, Z., Sun, J., Zhang, Y., & Wang, Y. (2015). Understanding SaaS adoption from the perspective of organizational users: A tripod readiness model. *Computers in Human Behavior*, *45*, 254–264. https://doi.org/10.1016/j.chb.2014.12.022

Yau, S., & An, H. (2011). Software Engineering Meets Services and Cloud Computing. *Computer*, *44*(10), 47–53. https://doi.org/10.1109/MC.2011.267

Yau, S. S., Pandya, K., & Choudhary, S. (2024). Regulatory Compliance in Software Services Using Emerging Technologies. *2024 IEEE International Conference on Software Services Engineering (SSE)*, 36–42. https://doi.org/10.1109/SSE62657.2024.00018

Yigitbasioglu, O. (2014). Modelling the Intention to Adopt Cloud Computing Services: A Transaction Cost Theory Perspective. *Australasian Journal of Information Systems*, *18*(3). https://doi.org/10.3127/ajis.v18i3.1052

Zhu, K., Kraemer, K. L., & Xu, S. (2006). The Process of Innovation Assimilation by Firms in Different Countries: A Technology Diffusion Perspective on E-Business. *Management Science*, *52*(10), 1557–1576. https://doi.org/10.1287/mnsc.1050.0487

Zissis, D., & Lekkas, D. (2012). Addressing cloud computing security issues. *Future Generation Computer Systems*, *28*(3), 583–592. https://doi.org/10.1016/j.future.2010.12.006

Liitteet

Liite 1. Haastattelurunko

1. **Haastattelun aloitus**
    a. Tutkimuksen tausta, tarkoitus ja kulku
    b. Tutkimuseettisyys: Haastateltavan oikeudet, yksityisyys, tallentaminen, julkaisu ja tietoturva
    c. Haastateltavan suostumus haastatteluun
2. **Haastateltavan taustatiedot**
    a. Mikä on työtehtäväsi tällä hetkellä?
        i. Millä toimialalla työskentelet?
        ii. Minkä kokoinen organisaatio?
        iii. Miten kauan olet toiminut vastaavissa tehtävissä?
    b. Millaista kokemusta sinulla on SaaS-järjestelmistä ja erityisesti niiden käyttöönottoprojekteista?
        i. Millaisia SaaS-järjestelmiä on otettu käyttöön?
        ii. Miten kuvailisit näiden järjestelmien kriittisyyttä organisaation toiminnalle?
        iii. Miten suuri käyttäjämäärä SaaS-järjestelmillä on/oli?
        iv. Millainen rooli sinulla on ollut SaaS-käyttöönotossa?
3. **SaaS-järjestelmien käyttöönoton havaitut riskit**
    a. Suorituskykyriskit

    Suorituskykyriskeillä viitataan erityisesti riskeihin, jotka liittyvät mahdolliseen tilanteeseen, jossa palveluntarjoaja tai asiakasorganisaatio ei onnistukaan saavuttamaan haluttua suorituskykyä tai toiminnan tasoa.

        i. Millaisia suorituskykyriskejä SaaS-järjestelmien käyttöönottopäätökseen liittyy ja miksi?
        ii. Minkä/mitkä koet keskeisimmäksi suorituskykyriskiksi?
    b. Tietoturva- ja tietosuojariskit

    Tietoturva- ja tietosuojariskeillä viitataan asiakkaan epävarmuuteen oman datansa ja organisaationsa turvallisuudesta sekä tietosuojavaatimusten noudattamisesta.

        i. Millaisia tietoturva- ja tietosuojariskejä SaaS-järjestelmien käyttöönottopäätökseen liittyy ja miksi?
        ii. Minkä/mitkä koet keskeisimmäksi tietoturva- ja tietosuojariskiksi?

c. Strategiset riskit

Strategiset riskit ovat sellaisia, joihin liittyy kriittisiä resursseja tai kyvykkyyksiä, jotka organisaatio saattaa menettää ulkoistaessaan sovelluksia SaaS-pilvipalvelumallia käyttäen.

i. Millaisia strategisia riskejä SaaS-järjestelmien käyttöönottopäätökseen liittyy ja miksi?

ii. Minkä/mitkä koet olevan keskeisin strateginen riski?

d. Taloudelliset riskit

Taloudellisilla riskeillä viitataan SaaS-järjestelmään liittyviä rahallisia riskejä, joita saattaa koitua asiakasorganisaatiolle.

i. Millaisia taloudellisia riskejä SaaS-järjestelmien käyttöönottopäätökseen liittyy ja miksi?

ii. Minkä/mitkä koet olevan keskeisin taloudellinen riski?

e. Psykososiaaliset riskit

Psykososiaalisilla riskeillä viitataan SaaS-järjestelmiin liittyviin psykologisiin sekä sosiaalisiin riskeihin, jotka saattavat vaikuttaa suoraan tai välillisesti asiakasorganisaatioon sekä erityisesti sen henkilöstöön.

i. Millaisia psykososiaalisia riskejä SaaS-järjestelmien käyttöönottopäätökseen liittyy ja miksi?

ii. Minkä/mitkä koet olevan keskeisin psykososiaalinen riski?

f. Projektiriskit

Projektiriskeillä tarkoitetaan projektin laajuudesta, monimutkaisuudesta tai henkilökunnan taitojen ylittymisestä johtuvia riskejä.

i. Millaisia projektiriskejä SaaS-järjestelmien käyttöönottopäätökseen liittyy ja miksi?

ii. Minkä koet olevan keskeisin projektiriski?

4. SaaS-järjestelmien käyttöönoton riskisuunnitelmat

a. Tehtiinkö ennen SaaS-järjestelmän käyttöönottopäätöstä riskisuunnitelmia?

i. Jos tehtiin

1. Miten analysointi ja suunnittelu tapahtui?
2. Millaisia riskisuunnitelmia tehtiin ennen käyttöönottopäätöstä?
3. Miten riskisuunnitelmat vaikuttivat käyttöönottopäätökseen?

ii. Jos ei tehty riskisuunnitelmia ennen käyttöönottopäätöstä

1. Minkä takia?

2. Tehtiinkö riskisuunnitelmia jossain muussa vaiheessa?

b. Pystytkö kommentoimaan suunnitelmien onnistumista?

c. Koetko, että olisi pitänyt tehdä (enemmän) riskisuunnitelmia jo ennen käyttöönottopäätöstä ja miksi?

d. Mitä mielestäsi erityisesti tulisi ottaa huomioon SaaS-järjestelmien riskienhallinnassa jo siinä vaiheessa, kun pohditaan SaaS-järjestelmien käyttöönottopäätöstä ja miksi?

5. Avoin osio

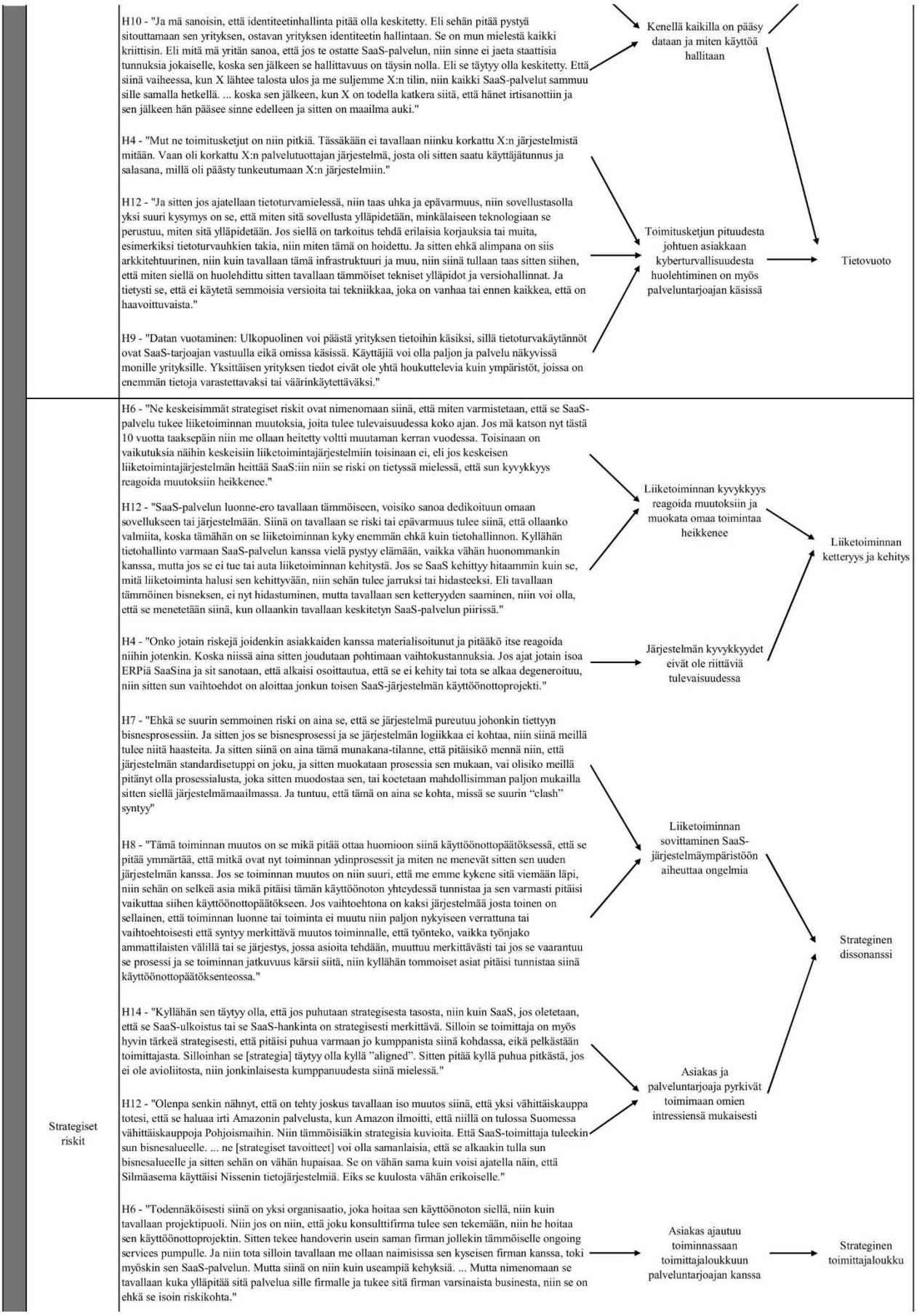
a. Onko sinulla vielä lisättävää johonkin aikaisempiin kohtiin tai haluaisitko kertoa vielä jotain, mitä tässä haastattelussa ei olla käsitelty?

