Anssi Jaakkola

JATKUVUUDEN HALLINNAN KEHITTÄMINEN: PIENTEN YRITYSTEN NÄKÖKULMA JA PILVIPALVELUIDEN ERITYISPIIRTEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2024

TIIVISTELMÄ

Jaakkola, Anssi
Jatkuvuuden hallinnan kehittäminen: pienten yritysten näkökulma ja pilvipalveluiden erityispiirteet
Jyväskylä: Jyväskylän yliopisto, 2024, 75 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Seppänen, Ville

Jatkuvuuden hallinta ja varautuminen ovat nousseet yhteiskunnalliseen keskusteluun viime vuosina. Aiheen ajankohtaisuudesta huolimatta jatkuvuuden hallintaa on tutkittu vain vähän pienten yritysten näkökulmasta. Samanaikaisesti pienet yritykset hyödyntävät keskeisissä liiketoiminnoissaan yhä enemmän pilvipalveluita, joten niiden jatkuvuuden hallinnan erityispiirteitä tulisi tutkia tarkemmin. Tämä tutkielma pyrkii täyttämään edellä mainittuja tutkimusaukkoja.

Tutkielmassa selvitettiin kirjallisuuskatsauksen ja empiirisen tutkimuksen avulla pienten suomalaisyritysten jatkuvuuden hallinnan tilaa ja haasteita. Lisäksi tutkielmassa kartoitettiin pilvipalveluihin liittyvää jatkuvuussuunnittelua kyseisissä yrityksissä, sekä selvitettiin millaisia asioita yritykset arvostavat pilvipalveluita koskevassa jatkuvuussuunnitelmassa. Tutkimuksen tulokset osoittavat, että jatkuvuuden hallinta ymmärretään pienyrityksissä monin eri tavoin ja siihen liittyviä toimia toteutetaan vaihtelevasti. Jatkuvuuden hallinta on pienissä yrityksissä keskittynyt fyysisen omaisuuden suojaamiseen ja henkilöstöriskeihin varautumiseen. Jatkuvuuden suunnittelu on pääosin sanallista ja intuitioon perustuvaa toimintaa: systemaattista riskien kartoittamista ja jatkuvuuden säännöllistä tarkastelua toteutetaan pienissä yrityksissä harvoin. Nykyiset ohjeet ja standardit koetaan pienille yrityksille soveltumattomiksi, eikä niitä siksi ollut hyödynnetty jatkuvuuden hallinnan toteuttamisessa. Lisäksi tutkielmassa selvisi, että digitaaliseen omaisuuteen tai työkaluihin kohdistuvia riskejä ei osata pienissä yrityksissä arvioida tai ottaa huomioon: esimerkiksi pilvipohjaiset IT-ratkaisut koetaan pääosin pelkästään jatkuvuutta parantavina tekijöinä, ilman että niiden jatkuvuusvaikutuksia on arvioitu. Edelleen tutkimuksessa havaittiin, että pienissä yrityksissä ei ole ammattitaitoa arvioida pilvipalveluihin liittyvän jatkuvuuden hallinnan riittävää tasoa, ja resurssien vähäisyyden takia aihetta ei ole voitu kattavasti käsitellä. Pienet yritykset arvostaisivatkin tutkimuksen mukaan helppokäyttöistä, opastavaa mallia pilvipalveluiden jatkuvuuden hallinnan toteuttamiseen. Mallin tulisi olla lisäksi päivittyvä ja helposti saatavilla uudelleen tarkastelua varten.

Asiasanat: jatkuvuuden hallinta, pienet yritykset, pilvipalvelut

ABSTRACT

Jaakkola, Anssi
Developing business continuity management: the perspective of small businesses and the special features of cloud services
Jyväskylä: University of Jyväskylä, 2024, 75 pp.
Cyber Security, Master's Thesis
Supervisor: Seppänen, Ville

Business continuity management and organizational resilience have become topics of social discussion in recent years. Despite the topicality of the topic, continuity management has been studied only to a limited extent from the perspective of small businesses. At the same time, small businesses are increasingly utilizing cloud services as part of their core business processes, so the specific characteristics of their business continuity management should be studied more closely. This thesis aims to fill these research gaps.

This study investigated the state and challenges of business continuity management in small Finnish companies through a literature review and empirical research. In addition, the study mapped out business continuity planning related to cloud services in these companies and identified what companies value in a continuity plan for cloud services. The results of the study show that business continuity management is understood in small businesses in many ways and actions related to it are implemented variably. Business continuity management in small businesses is focused on protecting physical assets and preparing for personnel risks. Business continuity planning is mainly verbal and intuition-based: systematic risk mapping and regular continuity review are rarely carried out in small businesses. In addition, the study found that small businesses do not know how to assess or consider risks related to digital assets or tools, and cloud-based IT solutions are mainly perceived as factors that improve business continuity without assessing their negative continuity effects. Additionally, the research found that small companies lack the expertise to assess the adequacy of continuity management related to cloud services, and due to limited resources, the topic has not been comprehensively addressed. Based on the results of the study, small businesses would appreciate an easy-to-use, instructive model for implementing cloud service continuity management. The model should also be up-to-date and easily available for re-evaluation.

Keywords: business continuity management, small enterprises, cloud computing

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Viimeaikaiset kriisit ovat nostaneet varautumisen ja liiketoimintojen jatkuvuuden varmistamisen yhteiskunnalliseen keskusteluun. Pohdittaessa keinoja yritysten selviytymiseen, liiketoiminnan jatkuvuuden hallinta on tunnustettu yhtenä tehokkaimmista tavoista toipua riskien aiheuttamista toiminnan häiriöistä. Se on olennainen osa yritysten toimintaa ja voi olla ratkaiseva tekijä koko organisaation olemassaolon kannalta. (Charoenthammachoke, Kodaka, Tang & Leelawt, 2020) Samanaikaisesti digitalisaatio on johtanut siihen, että yhä useampi yritys hyödyntää IT-palveluita, kuten tietoteknisiä laitteita, tietoverkkoja tai tietojärjestelmiä keskeisissä liiketoiminnoissaan: esimerkiksi tuotanto, viestintä, tilastointi, markkinointi, myynti ja HR perustuvat usein digitaalisiin ratkaisuihin. Samalla tietojärjestelmien kasvavat laskentatehovaatimukset, laitteiston kustannukset, saatavuuden varmistaminen, päivitettävyys ja monet muut tekijät ovat saaneet yritykset ulkoistamaan IT-palveluitaan ulkoisille palveluntarjoajille (Irsheid ym., 2022). Näitä internetin yli käytettäviä IT-palveluita kutsutaan yleisesti nimityksellä pilvipalvelut (Sahebjamnia ym., 2015). Pilvipalveluita hyödynnetäänkin yhä enemmän myös pienissä yrityksissä: tilastokeskuksen mukaan 10–19 henkeä työllistävistä yrityksistä 73 %, kertoi käyttävänsä maksullisia pilvipalveluita vuonna 2022, kun viisi vuotta aiemmin luku oli 57 % (Tilastokeskus, 2022). Vaikka pilvipalveluiden hyödyntäminen avaa uusia mahdollisuuksia, niiden käyttöön ja toimittamiseen liittyy erilaisia riskejä, jotka voivat aiheuttaa häiriöitä ja katkoksia yrityksen toimintaan (Sahebjamnia ym., 2015).

Huolimatta jatkuvuuden hallinnan ajankohtaisuudesta ja pilvipalveluiden käytön yleistymisestä, viimeaikaiset tutkimukset osoittavat, että pienet yritykset ovat vähemmän kiinnostuneita jatkuvuuden hallinnasta ja toteuttavat harvemmin jatkuvuussuunnittelua kuin suuremmat yritykset (Charoenthammachoke ym., 2020; Kato & Charoenrat, 2018; Kaufhold ym., 2018). Tämä johtuu tutkimusten mukaan siitä, että pienillä yrityksillä ei ole välttämättä käytössään samoja resursseja, ammattitaitoa tai joustavuutta jatkuvuuden parantamiseksi kuin suurilla yrityksillä, sekä siitä, että nykyisten ohjeistusten kuten ISO 22301 on todettu olevan liian kalliita, raskaita ja monimutkaisia pienten yritysten käyttöön (Thiel & Thiel, 2010; Verbano & Venturini, 2013). Väitettä tukee myös Niemimaan ja

Järveläisen (2013) tutkimus, jonka mukaan pienemmät yritykset pitävät IT-palveluiden jatkuvuussuunnitelmia liian raskaina luoda ja ylläpitää. Havaintoa voidaan pitää huolestuttavana, koska häiriöiden on todettu olevan erityisen haitallisia pienten yritysten toiminnalle (Verbano & Venturini, 2013). Aiheeseen onkin viime vuosina kiinnitetty enemmän huomiota, mutta aihetta tulisi tutkia edelleen, jotta pienten yritysten jatkuvuutta ja varautumista voidaan parantaa (Charoenthammachoke ym., 2020; Gao ym., 2013; Kato & Charoenrat, 2018). Tämän tutkimuksen kannalta on lisäksi huomionarvoista, että huolimatta pilvipalveluiden keskeisestä roolista pienten yritysten toiminnalle, niiden merkitystä, erityispiirteitä ja riskejä jatkuvuuden hallinnan näkökulmasta ei ole juuri tutkittu. Olemassa oleva tutkimus on keskittynyt pienten yritysten osalta koko organisaation jatkuvuuden hallintaan, jossa korostuvat pilvipalveluita enemmän perinteiset liiketoiminnan osa-alueet kuten fyysinen turvallisuus. Lisäksi tutkimus on osoittanut, että pilvipalveluihin liittyvät turvallisuusvastuut eivät aina ole täysin selkeitä ja ne vaihtelevat toimittajien sekä toimitusmallien välillä (Hendre & Joshi, 2015; Kyberturvallisuuskeskus, 2020a). Näistä syistä pilvipalveluiden jatkuvuuden hallinnan erityispiirteiden tutkiminen pienten yritysten näkökulmasta on tärkeää.

1.1 Tutkimusongelmat ja käytetyt menetelmät

Tässä tutkielmassa tarkastellaan jatkuvuuden hallinnan teoriaa ja parhaita käytänteitä, tutkitaan pienten yritysten jatkuvuuden hallinnan tilaa, sekä selvitetään millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta. Tutkielma avaa ensin, miten jatkuvuuden hallintaa tulisi teoriassa toteuttaa tieteellisten lähteiden, viranomaislähteiden, sekä alan standardien mukaisesti. Tämän jälkeen tutkielmassa selvitetään laadullisen tutkimuksen menetelmin miten pienet ja keskisuuret yritykset toteuttavat omaa jatkuvuuden hallintaansa. Tutkielman avulla voidaan myös saada selville, millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta. Näistä tavoitteista johdettuna tämän tutkielman tutkimuskysymykset ovat:

1. Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja onko siinä huomioitu pilvipalveluita?
2. Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?

Tutkimuskysymyksiin vastataan sekä kirjallisuuskatsauksen että empiirisen tutkimuksen avulla. Kirjallisuuskatsauksen tavoitteena on muodostaa ymmärrys siitä, miten jatkuvuuden hallintaa tulisi aiheesta tehdyn tutkimuksen, standardien ja erilaisten viranomaisohjeistusten mukaisesti toteuttaa. Kirjallisuuskatsaus vastaa siis omalta osaltaan tutkimuskysymykseen: ”Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa

pienten yritysten näkökulmasta?". Kirjallisuuskatsaus parantaa myös tutkijan omaa ymmärrystä jatkuvuuden hallinnan kokonaisuudesta ja toimii pohjana empiirisen tutkimuksen toteutukselle. Kirjallisuuskatsaus toteutettiin kuvailevana, narratiivisena kirjallisuuskatsauksena, jonka avulla pystyttiin muodostamaan laaja kuva käsiteltävästä aiheesta (Salminen, 2023). Tutkielman lähdemateriaalina toimi aiheeseen liittyvät tieteelliset artikkelit ja tutkimukset, suomalaisten viranomaisten tuottamat julkaisut, sekä aiheeseen liittyvät standardit. Viranomaislähteitä hyödynnettiin, koska jatkuvuuden hallintaa tehdään Suomessa lakeihin pohjautuen ja se on siten hyvin organisoitua ja yhdenmukaista toimintaa. Tutkielman tieteelliset lähteet etsittiin Google Scholarin avulla. Tieteellisistä lähteistä pyrittiin valitsemaan arvostettujen tieteellisten julkaisijoiden julkaisuja ja lähteitä arvioitiin viittausmäärien perusteella. Tieteellisiä lähteitä etsittiin muun muassa seuraavilla hakutermeillä ja niiden yhdistelmillä: "business continuity", "cloud computing", "business continuity in small enterprises", "business continuity management in SME:s", "business continuity and cloud computing", "cloud business continuity in small enterprises", "cloud business continuity in SMEs". Hakuja laajennettiin koskemaan pienten yritysten ohella myös keskisuuriin yrityksiin kohdistuvaa tutkimusta, koska saatavilla oli hyvin vähän pelkästään pieniin yrityksiin kohdistuvia tieteellisiä lähteitä. Tämä otettiin huomioon tutkimuksen laadun arvioinnissa.

Tutkielman empiirinen osuus toteutettiin laadullisena tutkimuksena. Empiirisen osion tavoitteena oli vastata tutkimuskysymykseen "Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja onko siinä huomioitu pilvipalveluita?", sekä kerätä pienyritysten näkemyksiä ominaisuuksista, joita yritykset arvostavat pilvipalveluita koskevassa jatkuvuussuunnittelussa. Täten empiirisen osion avulla kerättiin aineistoa myös toiseen tutkimuskysymykseen "Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?". Tiedonkeruumenetelmänä hyödynnettiin teemahaastattelua, jonka haastattelurunko määritettiin tutkimuskysymysten avulla. Tutkittaviksi yrityksiksi valittiin alle 50 henkilöä vakituisesti työllistäviä yrityksiä, joiden vuosiliikevaihto alitti 10 miljoonaa euroa. Nämä yritykset voidaan tilastokeskuksen mukaisesti määritellä pienyrityksiksi (Tilastokeskus, 2023). Tutkittavien yritysten tuli lisäksi hyödyntää pilvipalveluita osana keskeisiä liiketoiminnan prosessejaan, jotta tutkittavan aiheen tärkeys yrityksen toiminnalle voitiin varmistaa. Haastateltavat valittiin eri toimialoilta ja eri yrityksistä, jotta havaintoja voitiin tehdä monipuolisesti erilaisista yrityksistä. Haastatteluista saatu aineisto analysoitiin teema-analyysin avulla ja siitä havainnoitiin teemoja, joita hyödynnettiin tutkimuskysymyksiin vastaamisessa.

1.2 Tutkielman rakenne ja rajaukset

Tutkielma on jaettu seitsemään lukuun. Ensimmäisessä luvussa pohditaan tutkimuksen tarpeellisuutta, sekä esitellään tutkielman aihe, tutkimuskysymykset ja tutkimuskysymysten ratkaisemiseen käytetyt menetelmät. Luvut 2–4 käsittävät

tutkielman kirjallisuuskatsauksen. Toisessa luvussa kuvataan digitaalisen turvallisuuden viitekehys lukuun ottamatta jatkuvuuden hallinnan ja varautumisen kokonaisuutta, joka tälle tutkimukselle keskeisenä aiheena avataan luvussa kolme. Luku kolme esittelee lisäksi kolme jatkuvuuden hallintaan ja varautumiseen käytettyä mallia. Luvussa neljä avataan pilvipalveluiden määritelmä, sekä tarkastellaan pilvipalveluiden jatkuvuuden hallinnan teoriaa hyötyjen, haasteiden, vastuiden ja toteuttamisen näkökulmasta. Luvut 5–7 muodostavat tutkielman empiirisen osion. Luku viisi käsittelee tutkimuksen tutkimusotetta ja kuvaa tutkimuksen menetelmiä. Luvussa avataan tutkimuksen tiedonkeruumenetelmä ja kuvataan haastatteluiden toteutuksen ohella haastatteluista saadun aineiston käsittely ja analysointi. Luvussa kuusi esitellään empiirisen tutkimuksen keskeiset tulokset. Seitsemäs luku esittelee tuloksista johdetut johtopäätökset, pohtii tutkimukselle jatkotutkimusaiheita, sekä analysoi tutkimuksen luotettavuutta ja rajoituksia.

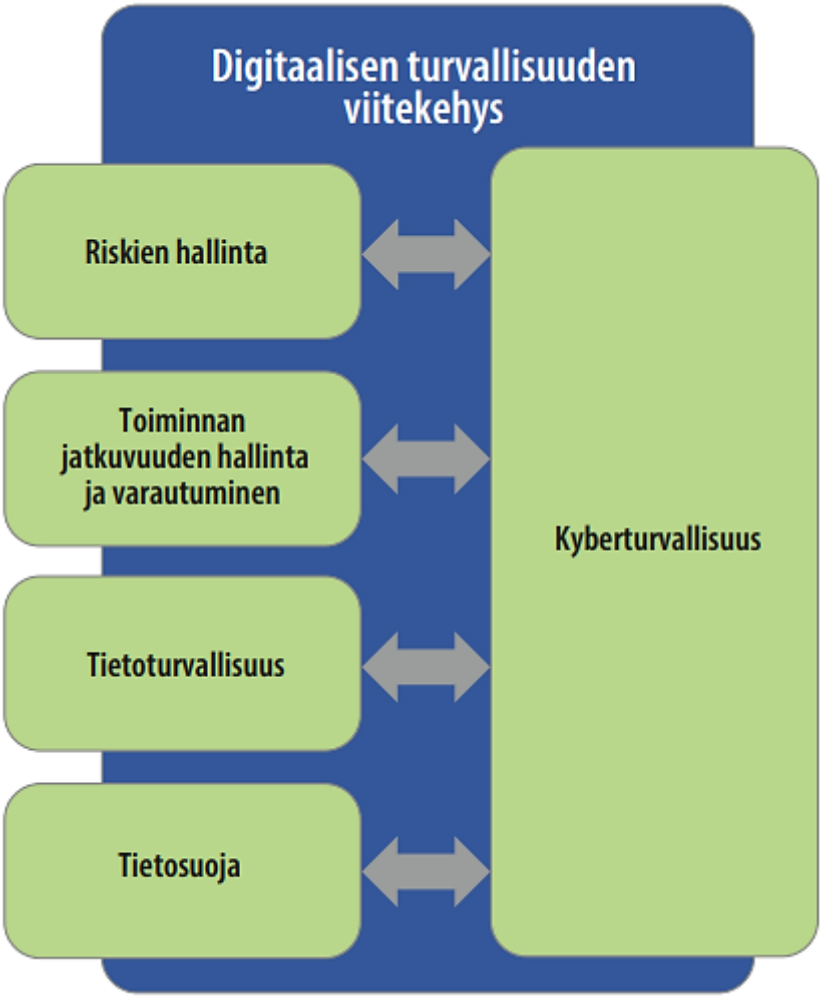
Tutkielman kohderyhmäksi on rajattu tilastokeskuksen määritelmän mukaiset pienet suomalaisyritykset, joille pilvipalvelut ovat keskeisessä roolissa liiketoimintojen toteuttamisessa. Tutkimuksen kontekstissa tällä tarkoitetaan, että yrityksen olisi joko mahdotonta tai erittäin vaikeaa toteuttaa liiketoimintaansa ilman pilvipalveluita. Kohderyhmään kuuluneet yritykset toteuttivat esimerkiksi pääosan palveluidensa myynnistä tai laskutuksesta pilvipohjaisiin ohjelmistoihin tukeutuen. Tutkimuksen ulkopuolelle rajattiin siis sellaiset yritykset, jotka hyödynsivät pilvipalveluita pelkästään liiketoiminnoille vähemmän kriittisissä tehtävissä, kuten viestinnässä. Lisäksi tutkimuksesta rajattiin pois sellaiset yritykset, jotka toteuttivat pilvipohjaisia ohjelmistoja liiketoimintanaan, koska tutkimus koski pilvipalveluiden osalta ainoastaan asiakkaan näkökulmaa. Yritysten toimialaa ei koettu hyödylliseksi rajoittaa, koska jatkuvuuden hallintaan liittyy paljon samankaltaisuuksia toimialasta riippumatta. Julkisen sektorin toimijat rajattiin tutkimuksen ulkopuolelle, koska ne toteuttavat jatkuvuuden hallintaa lainsäädäntöön pohjautuen ja ovat täten eri asemassa yksityiseen sektoriin nähden. Tutkielma keskittyy jatkuvuuden hallintaan hallinnollisena prosessina, johon kuuluvat erilaiset strategisen tason suunnitelmat, eikä se täten tarkastele syvällisemmin yksittäisiä operatiivisen tason toimia. Siksi tutkimus ei syvenny myöskään pilvipalveluiden teknisiin ominaisuuksiin tarvittavaa osaa tarkemmin.

2 DIGITAALISEN TURVALLISUUDEN KOKONAISUUS

Tässä luvussa käsitellään digitaalisen turvallisuuden kokonaisuutta. Kokonaisuuden hahmottaminen on tärkeää jatkuvuuden hallinnan teoreettisen viitekehyksen ymmärtämiseksi. Digitaalinen turvallisuus on valittu jatkuvuuden hallinnan viitekehykseksi, koska se voidaan nähdä kyberturvallisuuden synonyyminä, ja sen avulla on mahdollista kuvata niin kyberturvallisuuden kokonaisuus, riskien hallinnan merkitys jatkuvuuden hallinnalle, kuin toiminnan jatkuvuuden hallinnan ja varautumisen asemoituminen ja merkitys kokonaisuuden sisällä (Valtiovarainministeriö, 2020).