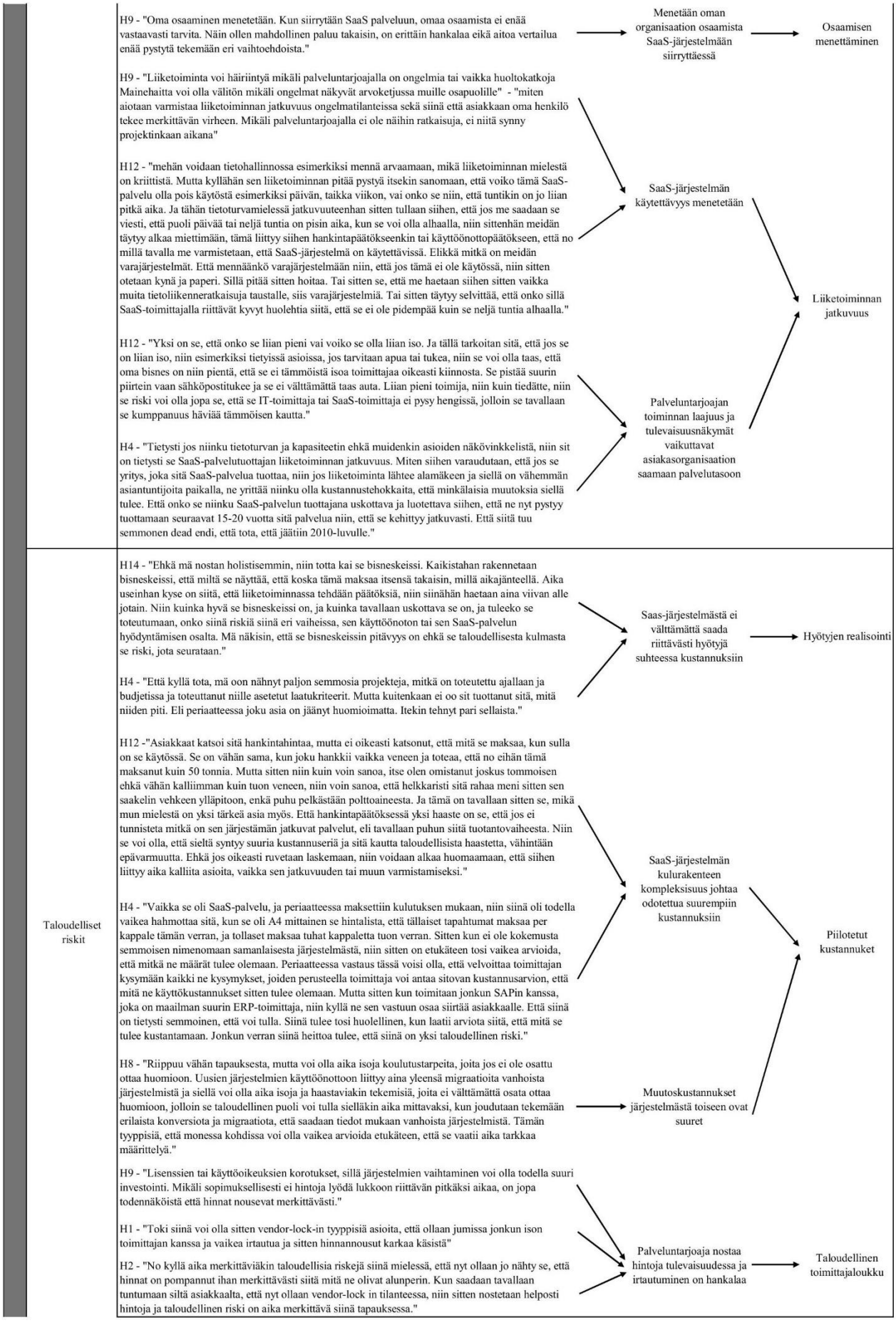
6. Haastattelun päättäminen

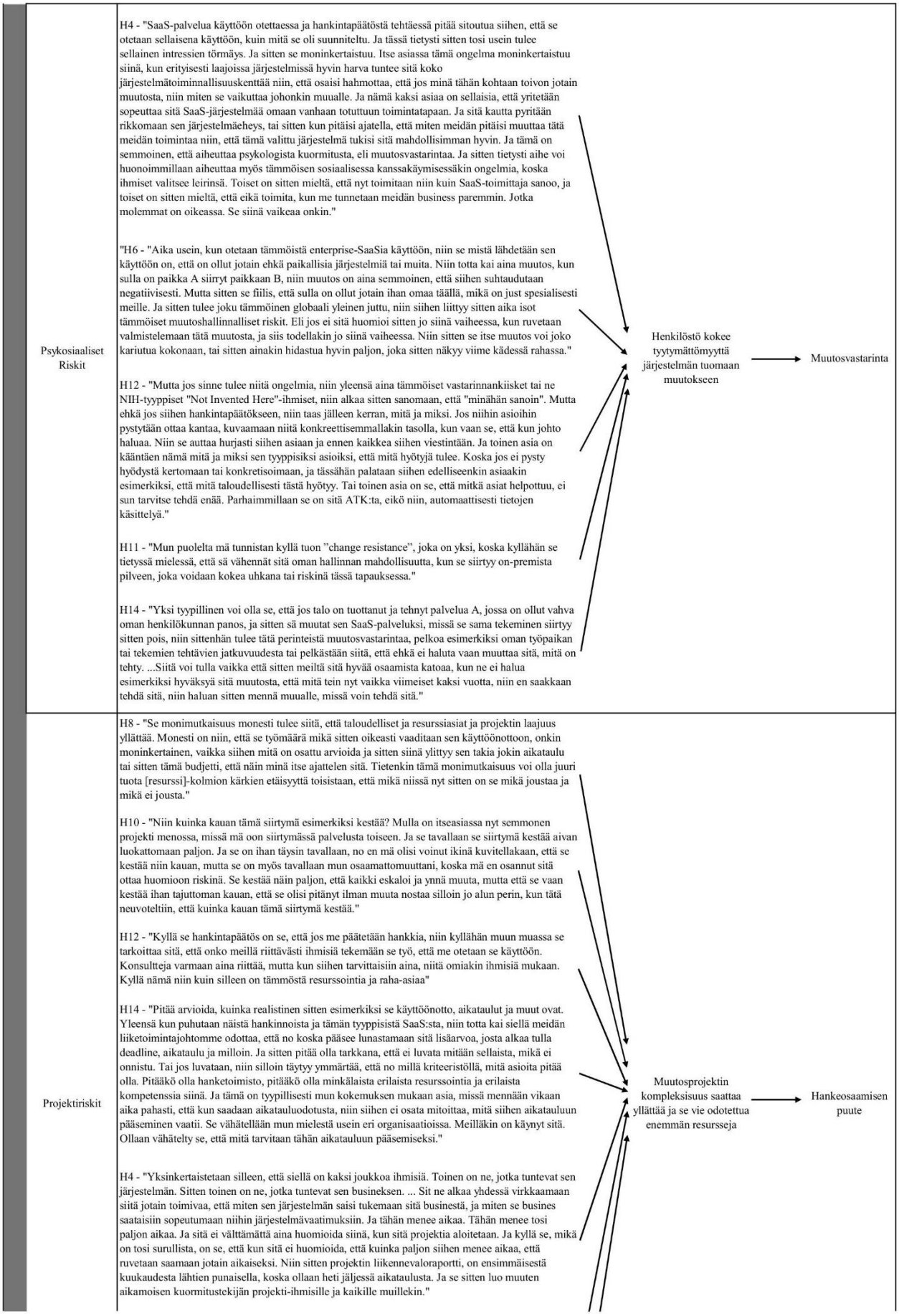
Liite 2. Analyysitaulukko SaaS-järjestelmän käyttöönottopäätökseen vaikuttavista havaituista riskeistä

SaaS-järjestelmän käyttöönottopäätökseen vaikuttavat havaitut riskit Suomessa toimivissa suurissa organisaatioissa

Yläluokka	Autenttiset lainaukset	Pelkistetty ilmaus	Alaluokka
Suorituskykyriskit	H3 - "Keskeisimmät riskit ovat tietoliikenteen määrässä, eli pystykö se toimittaja oikeasti skaalaamaan, jos tulee suuria loppukäyttäjäpiikkejä siihen palveluun." H4 - "Onks semmoista päiväkohtaista tai viikkokohtaista jotain kuormitushuippua. Esimerkiksi nyt meillä niinku täällä meidän alalla maanantai-aamupäivät on kuormitushuippuja. Ihmisiä tulee puhelimessa ja chatissa paljon enemmän sisään, kun mitä perjantai-ilta päivällä, et ihmiset ilmoittaa sairastavansa, maanantaiaamusta paljon. Niinku et onks tämmöstä niinku ajan yli heiluvaa kuormitusta."	Kuormitushuiput aiheuttavat ongelmatilanteita suorituskyvyssä	Käytön skaalautuvuus
	H2 - "No kyllä se on se käytön hitaus varmasti on ollut. Ehkä sitten kokonaan se saatavuuskin, että jos se on pois päältä eikä me voida tehdä asialle mitään, mutta kyllä se aika pitkälle kulminoituu siihen, että on hidas käyttää." H6 - "Niin onko esimerkiksi verkon nopeus riittävä, jotta pystytään toimimaan sen kanssa? Kun aikaisemmin on ollut paikallisia sovelluksia ja serverit on esimerkiksi samalla mantereella tai samassa maassa. Niin on ihan tästä nykyisestä hankkeesta ja itse asiassa muutamasta aikaisemmastakin. Niin mikä on siis sanotaan latenssi, jos meillä pyörii pannut vaikka Dublinissa, mutta käyttäjät on vaikka Australiassa. Niitä on joutunut sitten perkaamaan. Loppujen lopuksi ne on sitten aika hyvin pystytty mitigoimaan koska puhutaan kuitenkin tämmösistä globaaleista ratkaisuista."	Verkonnopeus- ja latenssiongelmat aiheuttavat ongelmia käytettävyyteen	Palvelun saatavuus ja käytettävyys
	H1 - "se datan sijainti on meille ehkä tärkeämpää ja sitten se että pystyykö ne pitämään sen pystyssä niin meillä on pieniä niitä pieniä hallinnonsovelluksia on sellaisia, että ne saattaa olla teoriassa ainakin jossain melkein sen firman omassa konesalissa jossain komerossa ja me halutaan yleensä aina ymmärtää että missä se on ja se liittyy sitten just siihen pystyykö ne pitämään sen pystyssä"	Lokaatio ja koko tuovat epävarmuutta palvelun saatavuuteen	
	H2 - "Ja yksi varmaan semmoinen mikä tuli niin noi integraatiot on aina semmoinen ikuinen juttu, että kun SaaS-järjestelmien käyttöönottoa ja riskejä mietitään niin varmasti se että saadaanko ne SaaS-järjestelmät integroitua meidän olemassa oleviin SaaS-järjestelmiin taikka meidän on-premi -järjestelmiin. Se on ehkä semmoinen mikä on nyt tullut tapetille näitten SaaSien myötä, että onko siellä näitä API:ja ja ja muita riittävästi." H14 - "Sitten otetaan toinen ääripää, otetaan joku liiketoimintaprosessin osaa tai kokonaista prosessia tuottava SaaS-järjestelmäkokonaisuus, joka pitää integroida vaikkapa meidän organisaation kanaviin. No sitten alkaakin olla vähän erilaiset tekniset vaatimukset, joiden osalta sitten kukin voi tietysti olla riski, jos ei sitä saada sovitettua. Nythän puhutaan siitä, että kun SaaS-järjestelmää tai SaaS-palvelua hankitaan, niin mulla varsinkin tai meidän porukalla on erityisenä intona katsoa, että miten se sopii tähän kokonaisarkkitehtuuriin mikä tällä alueella on, kun puhutaan liiketoiminnan kyvykkyyksistä prosesseista ja sitten niitä toteuttavista IT-järjestelmistä, niin miten tämä palanen istuu tähän ja mitä asioita pitää huomioida. Totta kai integraatiot on yksi tärkeä kulma, että okei, no miten standardilla, tavoilla sitä voi integroida. Yleensä halutaan, varsinkin kun ollaan tällä toimialalla, millä ollaan ja olemme vahvasti reguloitu, niin asiat täytyy tapahtua tietyllä tapaa ja sitten täytyy tiettyjä asioita huomioida. Ei ihan niin sanotusti voi ihan kaikkia tehdä, mitä tapoja on esimerkiksi integraatioiden suhteen, vaan täytyy olla aika hallittuja standardeja ja mekanismeja."	Järjestelmien integraatio aiheuttaa haasteita ja monimutkaisuutta	Järjestelmien integraatio
Tietoturva- ja tietosuojariskit	H5 - "Toinen näkökulma sitten tässä on se, että miten me saadaan omat tiedot takaisin, jos meillä tapahtuu jotain tai meillä tulee sopimuksellisesti haasteita tai me ei haluta jatkaa sitä käyttöä, niin miten me saadaan ne omat tietomme sieltä takaisin. Ikään kuin kotiutettua ja mahdollisesti vietyä uuteen järjestelmään. Niissä on tavallaan paljon enemmän riskejä kun siinä on-premisessä, joka on se perinteinen malli, koska silloinhan ne pörrää jossain meidän tai jonkun meidän infratoimittajan kellarissa ne pöntöt ja se tietohan on siellä."	Datan palauttaminen voi olla haasteellista	Datan ylläpito ja saavutettavuus
	H5 - "...kun ajatellaan sitä, että siellä on se jatkuvuus ja tiedon muuttumattomuus ja meillä se tiedon muuttumattomuus varsinkin on hyvin tarkkaa ja tärkeätä lääketeollisuudessa. Se on tavallaan semmoinen mikä SaaS-palveluissa on haaste, että aikaisemmin me ollaan pystytty on-premisessä hanskaamaan tämä muuttumattomuus sillä, että me otetaan tiettyjä backuppeja eli tavallaan meillä on tietty backup-frekvenssi ja tiettyjä backuppeja talletetaan ikään kuin ikuisesti, jolloin me pystytään aina palaamaan johonkin vanhaan kohtaan ja toteamaan että tämä tieto ei ole muuttunut siitä. Tai meillä on joku muu mekanismi kertakirjoitteisia levyjä tai muita. Sitten kun mennään sinne oikein ultimately hankaliin kohtiin. Mutta SaaS-palveluissa meillä ei tämmöistä vaihtoehtoa ole eikä mahdollisuutta. Eli meidän täytyy pystyä sitten luottamaan siihen SaaS-palveluun, että se on rakennettu oikein ja siellä on riittävät varmistukset tai synkronoinnoit eri konesaleihin ja niin edespäin."	Datan eheys voidaaan menettää	
	H1 - "voi olla ne vendoririskit, että jos se firma ei pysy pystyssä niin sitten taas että missä se meidän data on? Saadaanko se data turvaan, jos käy huonosti? Voiko se sijaita sellaisella alueella, että tulee alueellinen konflikti? Hoitaako ne backupit ja muut kuntoon"		
	H14 -" Otetaan tämä vaikka, että jos on joku EU-alue, onko paljon toimijoita, tulee geopoliittinen riski sitten, että onko tämä joku, vaikkapa, mikähän nyt on ollut pinnalla paljon, turha puhua tuonne itään päin, koska ne on kaikki pannassa, mutta otetaan vaikka joku sieltä välistä, joku Intia. Me tiedetään kaikki, että tosi paljon on "outsourcettu" Intiaan esimerkiksi sieltä tuotetaan paljon, tai no näinä päivinä varmaan Amerikkakin on vähän jännä, mutta nämähän on semmoisia riskejä kanssa, jotka huomioidaan."	Geopoliittiset tekijät ja tulevaisuuden epävarmuus aiheuttavat riskiä	Globaali toimintaympäristö
	H13 - "Tietenkin se, että se regulaatio muuttuu ja kaikkien pitäisi pysyä sitten kärryillä niistä muutoksista. Nyt jos puhutaan vaikka GDPR:stä, niin sekin muuttuu ja vaikka tästä EU AI actista. Se on itse asiassa hyvä esimerkki siitä, niin ne muuttuu ja kaikkien pitää pysyä kärryillä. Toinen on se myös, että tulkintoja on erilaisia. Eli jos ajatellaan, että me ollaan asiakas ja meillä on hyvin tiukka tulkinta ja sitten se emo-firma, jolta me ostetaan se itse platta, niin heillä voi olla tietynlainen tulkinta ja sitten heidän aliketjutus-vendoreillaan sovelluksien kehittäjällä voi olla aivan omalainen tulkinta. Se on se haaste siinä, että mikä tulkinta on oikea."	Lainsäädännöllisten velvoitteiden noudattaminen	
	H3 - "Jos aloittaa tuosta tietosuojan puolelta, vaikka ensin, niin siellä on yleensä se keskeinen kysymys, että missä ne datat on ja ketkä niihin datoihin pääsee käsiksi."		Tietosuoja-loukkaukset