Digitaalisen turvallisuuden tavoitteena on Valtiovarainministeriön (2020) mukaan kansalaisten, yhteisöjen, ja yhteiskunnan suojaaminen digitaalisessa ympäristössä vallitsevilta riskeiltä, sekä luottamuksen lisääminen eri yhteiskunnan toimijoiden välillä. Kokonaisuuden voidaan katsoa muodostuvan vahvasti toisiinsa sidoksissa olevista ja osittain myös päällekkäisistä osa-alueista: riskien hallinnasta, toiminnan jatkuvuuden hallinnasta ja varautumisesta, tietoturvallisuudesta, sekä tietosuojasta. Viitekehyksen eri osat on kuvattu kuviossa 1. Kuvioon voidaan etenkin kansainvälisissä yhteyksissä lisätä digitaaliseen turvallisuuteen kuulumattomia, valtiolliseen toimintaan liittyviä osa-alueita, kuten kyberdiplomatia sekä hybridivaikuttaminen, mitkä eivät kuitenkaan ole tämän tutkimuksen kannalta keskeisiä osa-alueita.

Tässä luvussa käsitellään digitaalisen turvallisuuden osa-alueet lukuun ottamatta jatkuvuuden hallinnan ja varautumisen osa-aluetta, joka käsitellään myöhemmin omassa luvussaan. Luvussa avataan osa-alueiden historiaa, kuvataan niiden toteuttamista organisaatioissa ja merkitystä digitaalisessa turvallisuudessa.



KUVIO 1 Digitaalisen turvallisuuden viitekehys (Valtiovarainministeriö, 2020, s. 16)

2.1 Riskien hallinta

Riskin käsitteestä ei ole olemassa yksimielisesti hyväksyttyä määritelmää. Oxfordin sanakirjan (2022) mukaan yleisesti ehdotettu alkuperä on latinankielisissä sanoissa resicum ja risicum, joilla tarkoitetaan vaaraa ja vahingon mahdollisuutta. Näiden sanojen alkuperänä on toiminut substantiivi resecare, joka tarkoittaa ”sitä, joka rikkoo”. Sana viittaa merenkulussa riskeinä pidettyihin riuttoihin ja karikkoihin. Toisena todennäköisenä alkuperänä pidetään arabiankielistä sanaa rizq, jolla tarkoitetaan onnea, hyvinvointia ja mahdollisuutta. (Oxford, 2022) Kuten historiassa, sanalla on myös nykyisin sekä negatiivinen että positiivinen merkitys: riski nähdään mahdollisuutena menetykseen, vahinkoon tai muuhun ei-toivottuun seuraukseen, mutta toisaalta myös asiana, jonka katsotaan todennäköisesti tuottavan hyvää, mutta joka on potentiaalinen uhan tai vaaran aiheuttaja (Aven, 2011; Haemmerle, Islam & Tedford, 2008).

Organisaatiot kohtaavat toiminnassaan useita erityyppisiä riskejä. Riskit voivat liittyä fyysiseen tai liiketoiminnalliseen ympäristöön, operatiiviseen ja strategiseen toimintaan tai esimerkiksi yrityksen talouteen liittyviin tekijöihin. Tuotteiden ja palveluiden monimutkaistuminen on kasvattanut riskeille altistumista ja riskien monimuotoisuutta: siksi riskien luokittelulla voidaan helpottaa riskien tunnistamista ja hallintaa. Riskejä voidaan jaotella useilla eri tapaa, mutta korkealla tasolla riskit voidaan jakaa luonnollisiin riskeihin, sekä riskeihin, jotka johtuvat keinotekoisista, ihmisen aiheuttamista tapahtumista (Gibb & Buchanan, 2006; Suomen Riskienhallintayhdistys ry, 2023b). Suomen riskienhallintayhdistys (2023b) jakaa organisaation kohtaamat riskit tarkemmin neljään kategoriaan:

- Strategisiin riskeihin, joilla tarkoitetaan organisaation strategian toteuttamiseen vaikuttavia riskejä. Tällaisia riskejä ovat esimerkiksi oikeat tai väärät (strategisen tason) valinnat, tuotteiden ja palveluiden vastaavuus asiakkaiden odotuksiin, uudet liiketoimintamahdollisuudet sekä kilpailijoiden, asiakkaiden ja toimittajien toiminta.
- Operatiiviset riskeihin, jotka ovat seurausta tapahtumista, jotka aiheutuvat riittämättömistä tai toimimattomista sisäisistä prosesseista tai järjestelmistä. Lisäksi riskit, jotka aiheutuvat riittämättömistä tai liian heikosti koulutetuista henkilöstöresursseista luetaan tähän kategoriaan.
- Taloudellisiin riskeihin, jotka tarkoittavat organisaation vakavaraisuuteen, pääomien riittävyyteen ja rahaprosessien toimivuuteen liittyviä riskejä. Taloudelliset riskit voivat toteutua useasta eri syystä, kuten korkojen muutoksista, puutteellisesta raportoinnista, tai heikosta pääomien hallinnasta.
- Vahinkoriskeihin, jotka aiheutuvat esimerkiksi palovahingoista, ympäristövahingoista, yritykseen kohdistuvista tai yrityksen tekemistä rikoksista, sekä keskeytyksistä aiheutuvista vahingoista.

Digitaalisen ympäristön kontekstissa riski voidaan nähdä verbinä: ISO 27005-standardi määrittelee riskin sellaisten uhkien toteutumiseksi, jotka hyödyntävät tietoon liittyviä haavoittuvuuksia ja aiheuttavat täten negatiivisia vaikutuksia organisaatiolle (International Organization for Standardization, 2018). Digitaalisessa ympäristössä olevista riskeistä on tullut yleisempiä ja niiden vaikutukset ovat voimistuneet liiketoimintojen pohjautuessa yhä enemmän digitaalisiin järjestelmiin. Siksi digitaalisen turvallisuuden merkitys on kasvanut viime vuosina. (Fazlida & Said, 2015)

Vastatakseen riskeihin ja ylläpitääkseen toimintaansa, organisaatiolla tulee olla vahva tietämys omien liiketoimintojensa sisällöstä sekä niihin liittyvistä vahvuuksista ja heikkouksista. Monissa tilanteissa riskejä voidaankin suunnitelmallisesti ennakoida ja hallita; tämän seurauksena on syntynyt nykyisen kaltainen organisaation riskienhallinta. Organisaation riskienhallinnalla tarkoitetaan systemaattisia prosesseja riskien tunnistamiseen sekä sellaisten menetelmien ja tekniikoiden valintaan ja käyttöönottoon, joilla

riskeistä johtuvia hyviä tai huonoja tapahtumia voidaan käsitellä hallitusti (Ferreira de Araújo Lima ym., 2020; Gao ym., 2013; Verbano & Venturini, 2013). Onnistunut riskienhallinta parantaa organisaation mahdollisuuksia menestyä ja vähentää epäonnistumisen todennäköisyyttä.

2.2 Tietoturvallisuus

Tiedon monimuotoisuuden takia tietoturvallisuuden alkuperää on vaikea määritellä; luottamuksellisen tiedon suojaamiseksi on suoritettu toimia jo kauan ennen tietokoneiden ja tietoverkkojen syntyä. Historiallisesti turvallisuus on yleensä rinnastettu fyysisiin käytänteisiin joilla arvokasta omaisuutta suojeltiin, joten tiedon salaamiseen liittyviä tekniikoita on löydetty jo muinaisesta Egyptistä, jonka olemassaolo päättyi noin vuonna 30 eaa (Leeuw & Bergstra, 2007; Soliman & Rinta-Kahila, 2020). Nykyisin yleistynyt määritelmä tietoturvallisuudesta tarkoittaa hallinnollisia ja teknisiä toimia, joiden tavoitteena on suojata ja säilyttää tiedon luottamuksellisuus, eheys ja saatavuus (Kyberturvallisuuskeskus, 2020b; SFS, 2022). Luottamuksellisuus tarkoittaa, että tiedot eivät ole muiden kuin tarkasteluun oikeutettujen saatavilla. Eheydellä viitataan siihen, että tietoja eivät voi muuttaa kuin siihen oikeutetut. Saatavuus puolestaan tarkoittaa, että tieto on siihen oikeutettujen tahojen saatavilla haluttuna aikana. (Kyberturvallisuuskeskus, 2020b) Suojattava tieto voi olla useassa eri muodossa kuten paperilla, paikallisesti tai ulkoisesti tallennettuina tiedostoina, puhuttuna tai esitettynä eri muodoissa. Tietoturvan tehtävänä on suojata tietoa kaikissa sen muodoissa., ja toisaalta tietoturvalla voidaan tarkoittaa oloja, joissa tietoturvaan liittyvät riskit ovat hallinnassa. (Kyberturvallisuuskeskus, 2020b; Sanastokeskus TSK ry, 2018)

Vealen ja Brownin tutkimuksessa (2020) havaittiin, että termiä tietoturvallisuus käytetään usein synonyyminä sanan kyberturvallisuus kanssa (Veale & Brown, 2020). Vaikka määritelmät ovat lähellä toisiaan ja sisältävät osittain samoja asioita, eivät käsitteet kuitenkaan ole täysin toisiaan vastaavia. Tietoturvallisuus on tieto-omaisuuden suojaamista mahdollisilta uhilta ja haavoittuvuuksilta, kun taas kyberturvallisuuteen liittyy keskeisesti kyberavaruudessa toimivien toimijoiden ja resurssien suojaaminen. Tällaiset toimijat tai resurssit voivat vaihdella kyberturvallisuudessa henkilöistä kodinkoneisiin, ja edelleen esimerkiksi kansalliseen kriittiseen infrastruktuuriin. Tietoturvallisuudessa tekijään viitataan ainoastaan osana suojaamisprosessin rooleja, ei suojattavana kohteena. (von Solms & van Niekerk, 2013)

Tietoturvallisuus voidaan nähdä merkityksellisenä asiana niin yksityishenkilöille kuin organisaatioille. Yksityishenkilöiden osalta tietoturvallisuus voi tarkoittaa esimerkiksi heitä koskevien tietojen asianmukaista suojaamista ja käyttöä. Yritysten ja muiden organisaatioiden osalta kyse on koko organisaatiota koskettavasta asiasta: Tietoturvallisuus on vahvasti liitoksissa organisaation kaikkiin toimintoihin, ja se voidaankin nähdä prosessina, jota ei voi ostaa valmiina tuotteena, vaan joka tulee luoda ja kehittää organisaatiokohtaisesti. (Soomro ym., 2016; von Solms & van Niekerk, 2013) Siksi organisaatiot hyödyntävät

lisääntyvissä määrin tietoturvallisuuden hallintajärjestelmiä suojaamaan tärkeimpiä resurssejaan. Näiden hallintajärjestelmien luomiseksi on olemassa ohjeistuksia sekä kansainvälisiä standardeja kuten ISO27001. Erilaisten ohjeiden tehtävänä on parantaa organisaation tietoturvaa tarjoamalla suosituksia esimerkiksi tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin. Hallintajärjestelmään sisältyy aiemmin kuvatun riskienhallinnan prosessiin pohjautuen esimerkiksi tietoturvapolitiikat, ympäristön turvallisuuden hallinta, henkilöstön koulutus, liiketoiminnan turvallisuuden tarkastelu, sekä erilaiset tekniset menettelyt kuten tietoverkkojen ja järjestelmien turvallisuuden hallinta ja valvonta. (SFS, 2022) Hallintajärjestelmiin voi lisäksi kuulua esimerkiksi tietoturvavalvomot, joissa digitaalista toimintaympäristöä voidaan valvoa keskitetysti (Kowtha ym., 2012).

Digitaalisen ympäristön osana tietoturvalla ja tietoturvallisuudella voidaan tarkoittaa erilaisia järjestelyjä edellä mainittujen luottamuksen, eheyden ja saatavuuden varmistamiseksi digitaalisessa ympäristössä. Tällaisia järjestelyjä ovat esimerkiksi digitaalisen tiedon salaaminen ja varmuuskopiointi, sekä palomuurin, virustorjuntaohjelmiston ja varmenteiden käyttö. Lisäksi tietoturvaan liittyy tietoa käsittelevien laitteistojen, ohjelmistojen, sekä tietoliikenteen turvaaminen. (Sanastokeskus TSK ry, 2018)

2.3 Tietosuoja

Tietosuoja käsitteenä on muuttunut historian aikana, mutta nykyisin tietosuojalla viitataan yksittäisen ihmisen yksityisyyden suojelemiseen ja yksilöä koskevien tietojen suojaamiseen oikeudettomalta käytöltä (Tieteen termipankki, 2024). Tietosuojan konsepti on ollut olemassa ennen tieto- ja viestintätekniikkaa, mutta nämä teknologiat ovat muuttaneet merkittävästi siihen liittyviä tapahtumia, vaikutuksia ja hallintakeinoja: jo 1980-luvulla Mason (1986) esitti, että tiedon lisääntynyt käyttö informaatioteknologian avulla aiheuttaa neljä ongelmaa: tiedon yksityisyys, tarkkuus, omistajuus ja saatavuus voivat olla uhattuna (Mason, 1986). Tietosuoja nähdään nykyisin ihmisoikeutena, ja Euroopan uusi tietosuoja-asetus GDPR paransikin huomattavasti rekisteröidyn oikeuksia ja asetti uusia velvollisuuksia henkilötietoja käsitteleville organisaatioille. (Euroopan parlamentin ja neuvoston asetus 2016/679)

Keskeisenä terminä tietosuojaan liittyy henkilötieto, jolla tarkoitetaan EU:n yleisen tietosuoja-asetuksen mukaan:

> ”Kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.”

Henkilötietoja ovat siis kaikki tiedot, jotka liittyvät suoraan luonnolliseen henkilöön. Tällaisia tietoja ovat mm. terveystiedot sekä arkaluontoiset henkilötiedot kuten henkilötunnus. (EU 2016/679:3)

Organisaatiot haluavat usein hyödyntää henkilötietoja paremman asiakaskokemuksen sekä lisäarvon tuottamiseen. Tietoa voidaan käsitellä eri tarkoituksissa ja organisaation osissa, kuten markkinoinnissa, tilausten käsittelyssä, myynnin apuna, hinnoittelussa ja johtamisessa (Chen & Popovich, 2003). Henkilötietoihin liittyvät rekisteröidyn oikeudet ja organisaatioiden halu hyödyntää henkilötietoja voivat kuitenkin olla ristiriitaisia. Henkilötietojen käsittelyyn on saatava suostumus rekisteröidyltä, ja rekisteröidyllä on oikeus peruttaa suostumuksensa. Lisäksi rekisteröidylle on ilmoitettava tietojen käsittelyn muutoksista ja siirroista. Siksi julkisilta-, ja muilta organisaatioilta, jotka käsittelevät laajamittaisesti henkilötietoja, vaaditaan muiden käsittelysääntöjen ohella myös tietosuojavastaavan nimittämistä. Tietosuojavastaavan tehtävänä on huolehtia tietosuojan alaisten henkilötietojen käsittelyn asianmukaisuudesta ja lainmukaisuudesta, sekä toimia valvontaviranomaisten yhteyspisteenä käsittelyyn liittyvissä asioissa. (EU 2016/679:3)

Digitaalisen turvallisuuden osa-alueena tietosuojalla tarkoitetaan ihmisten yksityisyyden suojelemista, sekä yksilöä koskevien tietojen suojaamista oikeudettomalta käytöltä digitaalisessa ympäristössä (Tieteen termipankki, 2024; Valtiovarainministeriö, 2020). Teknologian nopea kehitys on tuonut mukanaan uusia haasteita henkilötietojen suojeluun. Tietosuojan tärkeys ja merkitys ovat kasvaneet kommunikoinnin ja tietojen välityksen digitalisoituessa. Tietoja voidaan kerätä, koota ja analysoida nopeammin kuin koskaan, joten niiden hyödyntäminen myös vääriin tarkoituksiin on aiempaa tehokkaampaa. Väärinkäyttöä voi tapahtua esimerkiksi hyödyntämällä tietoa eri tarkoituksiin kuin niitä on alun perin kerätty, tai hyödyntämällä niitä luvattomien pääsyoikeuksien saamiseksi. (Bélanger & Crossler, 2011)

3 TOIMINNAN JATKUVUUDEN HALLINTA JA VARAUTUMINEN

Vaikka organisaatio olisi tunnistanut riskit, arvioinut niiden vakavuuden ja asettanut ne seurantaan, yllättävät tapahtumat voivat silti aiheuttaa toiminnan keskeytyksen. Esimerkiksi laiterikot, kyberhyökkäykset tai ongelmat palveluiden saatavuudessa voivat aiheuttaa yllättäviä katkoksia yrityksen toimintaan. Jotta toiminnot voitaisiin käynnistää uudelleen mahdollisimman pian ja vaivattomasti, on keskeistä suunnitella etukäteen, miten tilanteissa toimitaan. Jatkuvuuden hallinta tunnetaan yleisesti yhtenä tehokkaimmista tavoista, joilla organisaatio voi nopeuttaa palautumistaan riskien aiheuttamista vahingoista (Charoenthammachoke, Kodaka, Tang & Leelawt, 2020). Tässä luvussa kuvataan toiminnan jatkuvuuden hallinnan ja varautumisen teoriaa sekä sen asemoitumista edellä kuvatun digitaalisen turvallisuuden osa-alueena. Luku toimii teoriapohjana myöhemmin tutkielmassa toteutettavalle empiiriselle tutkimukselle. Luvussa jatkuvuuden hallinnan teoriaa kuvataan erilaisten mallien kautta, joita on valittu tarkasteltavaksi 3 kappaletta.

3.1 Jatkuvuuden hallinnan määritelmiä ja perusteita

Kirjallisuus liiketoiminnan palauttamiseksi katastrofeista yltää 1970-luvulle saakka, jolloin digitaalisen vallankumouksen katsotaan alkaneen; uuden informaatioteknologian myötä organisaatiot alkoivat kiinnittää huomiota sähköisen tietojenkäsittelyn haavoittuvuuteen. Tämän aikakauden jälkeen organisaatioiden kriisien tunnistamisessa, niiden hallinnassa ja niistä toipumisessa on tunnistettu useita eri kehitysvaiheita ja käytäntöjä, jotka ovat johtaneet nykyisenkaltaisen liiketoiminnan jatkuvuuden hallinnan syntyyn. (Herbane, 2010) Nykyaikaista jatkuvuuden hallintaa koskevassa kirjallisuudessa esiintyy käsitteelle hieman erilaisia määritelmiä –näiden käsitteiden merkitystä ja sisältöä avataan tässä kappaleessa.

Tutkielmassa aiemmin esitellyssä Valtiovarainministeriön (2020) digitaalisen turvallisuuden kokonaisuudessa jatkuvuuden hallinnasta puhutaan termin ”varautuminen” kanssa osana ”jatkuvuuden hallinta ja varautuminen” osa-aluetta. Jatkuvuuden hallinta ja varautuminen määritellään organisaation prosessiksi, jolla tunnistetaan toiminnan uhkat ja arvioidaan niiden vaikutukset organisaatiossa ja sen toimijaverkostossa sekä luodaan toimintatapa häiriötilanteiden hallinnalle ja toiminnan jatkuvuudelle olosuhteista riippumatta. Jatkuvuuden hallinta ja varautuminen on siis digitaalisen turvallisuuden osaprosessi, jonka tehtävänä on turvallisuuden kehittäminen ja jonka tavoitteena on tila, jossa kybertoimintaympäristöön voidaan luottaa ja sen toiminta turvataan. (Valtiovarainministeriö, 2020)

Niin ikään Valtiovarainministeriön (2016) julkaisemassa VAHTI-ohjeessa jatkuvuuden hallinta nähdään osana organisaation kokonaisturvallisuutta. Muita kokonaisturvallisuuden osioita ovat VAHTI-ohjeen mukaan mm. jatkuvuussuunnittelu, turvallisuusjohtaminen, riskienhallinta, häiriötilanteiden hallinta ja johtaminen, tilannekuvan muodostaminen sekä huoltovarmuus ja varautuminen. Ohjeessa jatkuvuuden hallinnasta ja -suunnittelusta puhutaan erillisinä termeinä. Nämä kaksi termiä sisältävät ohjeen mukaan osittain samoja toimia, mutta jatkuvuuden hallinta voidaan kuitenkin nähdä jatkuvuussuunnittelusta erillisenä esimerkiksi vuosikelloon sidottavissa olevana osana organisaation toimintaa. Jatkuvuuden hallinnan prosessin osioita ovat jatkuvuussuunnitelman luomisen jälkeen säännölliset tarkastukset, auditoinnit, testaaminen, budjetointi, raportointi sekä tarvittaessa päivittäminen. Jatkuvuussuunnittelun tavoitteena on VAHTI-ohjeen mukaan varmistaa organisaation ydintoimintojen mahdollisimman häiriötön toiminta kuvailemalla esimerkiksi varajärjestelyt ja toimenpiteet, jotka parantavat toimintaa häiriötilanteissa ja toipumista ongelmista. Edelleen sen tulee noudattaa johdon hyväksymiä jatkuvuuden hallinnan periaatteita, toteuttaa tarvittavat toimenpiteet toiminnan jatkuvuuden varmistamiseksi sekä ottaa huomioon toimintaympäristön ja sidosryhmien vaatimukset. (Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, 2016) Jatkuvuussuunnitteluun kuuluu siis ennen kaikkea proaktiivisia toimia ja suunnitelmia, jotka parantavat organisaation toimintaa häiriötilanteissa, ja edesauttavat niistä palautumista.