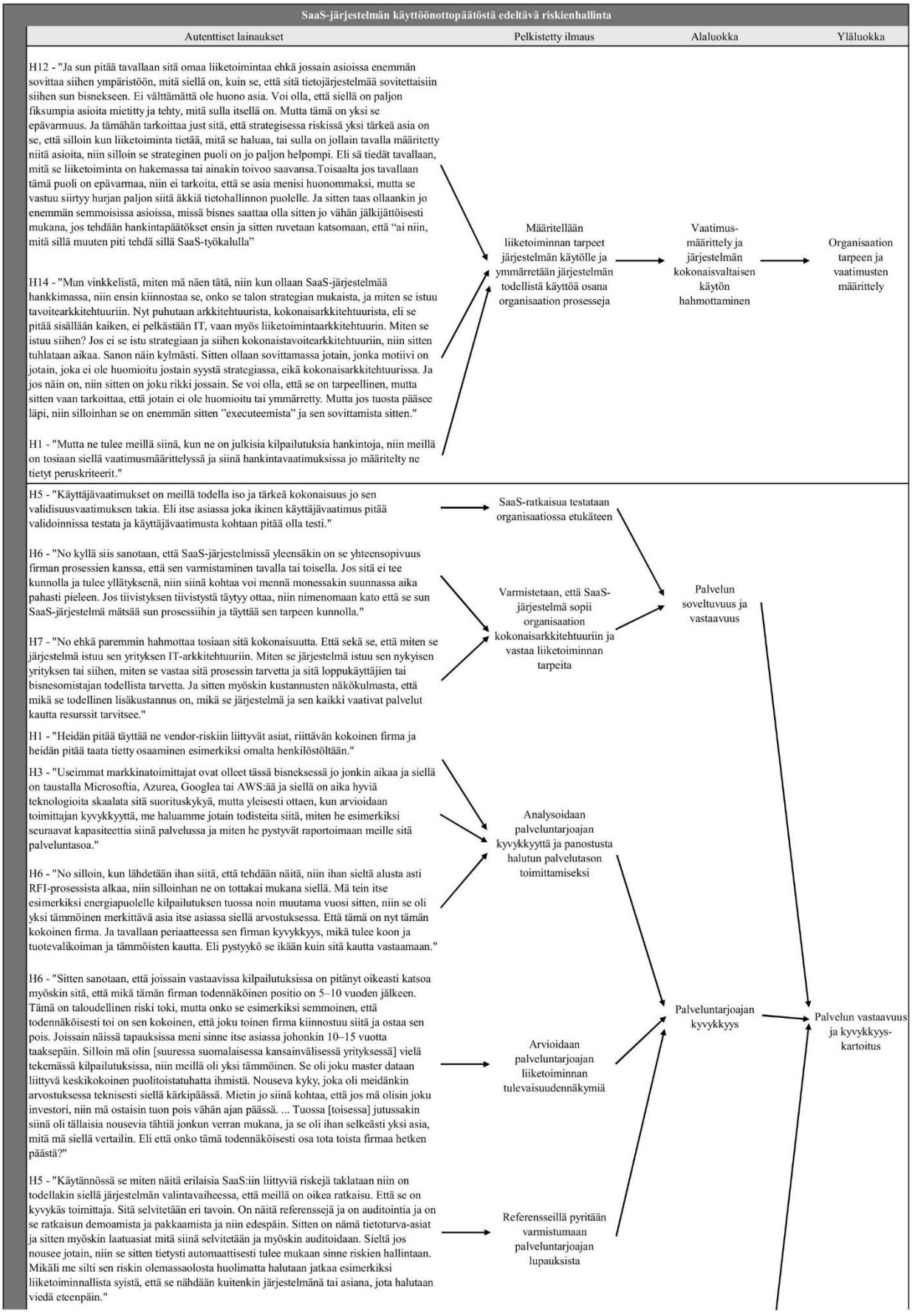

H10 - "Ja mä sanoisin, että identiteetinhallinta pitää olla keskitetty. Eli sehän pitää pystyä sitouttamaan sen yrityksen, ostavan yrityksen identiteetin hallintaan. Se on mun mielestä kaikki kriittisin. Eli mitä mä yritän sanoa, että jos te ostatte SaaS-palvelun, niin sinne ei jaeta staattisia tunnuksia jokaiselle, koska sen jälkeen se hallittavuus on täysin nolla. Eli se täytyy olla keskitetty. Että siinä vaiheessa, kun X lähtee talosta ulos ja me suljemme X:n tilin, niin kaikki SaaS-palvelut sammuu sille samalla hetkellä. ... koska sen jälkeen, kun X on todella katkera siitä, että hänet irtisanottiin ja sen jälkeen hän pääsee sinne edelleen ja sitten on maailma auki."
H4 - "Mut ne toimitusketjut on niin pitkiä. Tässäkään ei tavallaan niinku korkattu X:n järjestelmistä mitään. Vaan oli korkattu X:n palvelutuottajan järjestelmä, josta oli sitten saatu käyttäjätunnus ja salasana, millä oli päästy tunkeutumaan X:n järjestelmiin."
H12 - "Ja sitten jos ajatellaan tietoturvamielessä, niin taas uhka ja epävarmuus, niin sovellustasolla yksi suuri kysymys on se, että miten sitä sovellusta ylläpidetään, minkälaiseen teknologiaan se perustuu, miten sitä ylläpidetään. Jos siellä on tarkoitus tehdä erilaisia korjauksia tai muita, esimerkiksi tietoturvauhkien takia, niin miten tämä on hoidettu. Ja sitten ehkä alimpana on siis arkkitehtuurinen, niin kuin tavallaan tämä infrastruktuuri ja muu, niin siinä tullaan taas sitten siihen, että miten siellä on huolehdittu sitten tavallaan tämmöiset tekniset ylläpidot ja versiohallinnat. Ja tietysti se, että ei käytetä semmoisia versioita tai tekniikkaa, joka on vanhaa tai ennen kaikkea, että on haavoittuvaista."
H9 - "Datan vuotaminen: Ulkopuolinen voi päästä yrityksen tietoihin käsiksi, sillä tietoturvakäytännöt ovat SaaS-tarjoajan vastuulla eikä omissa käsissä. Käyttäjiä voi olla paljon ja palvelu näkyvissä monille yrityksille. Yksittäisen yrityksen tiedot eivät ole yhtä houkuttelevia kuin ympäristöt, joissa on enemmän tietoja varastettavaksi tai väärinkäytettäväksi."
Kenellä kaikilla on pääsy dataan ja miten käyttöä hallitaan
Toimitusketjun pituudesta johtuen asiakkaan kyberturvallisuudesta huolehtiminen on myös palveluntarjoajan käsissä
Tietovuoto
Strategiset riskit
H6 - "Ne keskeisimmät strategiset riskit ovat nimenomaan siinä, että miten varmistetaan, että se SaaS-palvelu tukee liiketoiminnan muutoksia, joita tulee tulevaisuudessa koko ajan. Jos mä katson nyt tästä 10 vuotta taaksepäin niin me ollaan heitetty voltti muutaman kerran vuodessa. Toisinaan on vaikutuksia näihin keskeisiin liiketoimintajärjestelmiin toisinaan ei, eli jos keskeisen liiketoimintajärjestelmän heittää SaaS:iin niin se riski on tietyssä mielessä, että sun kyvykkyys reagoida muutoksiin heikkenee."
H12 - "SaaS-palvelun luonne-ero tavallaan tämmöiseen, voisiko sanoa dedikoituun omaan sovellukseen tai järjestelmään. Siinä on tavallaan se riski tai epävarmuus tulee siinä, että ollaanko valmiita, koska tämähän on se liiketoiminnan kyky enemmän ehkä kuin tietohallinnon. Kyllähän tietohallinto varmaan SaaS-palvelun kanssa vielä pystyy elämään, vaikka vähän huonommankin kanssa, mutta jos se ei tue tai auta liiketoiminnan kehitystä. Jos se SaaS kehittyy hitaammin kuin se, mitä liiketoiminta halusi sen kehittyvään, niin sehän tulee jarruksi tai hidasteeksi. Eli tavallaan tämmöinen bisneksen, ei nyt hidastuminen, mutta tavallaan sen ketteryyden saaminen, niin voi olla, että se menetetään siinä, kun ollaankin tavallaan keskitetyn SaaS-palvelun piirissä."
H4 - "Onko jotain riskejä joidenkin asiakkaiden kanssa materialisoitunut ja pitääkö itse reagoida niihin jotenkin. Koska niissä aina sitten joudutaan pohtimaan vaihtokustannuksia. Jos ajat jotain isoa ERPiä SaaSina ja sit sanotaan, että alkaisi osoittautua, että se ei kehity tai tota se alkaa degeneroituu, niin sitten sun vaihtoehdot on aloittaa jonkun toisen SaaS-järjestelmän käyttöönottoprojekti."
H7 - "Ehkä se suurin semmoinen riski on aina se, että se järjestelmä pureutuu johonkin tiettyyn bisnesprosessiin. Ja sitten jos se bisnesprosessi ja se järjestelmän logiikkaa ei kohtaa, niin siinä meillä tulee niitä haasteita. Ja sitten siinä on aina tämä munakana-tilanne, että pitäisikö mennä niin, että järjestelmän standardisetuppi on joku, ja sitten muokataan prosessia sen mukaan, vai olisiko meillä pitänyt olla prosessialusta, joka sitten muodostaa sen, tai koetetaan mahdollisimman paljon mukailla sitten siellä järjestelmämaailmassa. Ja tuntuu, että tämä on aina se kohta, missä se suurin "clash" syntyy"
H8 - "Tämä toiminnan muutos on se mikä pitää ottaa huomioon siinä käyttöönottopäätöksessä, että se pitää ymmärtää, että mitkä ovat nyt toiminnan ydinprosessit ja miten ne menevät sitten sen uuden järjestelmän kanssa. Jos se toiminnan muutos on niin suuri, että me emme kykene sitä viemään läpi, niin sehän on selkeä asia mikä pitäisi tämän käyttöönoton yhteydessä tunnistaa ja sen varmasti pitäisi vaikuttaa siihen käyttöönottopäätökseen. Jos vaihtoehtona on kaksi järjestelmää josta toinen on sellainen, että toiminnan luonne tai toiminta ei muutu niin paljon nykyiseen verrattuna tai vaihtoehtoisesti että syntyy merkittävä muutos toiminnalle, että työnteko, vaikka työnjako ammattilaisten välillä tai se järjestys, jossa asioita tehdään, muuttuu merkittävästi tai jos se vaarantuu se prosessi ja se toiminnan jatkuvuus kärsii siitä, niin kyllähän tommoiset asiat pitäisi tunnistaa siinä käyttöönottopäätöksenteossa."
H14 - "Kyllähän sen täytyy olla, että jos puhutaan strategisesta tasosta, niin kuin SaaS, jos oletetaan, että se SaaS-ulkoistus tai se SaaS-hankinta on strategisesti merkittävä. Silloin se toimittaja on myös hyvin tärkeä strategisesti, että pitäisi puhua varmaan jo kumppanista siinä kohdassa, eikä pelkästään toimittajasta. Silloinhan se [strategia] täytyy olla kyllä "aligned". Sitten pitää kyllä puhua pitkästä, jos ei ole avioliitosta, niin jonkinlaisesta kumppanuudesta siinä mielessä."
H12 - "Olenpa senkin nähnyt, että on tehty joskus tavallaan iso muutos siinä, että yksi vähittäiskauppa totesi, että se haluaa irti Amazonin palvelusta, kun Amazon ilmoitti, että niillä on tulossa Suomessa vähittäiskauppoja Pohjoismaihin. Niin tämmöisiäkin strategisia kuvioita. Että SaaS-toimittaja tuleekin sun bisnesalueelle. ... ne [strategiset tavoitteet] voi olla samanlaisia, että se alkaakin tulla sun bisnesalueelle ja sitten sehän on vähän hupaisaa. Se on vähän sama kuin voisi ajatella näin, että Silmäasema käyttäisi Nissenin tietojärjestelmiä. Eiks se kuulosta vähän erikoiselle."
H6 - "Todennäköisesti siinä on yksi organisaatio, joka hoitaa sen käyttöönoton siellä, niin kuin tavallaan projektipuoli. Niin jos on niin, että joku konsulttifirma tulee sen tekemään, niin he hoitaa sen käyttöönottoprojektin. Sitten tekee handoverin usein saman firman jollekin tämmöiselle ongoing services pumpulle. Ja niin tota silloin tavallaan me ollaan naimisissa sen kyseisen firman kanssa, toki myöskin sen SaaS-palvelun. Mutta siinä on niin kuin useampiä kehyksiä. ... Mutta nimenomaan se tavallaan kuka ylläpitää sitä palvelua sille firmalle ja tukee sitä firman varsinaista businesta, niin se on ehkä se isoin riskikohta."
Liiketoiminnan kyvykkyys reagoida muutoksiin ja muokata omaa toimintaa heikkenee
Järjestelmän kyvykkyydet eivät ole riittäviä tulevaisuudessa
Liiketoiminnan ketteryys ja kehitys
Liiketoiminnan sovittaminen SaaS-järjestelmäympäristöön aiheuttaa ongelmia
Asiakas ja palveluntarjoaja pyrkivät toimimaan omien intressiensä mukaisesti
Strateginen dissonanssi
Asiakas ajautuu toiminnassaan toimittajaloukkuun palveluntarjoajan kanssa
Strateginen toimittajaloukku

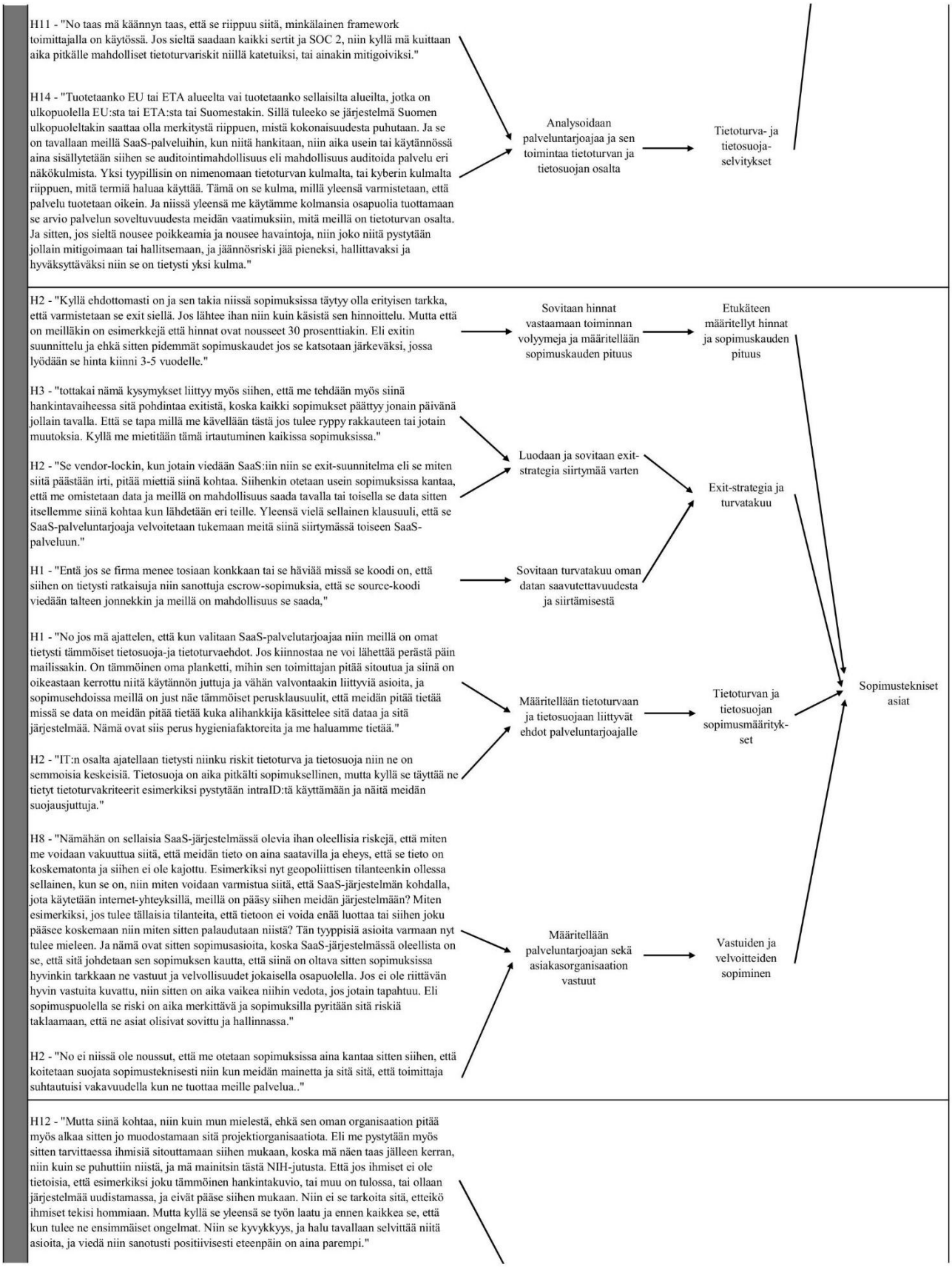

H9 - "Oma osaaminen menetetään. Kun siirrytään SaaS palveluun, omaa osaamista ei enää vastaavasti tarvita. Näin ollen mahdollinen paluu takaisin, on erittäin hankalaa eikä aitoa vertailua enää pystytä tekemään eri vaihtoehdoista."
Menetään oman organisaation osaamista SaaS-järjestelmään siirryttäessä
Osaamisen menettäminen
H9 - "Liiketoiminta voi häiriintyä mikäli palveluntarjoajalla on ongelmia tai vaikka huoltokatkoja Mainehaitta voi olla välitön mikäli ongelmat näkyvät arvoketjussa muille osapuolille" - "miten aiotaan varmistaa liiketoiminnan jatkuvuus ongelmatilanteissa sekä siinä että asiakkaan oma henkilö tekee merkittävän virheen. Mikäli palveluntarjoajalla ei ole näihin ratkaisuja, ei niitä synny projektinkaan aikana"
H12 - "mehän voidaan tietohallinnossa esimerkiksi mennä arvaamaan, mikä liiketoiminnan mielestä on kriittistä. Mutta kyllähän sen liiketoiminnan pitää pystyä itsekin sanomaan, että voiko tämä SaaS-palvelu olla pois käytöstä esimerkiksi päivän, taikka viikon, vai onko se niin, että tuntikin on jo liian pitkä aika. Ja tähän tietoturvamielessä jatkuvuuteenhan sitten tullaan siihen, että jos me saadaan se viesti, että puoli päivää tai neljä tuntia on pisin aika, kun se voi olla alhaalla, niin sittenhän meidän täytyy alkaa miettimään, tämä liittyy siihen hankintapäätökseenkin tai käyttöönottopäätökseen, että no millä tavalla me varmistetaan, että SaaS-järjestelmä on käytettävissä. Elikkä mitkä on meidän varajärjestelmät. Että mennäänkö varajärjestelmään niin, että jos tämä ei ole käytössä, niin sitten otetaan kynä ja paperi. Sillä pitää sitten hoitaa. Tai sitten se, että me haetaan siihen sitten vaikka muita tietoliikenneratkaisuja taustalle, siis varajärjestelmiä. Tai sitten täytyy selvittää, että onko sillä SaaS-toimittajalla riittävät kyvyt huolehtia siitä, että se ei ole pidempää kuin se neljä tuntia alhaalla."
SaaS-järjestelmän käytettävyys menetetään
Liiketoiminnan jatkuvuus
H12 - "Yksi on se, että onko se liian pieni vai voiko se olla liian iso. Ja tällä tarkoitan sitä, että jos se on liian iso, niin esimerkiksi tietyissä asioissa, jos tarvitaan apua tai tukea, niin se voi olla taas, että oma bisnes on niin pientä, että se ei tämmöistä isoa toimittajaa oikeasti kiinnosta. Se pistää suurin piirtein vaan sähköpostitukee ja se ei välttämättä taas auta. Liian pieni toimija, niin kuin tiedätte, niin se riski voi olla jopa se, että se IT-toimittaja tai SaaS-toimittaja ei pysy hengissä, jolloin se tavallaan se kumppanuus häviää tämmöisen kautta."
H4 - "Tietysti jos niinku tietoturvan ja kapasiteetin ehkä muidenkin asioiden näkövinkkelistä, niin sit on tietysti se SaaS-palvelutuottajan liiketoiminnan jatkuvuus. Miten siihen varaudutaan, että jos se yritys, joka sitä SaaS-palvelua tuottaa, niin jos liiketoiminta lähtee alamäkeen ja siellä on vähemmän asiantuntijoita paikalla, ne yrittää niinku olla kustannustehokkaita, että minkälaisia muutoksia siellä tulee. Että onko se niinku SaaS-palvelun tuottajana uskottava ja luotettava siihen, että ne nyt pystyy tuottamaan seuraavat 15-20 vuotta sitä palvelua niin, että se kehittyy jatkuvasti. Että siitä tuu semmonen dead endi, että tota, että jäätiin 2010-luvulle."
Palveluntarjoajan toiminnan laajuus ja tulevaisuusnäkymät vaikuttavat asiakasorganisaation saamaan palvelutasoon
Taloudelliset riskit
H14 - "Ehkä mä nostan holistisemmin, niin totta kai se bisneskeissi. Kaikistahan rakennetaan bisneskeissi, että miltä se näyttää, että koska tämä maksaa itsensä takaisin, millä aikajänteellä. Aika useinhan kyse on siitä, että liiketoiminnassa tehdään päätöksiä, niin siinähän haetaan aina viivan alle jotain. Niin kuinka hyvä se bisneskeissi on, ja kuinka tavallaan uskottava se on, ja tuleeko se toteutumaan, onko siinä riskiä siinä eri vaiheissa, sen käyttöönoton tai sen SaaS-palvelun hyödyntämisen osalta. Mä näkisin, että se bisneskeissin pitävyys on ehkä se taloudellisesta kulmasta se riski, jota seurataan."
Saas-järjestelmästä ei välttämättä saada riittävästi hyötyjä suhteessa kustannuksiin
Hyötyjen realisointi
H4 - "Että kyllä tota, mä oon nähnyt paljon semmosia projekteja, mitkä on toteutettu ajallaan ja budjetissa ja toteuttanut niille asetetut laatukriteerit. Mutta kuitenkaan ei oo sit tuottanut sitä, mitä niiden piti. Eli periaatteessa joku asia on jäänyt huomioimatta. Itekin tehnyt pari sellaista."
H12 -"Asiakkaat katsoi sitä hankintahintaa, mutta ei oikeasti katsonut, että mitä se maksaa, kun sulla on se käytössä. Se on vähän sama, kun joku hankkii vaikka veneen ja toteaa, että no eihän tämä maksanut kuin 50 tonnia. Mutta sitten niin kuin voin sanoa, itse olen omistanut joskus tommoisen ehkä vähän kalliimman kuin tuon veneen, niin voin sanoa, että helkkaristi sitä rahaa meni sitten sen saakelin vehkeen ylläpitoon, enkä puhu pelkästään polttoaineesta. Ja tämä on tavallaan sitten se, mikä mun mielestä on yksi tärkeä asia myös. Että hankintapäätöksessä yksi haaste on se, että jos ei tunnisteta mitkä on sen järjestämän jatkuvat palvelut, eli tavallaan puhun siitä tuotantovaiheesta. Niin se voi olla, että sieltä syntyy suuria kustannuseriä ja sitä kautta taloudellisista haastetta, vähintään epävarmuutta. Ehkä jos oikeasti ruvetaan laskemaan, niin voidaan alkaa huomaamaan, että siihen liittyy aika kalliita asioita, vaikka sen jatkuvuuden tai muun varmistamiseksi."
H4 - "Vaikka se oli SaaS-palvelu, ja periaatteessa maksettiin kulutuksen mukaan, niin siinä oli todella vaikea hahmottaa sitä, kun se oli A4 mittainen se hintalista, että tällaiset tapahtumat maksaa per kappale tämän verran, ja tollaset maksaa tuhat kappaletta tuon verran. Sitten kun ei ole kokemusta semmoisen nimenomaan samanlaisesta järjestelmästä, niin sitten on etukäteen tosi vaikea arvioida, että mitkä ne määrät tulee olemaan. Periaatteessa vastaus tässä voisi olla, että velvoittaa toimittajan kysymään kaikki ne kysymykset, joiden perusteella toimittaja voi antaa sitovan kustannusarvion, että mitä ne käyttökustannukset sitten tulee olemaan. Mutta sitten kun toimitaan jonkun SAPin kanssa, joka on maailman suurin ERP-toimittaja, niin kyllä ne sen vastuun osaa siirtää asiakkaalle. Että siinä on tietysti semmoinen, että voi tulla. Siinä tulee tosi huolellinen, kun laatii arviota siitä, että mitä se tulee kustantamaan. Jonkun verran siinä heittoa tulee, että siinä on yksi taloudellinen riski."
SaaS-järjestelmän kulurakenteen kompleksisuus johtaa odotettua suurempiin kustannuksiin
Piilotetut kustannuket
H8 - "Riippuu vähän tapauksesta, mutta voi olla aika isoja koulutustarpeita, joita jos ei ole osattu ottaa huomioon. Uusien järjestelmien käyttöönottoon liittyy aina yleensä migraatioita vanhoista järjestelmistä ja siellä voi olla aika isoja ja haastaviakin tekemisiä, joita ei välttämättä osata ottaa huomioon, jolloin se taloudellinen puoli voi tulla sielläkin aika mittavaksi, kun joudutaan tekemään erilaista konversiota ja migraatiota, että saadaan tiedot mukaan vanhoista järjestelmistä. Tämän tyyppisiä, että monessa kohdissa voi olla vaikea arvioida etukäteen, että se vaatii aika tarkkaa määrittelyä."
Muutoskustannukset järjestelmästä toiseen ovat suuret
H9 - "Lisenssien tai käyttöoikeuksien korotukset, sillä järjestelmien vaihtaminen voi olla todella suuri investointi. Mikäli sopimuksellisesti ei hintoja lyödä lukkoon riittävän pitkäksi aikaa, on jopa todennäköistä että hinnat nousevat merkittävästi."
H1 - "Toki siinä voi olla sitten vendor-lock-in tyyppisiä asioita, että ollaan jumissa jonkun ison toimittajan kanssa ja vaikea irtautua ja sitten hinnannousut karkaa käsistä"
H2 - "No kyllä aika merkittäviäkin taloudellisia riskejä siinä mielessä, että nyt ollaan jo nähty se, että hinnat on pompannut ihan merkittävästi siitä mitä ne olivat alunperin. Kun saadaan tavallaan tuntumaan siltä asiakkaalta, että nyt ollaan vendor-lock in tilanteessa, niin sitten nostetaan helposti hintoja ja taloudellinen riski on aika merkittävä siinä tapauksessa."
Palveluntarjoaja nostaa hintoja tulevaisuudessa ja irtautuminen on hankalaa
Taloudellinen toimittajaloukku