Niemimaa ym. (2019) ja Järveläinen (2013,2020) ovat tutkineet jatkuvuuden hallintaa useista eri näkökulmista painottuen IT-palveluita koskevaan jatkuvuuden hallintaan. Niemimaan ja Järveläisen tutkimuksissa jatkuvuuden hallinnasta puhutaan yleensä termillä liiketoiminnan jatkuvuuden hallinta, joka viittaa siihen, että näkökulma kattaa tietoturvallisuuden ja teknisten näkökohtien lisäksi myös liiketoimintaan liittyvät kysymykset (Gibb & Buchanan, 2006; Järveläinen, 2013). Heidän tutkimuksissaan jatkuvuuden hallinta tarkoittaa proaktiiviseen toimintaan pohjautuvia sosioteknisiä keinoja, joilla organisaation toimintojen jatkuvuus varmistetaan. Sosiaalisiin keinoihin kuuluvat heidän mukaansa esimerkiksi riskien tunnistaminen, valmius ja roolien jakaminen. Teknisiin keinoihin taas lukeutuvat esimerkiksi varmuuskopiot sekä infrastruktuurin ja muun omaisuuden redundanssi. (Järveläinen, 2020; Niemimaa ym., 2019; Niemimaa & Järveläinen, 2013) Niemimaan ja Järveläisen (2013) mukaan IT-palveluiden

jatkuvuuden hallinta voidaan määritellä koko organisaation kyvyksi jatkaa ennalta määrättyjen ja sovittujen IT-palveluiden tuottamista tai hyödyntämistä liiketoiminnan vaatimusten tukemiseksi keskeytyksen jälkeen. Lisäksi jatkuvuuden hallinta ei ole vain suunnitelma jatkuvuuden toteuttamiseksi, vaan kyvykästä organisaation toimintaa sekä yksilö- että ryhmätasolla (Niemimaa & Järveläinen, 2013). Voidaan siis nähdä, että Niemimaan ja Järveläisen (2013) mukaan IT-palveluiden jatkuvuuden hallinta on laajentunut koskemaan informaatioteknologian lisäksi myös sosiaalisia järjestelmiä sekä yrityksen muuta omaisuutta.

Liiketoiminnan jatkuvuuden hallinnan suurin julkaisu, Disaster Recovery Journal kuvaa jatkuvuuden hallintaa kattoterminä erilaisille suunnitelmille ja toimenpiteille, joilla varmistetaan yrityksen liiketoiminnan resilienssi. Liiketoiminnan jatkuvuuden hallinta koostuu organisaation valmiudesta hätätilanteisiin, kriisien hallinnasta, liiketoiminnan jatkuvuuden varmistamisesta, katastrofeista palautumisesta sekä toimittajien jatkuvuuden varmistamisesta. Julkaisun mukaan mikään näistä osa-alueista ei yksin varmista resilienttiä liiketoimintaa, vaan kaikki aihealueet tulee ottaa huomioon. Toimivaa jatkuvuuden hallintaa ei voida julkaisun mukaan saavuttaa ilman seuraavia organisaation sisäisiä ominaisuuksia:

- osaava, riittävästi koulutettu ja korkean varautumistason omaava henkilökunta
- yksinkertainen, tarkka ja toteuttamiskelpoinen jatkuvuussuunnitelma
- sekä saatavilla olevat, toimivat ja tarkoituksenmukaiset resurssit.

Lisäksi julkaisussa korostetaan, että jatkuvuuden hallintaa ei voida toteuttaa kaikissa organisaatioissa samalla tavalla, vaan se tulee olla suunniteltu organisaation tarpeet ja kyvykkyydet huomioiden, jotta haasteisiin ja vastoinkäymisiin voitaisiin vastata minimaalisin seurauksin. (Lambert, 2022)

3.2 Toiminnan jatkuvuuden ja varautumisen malleja

Jatkuvuuden hallintaan ja varautumisen toteuttamiseen on julkaistu useita viitekehyksiä jotka muistuttavat laajasti toisiaan, korostaen kuitenkin tiettyjä näkökohtia. Tässä kappaleessa esitellään niistä kolme: Niemimaan ja Järveläisen (2013) yleisiin jatkuvuussuunnittelun vaiheisiin perustuva malli, Valtioneuvoston julkaisemassa Julkisen hallinnon tietoturvallisuuden arviointikriteeristössä (myöh. Julkri) esitetty malli, sekä ISO 22301 -standardissa esitelty Plan-Do-Check-Act (PDCA) malliin pohjautuva jatkuvuuden hallinta. Mallit on pyritty valitsemaan siten, että ne kuvaisivat erilaisilla lähestymistavoilla toteutettua jatkuvuuden hallintaa: Niemimaa ja Järveläinen (2013) tarjoavat tutkimuksiin pohjautuvia näkökulmia jatkuvuuden hallintaan, Julkri-mallia hyödyntävät julkista hallintotehtävää toteuttavat tahot, ISO 22301 -standardi on yleisesti käytössä oleva ja tunnettu standardi kaiken tyyppisissä organisaatioissa, ja siihen liittyy sertifikaatti, jota organisaatio voi hyödyntää parantaakseen sidosryhmien luottamusta.

Lisäksi valittujen jatkuvuuden hallinnan mallien tuli olla hyödynnettävissä erityyppisissä organisaatioissa: Niemimaa & Järveläinen (2013) eivät ole rajanneet mallinsa kohderyhmää ja malli perustuu useista näkökulmista tehdyille tutkimuksille, Julkria voivat hyödyntää julkisen hallinnon organisaatioiden ohella soveltuvasti myös yksityisen sektorin organisaatioissa, ja ISO 22301 -standardissa mainitaan sen sopivan kaiken kokoisille ja tyyppisille organisaatioille (ISO 2019,Valtiovarainministeriö, 2022). Malleista voidaankin havainnoida samoja jatkuvuuden hallinnan vaiheita, kuten politiikan määrittely, riskien tunnistaminen ja vaikutusten arviointi, jatkuvuussuunnitelman kehittäminen ja muotoilu, jatkuvuussuunnitelman luominen, sekä testaaminen ja harjoittelu. Lisäksi mallien valitsemisen kriteerinä oli niiden soveltuminen nykyaikaiseen, digitalisoituneeseen toimintaympäristöön: jatkuvuuden hallinta on laajentunut koskemaan myös yrityksen digitaalista omaisuutta, ja täten pelkästään fyysistä maailmaa koskeviin riskeihin varautuminen ei yleensä varmista yrityksen toiminnan jatkuvuutta. Tämän tutkielman kannalta on lisäksi olennaista, että malleja voidaan hyödyntää myös pilvipalveluita koskevaan jatkuvuuden hallinnan suunnitteluun.

3.2.1 Niemimaan ja Järveläisen malli

Niemimaa ja Järveläinen (2013) esittelivät konferenssipaperissaan kolmeen tietojärjestelmätieteen tutkimukseen pohjautuvan mallin. Mallin muodostamisessa hyödynnetyt tutkimukset ovat Lindströmin ym. (2010), Bothan ja Von Solmsin (2004) sekä Gibbin ja Buchanan (2006) laatimia. Toteuttajat ovat tunnettuja jatkuvuussuunnittelun tutkijoita ja edellä mainittuihin tutkimuksiin on viitattu yhteensä yli 500 kirjallisessa lähteessä (Google Scholar, 2022a, 2022b, 2022c). Tutkimusten pohjalta toteutettu malli sisältää kaikki yleiset jatkuvuussuunnittelun vaiheet ja se huomioi jatkuvuuden hallintaa IT-palveluiden näkökulmasta muita tässä tutkielmassa esiteltyjä malleja enemmän (Niemimaa & Järveläinen, 2013). Mallin yksityiskohtien avaamiseksi on lisäksi hyödynnetty Herbanen ym. (2004) toteuttamaa tutkimusta, johon on viitattu yli 360 kertaa.

Jatkuvuuden hallinta ja varautumisen prosessi aloitetaan Niemimaan ja Järveläisen (2013) mukaan määrittämällä organisaation kyseisiä asioita käsittelevä politiikka. Politiikalla tarkoitetaan tässä yhteydessä kirjallista yleiskuvausta jatkuvuuden hallintaan liittyvän toiminnan tavoitteista, vastuista, resursseista, sekä muista käytänteistä. Politiikka tarkastetaan ja hyväksytään organisaation johdon toimesta. Tämä mahdollistaa johdon tuen, riittävän rajauksen, sekä valtuudet toteuttaa jatkuvuuden hallintaa ja varautumista. (Niemimaa & Järveläinen, 2013)

Toisena vaiheena jatkuvuuden hallintaan kuuluu olemassa olevien riskien tunnistaminen ja niiden vaikutusten arviointi omalle liiketoiminnalle. Tavoitteena on hahmottaa jatkuvuuden hallinnan strateginen arvo ja ymmärtää millaisia vaikutuksia riskien toteutumisella voi olla, sekä lisätä organisaation osastojen tietoisuutta jatkuvuudesta ja siitä, mitä palveluita on erityisesti suojattava, jotta häiriöiden vaikutukset liiketoimintaan minimoidaan. (Herbane ym., 2004; Niemimaa & Järveläinen, 2013)

Kolmannessa vaiheessa kehitetään ja muotoillaan jatkuvuussuunnitelman ääriviivat sekä laaditaan sen kehittämistä koskevat suunnitelmat. Rutiinitehtävien osalta suunnitelmien tulee olla riittävän yksityiskohtaisia, jotta kriisitilanteessa myös toisten työntekijöiden tehtävien suorittaminen on mahdollista (Lindström ym., 2010). Suunnitelman tulee lisäksi sisältää useita erilaisia skenaarioita, ja sille tulee nimetä avainhenkilöt, jotka hallinnoivat ja kehittävät suunnitelmaa (Moyer & Novick, 2012; Niemimaa & Järveläinen, 2013). Herbanen ym. (2004) mukaan suunnitelmakehys on hyvä laatia yhdessä eri viiteryhmien kesken, koska tämä todennäköisesti lisää organisaation työntekijöiden myöhempää sitoutumista suunnitelman noudattamiseen.

Neljäs vaihe on jatkuvuussuunnitelman laatiminen. Tässä vaiheessa luodaan yksityiskohtaiset toimintasuunnitelmat jokaiselle skenaariolle. Suunnitelmat ovat vahvasti toiminnan ohjaamiseen painottuvia ja valmistavat täten organisaatiota vastaamaan erilaisten skenaarioiden toteutumiseen käytännön tasolla. Lisäksi vaiheeseen voidaan sisällyttää suunnitelman implementointi organisaation it-palveluiden käytänteisiin, infrastruktuuriin sekä turvallisuusmenetelmiin. (Gibb & Buchanan, 2006; Niemimaa & Järveläinen, 2013)

Viides vaihe koostuu jatkuvuussuunnitelmien testauksesta sekä henkilöstön kouluttamisesta. Jatkuvuussuunnitelmat tulee testata säännöllisesti ja kattavasti, jotta voidaan varmistua niiden ajantasaisuudesta ja kattavuudesta. Gibbin ja Buchanan mukaan (2006) suunnitelmien testaus olisi suoritettava kolmen kuukauden kuluessa niiden käyttöönotosta, ja sen jälkeen vähintään vuoden välein. Testaus voidaan toteuttaa eri tavoin:

- Pöytätestauksena, jossa esimerkiksi menettelytavat, yhteystiedot, kutsupuut, suunnitelmien ja sen osien tunteminen sekä vaaditut aikamääreet häiriötilanteessa tarkistetaan ja niihin tehdään mahdolliset korjaukset sekä tarkennukset.
- Teknologiaan keskittyvänä testauksena, jossa varmistetaan laitteistojen toimivuus ja niiden resurssien riittävyys. Tällaisia laitteita ovat esimerkiksi varmuuskopiointiin ja virransyötön häiriötilanteisiin liittyvien laitteiden testaus.
- Prosesseihin tai palveluihin keskittyvänä testauksena, jossa arvioidaan henkilöstön kykyä vastata uhkiin tai tapahtumiin ja heidän palatumistaan niistä. Samanaikaisesti voidaan arvioida kuinka tarkasti henkilöstön jäsenet noudattavat jatkuvuussuunnitelmaa. (Gibb & Buchanan, 2006)

Viidenteen vaiheeseen kuuluvalla kouluttamisella varmistetaan, että jatkuvuussuunnittelun hyödyt ja tavoitteet ovat työntekijöille selkeitä. Lisäksi kouluttamisella pyritään laajemmin jatkuvuuden hallinnan tavoitteiden saavuttamiseen. Työntekijöiden koulutuksia tulisi suorittaa 6–12 kuukauden välein, tai aina kun uusia toimintatapoja tai järjestelmiä otetaan käyttöön. (Niemimaa & Järveläinen, 2013)

Viimeisenä vaiheena Niemimaan ja Järveläisen (2013) mallissa on ylläpitäminen ja päivittäminen. Vaiheen tarkoituksena on varmistua siitä, että jatkuvuussuunnitelmat vastaavat liiketoimintaympäristössä tapahtuneita muutoksia.

Organisaatiot kehittyvät ajan kuluessa, ja ilman suunnitelmien päivittämistä ja ylläpitoa ne eivät välttämättä enää vastaa organisaation tarpeita. Päivitettäessä jatkuvuuden hallintaa, tulee varmistaa esimerkiksi jatkuvuussuunnitelman dokumentaation ajantasaisuus, johdon ja muiden sidosryhmien sitoutuminen, sekä työntekijöiden tietoisuus rooleista, vastuista ja toimintaohjeista. Lisäksi tämä vaihe voidaan nähdä aloitusvaiheena erilliselle ylläpitämiseen liittyvälle prosessille, jonka säännönmukaisella noudattamisella varmistutaan edellä mainittujen tavoitteiden saavuttamisesta. (Lindström ym., 2010; Niemimaa & Järveläinen, 2013) Mallin kaikki vaiheet on kuvattu alla olevassa kuviossa 2.

KUVIO 2 Niemimaan ja Järveläisen malli (Niemimaa & Järveläinen, 2013)

3.2.2 Julkrissa esitetty jatkuvuuden ja varautumisen malli

Julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019) on säädetty julkista hallintotehtävää hoitaville organisaatioille tietoturvallisuustoimenpiteisiin liittyvistä vastuista ja vähimmäistasosta, tietototurvallisuuteen liittyvän

toimintaympäristön seuraamisesta, sekä velvollisuudesta varmistaa tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan (Valtiovarainministeriö, 2022). Lainsäädännön vaatimuksien täyttämiseksi Valtiovarainministeriö (2022) on laatinut arviointikriteeristön nimeltä Julkri. Julkrin käyttö tukee käyttäjiä tietoturvallisuuden ja henkilötietojen suojaamisen suunnittelussa, toteuttamisessa ja arvioinnissa. Julkri koostuu viidestä osa-alueesta, jotka muodostuvat pääkriteereistä ja niitä täydentävistä alakriteereistä. Pääkriteerit ovat hallinnollinen turvallisuus, fyysinen turvallisuus, tekninen turvallisuus, tietosuoja, ja tässä tutkielmassa esiteltävä osuus varautuminen ja jatkuvuuden hallinta. Julkrissa organisaation turvallisuus nähdään joukkona kriteereitä, jotka on täytettävä, jotta osa-alueen tavoitteet täytetään. Kriteeristön hyödyntämistä varten on luotu ohjelmistosovelluksilla käytettävä työkalu, jossa voi määritellä esiehdot ja tarkastella niihin perustuvia kriteereitä, sekä täydentää omaa edistymistä kriteerien täyttämiseksi. Valintojen jälkeen kriteerit jaetaan olennaisiin ja valinnaisiin. Kriteeri on olennainen, jos se on yhdenkin turvallisuusnäkökulman (luottamuksellisuus, eheys, saatavuus tai tietosuoja) perusteella olennainen. Lisäksi kriteeristöön liittyvässä työkalussa voi valita erilaisia käyttötapauksia, kuten asiantuntijatyön hankinta tai pilvipalvelun arviointi. (Valtiovarainministeriö, 2022).

Tämän tutkielman kannalta olennaiseen varautumisen ja jatkuvuuden hallinnan osa-alueeseen on koottu varautumista ja jatkuvuuden hallintaa normaalioloissa koskevia kriteereitä. Osa-alueen kriteerit koskevat pääosin saatavuudeltaan tärkeiksi tai kriittisiksi luokiteltuja kohteita. Saatavuudella tarkoitetaan Julkrissa sitä, miten tieto, tietojärjestelmä tai palvelu on hyödynnettävissä haluttuna aikana ja halutulla tavalla. Saatavuuden tasot ovat jaettu Julkrissa neljään kriittisyystasoon: vähäinen, normaali, tärkeä ja kriittinen. Vähäisen saatavuuden tasoon esimerkiksi IT-järjestelmien osalta voidaan luokitella henkilöstön pysäköintipaikkojen rekisteri ja kriittiseen saatavuuden tasoon esimerkiksi käyttäjän tunnistamiseen liittyvät palvelut. Vähäisen saatavuustason järjestelmiltä voidaan hyväksyä useita viikkoja kestäviä häiriöitä, kun taas kriittisen saatavuustason palveluiden häiriöistä tulee palautua minuuteissa. Kriteerien toteuttamisen järjestys on määritelty siten, että organisaatio tutustuu ensin varautumista ohjaavaan lainsäädäntöön ja määrittelee jatkuvuusvaatimukset. Näiden valmistuttua muiden osa-alueen kriteerien suunnittelulle ja toteutukselle ei ole määritelty suoritusjärjestystä. (Valtiovarainministeriö, 2022) Varautumisen ja jatkuvuuden hallinnan pääkriteerit, alakriteerit sekä niiden kuvaukset ja vaatimukset on kuvattu alla olevassa taulukossa 1.

TAULUKKO 1 Varautumisen ja jatkuvuuden hallinnan kriteerit (Valtiovarainministeriö, 2022)

Kriteeri	**Kuvaus**	**Vaatimus**
Varautumista ohjaava lainsäädäntö	Lainsäädäntö luo minimivaatimukset varautumiselle ja jatkuvuussuunnittelulle. Siksi organisaation tulee tuntea lainsäädäntö, sekä tunnistaa omat erityispiirteensä.	Organisaatio on tunnistanut toimintaansa ja palveluihinsa liittyvän ICT-varautumista koskevan lainsäädännön sekä kansallisella että EU: tasolla, sekä huomioinut

		muut ICT-varautumiseen liittyvät normit.
Jatkuvuusvaatimusten määrittely	Jatkuvuusvaatimuksilla määritetään palvelun tai järjestelmän palautumisajan tavoitteet, sekä miten paljon, tai kuinka pitkältä ajalta tietoa voidaan menettää. Tämän kriteerin alla on alakriteeri palveluiden kotiuttamista tai siirtoa koskeville vaatimuksille: palvelua hankittaessa tulee huomioida, että palvelua voi olla hankala kotiuttaa eli toteuttaa oman organisaation resursseilla tai siirtää toiselle palveluntarjoajalle.	Jatkuvuusvaatimukset on määritelty yhteistyössä riskienhallinnan, tietoturvan, tietosuojan, toiminnan sekä arkkitehtuurin kanssa. Ydintoimintojen ja -prosessien suojattavat palvelut ja järjestelmät on tunnistettu ja niille on asetettu saatavuustavoitteet em. prosessien mukaisesti.
Jatkuvuussuunnitelmat	Organisaation jatkuvuussuunnitelma on dokumentti, joka sisältää kuvauksen siitä, miten toiminta järjestetään jatkuvuutta uhkaavissa tilanteissa. Jatkuvuussuunnittelussa tunnistetaan ne palvelut, joista organisaation ydintoiminnot ovat riippuvaisia sekä arvioidaan mitä vaikutuksia ICT-palveluiden eripituisilla katkoilla on. Jatkuvuussuunnitelmassa voidaan esittää esimerkiksi käytettävissä oleva henkilöstö, avainhenkilöt ja heidän varahenkilönsä, sekä arvio varahenkilöiden saatavuudesta. Toiminnallisina ohjeina voidaan kuvata, miten häiriötilanteissa toimitaan ja viestitään, sekä kuinka häiriön jälkeen siirrytään takaisin normaaliin toimintaan. Kriteerin alla on alakriteeri jatkuvuussuunnitelmien säännölliselle testaamiselle ja harjoittelulle.	Jatkuvuussuunnitelma tulee laatia ja ottaa käyttöön. Jatkuvuussuunnitelmia tulee testata ja harjoitella säännöllisesti.
Resurssit ja osaaminen	Resurssien ja osaamisen varmistamisella tavoitellaan sitä, että jokainen työntekijä tuntee organisaation periaatteet koskien varatumista, sekä tietää oman tehtävänsä erilaisissa tilanteissa.	Henkilöt tuntevat omaan toimintaan liittyvät jatkuvuus- ja toipumissuunnitelmat, ja osaavat toimia niiden mukaan.
Henkilöstön saatavuus ja varajärjestelyt	Kriteerillä pyritään varmistamaan henkilöstön saatavuus häiriötilanteissa. Organisaatio voi tarvittaessa selvittää mitä lainsäädännöllisiä keinoja sillä on esimerkiksi lakko-oikeuksien poistamisen, hätätöiden käytön ja henkilövarausten osalta.	Organisaatio on suunnitellut henkilöstön saatavuuden, niihin liittyvät varajärjestelyt, sekä vaihtoehtoiset toimintatavat kriittisten tehtävien suorittamiseksi erityistilanteissa.
Tietoliikenteen varmistaminen	Tietoliikenteen varmistamisella ehkäistään palvelun saatavuuden ongelmia häiriötilanteissa. Tärkeiden palveluiden verkkoympäristöt ja tietoliikennepalvelut voidaan kahdentaa, ja varmistaa että yksittäisen tietoliikennekomponentin vikaantuminen ei keskeytä koko palvelun toimintaa.	Tietoliikennettä koskevissa palveluissa ja -sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus häiriötilanteissa.

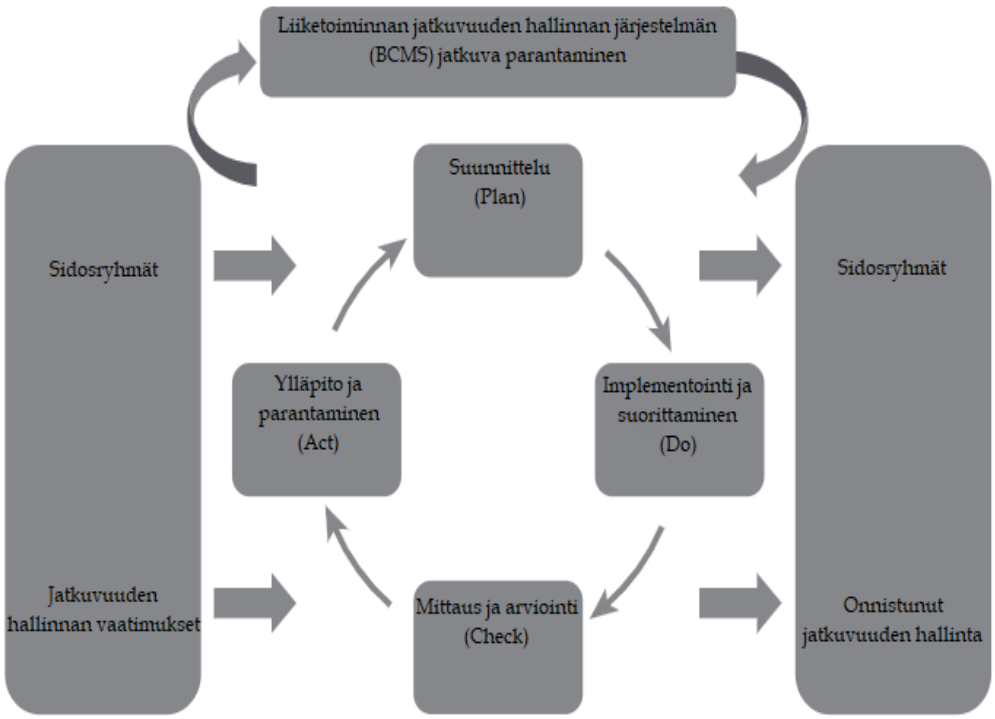
Tietoteknisten ympäristöjen varmentaminen	Kriteerillä pyritään varmistumaan siitä, että tärkeiden palveluiden tietotekniset ympäristöt eivät vikaannu niin, että ne aiheuttaisivat toiminnan edellyttämää palvelutasoa pidempiä käyttökatkoja.	Tietoteknisissä ympäristöissä ja niihin liittyvissä sopimuksissa on huomioitu toiminnan kannalta tärkeiden palveluiden saatavuus.
Vikasietoisuus	Järjestelmien vikasietoisuudella pyritään nopeaan palautumiseen silloin, jos jokin järjestelmän osa vikaantuu. Vikasietoisuutta voidaan parantaa esimerkiksi kahdentamalla järjestelmiä, säilyttämällä tietoa eri paikoissa, sekä ottamalla järjestelmistä suojakopioita. Kriteerin alla on alakriteeri riippuvuuksien vikasietoisuuden varmistamiseen: organisaation tulisi tunnistaa kriittiset palvelut sekä niihin liittyvät palveluketjut ja varmistaa että koko palveluketju on toteutettu riittävän vikasietoisesti.	ICT-infrastruktuuri sekä olennaiset tietojärjestelmät on toteutettu vikasietoiseksi ja käyttövarmoiksi riskiarvioon pohjautuen. Lisäksi eri palveluiden riippuvuudet muista palveluista ja toimijoista on otettu huomioon tietojenkäsittely-ympäristön ja sen vikasietoisuuden suunnittelussa.
Tietojärjestelmien toipumissuunnitelmat	Tietojärjestelmien toipumissuunnitelmiin määritellään organisaation toiminnan kannalta tärkeiden tietojärjestelmien häiriötilanteista palautumisen suunnitelmat. Minimitasot ICT-järjestelmien toimivuudelle voidaan määritellä jo SLA-sopimuksissa, mutta lisäksi ne voidaan määritellä toipumissuunnitelmassa.	Toipumissuunnitelmat on laadittu organisaation toiminnan kannalta tärkeiden tietojärjestelmien palauttamiseksi.

3.2.3 ISO 22301 -standardissa esitetty malli

ISO 22301 -standardissa jatkuvuuden hallinta nähdään osana laajempaa liiketoiminnan jatkuvuuden hallinnan järjestelmää. Hallintajärjestelmä auttaa organisaatiota tunnistamaan toimintaa uhkaavat riskit, pienentämään niiden todennäköisyyttä, sekä varautumaan ja reagoimaan häiriöihin ja palautumaan niistä. (International Organization for Standardization, 2019; SFS, 2023) Kokonaisvaltaisen järjestelmän avulla varmistetaan, että häiriötilanteen sattuessa suunnitelmien ohella myös tarvittavat resurssit ovat käytettävissä (Drewitt, 2013). Jatkuvuuden hallinta nähdään ISO-standardissa ennen kaikkea liiketoimintojen suojaamiseen liittyvänä toimena: jatkuvuuden hallinnan avulla pystytään havaitsemaan tulevat uhkaavat tapahtumat ja ennakoimaan niiden seurauksia, tavoitteena suojella organisaation sidosryhmiä, mainetta, brändiä ja liiketoimintoja (Charoenthammachoke ym., 2020; Drewitt, 2013). ISO 22301- standardi ei sisällä suoraa mallia liiketoiminnan jatkuvuuden hallintaan, mutta standardissa esitellään prosessi jatkuvuuden hallinnan kehittämiseen. Prosessi pohjautuu yleisesti käytettyyn PLAN-DO-CHECK-ACT (myöh. PDCA) -malliin, johon kaikki jatkuvuuden hallinnan osa-alueet tulee olla liitettynä (Drewitt, 2013; Estall, 2012). Mallin avulla aiemmin kehitettyä liiketoiminnan jatkuvuuden hallinnan järjestelmää voidaan jatkuvasti tarkkailla ja parantaa. PDCA-malli on alun perin kehitetty

erilaisten prosessien ohjaukseen 1930-luvulla. Malli on iteratiivinen, neliosainen prosessimalli, jossa prosessia tai tuotetta pyritään jatkuvasti parantamaan toistamalla osioita systemaattisesti osana päättymätöntä sykliä. (Patel & Deshpande, 2017)

PDCA-mallin mukainen jatkuvuuden hallinnan kehittäminen alkaa suunnitteluvaiheesta (Plan), jossa luodaan jatkuvuuden hallinnan politiikka, sekä määritellään dokumentointikäytänteiden ohella valvonta- ja virallistamismenettelyt. Politiikka on olennainen osa jatkuvuuden hallintaa, koska sen avulla varmistetaan toimien laajuus, niiden johdonmukainen ja objektiivinen käyttö, sekä kuvataan mitä osia jatkuvuuden hallintaan tulee sisällyttää. (Drewitt, 2013) Seuraavassa vaiheessa (Do) suoritetaan riskianalyysi, vaikutusanalyysi, implementoidaan politiikka, kontrollointitoimenpiteet, prosessit ja menettelytavat sekä aloitetaan näiden käyttö. Kolmas vaihe on mittaus ja arviointi (Check). Vaiheessa arvioidaan liiketoiminnan jatkuvuuden tavoitteita ja politiikkaa organisaation nykytilaan, ja raportoidaan mahdollisista muutostarpeista, puutteista ja laajennetaan järjestelmää tarpeen mukaan. Arviointia voidaan toteuttaa sisäisillä auditoinneilla, johdon suorittamilla arvioinneilla, tai dokumenttien ja tietojen kattavalla läpikäynnillä. Neljäs ja viimeinen vaihe on ylläpito ja parantaminen (Act). Vaiheessa toteutetaan korjaavia toimenpiteitä, pohjautuen edellisessä vaiheessa toteutettuun arviointiin, sekä aiemmin luotuun politiikkaan ja tavoitteisiin. Vaiheessa voi olla tarpeellista jatkuvuuden hallinnan laajuuden uudelleen arviointi, esimerkiksi muuttuneen turvallisuus- tai markkinatilanteen takia. (Estall, 2012) Kuviossa 3 on kuvattu liiketoiminnan jatkuvuuden hallintajärjestelmän PDCA-malli.



KUVIO 3 Liiketoiminnan jatkuvuuden hallinnan PDCA-malli (Estall, 2012, s. 9 mukaillen)

4 PILVIPALVELUT

Tiedon käsittelyyn ja tallentamiseen liittyvä teknologia on kehittynyt nopeasti viime vuosina. Tämä kehitys yhdessä internetin kehittymisen ja leviämisen kanssa on mahdollistanut uusia, ennen näkemättömän tehokkaita tapoja hyödyntää laskenta- ja tallentamistekniikoita. Yksi näistä tekniikoista on pilvilaskenta (Cloud Computing), josta tässä tutkielmassa käytetään sen toista yleistynyttä termiä: pilvipalvelut. (Avram, 2014) Tässä luvussa avataan pilvipalvelun määritelmä, kuvataan erilaisia pilvipalveluiden toteutus- ja palvelumalleja, sekä käsitellään pilvipalveluihin liittyvää jatkuvuuden hallintaa. Luku toimii edellisen luvun ohella teoriakehyksenä tutkielmassa toteutettavalle empiiriselle tutkimukselle.

Pilvipalvelut tarkoittavat resurssien kuten laskentatehon ja tallennustilan tarjoamista internetin välityksellä. Pilvipalvelut eivät siis teknologisesti ole uusi asia, vaan monien olemassa olevien teknologioiden yhdistelmä: kehitysaskeleet laskentatehossa, virtualisointitekniikassa, tallennuksessa, palvelimissa ja laajakaistaisissa internet-yhteyksissä ovat mahdollistaneet pilvipalveluiden olemassaolon. Edellä mainittuja teknologioita ei ole suunniteltu alun perin yhtenäiseksi kokonaisuudeksi, mutta pilvipalveluissa ne yhdistyvät toteuttaen näin teknisen ekosysteemin pilvipalveluille. (Avram, 2014)

Pilvipalveluiden tunnusmerkeistä on olemassa useita hieman toisistaan poikkeavia määritelmiä. Kyberturvallisuuskeskuksen julkaisema pilvipalveluiden arviointikriteeristö määrittelee pilvipalvelun seuraavasti:

> Pilvipalveluilla tarkoitetaan verkon yli saavutettavaa tietojenkäsittelykapasiteettia tai -palvelua, jonka tuottamisessa hyödynnetään jaettujen, skaalautuvien ja joustavien resurssien mallia, joka on automatisoitu osin itsepalveluperiaatteella tuotettavaksi. (Kyberturvallisuuskeskus, 2020a, s. 10)

Kyberturvallisuuskeskuksen määritelmän mukaan pilvipalvelut viittaavat siis sekä sovellusten toimittamiseen palveluna, että palvelinkeskusten, laitteistojen, tallennustilan ja ohjelmistojen tarjoamiseen internetin yli. Käyttäjä ei itse omista laitteistoa jota pilvipalveluiden tuottamiseen tarvitaan, vaan laitteisto on palveluntarjoajan omistuksessa tai hallinnassa (Avram, 2014; Kyberturvallisuuskeskus,

2020a). National Institute of Standards and Technology (myöh. NIST, 2011) määrittelee pilvipalvelun malliksi, joka mahdollistaa pääsyn kaikkialta saatavilla olevaan, sopivan kokoiseen ja tarpeen mukaan muuttuvaan jaettuun joukkoon mukautettavia laskentaresursseja. Nämä resurssit voidaan ottaa nopeasti käyttöön ja vapauttaa minimaalisella hallinnollisella vaivalla tai palveluntarjoajan kanssa käytävällä vuorovaikutuksella. (Mell & Grance, 2011) Vaikka määritelmät muuallakin kirjallisuudessa eroavat hieman toisistaan, yhdistää eri määritelmiä Avramin (2014) mukaan seuraavat piirteet:

- Maksu käytön mukaan: Pilvipalvelut eivät yleensä vaadi jatkuvaa sitoutumista, vaan palveluita laskutetaan niiden käytön mukaan.
- Joustava kapasiteetti ja äärettömien resurssien illuusio: Pilvilaskenta mahdollistaa resurssien skaalautumisen tarpeen mukaan, antaen vaikutelman äärettömistä resursseista.
- Itsepalvelukäyttöliittymä: Käyttäjät voivat hallinnoida ja konfiguroida palveluita suoraan itsepalvelukäyttöliittymän kautta.
- Abstraktit tai virtualisoidut resurssit: Resurssit, kuten tallennustila tai laskentateho, ovat abstrakteja tai virtualisoituja, jolloin käyttäjän ei tarvitse huolehtia fyysisestä infrastruktuurista.

Yhteenvetona pilvipalveluiden voidaan olevan palveluita ja ratkaisuja, joita tuotetaan ja käytetään internetin ylitse palveluntoimittajan laitteistolla. Pilvipalvelu on teknologia, joka hyödyntää ja yhdistää useita eri teknologioita sekä internetiä tiedon tallentamiseen ja sovellusten tuottamiseen.

Pilvipalveluiden suosio perustuu niiden kustannustehokkuuteen, helppokäyttöisyyteen sekä vaivattomuuteen (Hendre & Joshi, 2015). Pilvipalveluiden avulla yritykset voivat käyttää tarvitsemaansa IT-infrastruktuuria internetin välityksellä ilman omia laskenta- tai tallennusresursseja. Näin toteutuvat pienemmät pääomakustannukset alentavat yritysten kynnystä hyödyntää esimerkiksi laskentatehoa vaativia työkaluja ja nopeuttavat useissa tapauksissa yritysten markkinoille tuloa. (Avram, 2014) Tässä tutkimuksessa kohderyhmänä olevat pienet yritykset hyötyvät pilvipalveluiden pienistä aloitus- ja käyttökustannuksista, tasa-arvoistaen informaatioteknologian hyödyntämistä. Pilvipalvelut myös madaltavat IT:n luomia esteitä innovaatioille ja mahdollistavat uusien sovellusten ja palveluiden, kuten paikasta- ympäristöstä- tai kontekstista tietoisten, reaaliajassa toimivien sovellusten toteuttamisen. Koska laitteistoresursseja hallitaan ohjelmistojen kautta, ne voidaan ottaa nopeasti käyttöön tarpeen vaatiessa, joko ilman palveluntarjoajan osallistumista tai vähäisellä vuorovaikutuksella palveluntarjoajaan. Tämä mahdollistaa yritysten palveluiden helpon skaalaamisen asiakaskysyntään pohjautuen. (Avram, 2014)

Nykyisin pilvipalveluita voidaankin pitää lähes erottamattomana osana organisaatioiden toimintaa: Tilastokeskuksen tuottaman kyselyn mukaan maksullisia pilvipalveluita käytti Suomessa 81 % yrityksistä. Määrä on kasvanut kymmenessä vuodessa 30 %:lla. (Hendre & Joshi, 2015; Tilastokeskus, 2022) Globaalisti pilvipalveluihin liittyvien markkinoiden koko oli arvoltaan 569,31

miljardia dollaria vuonna 2022 ja sen ennustetaan kasvavan 2 432,87 miljardiin dollariin vuoteen 2030 mennessä (Fortune Business Insights, 2023).

4.1 Pilvipalveluiden toteutusmallit

Pilvipalveluista on kirjallisuudessa kolme yleisesti hyväksyttyä toteutusmallia: yksityinen pilvi (private cloud), yhdistelmäpilvi (hybrid cloud), sekä julkinen pilvi (public cloud). Joidenkin lähteiden mukaan on olemassa myös neljäs, eri toimijoista koostuva yhteisöpilvi (community/government cloud), mutta se on yleensä kuvattavissa muiden toteutusmallien kautta. Yhteisöpilven voidaan katsoa olevan tietyn joukon tai yhteisön omistama yksityinen pilvipalvelu. (Kyberturvallisuuskeskus, 2020a; Mell & Grance, 2011; Rani ym., 2015) Pilvipalveluiden erilaiset toteutusmallit palvelevat erilaisia tarpeita ja niiden hyödyt ja toisaalta myös haasteet ovat erilaiset.

Yksityisellä pilvipalvelulla tarkoitetaan vain yhdelle käyttäjälle tai organisaatiolle tuotettua palvelua. Keskeistä yksityiselle pilvipalvelulle on, että pilven toteuttamiseen vaadittava infrastruktuuri on varattu vain yhden organisaation käyttöön. (Mell & Grance, 2011) Usein yksityinen pilvipalvelu tarkoittaa yrityksen sisäisiä datakeskuksia, jotka eivät ole muiden organisaatioiden saatavilla, mutta palvelua voidaan tuottaa myös palveluntarjoajan konesalista (Armbrust ym., 2010; Kyberturvallisuuskeskus, 2020a). Yksityistä pilvipalvelua pidetään teoriassa turvallisimpana vaihtoehtona, koska haavoittuvuusavaruus pystytään yleensä rajaamaan tarkemmin kuin muissa toteutusmalleissa ja mikäli pilvi-infrastruktuuri sijaitsee omassa laitetilassa, voidaan sitä fyysisesti valvoa (Kyberturvallisuuskeskus, 2020a). Lisäksi se tarjoaa mahdollisuuden laajempaan yksilöintiin (Rani ym., 2015). Yksityisen pilven kustannukset voivat kuitenkin olla muita pilvipalveluiden käyttöönottomalleja korkeammat, koska skaalautumisedut menetetään keskitetyn toteutuksen vuoksi (Kaur & Kamboj, 2023). Kustannukset voivat muodostua esimerkiksi palvelinkapasiteetista, vaadittavista lisensseistä sekä ylläpidosta ja tietoliikenteestä. Lisäksi yksityisen pilven skaalautuvuus on huonompi kuin muilla toteutusmalleilla (Rani ym., 2015).

Julkinen pilvi tarkoittaa palvelua, jota tarjotaan julkisesti, ja joka on kenen tahansa hankittavissa. Siinä käytettävä pilvi-infrastruktuuri on siis tarkoitettu suuren yleisön avoimeen käyttöön ja infrastruktuurin omistaa yleensä valtio, akateeminen organisaatio tai yritys. (Mell & Grance, 2011) Palvelu tuotetaan lähes aina palveluntarjoajan konesalista ja on skaalautumisetujensa vuoksi yleensä edullisempi vaihtoehto kuin yksityinen pilvipalvelu. Julkinen pilvi mahdollistaa organisaatioille lähes rajattoman kapasiteetin, tarjoten kuitenkin turvallisen ja käyttövarman ympäristön. Julkiseen pilvipalveluun ja siinä käsiteltävään tietoon kohdistuu kuitenkin enemmän tietoturvauhkia muun muassa muiden käyttäjien ja ulkoisten toimijoiden kautta. (Kyberturvallisuuskeskus, 2020a)

Yhdistelmäpilvellä tarkoitetaan yksityisen ja julkisen pilven yhdistämistä yhdeksi palvelukokonaisuudeksi. Tällöin erillisistä pilvistä peräisin olevat infrastruktuurin osat yhdistetään toisiinsa, kuitenkin niin, että ne pysyvät erillisinä

kokonaisuuksina. (Mell & Grance, 2011) Yhdistämiseen käytetään standardoitua tai patentoitua tekniikkaa, joka mahdollistaa tiedon ja sovellusten siirrettävyyden eri pilvien välillä. Organisaation käytössä voi olla yksityinen pilvipalvelu, jota tarvittaessa täydennetään julkisessa pilvessä sijaitsevilla palveluilla. (Kyberturvallisuuskeskus, 2020a; Mell & Grance, 2011) Yhdistelmäpilvet tarjoavat julkisten pilvipalveluiden skaalautumisedut ja edulliset kustannukset, tarjoten samalla yksityisen pilvipalvelun hallittavuuden ja tietoturvan. Yhdistelmäpilven turvallisuus on kuitenkin riippuvainen siitä, kuinka paljon julkista pilvipalvelua hyödynnetään, sekä siitä miten tiedon tallentaminen ja rajapintojen turvallisuus on järjestetty (Kyberturvallisuuskeskus, 2020a).

4.2 Pilvipalveluiden palvelumallit

Pilvipalveluista on toteutusmallien lisäksi käytössä kolme erilaista palveluarkkitehtuurin mallia, joilla pilvipalveluita tarjotaan käyttäjille. Palvelumallit määrittelevät mitä palveluita asiakas toteuttaa itse, ja mitkä ovat palveluntarjoajan vastuulla. Palvelumallit ovat infrastruktuuri palveluna (Infrastructure as a Service, IaaS), ohjelmistoalusta palveluna (Platform as a Service, PaaS) sekä ohjelmisto palveluna (Software as a Service, SaaS). Tyypillinen vastuunjako on kuvattu alla olevassa taulukossa 2.