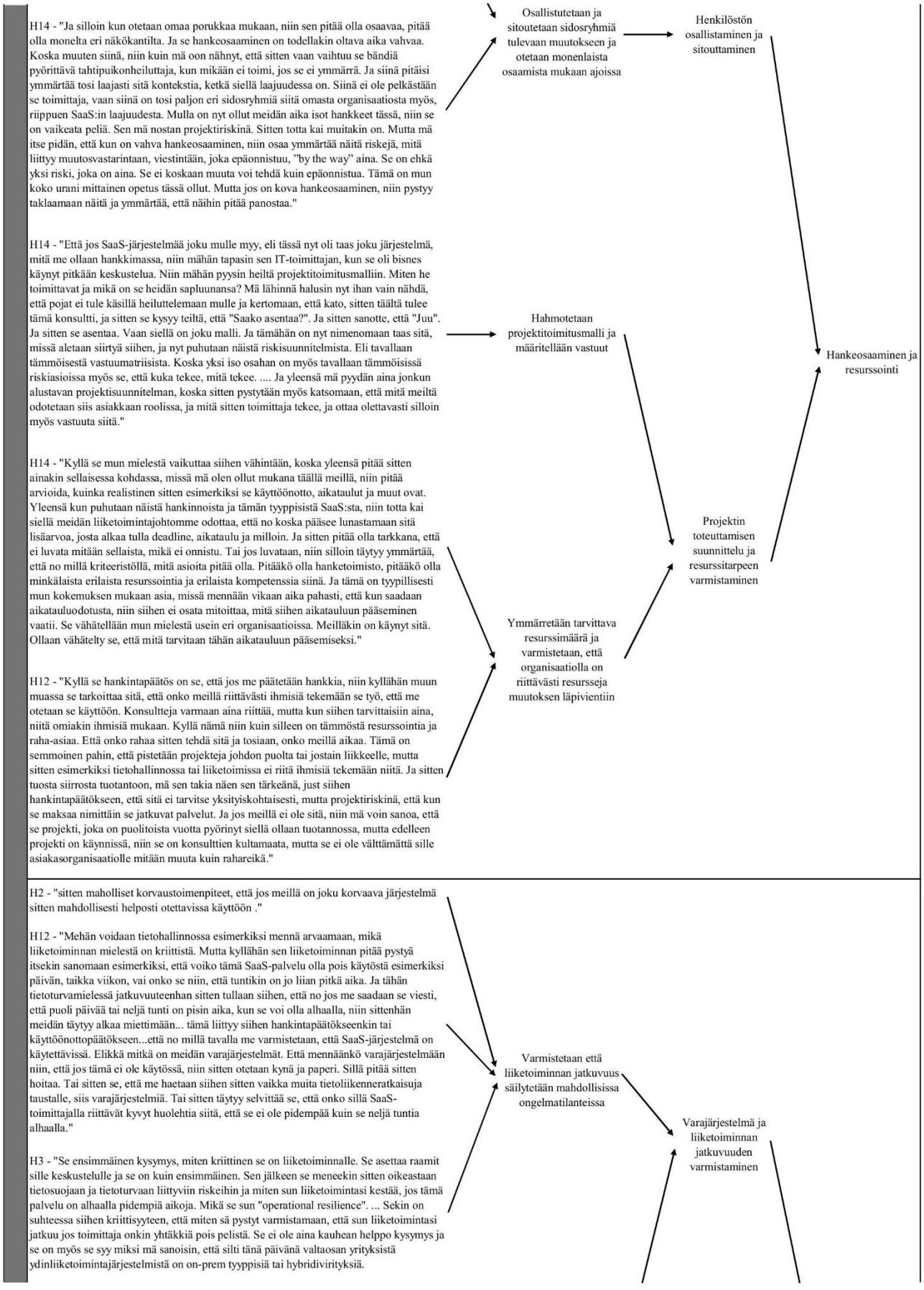

Psykosiaaliset Riskit
H4 - "SaaS-palvelua käyttöön otettaessa ja hankintapäätöstä tehtäessä pitää sitoutua siihen, että se otetaan sellaisena käyttöön, kuin mitä se oli suunniteltu. Ja tässä tietysti sitten tosi usein tulee sellainen intressien törmäys. Ja sitten se moninkertaistuu. Itse asiassa tämä ongelma moninkertaistuu siinä, kun erityisesti laajoissa järjestelmissä hyvin harva tuntee sitä koko järjestelmätoiminnallisuuskenttää niin, että osaisi hahmottaa, että jos minä tähän kohtaan toivon jotain muutosta, niin miten se vaikuttaa johonkin muualle. Ja nämä kaksi asiaa on sellaisia, että yritetään sopeuttaa sitä SaaS-järjestelmää omaan vanhaan totuttuun toimintatapaan. Ja sitä kautta pyritään rikkomaan sen järjestelmäeheys, tai sitten kun pitäisi ajatella, että miten meidän pitäisi muuttaa tätä meidän toimintaa niin, että tämä valittu järjestelmä tukisi sitä mahdollisimman hyvin. Ja tämä on semmoinen, että aiheuttaa psykologista kuormitusta, eli muutosvastarintaa. Ja sitten tietysti aihe voi huonoimmillaan aiheuttaa myös tämmöisen sosiaalisessa kanssakäymisessäkin ongelmia, koska ihmiset valitsee leirinsä. Toiset on sitten mieltä, että nyt toimitaan niin kuin SaaS-toimittaja sanoo, ja toiset on sitten mieltä, että eikä toimita, kun me tunnetaan meidän business paremmin. Jotka molemmat on oikeassa. Se siinä vaikeaa onkin."
"H6 - "Aika usein, kun otetaan tämmöistä enterprise-SaaSia käyttöön, niin se mistä lähdetään sen käyttöön on, että on ollut jotain ehkä paikallisia järjestelmiä tai muita. Niin totta kai aina muutos, kun sulla on paikka A siirryt paikkaan B, niin muutos on aina semmoinen, että siihen suhtaudutaan negatiivisesti. Mutta sitten se fiilis, että sulla on ollut jotain ihan omaa täällä, mikä on just spesialisesti meille. Ja sitten tulee joku tämmöinen globaali yleinen juttu, niin siihen liittyy sitten aika isot tämmöiset muutoshallinnalliset riskit. Eli jos ei sitä huomioi sitten jo siinä vaiheessa, kun ruvetaan valmistelemaan tätä muutosta, ja siis todellakin jo siinä vaiheessa. Niin sitten se itse muutos voi joko kariutua kokonaan, tai sitten ainakin hidastua hyvin paljon, joka sitten näkyy viime kädessä rahassa."
H12 - "Mutta jos sinne tulee niitä ongelmia, niin yleensä aina tämmöiset vastarinnankiisket tai ne NIH-tyyppiset "Not Invented Here"-ihmiset, niin alkaa sitten sanomaan, että "minähän sanoin". Mutta ehkä jos siihen hankintapäätökseen, niin taas jälleen kerran, mitä ja miksi. Jos niihin asioihin pystytään ottaa kantaa, kuvaamaan niitä konkreettisemmallakin tasolla, kun vaan se, että kun johto haluaa. Niin se auttaa hurjasti siihen asiaan ja ennen kaikkea siihen viestintään. Ja toinen asia on kääntäen nämä mitä ja miksi sen tyyppisiksi asioiksi, että mitä hyötyjä tulee. Koska jos ei pysty hyödystä kertomaan tai konkretisoimaan, ja tässähän palataan siihen edelliseenkin asiaakin esimerkiksi, että mitä taloudellisesti tästä hyötyy. Tai toinen asia on se, että mitkä asiat helpottuu, ei sun tarvitse tehdä enää. Parhaimmillaan se on sitä ATK:ta, eikö niin, automaattisesti tietojen käsittelyä."
H11 - "Mun puolelta mä tunnistan kyllä tuon "change resistance", joka on yksi, koska kyllähän se tietyssä mielessä, että sä vähennät sitä oman hallinnan mahdollisuutta, kun se siirtyy on-premista pilveen, joka voidaan kokea uhkana tai riskinä tässä tapauksessa."
H14 - "Yksi tyypillinen voi olla se, että jos talo on tuottanut ja tehnyt palvelua A, jossa on ollut vahva oman henkilökunnan panos, ja sitten sä muutat sen SaaS-palveluksi, missä se sama tekeminen siirtyy sitten pois, niin sittenhän tulee tätä perinteistä muutosvastarintaa, pelkoa esimerkiksi oman työpaikan tai tekemien tehtävien jatkuvuudesta tai pelkästään siitä, että ehkä ei haluta vaan muuttaa sitä, mitä on tehty. ...Siitä voi tulla vaikka että sitten meiltä sitä hyvää osaamista katoaa, kun ne ei halua esimerkiksi hyväksyä sitä muutosta, että mitä tein nyt vaikka viimeiset kaksi vuotta, niin en saakkaan tehdä sitä, niin haluan sitten mennä muualle, missä voin tehdä sitä."
Henkilöstö kokee tyytymättömyyttä järjestelmän tuomaan muutokseen
Muutosvastarinta
Projektiriskit
H8 - "Se monimutkaisuus monesti tulee siitä, että taloudelliset ja resurssiasiat ja projektin laajuus yllättää. Monesti on niin, että se työmäärä mikä sitten oikeasti vaaditaan sen käyttöönottoon, onkin moninkertainen, vaikka siihen mitä on osattu arvioida ja sitten siinä ylittyy sen takia jokin aikataulu tai sitten tämä budjetti, että näin minä itse ajattelen sitä. Tietenkin tämä monimutkaisuus voi olla juuri tuota [resurssi]-kolmion kärkien etäisyyttä toisistaan, että mikä niissä nyt sitten on se mikä joustaa ja mikä ei jousta."
H10 - "Niin kuinka kauan tämä siirtymä esimerkiksi kestää? Mulla on itseasiassa nyt semmonen projekti menossa, missä mä oon siirtymässä palvelusta toiseen. Ja se tavallaan se siirtymä kestää aivan luokattomaan paljon. Ja se on ihan täysin tavallaan, no en mä olisi voinut ikinä kuvitellakaan, että se kestää niin kauan, mutta se on myös tavallaan mun osaamattomuuttani, koska mä en osannut sitä ottaa huomioon riskinä. Se kestää näin paljon, että kaikki eskaloi ja ynnä muuta, mutta että se vaan kestää ihan tajuttoman kauan, että se olisi pitänyt ilman muuta nostaa silloin jo alun perin, kun tätä neuvoteltiin, että kuinka kauan tämä siirtymä kestää."
H12 - "Kyllä se hankintapäätös on se, että jos me päätetään hankkia, niin kyllähän muun muassa se tarkoittaa sitä, että onko meillä riittävästi ihmisiä tekemään se työ, että me otetaan se käyttöön. Konsultteja varmaan aina riittää, mutta kun siihen tarvittaisiin aina, niitä omiakin ihmisiä mukaan. Kyllä nämä niin kuin silleen on tämmöstä resurssointia ja raha-asiaa"
H14 - "Pitää arvioida, kuinka realistinen sitten esimerkiksi se käyttöönotto, aikataulut ja muut ovat. Yleensä kun puhutaan näistä hankinnoista ja tämän tyyppisistä SaaS:sta, niin totta kai siellä meidän liiketoimintajohtomme odottaa, että no koska pääsee lunastamaan sitä lisäarvoa, josta alkaa tulla deadline, aikataulu ja milloin. Ja sitten pitää olla tarkkana, että ei luvata mitään sellaista, mikä ei onnistu. Tai jos luvataan, niin silloin täytyy ymmärtää, että no millä kriteeristöllä, mitä asioita pitää olla. Pitääkö olla hanketoimisto, pitääkö olla minkälaista erilaista resurssointia ja erilaista kompetenssia siinä. Ja tämä on tyypillisesti mun kokemuksen mukaan asia, missä mennään vikaan aika pahasti, että kun saadaan aikatauluodotusta, niin siihen ei osata mitoittaa, mitä siihen aikatauluun pääseminen vaatii. Se vähätellään mun mielestä usein eri organisaatioissa. Meilläkin on käynyt sitä. Ollaan vähätelty se, että mitä tarvitaan tähän aikatauluun pääsemiseksi."
H4 - "Yksinkertaistetaan silleen, että siellä on kaksi joukkoa ihmisiä. Toinen on ne, jotka tuntevat sen järjestelmän. Sitten toinen on ne, jotka tuntevat sen busineksen. ... Sit ne alkaa yhdessä virkkaamaan siitä jotain toimivaa, että miten sen järjestelmän saisi tukemaan sitä businestä, ja miten se busines saataisiin sopeutumaan niihin järjestelmävaatimuksiin. Ja tähän menee aikaa. Tähän menee tosi paljon aikaa. Ja sitä ei välttämättä aina huomioida siinä, kun sitä projektia aloitetaan. Ja kyllä se, mikä on tosi surullista, on se, että kun sitä ei huomioida, että kuinka paljon siihen menee aikaa, että ruvetaan saamaan jotain aikaiseksi. Niin sitten projektin liikennevaloraportti, on ensimmäisestä kuukaudesta lähtien punaisella, koska ollaan heti jäljessä aikataulusta. Ja se sitten luo muuten aikamoisen kuormitustekijän projekti-ihmisille ja kaikille muillekin."
Muutosprojektin kompleksisuus saattaa yllättää ja se vie odotettua enemmän resursseja
Hankeosaamisen puute