TAULUKKO 2 Pilvipalveluiden palvelumallit (Kyberturvallisuuskeskus, 2020a, s. 10)

	IaaS	**PaaS**	**SaaS**
	Rajapinta (Interface)	Rajapinta (Interface)	Rajapinta (Interface)
	Sovellus (Application)	Sovellus (Application)	Sovellus (Application)
	Ratkaisupino (Solution stack)	Ratkaisupino (Solution stack)	Ratkaisupino (Solution stack)
Asiakas (Customer/ Tenant)	Käyttöjärjestelmä (Operating system)	Käyttöjärjestelmä (Operating system)	Käyttöjärjestelmä (Operating system)
Palveluntarjoaja (Provider)	Virtualisointi (Virtualisation)	Virtualisointi (Virtualisation)	Virtualisointi (Virtualisation)
	Laskenta ja tallennus (Compute & Storage)	Laskenta ja tallennus (Compute & Storage)	Laskenta ja tallennus (Compute & Storage)
	Verkko (Networking)	Verkko (Networking)	Verkko (Networking)
	Palvelinkeskus (Facility)	Palvelinkeskus (Facility)	Palvelinkeskus (Facility)

IaaS-palvelumallin voidaan kuvata olevan pilvipalveluiden pohjataso, jonka päälle kaikki muut palvelumallit toteutetaan. IaaS-mallissa vain palveluiden tuottamiseen liittyvä infrastruktuuri kuten tallennustila, laitteisto, verkkoyhteys sekä laskentateho ostetaan palveluna. Tällöin asiakas voi itse valita esimerkiksi käyttämänsä käyttöjärjestelmän. Pilvipalvelun tarjoaja isännöi infrastruktuuria ja käyttäjät hyödyntävät näitä resursseja virtualisoidussa ympäristössä. Palveluntarjoaja tarjoaa resursseja asiakkaan tarpeen mukaisesti ja luo yhden tai useamman virtuaalikoneen tarpeeseen pohjautuen. Näin syntyvässä virtuaalisessa ympäristössä asiakas voi luoda ja käyttää ohjelmistoja tai hyödyntää virtuaalisen koneen tallennustilaa. Asiakasta veloitetaan erilaisten käytettyjen resurssien kuten muistin, laskentatehon ja tallennustilan mukaisesti, joten se voi olla edullisempi vaihtoehto kuin oman fyysisen tallennustilan, palvelinten ja verkkoinfrastruktuurin hankinta. Amazon EC2 ja S3, GoGrid ovat esimerkkejä IaaS-palvelumallilla tarjottavista pilvipalveluista. (Kaur & Kamboj, 2023)

PaaS-mallissa ostetaan kokonaisuutena virtuaalinen alusta, joka sisältää usein tallennustilan, käyttöjärjestelmän, tietokannat, palvelimet, verkkoyhteydet sekä suoritusympäristön eri ohjelmointikielille. IaaS-mallissa tarjottavan infrastruktuurin lisäksi asiakas saa PaaS-mallissa käyttöönsä palveluntarjoajan kehitysympäristön, jolla hän voi toteuttaa esimerkiksi ohjelmistokehitystä ilman syvällistä ymmärrystä alustan teknologisista yksityiskohdista. Asiakas ei itse hallinnoi pilvipalvelun toteuttamiseen vaadittavaa infrastruktuuria, vaan palveluntarjoajan vastuulla on varmistaa, että kehitysympäristö on riittävän kestävä sekä joustava ja että sen resurssit ovat riittävät. (Kaur, 2019; Kaur & Kamboj, 2023) PaaS-malli tarjoaa siis kaiken tarvittavan pilvipohjaisten ohjelmistojen kehittämiseen ja suorittamiseen: asiakkaan ei tarvitse huolehtia virtuaaliympäristön ylläpitämisestä tai päivittämisestä, vaan hänen vastuulleen jää ainoastaan siellä luotujen sovellusten ylläpitäminen (Kaur, 2019; Mell & Grance, 2011). Tunnetuin PaaS-mallilla tarjottava pilvipalvelu on Microsoft Azure (Kaur & Kamboj, 2023).

SaaS-palvelumallissa palveluntarjoaja tuottaa palvelun kokonaisuudessaan ja sen voidaankin nähdä olevan palvelumallien ylin taso (Kaur & Kamboj, 2023). Asiakas ei hallinnoi ohjelmiston toteuttamiseen vaadittavaa IT-infrastruktuuria kuten verkkoa, palvelimia, käyttöjärjestelmiä tai edes yksittäisen ohjelmiston ominaisuuksia. Käyttäjällä voi kuitenkin olla rajoitettu mahdollisuus mukauttaa ohjelmiston asetuksia omia tarpeitaan vastaavaksi. (Mell & Grance, 2011) SaaS-ohjelmistoja hyödynnetään erilaisilla laitteilla, kuten tietokoneilla, tableteilla ja älypuhelimilla, käyttäen ohjelmiston tarjoamaa käyttöliittymää. Käyttöliittymä voi olla esimerkiksi verkkoselain tai ohjelmointirajapinta. (Mell & Grance, 2011) Ohjelmiston käyttö ei siis välttämättä vaadi ohjelmiston asentamista laitteelle. SaaS-palvelumalliin pohjautuvia ohjelmistoja ovat esimerkiksi Google Drive, sähköpostipalvelut, sekä CRM-järjestelmä Salesforce (Kaur & Kamboj, 2023).

4.3 Pilvipalveluiden jatkuvuuden hallinta

Pilvipalveluita voidaan pitää usein järkevimpänä tapana toteuttaa tiedon säilömistä ja prosessointia niitä hyödyntävän asiakkaan näkökulmasta. Pilvipalveluiden etuina luetellaan tutkimuksissa mm. ketteryys ohjelmistojen valinnassa ja vaihtamisessa, joustavat ja paremmin erikokoisille yrityksille sopivat palvelumallit, vähäinen investointeihin sidottava pääoma sekä ohjelmistojen toimintavarmuus. Lisäksi pilvipalveluiden voidaan nähdä olevan turvallisempia kuin on-premise-ohjelmistot, koska pilvipalvelun tarjoajilla on taloudellisia motiiveja asiakkaiden suojelemiseksi. (Cloud security alliance, 2017) Ulkoistetun luonteensa vuoksi pilvipalvelut luovat asiakasyrityksille kuitenkin myös erilaisia riskejä perinteisiin IT-ratkaisuihin verrattuna (Agarwal & Agarwal, 2011). Seuraavassa luvussa tarkastellaan pilvipalveluihin liittyvää jatkuvuuden hallintaa aiemmin määritellyn toiminnan jatkuvuuden hallinnan ja varautumisen kontekstissa: millaisia hyötyjä eri toimitusmalleilla toimitettavien pilvipalveluiden käytöstä on asiakasorganisaatiolle toiminnan jatkuvuuden parantamisen näkökulmasta, ja toisaalta millaisia haasteita siihen liittyy. Lisäksi luvussa käsitellään asiakasyrityksen jatkuvuuden hallinnan keskeisiä toimia, sekä jatkuvuuden hallintaan liittyvien vastuiden jakautumista pilvipalvelun toimittajan ja asiakkaan välillä. Teoria toimii pohjana tutkimukselle, jossa selvitettiin pienyritysten käyttämien pilvipalveluiden jatkuvuussuunnittelua.

4.3.1 Pilvipalveluiden hyödyt jatkuvuuden hallinnan näkökulmasta

Pilvipalveluiden todetaan usein tuovan etuja ja hyötyjä yrityksille, joilla ei ole kyvykkyyksiä tai resursseja hankkia ja ylläpitää omia IT-palveluita (Agarwal & Agarwal, 2011; Armbrust ym., 2010; Grobauer ym., 2011; Hendre & Joshi, 2015). Pilvipalveluita ja organisaation siitä saamia hyötyjä on käsitelty viimeaikaisessa kirjallisuudessa paljon, ja sieltä onkin tunnistettavissa seuraavat organisaation jatkuvuutta parantavat ominaisuudet:

1. Fyysisen turvallisuuden parantuminen. Pilvipalvelut voidaan pohjimmiltaan kuvitella käyttöoikeuksina jossain muualla sijaitseviin laskentaresursseihin. Tästä syystä pilvipalvelut rikkovat fyysiseen ympäristöön liittyvän laitteistoriippuvuuden palvelun käyttäjän näkökulmasta: palvelun käyttöä voidaan esimerkiksi jatkaa toisella laitteella aiemman rikkouduttua ja laitetta voidaan myös siirrellä paikasta toiseen. (Staalinprasannah & Suriya, 2013) Tämä pienentää fyysiseen turvallisuuteen liittyviä uhkia esimerkiksi onnettomuuksien, varkauksien tai pandemioiden tapauksissa. Fyysisestä sijainnista ja laitteistosta riippumaton työskentely helpottaa huomattavasti etenkin pienyrityksen resurssien allokointia ja varautumista. (Ristov ym., 2011)
2. Parantunut tietoturva. Tietoturvan näkökulmasta pilvipalvelut tarjoavat usein paikallista toteutusta paremman vaihtoehdon: Pilvipalveluihin

liittyvät turvallisuusvaatimukset ovat usein samat kuin perinteisissäkin toteutuksissa, mutta vastuita voidaan jakaa ulkoiselle toimijalle. Riippuen pilvipalvelun palvelumallista, voi toimittajan vastuulla olla lähes kaikki turvallisuuteen liittyvät osa-alueet. Vaikka pilvipalvelu toimitettaisiin muuna kuin kaiken kattavana SaaS -ohjelmistona, on palveluntarjoajalla kaikissa tapauksissa vähintäänkin vastuu järjestää hallintatason käytön turvallisuus ja taata riittävien työkalujen saatavuus asiakkaalle. Hallintatasolla tarkoitetaan pilvipalveluiden hallintaan ja valvontaan liittyviä työkaluja ja käyttöliittymiä. Järjestelmänvalvojien ja muiden turvallisuudesta vastaavien henkilöiden palkkaaminen voi olla pienemmille organisaatioille liian suuri kustannuserä, kun taas pilvipalveluita laajalle joukolle asiakkaita tarjoavalla organisaatiolla on usein enemmän resursseja hyödynnettäväksi turvallisuuden ylläpitämiseen. Hallinnointi on niin ikään usein helpompaa ja tehokkaampaa kun turvallisuuteen liittyvät työkalut ovat käytettävissä yksillä tunnuksilla. (Cloud security alliance, 2017) Tämä parantaa esimerkiksi yrityksen tietoverkkojen turvallisuutta sekä käyttöoikeuksien hallintaa (Ristov ym., 2011). Pilvipalveluiden tarjoajalla on lisäksi taloudellinen kannustin pitää asiakkaiden tiedot turvassa ja palvelu toimimassa mahdollisimman lyhyin käyttökatkoin (Cloud security alliance, 2017).

3. Ketteryyden ja joustavuuden parantuminen. Pilvipalveluiden käyttö mahdollistaa infrastruktuurin toteuttamisen ja ylläpidon, palveluiden ajamisen, sekä aiheeseen liittyvän osaamisen siirtämisen siihen erikoistuneille organisaatioille. Tämä nopeuttaa päätöksentekoprosesseja, ja auttaa yritystä keskittymään liiketoimintansa päätavoitteisiin. (Ercan, 2010) Ulkoistamalla ei-kriittiset sovellukset ja niiden tiedot pilveen suorituskykyisempiin ympäristöihin vapauttaa yrityksen IT-asiantuntijat keskittymään yritykselle kriittisiin asioihin.
4. Toimintavarmuus. Tyypillisesti pilvipalveluita ajetaan suurten toimittajien palvelimilla, joilla on tietoturvaan liittyvien motivaatioiden ohella intressi pitää myös asiakkaiden palvelut toiminnassa. Isot ja pilvipalveluiden tuottamiseen erikoistuneet toimijat noudattavat ja niiltä vaaditaan usein parempaa varmuuskopioiden hallintaa, maantieteellistä hajauttamista, sekä tiedon oikeellisuuden varmentamista. Etenkin SaaS -palveluissa käyttökatkokset käyttäjille ovat usein todella lyhyitä tai jopa huomaamattomia riippumatta siitä mitä palvelua käyttävän organisaation työntekijöille tai infrastruktuurille tapahtuu. (Ristov ym., 2011) Lisäksi Ristov ym (2011) mainitsee että pilvipalveluiden tarjoama redundanssi ja skaalautuvuus tarjoavat paremman kestävyyden hajautettuja palvelunestohyökkäksiä vastaan, sekä nopeamman palautumisen vakavista häiriöistä perinteisiin on-site toteutuksiin verrattuna.

4.3.2 Pilvipalveluiden haasteet jatkuvuuden hallinnan näkökulmasta

Pilvipalveluiden käyttöön liittyy eduista huolimatta paljon riskejä, jotka voivat vaikuttaa merkittävästi yrityksen toiminnan jatkuvuuteen. Pilvipalveluiden

tietoturvahaasteiden kirjo on laajempi ja monimuotoisempi kuin on premise -toteutuksissa: oman infrastruktuurin sijaan tiedon tallennus ja käsittely voi tapahtua fyysisesti missä päin maailmaa tahansa. Lisäksi tiedon tallennuksen ja käsittelyn tarkkaa sijaintia voi olla vaikea määrittää: kyseiset toiminnot voidaan toteuttaa eri maassa kuin mihin palveluita tarjoava yritys on rekisteröity. (Grobauer ym., 2011; Kyberturvallisuuskeskus, 2020) Lisäksi pilvipalveluille on tyypillistä, että riskit ovat moniulotteisia: uhat voivat kohdistua sekä asiakkaaseen että palveluntarjoajaan ja vastuu niiden torjunnasta voi olla samanaikaisesti usealla taholla. Haasteena on lisäksi se, että verkottuneen luonteensa takia yhdenkin riskin toteutuminen voi estää koko palvelun käytön. (Kyberturvallisuuskeskus, 2020a)

Esimerkiksi Hendre ja Joshi (2015), Agarwal ja Agarwal (2011) ja Ristov ym. (2011) esittävät artikkeleissaan pilvipalveluihin liittyvän niiden eduista huolimatta paljon erilaisia jatkuvuutta vaarantavia uhkia. Turvallisuuteen liittyviä riskejä palveluntoimittajan osalta ovat esimerkiksi tietovuodot, tiedon katoaminen palvelimilta, sekä palvelunestohyökkäykset (Agarwal & Agarwal, 2011). Teknologiaan liittyvistä riskeistä Agarwal ja Agarwal (2011) mainitsevat etenkin virtualisoinnista aiheutuvat riskit: Virtualisoinnin avulla palvelutoimittaja ajaa useita järjestelmiä yhdessä fyysisessä järjestelmässä jakaen samat laitteistoresurssit. Virtualisointi vaatii monimutkaista konfigurointia, jonka vuoksi niihin voi jäädä tietoturva-aukkoja (Agarwal & Agarwal, 2011). Vaikka pilvipalveluntoimittajan laitteisto on usein paremmin hajautettu ja suojattu kuin perinteisen organisaation, palveluntoimittajaan kohdistuu niin ikään fyysiseen turvallisuuteen liittyviä uhkia: erilaiset luonnonkatastrofit, tulipalot, vahingot, sähkön saatavuus ja yhteiskunnan kriisitilanteet vaikuttavat pilvipalvelua tarjoavan organisaation jatkuvuuteen. (Ristov ym., 2011) Tämänkaltaisia turvallisuusuhkia voi olla vaikea arvioida monikansallisten pilvipalvelun tarjoajien tapauksessa. Monikansallisiin palveluntarjoajiin voi kohdistua myös laajemmin lainsäädäntöjohdannaisia riskejä, jotka heijastuvat asiakasyritykseen. Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädäntöihin, jotka voivat velvoittaa pilvipalveluntarjoajaa toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan heille pääsy asiakkaiden salassa pidettäviin tietoihin. (Kyberturvallisuuskeskus, 2020a) Tällaiset tapahtumat ja tietopyynnöt voivat aiheuttaa ennakoimattomia katkoksia pilvipalveluiden käyttöön ja vaarantavat salassa pidettävän tiedon turvallisuuden.

Asiakkaaseen suoraan kohdistuvia uhkia ovat esimerkiksi käyttäjätunnusten kaappaaminen ja tämän jälkeen niiden hyödyntäminen haitallisiin tarkoitusperiin, huonosti suojatut ohjelmointirajapinnat, pilviohjelmistojen väärinkäyttö sekä loppukäyttäjien ymmärtämättömyys ja välinpitämättömyys riskien olemassaolosta: esimerkiksi varjo-it:n käytön nopea kasvu COVID -19 pandemian takia aiheuttaa lisääntyviä tietoturvariskejä organisaatiolle. (Akello, 2022) Organisaation hallinnon panostukset tietoturvaan voivat niin ikään vähentyä pilvipalveluiden oletetun turvallisuuden myötä, ja näin pilvipalveluiden kustannussäästöt saatetaan käyttää muihin kohteisiin (Ristov ym., 2011). Kustannushyödyt tulisi Ristovin ym. (2011) mukaan kuitenkin investoida uudelleen tietoturvaan kuten

pilvipalvelutarjoajien turvallisuuden hallinnan kartoittamiseen, turvallisuuteen liittyvien kontrollien käyttöönottoon ja säännöllisten turvallisuusarviointien tekemiseen varsinkin IaaS- ja PaaS-palveluiden tapauksissa.

4.3.3 Jatkuvuuden hallinnan vastuut tarjoajan ja asiakkaan välillä

Vastuut pilvessä olevan tiedon suojaamisesta, saatavuudesta ja eheydestä jakautuvat pilvipalveluntarjoajan ja asiakkaan kesken hieman eri tavoin, riippuen palveluiden toimittajasta ja toimitettavan pilvipalvelun palvelumallista. Nämä vastuut eivät ole aina täysin selkeitä. (Hendre & Joshi, 2015) NIST SP 800-210 (2020) nostaa esimerkiksi IaaS -palvelumallilla myytävät pilvipalvelut: IaaS-järjestelmät voivat tarjota erilaisia palveluita ja ominaisuuksia, ja vastuiden jakautuminen riippuu tarjottavien resurssien ja hallintaominaisuuksien yhdistelmästä ja määrästä. Muista palvelumalleista löytyy niin ikään eroja. Esimerkiksi pääsynhallintaa toteutetaan usein jaetulla mallilla PaaS- ja SaaS-palvelumalleissa: PaaS-palvelussa ohjelmistokehittäjät saattavat olla vastuussa pääsynhallinnasta yhdessä pilvipalveluntarjoajan kanssa, kun taas SaaS-palvelussa sisäiset sovelluksen käyttäjät jakavat vastuun pääsynhallinnasta yhdessä pilvipalveluntarjoajan kanssa. Edelleen pilvipalveluntarjoaja vastaa yleensä pilvipalveluihin liittyvästä fyysisestä infrastruktuurista kuten palvelinlaitteista ja verkoista, mutta jatkuvuuden hallinnan näkökulmasta asiakkaalla voi olla vastuu omien virtuaalisten resurssiensa kuten tallennustilan riittävyydestä ja riittävän vahvasta suojaamisesta, sekä käyttämiensä verkkojen suojelusta. (Hu ym., 2020)

Suomen valtionhallinnon julkaisemassa PiTuKri-ohjeessa (2020) pilvipalveluihin liittyvien vastuiden jakautumista jatkuvuuden hallinnan osalta on kuvattu pohjautuen toimitusmalleihin, joista tässä tutkielmassa puhutaan palvelumalleina. Myös PiTuKri sisältää maininnan siitä, että käytännössä pilvipalveluiden ilmentymät eroavat toisistaan sekä teknisten toteutusten että vastuujaon osalta. Aiemmin tässä tutkielmassa määriteltyyn jatkuvuuden hallintaan liittyviä tehtäviä asiakkaan ja toimittajan välillä voidaan havainnoida PiTuKrissa esiehtojen, turvallisuusjohtamisen, fyysisen turvallisuuden sekä käyttöturvallisuuden osa-alueilta ja palveluntarjoajalle kuuluvien jatkuvuuden hallinnan vastuiden voidaan havainnoida olevan samat palvelumallista riippumatta. Palveluntarjoajan vastuisiin kuuluvat PiTuKrin mukaisesti seuraavat jatkuvuuden hallinnan osa-alueet:

- Palveluntarjoajan tulee tarjota asiakkaalle riittävän yksityiskohtainen järjestelmäkuvaus, jotta kuvauksen pohjalta pystytään arvioimaan palvelun yleistä soveltuvuutta ja riskejä suhteessa asiakkaan käyttötapaukseen.
- Palveluntarjoajan tulee suunnitella, toteuttaa, testata ja kuvata jatkuvuuden hallinnan prosessit ja menettelyt siten, että vastaaminen palvelutasosopimusten ja lainsäädännön velvoitteisiin on mahdollista.
- Pilvipalvelusta on ohjeet palvelun turvalliseen ylläpitoon ja hallinnointiin.
- Pilvipalvelun konesalien ja vastaavien tilojen toiminnan jatkuvuus on suojattu riskejä vastaan.