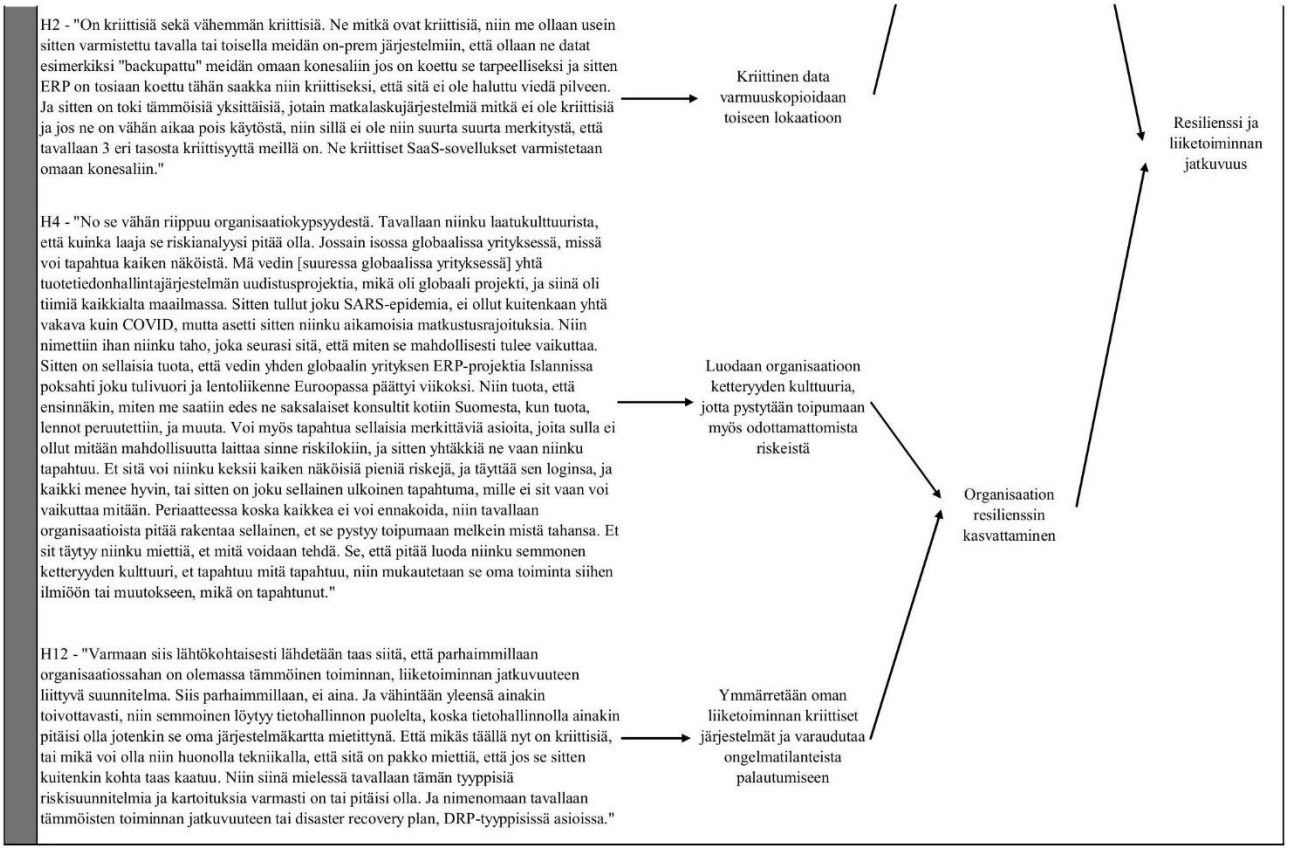
	H7 - "No kyllä me ainakin ollaan yritetty siinä vaiheessa, kun tehdään tavallaan se bisneskeissi, joka viedään sinne päätöksentekoon, niin siinä arvioidaan aina myöskin sitä projektin kustannusta ja kuormittavuutta. Toki se on yksi tekijä siinä valintaprosessissa, että jos me todetaan, että jollain on hyvin hioutunut se implementointiprosessi ja sieltä tulee valmiiksi annetut resurssit suurin piirtein kylkiäisenä, niin toki se on plussaa kuin se, että sä joudut itse ruveta haalimaan sitä kasaan tai että sulla on kallis partneri tai jotain vastaavaa." H2 - "Siinä on riskinä siis se, että sieltä löytyy meidän liiketoiminnalle joku erittäin tärkeä ominaisuus, jota siinä SaaS:ssa ei yhtäkkiä olekaan. Siinä joudutaan tekemään töitä, että kaikki meidän prosessit oikeasti uppoo siihen julkipilven ERP:iin, joka on hyvin standardi ja ominaisuuksiltaan rajallinen vanhaan verrattuna. Ehkä se on se keskeinen projektiriski, että ei olla riittävästi pystytty isossa hankinnassa selvittämään sitä, onko se oikeasti meille sopiva juuria myöten."	

Liite 3. Analyysitaulukko käyttöönottopäätöstä edeltävästä riskienhallinnasta




H11 - "No taas mä käännyn taas, että se riippuu siitä, minkälainen framework toimittajalla on käytössä. Jos sieltä saadaan kaikki sertit ja SOC 2, niin kyllä mä kuittaan aika pitkälle mahdolliset tietoturvariskit niillä katetuiksi, tai ainakin mitigoiviksi."
H14 - "Tuotetaanko EU tai ETA alueelta vai tuotetaanko sellaisilta alueilta, jotka on ulkopuolella EU:sta tai ETA:sta tai Suomestakin. Sillä tuleeko se järjestelmä Suomen ulkopuoleltakin saattaa olla merkitystä riippuen, mistä kokonaisuudesta puhutaan. Ja se on tavallaan meillä SaaS-palveluihin, kun niitä hankitaan, niin aika usein tai käytännössä aina sisällytetään siihen se auditointimahdollisuus eli mahdollisuus auditoida palvelu eri näkökulmista. Yksi tyypillisin on nimenomaan tietoturvan kulmalta, tai kyberin kulmalta riippuen, mitä termiä haluaa käyttää. Tämä on se kulma, millä yleensä varmistetaan, että palvelu tuotetaan oikein. Ja niissä yleensä me käytämme kolmansia osapuolia tuottamaan se arvio palvelun soveltuvuudesta meidän vaatimuksiin, mitä meillä on tietoturvan osalta. Ja sitten, jos sieltä nousee poikkeamia ja nousee havaintoja, niin joko niitä pystytään jollain mitigoimaan tai hallitsemaan, ja jäännösriski jää pieneksi, hallittavaksi ja hyväksyttäväksi niin se on tietysti yksi kulma."
Analysoidaan palveluntarjoajaa ja sen toimintaa tietoturvan ja tietosuojan osalta
Tietoturva- ja tietosuoja-selvitykset
H2 - "Kyllä ehdottomasti on ja sen takia niissä sopimuksissa täytyy olla erityisen tarkka, että varmistetaan se exit siellä. Jos lähtee ihan niin kuin käsistä sen hinnoittelu. Mutta että on meilläkin on esimerkkejä että hinnat ovat nousseet 30 prosenttiakin. Eli exitin suunnittelu ja ehkä sitten pidemmät sopimuskaudet jos se katsotaan järkeväksi, jossa lyödään se hinta kiinni 3-5 vuodelle."
Sovitaan hinnat vastaamaan toiminnan volyymeja ja määritellään sopimuskauden pituus
Etukäteen määritellyt hinnat ja sopimuskauden pituus
H3 - "tottakai nämä kysymykset liittyy myös siihen, että me tehdään myös siinä hankintavaiheessa sitä pohdintaa exitistä, koska kaikki sopimukset päättyy jonain päivänä jollain tavalla. Että se tapa millä me kävellään tästä jos tulee ryppy rakkauteen tai jotain muutoksia. Kyllä me mietitään tämä irtautuminen kaikissa sopimuksissa."
H2 - "Se vendor-lockin, kun jotain viedään SaaS:iin niin se exit-suunnitelma eli se miten siitä päästään irti, pitää miettiä siinä kohtaa. Siihenkin otetaan usein sopimuksissa kantaa, että me omistetaan data ja meillä on mahdollisuus saada tavalla tai toisella se data sitten itsellemme siinä kohtaa kun lähdetään eri teille. Yleensä vielä sellainen klausuuli, että se SaaS-palveluntarjoaja velvoitetaan tukemaan meitä siinä siirtymässä toiseen SaaS-palveluun."
Luodaan ja sovitaan exit-strategia siirtymää varten
Exit-strategia ja turvatakuu
H1 - "Entä jos se firma menee tosiaan konkkaan tai se häviää missä se koodi on, että siihen on tietysti ratkaisuja niin sanottuja escrow-sopimuksia, että se source-koodi viedään talteen jonnekkin ja meillä on mahdollisuus se saada,"
Sovitaan turvatakuu oman datan saavutettavuudesta ja siirtämisestä
H1 - "No jos mä ajattelen, että kun valitaan SaaS-palvelutarjoajaa niin meillä on omat tietysti tämmöiset tietosuoja-ja tietoturvaehdot. Jos kiinnostaa ne voi lähettää perästä päin mailissakin. On tämmöinen oma planketti, mihin sen toimittajan pitää sitoutua ja siinä on oikeastaan kerrottu niitä käytännön juttuja ja vähän valvontaakin liittyviä asioita, ja sopimusehdoissa meillä on just näe tämmöiset perusklausuulit, että meidän pitää tietää missä se data on meidän pitää tietää kuka alihankkija käsittelee sitä dataa ja sitä järjestelmää. Nämä ovat siis perus hygieniafaktoreita ja me haluamme tietää."
H2 - "IT:n osalta ajatellaan tietysti niinku riskit tietoturva ja tietosuoja niin ne on semmoisia keskeisiä. Tietosuoja on aika pitkälti sopimuksellinen, mutta kyllä se täyttää ne tietyt tietoturvakriteerit esimerkiksi pystytään intraID:tä käyttämään ja näitä meidän suojausjuttuja."
Määritellään tietoturvaan ja tietosuojaan liittyvät ehdot palveluntarjoajalle
Tietoturvan ja tietosuojan sopimusmäärityk-set
H8 - "Nämähän on sellaisia SaaS-järjestelmässä olevia ihan oleellisia riskejä, että miten me voidaan vakuuttua siitä, että meidän tieto on aina saatavilla ja eheys, että se tieto on koskematonta ja siihen ei ole kajottu. Esimerkiksi nyt geopoliittisen tilanteenkin ollessa sellainen, kun se on, niin miten voidaan varmistua siitä, että SaaS-järjestelmän kohdalla, jota käytetään internet-yhteyksillä, meillä on pääsy siihen meidän järjestelmään? Miten esimerkiksi, jos tulee tällaisia tilanteita, että tietoon ei voida enää luottaa tai siihen joku pääsee koskemaan niin miten sitten palaudutaan niistä? Tän tyyppisiä asioita varmaan nyt tulee mieleen. Ja nämä ovat sitten sopimusasioita, koska SaaS-järjestelmässä oleellista on se, että sitä johdetaan sen sopimuksen kautta, että siinä on oltava sitten sopimuksissa hyvinkin tarkkaan ne vastuut ja velvollisuudet jokaisella osapuolella. Jos ei ole riittävän hyvin vastuita kuvattu, niin sitten on aika vaikea niihin vedota, jos jotain tapahtuu. Eli sopimuspuolella se riski on aika merkittävä ja sopimuksilla pyritään sitä riskiä taklaamaan, että ne asiat olisivat sovittu ja hallinnassa."
H2 - "No ei niissä ole noussut, että me otetaan sopimuksissa aina kantaa sitten siihen, että koitetaan suojata sopimusteknisesti niin kun meidän mainetta ja sitä sitä, että toimittaja suhtautuisi vakavuudella kun ne tuottaa meille palvelua.."
Määritellään palveluntarjoajan sekä asiakasorganisaation vastuut
Vastuiden ja velvoitteiden sopiminen
Sopimustekniset asiat
H12 - "Mutta siinä kohtaa, niin kuin mun mielestä, ehkä sen oman organisaation pitää myös alkaa sitten jo muodostamaan sitä projektiorganisaatiota. Eli me pystytään myös sitten tarvittaessa ihmisiä sitouttamaan siihen mukaan, koska mä näen taas jälleen kerran, niin kuin se puhuttiin niistä, ja mä mainitsin tästä NIH-jutusta. Että jos ihmiset ei ole tietoisia, että esimerkiksi joku tämmöinen hankintakuvio, tai muu on tulossa, tai ollaan järjestelmää uudistamassa, ja eivät pääse siihen mukaan. Niin ei se tarkoita sitä, etteikö ihmiset tekisi hommiaan. Mutta kyllä se yleensä se työn laatu ja ennen kaikkea se, että kun tulee ne ensimmäiset ongelmat. Niin se kyvykkyys, ja halu tavallaan selvittää niitä asioita, ja viedä niin sanotusti positiivisesti eteenpäin on aina parempi."


H14 - "Ja silloin kun otetaan omaa porukkaa mukaan, niin sen pitää olla osaavaa, pitää olla monelta eri näkökantilta. Ja se hankeosaaminen on todellakin oltava aika vahvaa. Koska muuten siinä, niin kuin mä oon nähnyt, että sitten vaan vaihtuu se bändiä pyörittävä tahtipuikonheiluttaja, kun mikään ei toimi, jos se ei ymmärrä. Ja siinä pitäisi ymmärtää tosi laajasti sitä kontekstia, ketkä siellä laajuudessa on. Siinä ei ole pelkästään se toimittaja, vaan siinä on tosi paljon eri sidosryhmiä siitä omasta organisaatiosta myös, riippuen SaaS:in laajuudesta. Mulla on nyt ollut meidän aika isot hankkeet tässä, niin se on vaikeata peliä. Sen mä nostan projektiriskinä. Sitten totta kai muitakin on. Mutta mä itse pidän, että kun on vahva hankeosaaminen, niin osaa ymmärtää näitä riskejä, mitä liittyy muutosvastarintaan, viestintään, joka epäonnistuu, "by the way" aina. Se on ehkä yksi riski, joka on aina. Se ei koskaan muuta voi tehdä kuin epäonnistua. Tämä on mun koko urani mittainen opetus tässä ollut. Mutta jos on kova hankeosaaminen, niin pystyy taklaamaan näitä ja ymmärtää, että näihin pitää panostaa."
Osallistutetaan ja sitoutetaan sidosryhmiä tulevaan muutokseen ja otetaan monenlaista osaamista mukaan ajoissa
Henkilöstön osallistaminen ja sitouttaminen
H14 - "Että jos SaaS-järjestelmää joku mulle myy, eli tässä nyt oli taas joku järjestelmä, mitä me ollaan hankkimassa, niin mähän tapasin sen IT-toimittajan, kun se oli bisnes käynyt pitkään keskustelua. Niin mähän pyysin heiltä projektitoimitusmalliin. Miten he toimittavat ja mikä on se heidän sapluunansa? Mä lähinnä halusin nyt ihan vain nähdä, että pojat ei tule käsillä heiluttelemaan mulle ja kertomaan, että kato, sitten täältä tulee tämä konsultti, ja sitten se kysyy teiltä, että "Saako asentaa?". Ja sitten sanotte, että "Juu". Ja sitten se asentaa. Vaan siellä on joku malli. Ja tämähän on nyt nimenomaan taas sitä, missä aletaan siirtyä siihen, ja nyt puhutaan näistä riskisuunnitelmista. Eli tavallaan tämmöisestä vastuumatriisista. Koska yksi iso osahan on myös tavallaan tämmöisissä riskiasioissa myös se, että kuka tekee, mitä tekee. .... Ja yleensä mä pyydän aina jonkun alustavan projektisuunnitelman, koska sitten pystytään myös katsomaan, että mitä meiltä odotetaan siis asiakkaan roolissa, ja mitä sitten toimittaja tekee, ja ottaa olettavasti silloin myös vastuuta siitä."
Hahmotetaan projektitoimitusmalli ja määritellään vastuut
Hankeosaaminen ja resurssointi
H14 - "Kyllä se mun mielestä vaikuttaa siihen vähintään, koska yleensä pitää sitten ainakin sellaisessa kohdassa, missä mä olen ollut mukana täällä meillä, niin pitää arvioida, kuinka realistinen sitten esimerkiksi se käyttöönotto, aikataulut ja muut ovat. Yleensä kun puhutaan näistä hankinnoista ja tämän tyyppisistä SaaS:sta, niin totta kai siellä meidän liiketoimintajohtomme odottaa, että no koska pääsee lunastamaan sitä lisäarvoa, josta alkaa tulla deadline, aikataulu ja milloin. Ja sitten pitää olla tarkkana, että ei luvata mitään sellaista, mikä ei onnistu. Tai jos luvataan, niin silloin täytyy ymmärtää, että no millä kriteeristöllä, mitä asioita pitää olla. Pitääkö olla hanketoimisto, pitääkö olla minkälaista erilaista resurssointia ja erilaista kompetenssia siinä. Ja tämä on tyypillisesti mun kokemuksen mukaan asia, missä mennään vikaan aika pahasti, että kun saadaan aikatauluodotusta, niin siihen ei osata mitoittaa, mitä siihen aikatauluun pääseminen vaatii. Se vähätellään mun mielestä usein eri organisaatioissa. Meilläkin on käynyt sitä. Ollaan vähätelty se, että mitä tarvitaan tähän aikatauluun pääsemiseksi."
Projektin toteuttamisen suunnittelu ja resurssitarpeen varmistaminen
Ymmärretään tarvittava resurssimäärä ja varmistetaan, että organisaatiolla on riittävästi resursseja muutoksen läpivientiin
H12 - "Kyllä se hankintapäätös on se, että jos me päätetään hankkia, niin kyllähän muun muassa se tarkoittaa sitä, että onko meillä riittävästi ihmisiä tekemään se työ, että me otetaan se käyttöön. Konsultteja varmaan aina riittää, mutta kun siihen tarvittaisiin aina, niitä omiakin ihmisiä mukaan. Kyllä nämä niin kuin silleen on tämmöstä resurssointia ja raha-asiaa. Että onko rahaa sitten tehdä sitä ja tosiaan, onko meillä aikaa. Tämä on semmoinen pahin, että pistetään projekteja johdon puolta tai jostain liikkeelle, mutta sitten esimerkiksi tietohallinnossa tai liiketoimissa ei riitä ihmisiä tekemään niitä. Ja sitten tuosta siirrosta tuotantoon, mä sen takia näen sen tärkeänä, just siihen hankintapäätökseen, että sitä ei tarvitse yksityiskohtaisesti, mutta projektiriskinä, että kun se maksaa nimittäin se jatkuvat palvelut. Ja jos meillä ei ole sitä, niin mä voin sanoa, että se projekti, joka on puolitoista vuotta pyörinyt siellä ollaan tuotannossa, mutta edelleen projekti on käynnissä, niin se on konsulttien kultamaata, mutta se ei ole välttämättä sille asiakasorganisaatiolle mitään muuta kuin rahareikä."
H2 - "sitten mahdolliset korvaustoimenpiteet, että jos meillä on joku korvaava järjestelmä sitten mahdollisesti helposti otettavissa käyttöön ."
H12 - "Mehän voidaan tietohallinnossa esimerkiksi mennä arvaamaan, mikä liiketoiminnan mielestä on kriittistä. Mutta kyllähän sen liiketoiminnan pitää pystyä itsekin sanomaan esimerkiksi, että voiko tämä SaaS-palvelu olla pois käytöstä esimerkiksi päivän, taikka viikon, vai onko se niin, että tuntikin on jo liian pitkä aika. Ja tähän tietoturvamielessä jatkuvuuteenhan sitten tullaan siihen, että no jos me saadaan se viesti, että puoli päivää tai neljä tunti on pisin aika, kun se voi olla alhaalla, niin sittenhän meidän täytyy alkaa miettimään... tämä liittyy siihen hankintapäätökseenkin tai käyttöönottopäätökseen...että no millä tavalla me varmistetaan, että SaaS-järjestelmä on käytettävissä. Elikkä mitkä on meidän varajärjestelmät. Että mennäänkö varajärjestelmään niin, että jos tämä ei ole käytössä, niin sitten otetaan kynä ja paperi. Sillä pitää sitten hoitaa. Tai sitten se, että me haetaan siihen sitten vaikka muita tietoliikenneratkaisuja taustalle, siis varajärjestelmiä. Tai sitten täytyy selvittää se, että onko sillä SaaS-toimittajalla riittävät kyvyt huolehtia siitä, että se ei ole pidempää kuin se neljä tuntia alhaalla."
H3 - "Se ensimmäinen kysymys, miten kriittinen se on liiketoiminnalle. Se asettaa raamit sille keskustelulle ja se on kuin ensimmäinen. Sen jälkeen se meneekin sitten oikeastaan tietosuojaan ja tietoturvaan liittyviin riskeihin ja miten sun liiketoimintasi kestää, jos tämä palvelu on alhaalla pidempiä aikoja. Mikä se sun "operational resilience". ... Sekin on suhteessa siihen kriittisyyteen, että miten sä pystyt varmistamaan, että sun liiketoimintasi jatkuu jos toimittaja onkin yhtäkkiä pois pelistä. Se ei ole aina kauhean helppo kysymys ja se on myös se syy miksi mä sanoisin, että silti tänä päivänä valtaosan yrityksistä ydinliiketoimintajärjestelmistä on on-prem tyyppisiä tai hybridiviritykseä.
Varmistetaan että liiketoiminnan jatkuvuus säilytetään mahdollisissa ongelmatilanteissa
Varajärjestelmä ja liiketoiminnan jatkuvuuden varmistaminen