Asiakkaan vastuut sen sijaan vaihtelevat PiTuKrin mukaan palvelumallin mukaan:

- Asiakkaan vastuulla on jokaisen palvelumallin tapauksessa vähintään omien liiketoimintojen jatkuvuussuunnitelman laatiminen.
- PaaS- ja IaaS-palvelumalleissa asiakkaan tulee lisätä varmuus ja palautusprosessien suunnittelu, toteutus, testaus ja kuvaus osaksi jatkuvuussuunnitelmaa. Tämä koskee tarjottavan infrastruktuurin tai alustan päällä toimivia asiakkaan omia pilvipalveluita. Lisäksi IaaS-palvelumallin mukaisesti ostettavassa pilvipalvelussa asiakkaan tulee huolehtia varmuuskopioiden suojaamisesta niiden elinkaaren ajan.
- PaaS- ja IaaS-palvelumalleissa järjestelmäkuvauksen laatiminen omaa palvelua koskien. (Kyberturvallisuuskeskus, 2020a)

Voidaankin todeta, että jatkuvuuden hallinnan vastuut vaihtelevat eri palvelumallien mukaan. Pilvipalvelun ostaminen ohjelmisto palveluna -palvelumallina vähentää merkittävästi asiakkaan vastuita, mutta ei poista niitä kokonaan. Keskeistä vastuiden ymmärtämisessä ja määräytymisessä on kommunikointi: asiakkaan tulee olla tietoinen siitä, mitkä ovat hänen vastuunsa pilvessä olevan datan suojaamiseen ja toiminnan jatkuvuuteen liittyen. Niin ikään pilvipalveluntarjoajan tulee kommunikoida asiakkaille heidän vastuunsa ja hallintaoikeuksiensa laajuus. (Hu ym., 2020; Kyberturvallisuuskeskus, 2020a) PiTuKri-ohjeessa (2020) velvoitetaan toimittajaa kuvaamaan, jakamaan ja tiedottamaan turvallisuuteen liittyvät vastuut palvelua hankkivalle organisaatiolle (Kyberturvallisuuskeskus, 2020a). Kommunikointi tulee olla siis molemminpuolista ja asiakkaan tulee tarvittaessa vaatia tietoja tarjoajalta. Vastuiden kuvaaminen voidaan käytännössä toteuttaa erilaisilla sopimuksilla, kuten esimerkiksi palvelutasosopimuksella. Hyvin laadittu sopimus sisältää ongelmatilanteiden hallintaan liittyvän osuuden, joka sisältää kuvauksen niistä toimenpiteistä, jotka toteutetaan ennalta odottamattoman tilanteen ilmaantuessa. Hyvä sopimus myös selventää molemmille osapuolille palvelukokonaisuuden sisällön, yksinkertaistaa monimutkaisia asioita, sekä poistaa epärealistisia odotuksia osapuolten välillä. (Kandukuri ym., 2009)

4.3.4 Pilvipalveluiden jatkuvuuden hallinnan toteuttaminen

Pilvipalveluiden jatkuvuutta ohjeistavaa kirjallisuutta on saatavilla vähemmän kuin koko organisaation jatkuvuuden hallintaan keskittyvää ohjeistusta. Tähän alalukuun hyödynnettiin jatkuvuuden hallinnan kirjallisuuden ohella Ristovin ym. (2011) laatimaa artikkelia pilvipalveluiden haasteista jatkuvuuden hallinnan näkökulmasta, sekä Kyberturvallisuuskeskuksen PiTuKri-ohjetta. Ristovin ym. (2011) artikkeli valittiin lähteeksi, koska sieltä on tunnistettavissa selkeitä toimia jatkuvuuden hallinnan toteuttamiseksi pilvipalveluiden näkökulmasta. Ristovin kirjoittamia tekstejä on käytetty lähteenä yli 2000 kertaa ja hän on voittanut useita akateemisia palkintoja (ResearchGate, 2024).

Jatkuvuuden hallinta tulee aloittaa Ristovin ym. (2011) mukaan pilvipalvelua hankkivan organisaation toimesta jo ennen hankintapäätöstä. Ensin tulee tehdä riskien tunnistaminen ja arviointi, joka toimii pohjana kaikelle tulevalle arvioinnille. Ristovin ym. (2011) mukaan yrityksen tulee kehittää toimintapa, jonka avulla arvioidaan, onko kohteena oleva järjestelmän mahdollista toimia pilvipohjaisena ratkaisuna ja millaisia riskejä ratkaisuun mahdollisesti liittyy. Turvallisuuden ja riskien arvioinnissa voidaan käyttää erilaisia menetelmiä ja arviointiin vaikuttaa vahvasti millaisella palvelumallilla pilvipalvelu toteutetaan. Joissain tapauksissa voi olla riittävää hyödyntää palveluntarjoajan itsensä tuottamia arviointeja tai esimerkiksi sopimusteknisiä sitoumuksia, kun taas joissain tapauksissa taas on perusteltua edellyttää lisäksi ulkopuolisen tahon tekemää riippumatonta selvitystä (Kyberturvallisuuskeskus, 2020a). Arvioitaessa pilvipalvelun soveltuvuutta omaan toimintaan, voidaan arvioida esimerkiksi tietojen arkaluonteisuutta, sekä tarpeellisuutta tilanteissa, joissa internet-yhteys ei toimi (Kyberturvallisuuskeskus, 2019). Riskien tunnistamisen ja arvioinnin jälkeen riskejä vertaillaan muihin toteutustapoihin (Ristov ym., 2011).

Kun riskit on arvioitu, voidaan kartoittaa kyseisiä pilvipalveluita tuottavat toimijat ja tehdä päätös siitä, onko pilvipohjaiseen ratkaisuun siirtyminen tarkoituksenmukaista kyseisen järjestelmän kannalta. Tulevaisuutta ajatellen riskien arviointimekanismi tulee sisällyttää osaksi pilvipohjaisten järjestelmien elinkaarisuunnittelua, jotta riskejä arvioidaan säännöllisesti uudelleen. (Ristov ym., 2011) Mikäli pilvipohjaiseen ratkaisuun ohjelmistoon päädytään, aloitetaan pohdinta sopivasta palveluntarjoajasta. Palveluntarjoajaa valittaessa on hyvä pohtia palvelun turvallisuuden lisäksi omaa sekä palveluntarjoajan toiminnan jatkuvuutta, erilaisia palvelutasoja sekä palveluntarjoajan kokoa. Tärkeitä selvitettäviä asioita ovat mm. seuraavat:

- Miten palveluntarjoaja on varmistunut siitä, että palvelu ja asiakkaan palveluun tallennettavien tietojen saatavuus varmistetaan?
- Kuinka palvelu on suojattu esimerkiksi laitteistorikkojen tai virhekonfiguraatioiden varalta?
- Kuinka asiakkaan tiedot ja keskeiset konfiguraatiot on varmuuskopioitu?
- Miten varmuuskopiot on suojattu?
- Miten mahdollisimman nopea toipuminen häiriötilanteesta on varmistettu?
- Mitkä ovat palveluntarjoajan kriittiset prosessit ja miten ne on suojattu? (Kyberturvallisuuskeskus, 2019)

Mikäli mahdollista, on syytä kartoittaa myös pilvipalvelun tarjoajan hyödyntämät kolmannen osapuolen palvelut ja millaisia riskejä niihin liittyy. (Kyberturvallisuuskeskus, 2020a) Kun päätös hankinnasta on tehty ja toimittaja valittu, pilvipalvelua hankkivan organisaation tulee laatia jatkuvuussuunnitelma tai täydentää olemassa olevaa jatkuvuussuunnitelmaa siten, että se huomioi uuden järjestelmän tuomat muutokset.

Sekä uusien, että jo käytössä olevien pilvipalveluiden osalta jatkuvuussuunnitelmaan tulee olla arvioitu niiden vaikutuksia ja riskejä liiketoiminnalle. Organisaation tulee arvioida jatkuvuussuunnitelmassaan pilvipalvelun kriittisyys liiketoiminnan kannalta, millaista palvelutasoa pilvipalvelulta vaaditaan, sekä miten häiriötilanteissa toimitaan. Jatkuvuussuunnitelmassa on hyvä kuvata varayhteyksien ja -järjestelmien käyttö, varmuuskopioinnin menetelmät, sekä jatkuvuuteen liittyvät vastuut henkilöittäin tai ryhmittäin. Asiakkaan organisaatiossa tulisi olla lueteltuna pilvipalvelun pääkäyttäjän merkitys ja tehtävät jatkuvuuden toteuttamisessa, käyttäjien toiminta häiriötilanteissa ja niistä palautumisessa, sekä teknisen tuen rooli ongelmien selvittäjänä. Asiakasorganisaation koon mukaan pilvipalvelun pääkäyttäjällä ja johdolla on päävastuu jatkuvuuden hallinnan toteuttamisessa. Jatkuvuussuunnitelmaan tulee sisällyttää erilaisia skenaarioita, joissa pilvipalvelun tarjoaja ei pysty tuottamaan palveluaan. (Kyberturvallisuuskeskus, 2020a; Ristov ym., 2011)

Pilvipalvelun käytön aikana noudatetaan jatkuvuussuunnitelmaan kirjattuja toimia jatkuvuuden hallinnan toteuttamiseksi. Palvelumallista riippuen, tulee asiakkaan vähintään hallita käyttäjiä ja käyttäjien käyttöoikeuksia omalta osaltaan, pitää yllä ja kehittää jatkuvuuden hallinnan suunnitelmaa sekä ottaa varmuuskopiot tarvittavilta osin. Lisäksi asiakkaan velvollisuutena on noudattaa Suomen lainsäädäntöä esimerkiksi tietosuojan osalta. (Kyberturvallisuuskeskus, 2019, 2020) Asiakkaan tulee testata jatkuvuussuunnitelmaa säännöllisesti ja harjoitella siihen liittyviä skenaarioita. Näillä toimilla varmistutaan, että suunnitelma on ajantasainen ja se toimii käytännössä. Testaamisella ja skenaarioiden harjoittelulla voidaan myös havaita mahdolliset puutteet ja virheet suunnitelmassa. (Kyberturvallisuuskeskus, 2020a; Niemimaa ym., 2019)

5 TUTKIMUKSEN TOTEUTUS

Tässä luvussa kuvataan empiirisen tutkimuksen tutkimusotetta, sekä avataan tutkimuksen tiedonkeruu- ja analysointimenetelmät. Lisäksi luvussa kuvataan kirjallisuuskatsauksen merkitystä tutkimukselle, sekä analysoidaan tutkimuksen luotettavuutta ja tehtyjen tutkimusmenetelmävalintojen sopivuutta. Tutkimuksen tavoitteena on haastattelujen ja kirjallisuuskatsauksen perusteella vastata tutkimuskysymyksiin:

1. Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja onko siinä huomioitu pilvipalveluita?
2. Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?

Tutkimuksen empiiristä osiota pohjustavat luvut 2–5, jotka toteutettiin kirjallisuuskatsauksena. Kirjallisuuskatsauksen tavoitteina olivat syvällisempi tutkimusaiheen tuntemus, joka on edellytyksenä onnistuneen tutkimuksen onnistumiselle, sekä vastaaminen osittain tutkimuskysymykseen ”Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?”. Tarkemmin kirjallisuuskatsauksen tavoitteena oli avata tutkimuksen kannalta olennaisten aihepiirien kuten pilvipalveluiden ja digitaalisen turvallisuuden sisältö, hahmottaa jatkuvuuden hallinnan kokonaisuutta, sekä selvittää onko aiheesta aiempaa tutkimustietoa pienten yritysten näkökulmasta. Kirjallisuuskatsauksessa esiin nousseita tuloksia peilattiin empiirisessä osiossa saatuihin pienyritysten näkökulmiin aiheesta ja näin muodostettiin vastaukset tutkimuskysymyksiin.

5.1 Tutkimusote

Tämän tutkimuksen tavoitteena oli selvittää millaisia käytänteitä pienillä suomalaisyrityksillä on käytössä jatkuvuuden hallintaan ja ovatko kyseiset yritykset

huomioineet pilvipalveluita osana jatkuvuuden hallintaansa. Lisäksi tavoitteena oli selvittää, millaisia elementtejä sisältyy onnistuneeseen pilvipalveluita koskevaan jatkuvuuden hallintaan. Tutkimus on toteutettu laadullisena tutkimuksena. Laadullisessa tutkimuksessa tuloksia ei voida yleistää sen tilastollisessa merkityksessä, mutta tutkittavan ilmiön pohjalta voidaan silti lisätä ymmärrystä muita vastaavanlaisia tapauksia varten. Laadullisella tutkimuksella ei pyritä tekemään tilastollisia päätelmiä, vaan löytämään lisää näkökulmia olemassa olevaan tietoon, ymmärtää tutkittavaa ilmiötä paremmin, sekä tavoitella yleiskatsausta tutkittavaan ongelmaan. (Hirsijärvi ym., 2009) Puusan ja Juutin (2020) mukaan laadullisessa tutkimuksessa pyritään lisäksi saamaan erityisesti subjektiivisia näkemyksiä tutkimusongelmaan. Laadullisen tutkimusotteen käyttö tässä tutkimuksessa onkin perusteltua, koska tutkimuksessa pyritään saamaan subjektiivista näkökulmaa tutkimusongelmaan: tavoitteena on kerätä tutkimuksen kohteena olevien yritysten omia käytänteitä ja ajatuksia jatkuvuuden hallinnasta sekä pilvipalveluista ja niihin liittyvästä jatkuvuuden suunnittelusta. Tutkimuksen avulla ymmärrys tutkittavasta ilmiöstä kasvaa valitusta näkökulmasta, ja tutkimus tarjoaa samalla yleiskatsauksen tutkittavaan ongelmaan.

5.2 Tiedonkeruumenetelmä

Tutkimuksen empiirisen osion tiedonkeruumenetelmänä hyödynnettiin haastatteluja. Haastattelututkimukset ovat yleisimpiä tiedonkeruumenetelmiä laadullisissa informaatioteknologiaa koskevissa tutkimuksissa (Myers & Newman, 2007). Haastattelutyypiksi valittiin puolistrukturoitu teemahaastattelu, joka toteutettiin yksilöhaastatteluna. Puolistrukturoidulle haastattelulle ominaisia piirteitä ovat tutkijan etukäteen suorittama tutustuminen käsiteltävään ilmiöön, sekä näiden pohjalta toteutettu haastattelurunko sekä haastattelu, jonka tavoitteena on selvittää haastateltavien subjektiivisia kokemuksia. (Hirsijärvi & Hurme, 2022; Myers & Newman, 2007)

Jatkuvuuden hallinta on laaja käsite ja se pitää sisällään laajasti erilaista teoriaa, toimenpiteitä ja ohjeistusta, eikä se siksi välttämättä ole etenkään pienille yrityksille tuttu aihepiiri. Lisäksi tutkimuksen toisena aihealueena oleva pilvipalveluiden kokonaisuus voidaan toteuttaa useilla eri toimitus- tai palvelumalleilla ja siihen liittyvä asiantuntemus ei ole välttämättä pienten ja keskisuurten yritysten ydinliiketoimintaa. Puolistrukturoidussa haastattelussa haastattelijalla on mahdollista esittää lisäkysymyksiä, sekä tarkentaa kysymysten muotoilua minkä ansiosta suuria kokonaisuuksia voitiin haastattelussa käsitellä kattavammin. (Myers & Newman, 2007) Kyseiselle haastattelumenetelmälle on lisäksi tyypillistä, että haastattelukysymykset voidaan osittain muotoilla etukäteen, mutta haastattelijalla on myös mahdollisuus improvisoida saadakseen lisätietoa tutkimuksen kannalta keskeisistä asioista (Tuomi & Sarajärvi, 2018). Tämä helpotti oikean tiedon keräämistä kompleksisesta kokonaisuudesta. Teemahaastattelun valintaa puolsi myös haastateltavien asiantuntemuksen vaihtelevuus: Teemahaastattelussa kysymykset on järjestetty teemoittain, mutta tarvittaessa niiden

järjestystä ja muotoa voidaan muokata haastattelun yhteydessä haastateltavan aihepiirin tuntemukseen pohjautuen (Tuomi & Sarajärvi, 2018). Puolistrukturoitu haastattelu mahdollistaa kysymyksiin vastaamisen omin sanoin eikä sido tiettyihin vastausvaihtoehtoihin, ja se korostaakin ihmisten tulkintoja asioista ja niiden merkityksistä (Hirsijärvi & Hurme, 2022).

Puolistrukturoitua teemahaastattelua voidaan pitää onnistuneena valintana, koska haastateltavien aihealueen ymmärrys, sekä rohkeus vastata kysymyksiin kasvoi haastattelun aikana, ja valittu haastattelumenetelmä mahdollisti liikkumisen haastatteluteemojen välillä ilman strukturoitua etenemistapaa. Haastateltavat kertoivat näkemyksiään aiheesta kysymättäkin, ja toisaalta haastattelun painopiste saattoi siirtyä liiaksi tiettyyn aihepiiriin, jolloin haastattelijan oli johdateltava haastattelua oikeaan suuntaan. Teemahaastatteluiden luonteeseen kuulukin, että tutkijan lisäksi myös tutkittava toimii tarkentajana: omilla vastauksillaan hän tarkentaa ja syventää tutkimuksessa käytäviä teemoja (Hirsijärvi & Hurme, 2022). Haastattelumenetelmä mahdollisti myös yrityskohtaisten tarkentavien kysymysten kysymisen, sekä vastaajien mielipiteiden tarkemman kartoittamisen apukysymysten avulla. Myers ja Newman (2007) mainitsevatkin, että haastateltava on usein täysin tuntematon haastattelijalle, eikä tällöin välttämättä täysin luota haastattelijaan. Vapaamuotoisemman keskustelun avulla haastatteluissa saavutettiin luottamus, joka lisäsi vastauksien syvyyttä ja laajensi haastateltavien vastauksia.

5.3 Haastatteluiden toteutus

Haastatteluissa hyödynnettiin haastattelurunkoa, joka oli jaettu kolmeen osioon tutkittavien teemojen mukaan. Hirsjärvi ja Hurme (2022) korostavat haastatteluteemojen suunnittelua etukäteen: Teemat on valittava siten että haastattelun avulla on kerättävissä aineisto, josta voidaan tehdä luotettavasti tutkittavaa ilmiötä koskevia päätelmiä. (Hirsijärvi & Hurme, 2022) Haastatteluteemoja suunniteltiin peilaten niitä tutkimusongelmiin ja kirjallisuuskatsauksen avulla saatuun aihetietoon ja teemoista keskusteltiin yhdessä opinnäytetyön ohjaajan kanssa. Vaikka teemahaastatteluissa improvisoinnille jää tilaa, on Puusan ym. (2020) mukaan etukäteen mietitty haastattelurunko hyödyllinen tarkoituksenmukaisen tiedon saamiseksi. Teemat haastatteluun oli aseteltu väljästi, jotta haastateltava kykeni vastaamaan haastattelukysymyksiin omin sanoin. Haastattelurunko on kuvattu liitteessä 1.
Haastateltavien yritysten valinnassa korostettiin ensisijaisesti kahta kriteeriä:

1. Haastatteluun valittujen yritysten liikevaihto ja henkilöstömäärä sijoittuivat Tilastokeskuksen määrittelyn mukaisesti pienten yritysten kokoluokkaan. Tämä tarkoitti vakituiselta henkilöstömäärältään alle 50 hengen yrityksiä, joiden vuosiliikevaihto on alle 10 miljoonaa euroa (Tilastokeskus, 2023). Liikevaihtotietoihin hyödynnettiin Kauppalehden ja Fonectan yrityshakua.

2. Haastateltavien yritysten tuli hyödyntää pilvipalveluita osana keskeisiä liiketoimintojaan.

Näitä kahta kriteeriä noudattavia yrityksiä etsittiin Fonectan yrityshaun avulla ja yrityksiin otettiin yhteyttä sähköpostitse. Sähköpostikutsuissa esiteltiin tutkittava aihe, jatkuvuuden hallinnan määritelmä, sekä haastattelussa käsiteltävät teemat. Lisäksi kutsussa avattiin tutkimuksen merkitystä pienyritysten jatkuvuuden hallinnalle. Sähköpostikutsut lähetettiin toistamiseen kahden viikon kuluttua, mikäli vastausta haastattelukutsuun ei ollut saatu. Haastattelukutsuja lähetettiin 30 yritykselle, josta 6 hyväksyi kutsun. Haastatteluita toteutettiin viisi kappaletta yhden haastattelun peruunnuttua, ja ne toteutettiin vuoden 2023 keväällä.

Pääosa haastatteluista toteutettiin etäyhteydellä hyödyntäen Zoom-videoneuvottelualustaa. Yksi haastatteluista toteutettiin kasvokkain Jyväskylän yliopiston toimitiloissa. Haastatteluiden kielenä oli suomi ja jokainen haastattelu nauhoitettiin litterointia varten joko Zoom-videoneuvottelualustan nauhoitustyökalulla tai yliopiston hyväksymällä nauhurilla. Haastatteluaineistot tallennettiin yliopiston ohjeistuksen mukaisesti verkkolevylle (Jyväskylän yliopisto, 2022). Haastatteluissa ei ollut aikarajaa, vaan haastattelua jatkettiin, kunnes tutkittavat teemat olivat tutkijan näkemyksen mukaisesti katettu. Haastatteluiden keskimääräiseksi kestoksi muodostui noin 60 minuuttia, mutta kaksi haastatteluista kesti noin 90 minuuttia. Haastattelut toteutettiin yksilöhaastatteluina.