H2 - "On kriittisiä sekä vähemmän kriittisiä. Ne mitkä ovat kriittisiä, niin me ollaan usein sitten varmistettu tavalla tai toisella meidän on-prem järjestelmiin, että ollaan ne datat esimerkiksi "backupattu" meidän omaan konesaliin jos on koettu se tarpeelliseksi ja sitten ERP on tosiaan koettu tähän saakka niin kriittiseksi, että sitä ei ole haluttu viedä pilveen. Ja sitten on toki tämmöisiä yksittäisiä, jotain matkalaskujärjestelmiä mitkä ei ole kriittisiä ja jos ne on vähän aikaa pois käytöstä, niin sillä ei ole niin suurta suurta merkitystä, että tavallaan 3 eri tasosta kriittisyyttä meillä on. Ne kriittiset SaaS-sovellukset varmistetaan omaan konesaliin."
Kriittinen data varmuuskopioidaan toiseen lokaatioon
H4 - "No se vähän riippuu organisaatiokypsyydestä. Tavallaan niinku laatukulttuurista, että kuinka laaja se riskianalyysi pitää olla. Jossain isossa globaalissa yrityksessä, missä voi tapahtua kaiken näköistä. Mä vedin [suuressa globaalissa yrityksessä] yhtä tuotetiedonhallintajärjestelmän uudistusprojektia, mikä oli globaali projekti, ja siinä oli tiimiä kaikkialta maailmassa. Sitten tullut joku SARS-epidemia, ei ollut kuitenkaan yhtä vakava kuin COVID, mutta asetti sitten niinku aikamoisia matkustusrajoituksia. Niin nimettiin ihan niinku taho, joka seurasi sitä, että miten se mahdollisesti tulee vaikuttaa. Sitten on sellaisia tuota, että vedin yhden globaalin yrityksen ERP-projektia Islannissa poksahti joku tulivuori ja lentoliikenne Euroopassa päättyi viikoksi. Niin tuota, että ensinnäkin, miten me saatiin edes ne saksalaiset konsultit kotiin Suomesta, kun tuota, lennot peruutettiin, ja muuta. Voi myös tapahtua sellaisia merkittäviä asioita, joita sulla ei ollut mitään mahdollisuutta laittaa sinne riskilokiin, ja sitten yhtäkkiä ne vaan niinku tapahtuu. Et sitä voi niinku keksii kaiken näköisiä pieniä riskejä, ja täyttää sen loginsa, ja kaikki menee hyvin, tai sitten on joku sellainen ulkoinen tapahtuma, mille ei sit vaan voi vaikuttaa mitään. Periaatteessa koska kaikkea ei voi ennakoida, niin tavallaan organisaatioista pitää rakentaa sellainen, et se pystyy toipumaan melkein mistä tahansa. Et sit täytyy niinku miettiä, et mitä voidaan tehdä. Se, että pitää luoda niinku semmonen ketteryyden kulttuuri, et tapahtuu mitä tapahtuu, niin mukautetaan se oma toiminta siihen ilmiöön tai muutokseen, mikä on tapahtunut."
Luodaan organisaatioon ketteryyden kulttuuria, jotta pystytään toipumaan myös odottamattomista riskeistä
H12 - "Varmaan siis lähtökohtaisesti lähdetään taas siitä, että parhaimmillaan organisaatiossahan on olemassa tämmöinen toiminnan, liiketoiminnan jatkuvuuteen liittyvä suunnitelma. Siis parhaimmillaan, ei aina. Ja vähintään yleensä ainakin toivottavasti, niin semmoinen löytyy tietohallinnon puolelta, koska tietohallinnolla ainakin pitäisi olla jotenkin se oma järjestelmäkartta mietittynä. Että mikäs täällä nyt on kriittisiä, tai mikä voi olla niin huonolla tekniikalla, että sitä on pakko miettiä, että jos se sitten kuitenkin kohta taas kaatuu. Niin siinä mielessä tavallaan tämän tyyppisiä riskisuunnitelmia ja kartoituksia varmasti on tai pitäisi olla. Ja nimenomaan tavallaan tämmöisten toiminnan jatkuvuuteen tai disaster recovery plan, DRP-tyyppisissä asioissa."
Ymmärretään oman liiketoiminnan kriittiset järjestelmät ja varaudutaa ongelmatilanteista palautumiseen
Organisaation resilienssin kasvattaminen
Resilienssi ja liiketoiminnan jatkuvuus

Liite 4. Aineistonhallintasuunnitelma

TURUN YLIOPISTO
Kirjasto

Opiskelijan aineistonhallintasuunnitelma

Tämän dokumentin avulla voit suunnitella tutkimusaineistosi hallintaa. Yksityiskohtaisemmat ohjeet kuhunkin osioon löydät Opiskelijan aineistonhallintaoppaasta.

1. Tutkimusaineisto

Tutkimusaineistolla tarkoitetaan kaikkea sitä aineistoa, millä tutkimuksen analyysi ja tulokset voidaan todentaa ja toisintaa. Se voi olla esim. erilaisia mittaustuloksia, kyselyistä ja haastatteluista syntyvää dataa, äänitteitä ja videoita, muistiinpanoja, ohjelmistoja, lähdekoodeja, biologisia näytteitä, tekstinäytteitä ja keruuaineistoja.

Listaa alla olevaan taulukkoon kaikki tutkimuksessasi käyttämäsi tutkimusaineisto. Huomaa, että aineisto saattaa koostua useammasta eri aineistotyypistä, muista kirjata kaikki eri aineistotyypit. Listaa sekä digitaalinen että fyysinen tutkimusaineisto.

Aineistotyyppi	**Sisältää henkilötietoja***	**Tuotan aineiston itse**	**Joku muu on tuottanut aineiston**	**Muuta huomioitavaa**
Aineistotyyppi 1: *Haastattelujen tallenteet*		x		Haastattelut tallennetaan haastattelujen aikana käyttäen älypuhelimen Tallennus-työkalua tai Microsoft Teamsin Tallenna-toimintoa. Tallenteet siirretään suojattuun pilvikansioon Microsoft OneDriveen ja poistetaan laitteiden sisäisestä tallennustilasta.
Aineistotyyppi 2: Litteroidut haastattelut		x		Litteroidut haastattelut tallennetaan kirjallisessa muodossa suojattuun pilvikansioon Microsoft OneDriveen.

* Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen. Esimerkkejä henkilötiedoksi katsotuista tiedoista löydät Tietosuojavaltuutetun toimiston sivuilta

TURUN YLIOPISTO
Kirjasto

2. Henkilötietojen käsittely tutkimuksessa

Mikäli aineistosi sisältää henkilötietoja, olet velvoitettu noudattamaan EU:n tietosuoja-asetusta (GDPR) sekä Suomen tietosuojalakia. Henkilötietoja sisältävän aineiston osalta sinun tulee laatia tutkittavillesi tietosuojailmoitus sekä selvittää, kuka toimii aineiston osalta rekisterinpitäjänä.

Laadin tutkittavilleni tietosuojailmoituksen** ja toimitan sen heille ennen aineiston keruuta ☐

Henkilötietojen osalta rekisterinpitäjänä** toimii opiskelija ☐ yliopisto ☐

Aineistoni ei sisällä henkilötietoja ☒

**Lisätietoja yliopiston intranetin Tietosuojaohjeita opinnäytetyöhön -sivulta

3. Aineiston käyttöön liittyvät luvat ja oikeudet

Selvitä mitä lupia ja oikeuksia aineistojen käyttöön liittyy. Ole tarvittaessa yhteydessä opinnäytteesi ohjaajaan. Kuvaile jokaisen aineistotyypin osalta niiden käyttöön liittyvät luvat ja oikeudet, voit tarvittaessa lisätä aineistotyyppejä listaukseen.

3.1 Itse tuotettu aineisto

Saatat tarvita erillisiä lupia keräämäsi tai tuottamasi aineiston käyttöön sekä tutkimuksessa että tulosten julkaisemisessa. Mikäli olet arkistoimassa aineistoasi, pyydä tutkittavilta tarvittavat luvat aineiston arkistoimiseen ja jatkokäyttöön. Selvitä myös, vaatiiko valitsemasi arkisto kirjallisia lupia tutkittavilta.

Tarvittavat luvat ja niiden hankkiminen

Aineistotyyppi 1: Lupa haastattelun tallentamiseen. Lupa haastattelun tallentamiseen kysytään haastateltavalta suullisesti ennen haastattelun alkua.

Aineistotyyppi 2: Lupa haastattelun litterointiin. Lupa haastattelun litterointiin kysytään haastateltavalta suullisesti ennen haastattelun alkua.

3.2 Jonkun muun tuottama aineisto

Onko sinulla tarvittavat luvat aineiston käyttöön tutkimuksessa ja tulosten julkaisemiseen? Liittyykö aineistoon tekijänoikeuksia tai käyttölisenssejä? Huomioi, että esimerkiksi julkaisujen kuvien ja kaavioiden käyttö saattaa edellyttää lupaa.

Aineistoon liittyvät oikeudet ja lisenssit

-

4. Aineiston säilyttäminen tutkimuksen aikana

Missä säilytät aineistoasi tutkimuksen aikana?

Yliopiston verkkokansiossa ☐
Yliopiston tarjoamassa Seafile-pilvipalvelussa ☐
Jossakin muualla, missä? Microsoftin OneDriven suojatussa pilvikansiossa. ☒

Yliopiston tallennuspalvelut huolehtivat automaattisesti tietoturvasta ja varmuuskopioinnista. Jos valitset tallentamisen muualle kuin yliopiston palveluihin, kuvaa, miten huolehdit tietoturvasta ja varmuuskopioinnista. Muista varmistaa, mihin tallennat aineiston aina sitä muokattuasi.

Tietoturvasta huolehditaan Microsoftin OneDriven tietoturvan avulla ja tiedostot jaetaan ainoastaan tätä tutkimusta tekevien henkilöiden kesken. Varmuuskopiointi tapahtuu luomalla kopiot alkuperäisistä tiedostoista samaan suojattuun verkkokansioon.

Jos käytät tallentamiseen puhelinta, tarkista etukäteen, minne ääni tai video tallentuu. Jos käytät tallentamiseen kaupallisia pilvipalveluita (iCloud, Dropbox, GoogleDrive jne.) ja aineistosi sisältää henkilötietoja, varmista, että tietosuojailmoituksessa antamasi tiedot tietojen siirtymisestä vastaavat laitteistosi asetuksia. Kaupallisten pilvipalveluiden käyttö merkitsee tietojen siirtoa kolmansiin maihin.

5. Aineiston dokumentointi ja metadata

Miten kuvailet aineistosi niin, että ulkopuolinenkin ymmärtää, millaista aineisto on? Miten itse tarpeen tullen palautat vuosien kuluttua mieleesi, mistä aineistosi koostuu?

5.1 Aineiston dokumentointi

Pystytkö kertomaan, mitä aineistollesi on tapahtunut tutkimuksen teon aikana? Aineiston dokumentointi on keskeisessä osassa aineistoon tehtyjen muutosten jäljittämisessä.

Käytän aineiston dokumentointiin

tutkimuspäiväkirjaa ☐
erillistä dokumenttia, johon kirjaan aineiston pääasiat, kuten tehdyt muutokset, analyysin vaiheet sekä esim. muuttujien merkitykset ☒
aineiston mukana kulkevaa readme-tiedostoa, jossa kuvataan aineiston pääasiat ☐
jotain muuta, mitä? ☐

5.2 Aineiston järjestys ja eheys

Miten pidät aineistosi järjestyksessä ja ehyenä, ja vältät sen tahattomat muutokset?

Säilytän alkuperäisen aineiston erillään tutkimuksenteon aikana käyttämästäni aineistosta, jotta voin palata alkuperäiseen, jos tarvetta ilmenee. ☒

Versionhallinta: mietin jo ennen tutkimuksenteon alkua, miten tulen nimeämään eri aineistoversiot ja noudan sitä systemaattisesti ☒

Tiedostan jo tutkimuksen alussa aineistoni elinkaaren, ja varaudun tilanteisiin, joissa data saattaa huomaamatta muuttua, kuten esim. nauhoitus, litterointi, konversio toiseen tiedostomuotoon, tallentaminen jne. ☒

5.3 Metadata

Metadata on kuvaus aineistostasi. Metadatan perusteella henkilö, joka ei tunne aineistoasi, ymmärtää, millaista aineistosi on. Metadataa voi olla mm. tiedoston nimi, sijainti, koko ja tieto aineiston tuottajasta. Tarvitsetko metadataa?

Tallennan aineistoni arkistoon tai tietopankkiin, joka huolehtii metadatasta puolestani. ☐

Minun pitää luoda metadata, koska arkisto, johon tallennan aineiston edellyttää sitä. ☐

En tallenna aineistoani julkiseen arkistoon, enkä tarvitse metadataa. ☒

6. Aineisto tutkimuksen valmistuttua

Olet vastuussa aineistostasi myös tutkimuksen valmistumisen jälkeen. Varmista, että käsittelet sitä tekemiesi sopimusten mukaisesti. Yliopiston suosittelema säilytysaika on viisi vuotta, poikkeuksena kuitenkin lääketieteen alan aineistot, joiden säilytysaika on 15 vuotta. Henkilötietoja voi säilyttää vain sen aikaa, kun tarve on. Jos olet sitoutunut tuhoamaan aineiston määräajan päätyttyä, sinun on huolehdittava siitä, vaikka et olisi enää opiskelija. Myös yliopiston tallennusratkaisuja käytettäessä aineiston tuhoaminen on sinun vastuullasi.

Mitä aineistollesi tapahtuu, kun tutkimus valmistuu?

Haastattelujen tallenteet tuhotaan 6 kuukauden jälkeen tutkielman valmistumisesta, mutta litteroidut haastattelut säilytetään Yliopiston suositusten mukaisesti 5 vuotta, jonka jälkeen ne tuhotaan. Täten varmistutaan siitä, että tutkimuksen aineistoon voidaan tarvittaessa palata, jos tarve niin vaatii.

Jos säilytät dataa, kuvaa, missä: Data säilytetään Microsoftin suojatulla pilvipalvelimella Onedrivessa. Data on anonyymiä, eikä täten sisällä henkilötietoja.

Aineistonhallintasuunnitelma kannattaa pitää ajan tasalla läpi tutkimuksen.

Lisätietoja Turun yliopiston kirjaston laatimasta Opiskelijan aineistonhallintaoppaasta