Jatkuvuuden hallinta on osa yrityksen kokonaisturvallisuutta, se on kokoelma ohjeita ja toimintatapoja, joilla yritys varmistaa liiketoimintansa jatkuvuuden. (Lambert, 2022; Valtiovarainministeriö, 2020) Jatkuvuuden hallintaan liittyville toimille on siksi oltava johdon tuki ja jatkuvuuden hallinnan toteuttamisessa on keskeistä kommunikointi johdon sekä liiketoimintojen välillä (Niemimaa & Järveläinen, 2013). Jatkuvuuden hallinta ja sen suunnittelu voidaankin nähdä ennen kaikkea osana yrityksen hallintoa ja johtamista. Vaikka jatkuvuuden hallinta on osa kaiken kokoisten yritysten toimintaa, huomioitiin aineistonkeruussa se seikka, että jatkuvuuden hallinta terminä ei välttämättä ole yrityksille tuttu. Tästä syystä haastateltavien saaminen voi olla erittäin hankalaa. Riittävän kokoista aineistoa puoltaa se seikka, että laadullisissa tutkimuksissa ei pyritä tilastollisiin yleistyksiin, vaan esimerkiksi ymmärtämään tiettyä toimintaa. Laadullisessa tutkimuksessa onkin tärkeää, että henkilöt joilta tietoa kerätään tietävät tutkittavasta ilmiöstä mahdollisimman paljon. (Tuomi & Sarajärvi, 2018) Tutkimuksessa lukumäärää korvattiinkin haastateltavien laadulla: haastateltaviksi valikoitiin yritysten toimitusjohtajia tai muita esihenkilöitä, jotka osana toimenkuvaansa vastaavat yrityksen jatkuvuuden hallinnan toteuttamisesta. Lisäksi haastateltavien tuli olla osana hallinnoimassa yrityksessä käytettäviä pilvipalveluita. Kaikki haastateltavat hyödynsivätkin pilvipalveluita osana päivittäistä työtään ja vastasivat niiden hankinnasta ja käytöstä yrityksessä. Haastateltavat ja heidän edustamansa yritykset toimivat eri toimialoilla, tarjoten näin erilaisia näkökulmia aiheeseen. Taulukkoon 3 on koostettu haastateltujen henkilöiden taustatiedot.

TAULUKKO 3 Haastateltavien taustatiedot

Tunnus	**Yrityksen koko (hlöä)**	**Titteli**	**Toimenkuva**
H1	25	Tuotantojohtaja	Liiketoiminnan johtaminen, järjestelmien hallinta, henkilöstöhallinto
H2	2	Yrittäjä/Toimitusjohtaja	Liiketoiminnan johtaminen, myynti ja markkinointi ulkomaille, tuotekehitys, järjestelmien hallinta
H3	9	IT-asiantuntija/tiiminvetäjä	Järjestelmien ylläpito ja kehittäminen. Varautuminen ja riskienhallinta
H4	17	Yrittäjä/Toimitusjohtaja	Myynti, markkinointi, Yrityksen hallinto
H5	2	Yrittäjä/Toimitusjohtaja	Hallinto, markkinointi ja myynti

Haastatteluiden aluksi haastatelluilta selvitettiin heidän toimenkuvansa ja tittelinsä yrityksessä. Tämän jälkeen varmistettiin, että heidän yrityksensä keskeisissä liiketoiminnoissa hyödynnetään pilvipalveluita. Lisäksi haastateltaville esiteltiin jatkuvuuden hallinnan määritelmä, sekä kuvattiin mitä pilvipalveluilla tässä tutkimuksessa tarkoitetaan. Taustatietojen ja keskeisten käsitteiden määrittelyn jälkeen haastattelu toteutettiin haastattelurunkoon pohjautuen. Haastattelurunko oli jaettu tutkimuskysymysten avulla seuraaviin teemoihin: jatkuvuuden hallinta, pilvipalvelut, sekä pilvipalveluita koskeva jatkuvuuden hallinta. Pilvipalveluihin liittyen haastateltavilta kartoitettiin pilvipalveluiden merkitystä ja tarkoitusta yrityksen toiminnassa, sekä sitä millaisia riskejä heidän käyttämiinsä pilvipalveluihin liittyy ja ovatko he huomioineet näitä riskejä. Jatkuvuuden hallintaan liittyen haastateltavilta kartoitettiin heidän näkemyksiään aiheesta, sekä heidän edustamansa yrityksen tilaa jatkuvuuden hallinnan osalta. Kolmanteen teemaan liittyen haastateltavilta tiedusteltiin heidän näkemyksiään pilvipalveluiden jatkuvuuden hallintaan liittyen. Lisäksi kartoitettiin millaiset tekijät parantaisivat kyseisen yrityksen varautumista ja yritystoiminnan jatkuvuutta pilvipalveluiden osalta. Kaikissa haastatteluissa teemoja käsiteltiin saman haastattelurungon kautta, mutta usein haastateltaville esitettiin lisäkysymyksiä heidän vastauksiinsa perustuen. Merkittävänä huomiona haastatteluista

tehtiinkin, että usein tutkimuksen kannalta olennaista tietoa saatiin haastattelurungon ulkopuolelta olevilla kysymyksillä.

5.4 Haastatteluaineiston käsittely ja analysointi

Haastatteluaineiston käsittely aloitettiin katsomalla videomuotoiset haastattelut ja kuuntelemalla äänimuodossa oleva haastattelu. Tämä palautti haastatteluiden sisällön mieleen. Videomuotoisista haastatteluista irrotettiin tämän jälkeen ääniraidat ja muodostuneille ääniraidoille suoritettiin litterointi. Litteroinnit suoritettiin vuoden 2023 marraskuussa hyödyntäen tietoarkiston litterointiohjetta (Tietoarkisto, 2023). Litteroinneissa noudatettiin sanatarkkaa litterointia, kuitenkin niin, että puheen sisältämät takeltelut, tauot ja saman asian toistaminen poistettiin. Litteroinnin yhteydessä haastatteluista korostettiin tutkimusaiheelle keskeisiä vastauksia yliviivaamalla, eli aineistolle toteutettiin laadulliselle tutkimukselle tyypillistä luokittelua (Hirsijärvi & Hurme, 2022). Litteroiduista haastatteluista kertyi aineistoa yhteensä 36 sivua.

Laadullisen aineiston analyysin tarkoituksena on luoda aineistoon selkeyttä ja siten tuottaa uutta tietoa tutkittavasta asiasta (Eskola & Suoranta, 1998). Hirsijärvi ja Hurme (2022) ohjeistavat teemahaastattelun tekijää miettimään aineiston analyysitapaa jo aineistoa kerättäessä. Kun tutkija tekee haastattelua, hän voi jo haastatellessaan tehdä havaintoja ilmiöistä erilaisiin teemoihin pohjautuen (Hirsijärvi & Hurme, 2022). Tämän tutkimuksen tavoitteena oli tutkia pienten yritysten jatkuvuuden hallinnan käytänteitä, sekä selvittää millaisia ominaisuuksia onnistunut pilvipalveluita koskeva jatkuvuussuunnitelma sisältää. Haastateltavien vastauksissa oli havaittavissa toistuvia teemoja ja täten tutkimuksen analysointimenetelmäksi valittiin teema-analyysi, josta käytetään myös nimitystä teemoittelu. Teemoittelussa aineistosta etsitään ja paikannetaan tutkimusongelman kannalta olennaisia teemoja. (Eskola & Suoranta, 2008) Tämän tutkimuksen haastattelurunko oli niin ikään jaettu teemoihin. Juhila (2023) kuitenkin muistuttaa verkkokäsikirjassaan, että haastattelun teemat eivät ole sama asia kuin analyysin tuloksena syntyvän aineiston teemat: aineistosta esiin nousevat teemat syntyvät analyysin tuloksena – eivät niin, että tutkijalla on mielessään teemat, joihin hän sijoittelee aineistonsa palasia. Syntyviä teemoja ei siis tässä tutkielmassa jaettu etukäteen, vaan niitä havainnoitiin haastatteluiden jälkeen. Teemoittelussa hyödynnettiin Microsoft Excel -työkalua. Teemoittelu aloitettiin koostamalla vastaukset kysymyksittäin ja värikoodaamalla haastateltavien vastaukset eri väreillä. Koosteen jälkeen haastatteluvastauksista oli mahdollista poimia niitä yhdistäviä teemoja. Teemat jaoteltiin tämän jälkeen tutkimusongelmien mukaan seuraavasti:

- Tutkimusongelman ”Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja onko siinä huomioitu pilvipalveluita?” alle kerättiin tietoa siitä, miten pienet yritykset ovat huomioineet riskejä ja miten ne ovat varautuneet erilaisiin toiminnan häiriötilanteisiin sekä sitä, onko

pilvipalveluihin liittyviä jatkuvuusriskejä huomioitu yritysten jatkuvuussuunnittelussa. Tavoitteena oli kartoittaa tutkimusongelmaan vastaamisen ohella sitä, millä tasolla pienten yritysten valmius toteuttaa jatkuvuussuunnittelua on, ja millaisten haasteisiin yritykset ovat törmänneet pohtiessaan toimintansa jatkuvuuden varmistamista. Keskeistä tutkimusongelmaan vastaamisen kannalta oli lisäksi selvittää pilvipalveluiden merkitystä ja käyttökohteita haastateltavissa yrityksissä, täten voitiin varmistaa tutkimusongelman merkityksellisyys. Lisäksi tutkimusongelman yhteydessä selvitettiin missä määrin yritys hyödyntää pilvipalveluita ja miten niiden merkitys on viimeisten vuosien aikana muuttunut.

- Toisen tutkimusongelman ”Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?” alle kerättiin haastateltavien esiin nostamia teemoja pilvipalveluihin liittyvän jatkuvuuden parantamiseen. Tähän tutkimusongelmaan liittyen kartoitettiin yritysten kokemia riskejä pilvipalveluihin liittyen, sekä sitä ovatko he kokeneet pilvipalveluista johtuvia toiminnan häiriöitä. Tämän jälkeen haastateltavilta kartoitettiin tekijöitä, jotka he kokivat haasteellisina pilvipalveluiden jatkuvuutta suunniteltaessa, sekä tekijöitä, jotka helpottaisivat pilvipalveluita koskevan jatkuvuussuunnitelman laadintaa ja päivittämistä. Lisäksi kartoitettiin yritysten valmiuksia toteuttaa ja noudattaa jatkuvuuden hallintaa osana päivittäistä toimintaa.

Tieteellisessä tutkimuksessa haastatteluista tehtyjä havaintoja ei voida kuitenkaan Puusan ja Juutin (2020) mukaan hyväksyä sellaisenaan, vaan ne tulee purkaa osiin ja niitä tulee tarkastella kriittisesti. Haastatteluaineistosta etsittiinkin myös selvästi erilaisia vastauksia, jotta samankaltaisuutta voitiin vahvistaa ja jotta tuloksia ei yleistettäisi liikaa. Havainnoista, sekä myöhemmin niistä johdetuista teemoista pyrittiin muodostamaan kokonaisuuksia, jollaisia ei yksittäisistä vastauksista voitaisi muodostaa. Syntyneitä teemoja peilattiin suhteessa yksittäisiin havaintoihin, jotta kokonaisuuden ja syntyneiden teemojen yhteensopivuus voitiin varmistaa.

6 TULOKSET

Tässä luvussa esitellään empiirisen tutkimuksen keskeisimmät tulokset jaoteltuna alalukuihin tutkimuskysymysten, ja edelleen teemojen mukaisesti. Ensimmäiseen tutkimusongelman ”Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja onko siinä huomioitu pilvipalveluita?” ratkaisemiseksi etsittiin teemoja pienyritysten jatkuvuuden hallinnan käytänteistä, sekä pilvipalveluiden roolista osana jatkuvuuden hallintaa. Toisen tutkimusongelman ”Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?” alle kerättiin empiirisessä osiossa havaittuja tekijöitä, joita pienet yritykset kertoivat arvostavansa pilvipalveluita koskevassa jatkuvuussuunnitelmassa. Haastattelussa esiinnousseita teemoja peilattiin myös kirjallisuuskatsauksessa läpikäytyyn teoriaan, jotta jatkuvuuden hallinnalle keskeisiä asioita voitiin havainnoida.

6.1 Jatkuvuuden hallinnan toteuttaminen

Tässä luvussa kuvataan haastatteluissa esiin tulleita teemoja, jotka vastaavat tutkimusongelman: ”Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja siinä huomioitu pilvipalveluita?” jatkuvuuden hallinnan toteuttamista koskevaan osaan. Haastateltavia pyydettiin kuvaamaan mitä jatkuvuuden hallinta heidän yrityksessään tarkoittaa ja kenen vastuulla jatkuvuuden hallinnan toteuttaminen on. Lisäksi tiedusteltiin jatkuvuuden hallintaan liittyvien asioiden huomiointia, sekä kartoitettiin yritysten laatimia toimintaohjeita ja dokumentteja jatkuvuuden hallintaan liittyen.

6.1.1 Jatkuvuuden hallinnan merkitys

Yrityksille avattiin haastattelukutsun ohella myös haastattelun alussa jatkuvuuden hallinnan käsite. Tämän jälkeen haastateltavilta kysyttiin, miten he kokevat jatkuvuuden hallinnan ja siihen liittyvien toimien merkityksen yrityksessään. Kaikki yritykset tunnistivat, että liiketoiminnan jatkuvuuteen liittyvät toimet

ovat tärkeitä ja jatkuvuussuunnittelu on tärkeä osa kaikenkokoisten yritysten toimintaa.

> H1: Meillä ja varmasti monella muullakin yrityksellä ehkä vähän liian vähän käytetään siihen aikaa ja luotetaan että ne toimivat ja on aina käytettävissä. Sitten siinä on tietysti se, että mikä on sen yrityksen kriittinen piste, että miten pitkään voi olla ilman jotain palvelua.

> H2: Joo toistaiseksi ei ole ollut kyllä mitään [ongelmia]. Nämä kotimaan verkot on sen verran hyviä ja laadukkaasti tehtyjä että niissä ei ole ongelmaa. Mutta sitten kun ruvetaan menemään ulkomaille niin sitten ruvetaankin kysymään vähän eri lailla sitä, että selvitetään ensin ne haasteet ennen kuin ruvetaan sitten rakentamaan sitä (liiketoimintaa).

> H5: Tää oli semmoinen osa-alue mitä ei oikein edes ole osannut ajatellakaan. Jos pilvipalveluille tai muille It-puolen asioille tapahtuu jotain tai jos jotakin menee muuten tosi pahasti mönkään, niin miten sitten pärjätään.

Lähes kaikki yritykset olivat kokeneet häiriöitä jotka haittasivat liiketoiminnan jatkuvuutta, mutta eivät olleet kokeneet liiketoimintansa vaarantuneen häiriöstä. Häiriöt liittyivät pääosin järjestelmiin tai yrityksille tärkeiden yhteistyökumppaneiden toimintaan. Jatkuvuuden hallinnan merkitys tunnistettiin, mutta mahdollisia toimenpiteitä jatkuvuuden ja varautumisen parantamiseksi ei ollut pohdittu, eikä asian korjaamiseksi ollut tehty kattavia toimenpiteitä. Jatkuvuuden hallinnan toteuttamisen keinoja, sekä syitä puutteelliselle toteuttamiselle on avattu lisää seuraavissa alaluvuissa.

6.1.2 Suunnitelmien puute, sirpaleisuus ja suppea kattavuus

Yhtä lukuun ottamatta kaikki yritykset olivat tehneet jatkuvuuteen liittyviä toimia, mutta toimien merkitys ja kattavuus oli vaihtelevaa. Etenkin perinteisiin liiketoiminnan riskeihin oli varauduttu. Tämä tarkoitti esimerkiksi varatyökalujen ja -materiaalin hankkimista, kilpailutilanteen ja uusien trendien seuraamista, sekä uusien liiketoimintamahdollisuuksien kartoittamista:

> H1: Kyllä nimenomaan sitten taas näiden muiden työkalujen osalta mistä just puhuinkin, on sitten suunnitelmat olemassa ja varauduttu asioihin. Esimerkiksi on työkaluja hallilla, jos menee työntekijällä työkalut hajalle niin voi sieltä hakea uuden ja muutenkin kalustoon liittyvät jutut. Onhan meillä peräkärryjäkin periaatteessa varalla tai heti saatavilla lisää tai kaluston tapauksessa myös sitten semmoinen vakio huoltopaikka missä [kalustoa] voi huoltaa. Kyllä tämmöisessä sitten puolestaan on sitten varauduttu. Näissä käytännön asioissa.

> H3: Hankkeita ja ajatuksia uusista hankkeista on koko ajan menossa, eli liiketoimintaa pyritään sillä tavalla jatkamaan. Totta kai se tarkoittaa [myös] sitä, että meidän pitää koko ajan katsoa, että mitä maailmalla syntyy uudenlaisia mahdollisuuksia ja miten tekniikka menee eteenpäin, että on tavallaan sitä semmoista päivittäistä kouluttautumista myös ja yrittää pysyä kärryillä siinä, että olisiko mahdollisuus tehdä paremmin asioita teknisessä mielessä myös.

Kirjallisuuden mukaisesti jatkuvuuden hallinnalle on keskeistä tunnistaa liiketoimintaan liittyvät ydintoiminnot (Niemimaa ym., 2019; Valtionhallinnon tietoja kyberturvallisuuden johtoryhmä, 2016). Haastateltavat tunnistivat yritystensä keskeisen liiketoiminnan ja siihen liittyvät tärkeimmät tukiprosessit, mutta eivät olleet pohtineet riskien tunnistamista, analysointia ja vastatoimien määrittämistä riskeille. Kahdessa yrityksessä asiasta oli keskusteltu johdon piirissä, mutta koottua dokumenttia yrityksen jatkuvuuden hallinnasta ei yhdessäkään yrityksessä ollut toteutettu, vaan jatkuvuuteen liittyvä dokumentaatio oli hajanaista ja satunnaisiin toimintoihin liittyvää. Yksi vastaajista kertoi, että heillä on kuvattuja toimintamenettelyjä esimerkiksi työssä tarvittavien tarvikkeiden toimituskatkosten varalle: Toimittajasopimuksia oli useita, ja omat varastot mahdollistivat toiminnan jatkuvuuden lyhyissä katkoksissa näiden osalta. Toimintamenettelyjä koskevat suunnitelmat eivät kuitenkaan kattaneet kaikkia liiketoimintaan liittyviä prosesseja, vaan keskittyivät työtarvikkeiden saatavuuteen. Jatkuvuuden hallintaa koskevassa kirjallisuudessa korostuu myös proaktiivisuus (Gibb & Buchanan, 2006; Niemimaa & Järveläinen, 2013; Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, 2016). Haastateltavien yritysten edustajat kuitenkin kertoivat toteuttavansa pääosin reaktiivisia toimia kohdatessa jatkuvuutta uhkaavia tapahtumia:

> H2: No ei kirjallisesti ole [kirjattu asioita]. Se on ollut vähän tilannekohtaista se [varautuminen]. Enemmän sysätään jatkuvuuteen liittyviä vastuita alihankkijoille, joiden avulla liiketoimintaa osittain toteutetaan

> H4: Me on tässä nyt 10 v toimittu siten, että osa [henkilökunnasta] on ollut alusta asti mukana niin se on aika vakiintunutta toimintaa. Ei ole kirjallisia ohjeita olemassa vaikkapa poikkeustilanteisiin liittyen.

> H5: No ei kirjallisesti ei ole [suunnitelmia]. Se on ollut vähän tilannekohtaista, että jos on vaikka sähköposti ollut poissa käytöstä hetkellisesti tai sitten jos on jossain muissa noissa yhteyksissä ollut (ongelmaa), että vaikka postin kautta ei olla pystytty lähettämään paketteja kun, ei päästä tulostamaan niitä osoitekortteja niin sitten ollaan manuaalisesti vaihdettu niitä toiselle kuljetusyhtiölle, mutta ei ole mitään semmoista kirjallista dokumenttia olemassa.

Osa yrityksistä oli kuitenkin laatinut erilaisia toimintaohjeita esimerkiksi työntekijöille ja järjestelmien korvaamiseen. Yksi yrityksistä oli kuvannut erilaisia skenaarioita ja toimintasuunnitelmia skenaarioiden varalle. Yksikään yrityksistä ei ollut etsinyt tietoa jatkuvuuden hallintaan liittyen, eikä toteutukseen ollut katsottu mallia.

> H1: Ei taida olla mitään selkeetä mallia kyllä, että ehkä poimittu vähän niinku eri paikoista näkemystä asiaan ja sitten itse muodostettu käytännössä se suunnitelma. Sellaisella itselle sopivalla muodolla.

> H2: No suoranaisesti ei [ole etsitty tietoa], mutta niistä on kyllä puhuttu. Siis näiden toimijoiden kanssa on sitten puhuttu, mutta siitä ei ole mustaa valkoisella.

Kaikki haastateltavat kertoivat, että haasteeksi tai esteeksi jatkuvuuden suunnittelulle oli muodostunut yleensä resurssien, pääosin ajan tai rahan puute. Haastateltavat kokivat, että ennakoitavia ja huomioon otettavia asioita oli pienestä yrityskoosta huolimatta paljon, eikä heillä ollut mahdollisuuksia toteuttaa jatkuvuuden hallintaa kirjallisuudessa määritellyssä laajuudessa. Lisäksi jatkuvuuden tilan säännönmukainen tarkastelu koettiin haastavaksi, koska varsinaiset työtehtävät vaativat paljon aikaa:

> H3: No ainakin omasta puolesta voi sanoa, että aika on aina kortilla. Se on ehkä se kaikista suurin. Tietenkin pieni yritys ja kaikkien pitää aika paljon tehdä sitten kaikennäköistä hommaa, niin siinä mielessä, että kun ei ole isoja organisaatioita, että voitaisiin laittaa ja pilkkoa palasiin ja jakaa vastuualueita, joista pidettäisiin koko ajan huolta, että se ajan löytäminen ja asettaminen sitten niihin päivän rutiineihin, niin se on ehkä se suurin haaste teknisessä mielessä.

> H1: Aika, resurssit, henkilöstöresurssit ja että olisi vähintään suunnitelma siitä, että milloin seuraavan kerran katsotaan sitä. Ja sitten se, että jos tulee semmoisia yllättäviä juttuja mieleen ennen sitä suunniteltua palaveria, että pystyis tai kerkeis käyttämään aikaa. Käytäisiin läpi ennen kuin on se suunniteltu ajankohta. Ehkä jos miettii miten sen ylläpitäminen niin nimenomaan nuo asiat tulee mieleen.

> H2: Valmiit mallit ja sitten semmoinen automaatti raportointi. Että tulisi semmoinen automaatti raportti tietyn väliajoin. Helpottaisi jatkuvuuden hallinta, että se pysyisi ajantasaisena se homma.

> H5: Ehkä isompana varmaan oman ajan resursointi. Ja se, että ei oikein niinku ole osannut lähteä liikkeelle selvittämään asian tai ei ole tiennyt, että miten pitäisi toimia ja mihin pitäisi keskittyä.

6.1.3 Henkilöstöriskit ja jatkuvuuden hallinnan vastuut

Henkilöstöriskeihin oli varauduttu yritysten pienestä työntekijämäärästä huolimatta hyvin. Niemimaan ja Järveläisen (2013) mukaan yrityksen jatkuvuudelle on tärkeää, että rutiinitehtävien hoitaminen on mahdollista useamman kuin yhden työntekijän toimesta. Yleisin varautumiskeino yrityksissä oli henkilöstön kouluttaminen siten, että työntekijöillä on ammattitaito tehdä myös toisen työntekijän työtehtäviä. Haastateltavat kertoivat myös, että työntekijät hoitavat laajasti erilaisia tehtäviä ja usein useammalla kuin yhdellä työntekijällä oli samat työtehtävät:

> H3: Jokaisella on tässä oma ruutunsa ja sitten kun pieni firma niin ne on vähän päällekkäinkin ne roolit. Jos joku henkilöstöstä on jostain syystä pois niin hommat ei kuitenkaan pysähdy. Laajasti sitä vastuuta on jaettu.

> H4: Se menee silleen, että vaikka tulisi uusi työntekijä, niin sekin tulee ensin tavallaan oppiin sinne tunnille. Tai sitten jos tulee aspaan joku uusi niin sekin tulee oppiin ja sen kanssa sitten käydään asiat läpi.

Jatkuvuuden vastuiden määrittäminen on keskeinen osa jatkuvuuden hallintaa ja se on kirjallisuuden mukaan yksi ensimmäisistä jatkuvuussuunnittelun vaiheista (Estall, 2012; Niemimaa & Järveläinen, 2013; SFS, 2023). Jatkuvuuden hallinnan vastuut tunnistettiin haastateltavissa yrityksissä hyvin. Kokonaisvastuu varautumisesta oli lähes kaikkien haastateltavien mukaan johdolla ja yrittäjillä, mutta osassa yrityksistä jatkuvuuden varmistamiseen liittyviä keskusteluja käytiin myös väliportaissa ja työntekijätasolla.

> H1: No kyllä päävastuu on toimitusjohtajalla. Päävastuu on hänellä, mutta mä oon oikeastaan se ensimmäinen joka käytännön tasolla siitä vastaa. Mutta sitten oikeastaan nuo pienemmät yksittäiset jutut mitkä sitten liittyvät jatkuvuuden hallintaan niin niitä asioita käydään läpi sitten muuten tässä työnjohdon ja tuotannonjohdon ja yksikön päälliköiden ja ketä nyt on (johtoa) niin kesken. Välillä käydään niitä asioita läpi suullisesti ja välillä saatetaan kirjata johonkin ylös, mutta ei välttämättä suoraan sitä virallista dokumentaatiota päivitetä tai käydä sen tilaa läpi. Pohditaan ja suunnitellaan asioita paljon keskenämme, mutta sitä meidän varsinaista suunnitelmaamme ei välttämättä tuommoisessa tilanteessa tule katsottua läpi. Se on sitten asia erikseen.
>
> H2: Kyllä jatkuvuuteen liittyvät asiat on täysin mun [toimitusjohtajan] vastuulla.
>
> H3: Lopultahan se on toi meidän toimitusjohtajamme ja yrittäjät, jotka vastaa ja jotka kertoo mitä tehdään [poikkeustilanteissa].

6.2 Pilvipalveluiden huomiointi osana jatkuvuuden hallintaa

Osana jatkuvuuden hallinnan toteuttamista, selvitettiin yrityksistä myös pilvipalveluiden merkitystä ja huomiointia osana jatkuvuuden hallintaa. Haastateltavia pyydettiin kertomaan pilvipalveluiden merkityksestä yritykselle, pilvipalveluihin liittyvistä riskeistä, sekä varautumisen ja jatkuvuuden toteuttamisesta pilvipalveluiden osalta. Pilvipalveluiden palvelumalleista korostui SaaS-mallilla toteutetut palvelut. Haastateltavat yritykset hyödynsivät pilvipalveluita osana keskeisiä liiketoiminnan prosessejaan. Kaikki haastateltavat kertoivat pilvipalveluiden merkityksen kasvaneen vahvasti viime vuosina, ja moni haastateltavista totesi, että liiketoiminnan toteuttaminen olisi joko täysin mahdotonta tai erittäin haastavaa ilman pilvipohjaisia järjestelmiä.

> H1: Joo elikkä tota, tuo on tietysti aika laaja kysymys. Varmaan vastaan sitten mitä kaikkea meillä tehdään. Meillähän käytetään pilvitallennustilaa. Sähköpostit ja ryhmävideopalvelut ja muut toki kuuluvat sinne, mutta sitten meillä on pilvessä sitten tämmöisiä taulukkolaskentaohjelmia, joilla lasketaan esimerkiksi menekkiä ja kuinka paljon on tullu hävikkiä ym. Taulukkolaskentaa käytetään vielä manuaalisesti semmoisiin tiettyihin juttuihin ja sitten meillä on toiminnanohjausjärjestelmässä meidän henkilöstömme tiedot ja varsinkin sesongin aikana kerätään kaikista työntekijöistä tietoa. Kaikkien tiedot löytyvät sieltä [toiminnanohjausjärjestelmästä]: numerot ja sähköpostit ja muut tarvittavat tiedot mitä meidän tarvitsee tietää. Käytännössä se toiminnanohjausjärjestelmä on se mistä löytyy yrityksen ydindata. Siellä on oikeastaan

> kaikki. Käytännössä kaikki tiedot mitä yrityksellä on. Sitten riippuen siitä, että missä roolissa on yrityksessä, että mihin kaikkiin tietoon pääsee käsiksi.
>
> H3: Joo tuota lähinnä mä näkisin, että meidän suurin haasteemme mikä on, ja minkä takia noihin pilvipalveluihin on kannattanut siirtyä ja mennä niin on materiaalin koko. Elikkä tarvitaan aika paljon tilaa ja sitten tietenkin toinen juttu on se, että kun käyttäjäkunta on lisääntynyt aika kovasti, niin tarvitaan kapasiteettia, että pystytään tarjoamaan sekä materiaali että laatua.
>
> H4: No onhan ne toiminnan tavallaan kulmakiviä. Ilman niitä ei tultaisi millään toimeen.
>
> H5: Tärkeä osa yrityksen liiketoiminnasta tapahtuu verkossa, että jotenkin se on semmoinen vähän abstrakti käsitys. Siellä on kaikki. Siellä on meidän kuvapankit ja sieltä siirtyy meidän aineistomme kirjanpitäjälle ja tietenkin sähköpostiliikenne ja sitten verkkosivusto ja sitä kautta sitten kaikki maksu ja nuo logistiikka järjestelmät. Onhan sen merkitys on tosi iso.

Tutkimuksissa on selvinnyt, että pilvipalveluihin liittyvät turvallisuusvastuut toimittajan ja asiakkaan välillä eivät ole aina täysin selkeitä (Ghaffari ym., 2016; Hendre & Joshi, 2015). Tämä voi johtaa jatkuvuuden vaarantumiseen tai heikentymiseen, koska kaikkia riskejä ei välttämättä huomioida. Kyseiseen havaintoon liittyen haastateltavilta kysyttiin, ovatko he tietoisia yrityksensä vastuista pilvipalveluiden turvallisuuteen liittyen ja ovatko yritykset käyneet keskustelua toimittajan kanssa asiasta. Vastauksista kävi ilmi, että yhtä lukuun ottamatta haastateltavat yritykset eivät olleet kommunikoineet palveluntarjoajan kanssa turvallisuuteen liittyvistä vastuista, eivätkä yritykset olleet perehtyneet yleisiin jakolinjoihin vastuiden osalta.

> H2: Kyllä se vastuu on viritetty ihan täysin niinku heille. Joo että he vastaa siitä sitten, että jos siellä jotain tapahtuu niin he vastaa sitten siitä.
>
> H3: Kyllähän ne on meidän sopimuksiimme kirjattu, että mikä kuuluu kenellekin ja kuka vastaa mistäkin että. Ne on sillä tasolla. Silloin kun kyseinen toiminta on aloitettu. Ja tietysti keskustelua käydään aina silloin kun on tarpeen.
>
> H4: No ei ole ollut silleen. Tavallaan luotto on ollut siihen, että ne on hoitanut sen oman osansa. Ei olla kyseenalaistettu sitä.

Yrityksen oma jatkuvuuden hallinta aloitetaan riskien tunnistamisella ja vaikutusten määrittämisellä (Niemimaa & Järveläinen, 2013). Haastateltavilta kysyttiin, millaisia riskejä heidän käyttämiinsä pilvipalveluihin jatkuvuuden näkökulmasta liittyy. Kaikki vastaajat kertoivat, että käyttökatkokset, sekä tietoturvaan liittyvät riskit kuten pääsynhallinnan ongelmat ja hakkerointi voivat olla potentiaalisia riskejä jatkuvuuden hallinnan näkökulmasta. Haasteet järjestelmien hallinnassa toistuivat niin ikään useiden haastateltavien vastauksissa: järjestelmien lukumäärä ei ollut selvillä, pääsyoikeuksien hallinta koettiin haasteelliseksi, ja salasanojen kasvanut lukumäärä aiheutti yhden haastateltavan mukaan riskin

jatkuvuudelle. Vastaajat kuitenkin kokivat riskit pieniksi ja luottivat vahvasti palveluntoimittajiin ja heidän kykyynsä vastata riskeihin.

> H2: No siis tänä päivänä se hakkerointi on niin kun selkeästi suurin. En mä oikein muuta uhkaa näe muuta kuin siinä, että joku haluaa kaataa ne sivut sieltä tai sitten että hakkeroi ne sivut ja muuntaa niitä tuloksia mitä siellä on. Enemmän sysätään sitä vastuuta sitten niille alihankkijoille, jotka toimittaa sen mittausdatan ja raportoinnin, niin me velvoitetaan sitten taas niiltä, että se pitää toimia häiriöttömästi ja heidän varmuuskopioihinsa sitten tukeudutaan siinä vaiheessa, jos jotain tulee.

> H3: Tietysti tää kumppanien valinta on tärkeä asia tässä, kun meillä on näitä omia palveluja tehty. Nää on ollut kyllä ihan tämmöisiä tarkoin valittuja kotimaisia toimijoita, joiden kanssa on rakennettu näitä palveluita. Keskusteluyhteys on hyvä ja vastataan nopeasti, jos jotain häiriöitä tulee.

> H5: Varsinkin nyt viimeisen vuoden aikana korostunut tuo itänaapurin tilanne minkälaisia palvelunestohyökkäyksiä pelkästään sieltä käsin pystytään tekemään ja saati sitten kaikki muut tahot siihen päälle. Onhan ne silleen aika isoja riskejä, mutta jotenkin palvelujen ostajana niin on vaan tuudittautunut siihen, että nää palvelut ja ylläpitäjät ja tuottajat niin että heillä on sitten se vastuu ja jollain lailla velvollisuuskin varautua siihen, että itse pystyisi sitten ostamaan jollain lailla turvallista tuotetta tai palvelua.

> H4: No kyllä mä sen koen silleen, että kun me olemme jonkun asiakkaita, niin ne [palvelutoimittajat] on tavallaan vastuussa, että se on suojassa siellä se tieto. Meillä lähinnä on se [vastuu], että kukaan ei niinku pääse siihen tietoon meidän koneiden kautta sitten. Mitään sellaista erillistä dokumentaatiota ei ole, että jos tulisi joku palvelunestohyökkäys tai jotain muuta. Jonkin verran on esimerkiksi myyntikampanjan yhteydessä ostettu meidän nettisivuillemme lisää palvelinkaistaa. Se olisi tyhmää, jos se lakkaisi toimimasta juuri silloin kun ihminen on ostamassa. Silloin jäisi varmasti kaupat tekemättä.

Haastattelussa kysyttiin riskien jälkeen sitä, miten hyvin yritykset mielestään ovat varautuneet näihin riskeihin. Riippuvuuksia liiketoiminnan ja pilvipalveluiden välillä ei ollut yrityksissä juuri pohdittu, vaan haastateltavat pohtivat pilvipalveluiden merkitystä liiketoiminnalleen haastattelun aikana. Yritykset kertoivat kahta yritystä lukuun ottamatta, että riskien ja niiden todennäköisyyksien hahmottaminen, vastuiden tiedostaminen, sekä vaikutusten arviointi on hankalaa.

> H4: Ei [ole riskejä kartoitettu järjestelmien välillä], että kyllä se vertailu on ollut enemmän sitä, että tavallaan se toiminnallisuus suhteessa siihen hinnoitteluun, että kyllä siellä varmasti olisi paljon tehostettavaa.

> H1: Kun on niin vähän aikaa, että meidänkin firmassamme ei niinku ole käytännössä resursseja. Sanotaan että minä olen varmaan sellainen, jolla on eniten annettavaa siihen asiaan firman sisältä. [Ei ole tietoa] että miten sitä laadittaisiin sitä ohjausta niihin liittyen, mutta kun ei ole aikaa ja resursseja siihen hommaan, niin käytännössä se olisi kaikista helpoin, kun joku vaan sanoisi, että miten se tehdään. Kyllä se aika ja resurssi menee kaikkeen ns. "muka" tärkeään. Tässä hommassa varmaan monella muullakin

> [on], että ei välttämättä tommoista jatkuvuuden hallinnan suunnittelua pilvipalveluiden osalta tule tehtyä. Pitäisi olla joku, joka sanoo mitä tehdä.

Pohdittaessa pilvipalveluihin liittyviä jatkuvuusriskejä, nähtiin pilvipalvelut yrityksissä lähinnä jatkuvuutta parantavana tekijänä ja erilaisten toimintaa haittaavien häiriöiden kohdatessa vastaajat luottivat, että asiakkaana heidän tulee saada riittävän hyvää palvelua palveluntoimittajalta. Tämän voidaan tulkita tarkoittavan sitä, että haastateltavien mielestä pilvipalveluihin liittyvä varautuminen on lähes täysin pilvipalveluiden tarjoajan vastuulla. Riittävän hyvää palvelutasoa tai käyttökatkosten maksimipituutta ei yksikään yrityksistä ollut pilvipalveluille määrittänyt. Pilvipalveluiden jatkuvuuden kokemista ja merkitystä on kuvattu alla olevissa lainauksissa.

> H1: Se [liiketoiminta] niinku vaatii ton, että me pystytään kaikki löytää se tieto heti ihan sama missä me sitten työskentelemmekin.

> H3: Ja lähinnä on tärkeä [pilvipalveluilla] varmistaa se, että materiaalit varmasti on sitten jossain tallessa, että vaikka ympäristöt ja nämä menisi joskus aivan totaalisesti kiinni, niin se materiaali sitten löytyy jostain. Sitä kun on aika reilusti.

> H4: No esimerkiksi se oli hyvä esimerkki, kun se emolevy siitä koneesta kärähti. Niin nyt kun ne on siellä pilvessä, niin tavallaan tietää, että ihan sama, että sitten voi käydä hakemassa, vaikka samana päivänä uuden [tietokoneen] siihen [tilalle] ja tavallaan se data on pilvitallennustilassa ja sitten asiakkuuksien data on siellä kulunhallintajärjestelmän pilvessä ja siruavaimet. Ja laskutustiedot on laskutusjärjestelmässä. Ni jatkuvuutta ajatellen kaikki rauta voi mennä rikki, mutta uskon kun ne on tuommoisessa pilvessä niin eiköhän siellä ole aika hyvät varmuuskopion varmuuskopiot.

6.3 Onnistuneen pilvipalveluita koskevan jatkuvuussuunnitelman ominaisuuksia

Tähän osioon kerättiin teema-analyysin avulla yritysten vastauksista esiinnousseita teemoja, joita yritykset arvostaisivat onnistuneessa pilvipalveluita koskettavassa jatkuvuussuunnittelussa. Teemat on esitelty erillisissä alaluvuissa. Haastateltavilta kysyttiin ensin, pitäisivätkö he valmista ohjetta hyödyllisenä. Haastateltavat olivat yksimielisiä siitä, että jos olemassa olisi nimenomaan heille sopiva malli, olisi se heidän yrityksellensä hyödyllinen.

> H4: Jos joku tällaisen kehittäisi, niin kyllähän siihen kannattaisi varmasti ainakin tutustua. että olisiko kenties tehokkaampaa tai ei olisi niin sirpaleista.

> H3: Ajatus on sinänsä hyvä, mutta sen pitäisi oikeasti palvella pienenkin yrityksen liiketoimintaa eikä tuoda vaan lisää töitä. Sellaiseen mä en ole vielä törmännyt ja siksi minusta on tullut vähän skeptinen.

> H1: No siis en mä osaa oikein ajatella tuota miltään muulta kannalta tällä hetkellä, kun siltä, että olisi joku selkeä ohjeistus, miten se kannattaisi tehdä. Kun on niin vähän

aikaa, että meidänkin firmassamme ei ole käytännössä mahdollista toteuttaa sitä muuten.

6.3.1 Helppokäyttöisyys, selkeys ja ymmärrettävä kieli

Haastateltavat olivat yksimielisiä siitä, että pilvipalveluita koskevan jatkuvuussuunnitelman tulisi olla selkeä ja ymmärrettävä, sekä riittävän helppokäyttöinen pienten yritysten resursseilla hyödynnettäväksi. Aiemmin tutkielmassa esiteltyjen mallien voidaankin havainnoida olevan kattavia, mutta toisaalta myös sisältävän paljon resursseja vaativia vaiheita, kuten analyysejä, suunnitelmia ja testaamista (Niemimaa & Järveläinen, 2013; SFS, 2023). Yhdellä haastateltavalla oli kokemusta jatkuvuuden hallinnan kokonaisjärjestelmistä ja hänen mielestään ne olivat liian hankalalukuisia sekä raskaita pienten yritysten käyttöön. Malli ei saisi hänen mukaansa aiheuttaa kohtuuttomasti vaivaa, koska silloin sitä ei todennäköisesti hyödynnettäisi. Myös muut haastateltavat toivoivat, että jatkuvuussuunnitteluun hyödynnettävä malli olisi riittävän helppokäyttöinen, jotta sen hyödyntäminen onnistuisi myös ilman vahvaa aihealueen tuntemusta.

> H3: Olin edellisessä työpaikassa, jossa meillä oli laatujärjestelmiä käytössä, mutta ainakin silloin niitä otettiin käyttöön lähinnä toimeksiantajan vaatimuksesta, eikä niistä oikeasti ollut mitään hyötyä. Ne oli semmoista sanotaanko korkealentoista toimintaan nähden, ei kovin käytännönläheistä. Me teimme sitten ihan omat suunnitelmat ja mentiin niiden mukaan. Kun niiden seurannasta ei saatu mitään hyötyä, tai ei ollut mitään seurantaa, niin ei sieltä löytynyt sille alalle semmoista mikä olisi liiketoimintaa hyödyntänyt.

> H2: Se [jatkuvuussuunnittelun malli] olisi tosiaan kirjoitettu sellaisella kielellä, että niin sanottu tavallinen ihminen, -ei nörtti- niin ymmärtää myös mistä on kyse ja mitä pitää tehdä. Välttäisin kaikkia semmoisia termejä, jotka esimerkiksi mulle ei kerro mitään. Niin silloin varmaan löytyy se kohderyhmä.

> H5: No ehkä tietenkin semmoinen mahdollisimman laaja, josta pystyisi poimimaan ne mitkä omaa liiketoimintaa koskettaa. Niin se olisi ainakin semmoinen jollain lailla ymmärrystä lisäävä ja silmiä avaava. Kun ei osaa itse välttämättä kaikkea edes huomioida, niin siitä saisi hyvin osviittaa.

Kolme haastateltavaa nosti esiin mallin selkeyden. Nämä haastateltavat toivoivat, että helppokäyttöisyyden lisäksi mallissa kerrottaisiin selkeästi sen tarkoitus, käyttötilanteet ja vaadittavat toimenpiteet. Mallin tulisi haastateltavien mukaan kuvata riittävän yksityiskohtaisesti asiat, joita tulisi huomioida pilvipalveluiden jatkuvuuden hallintaa suunnitellessa. Jatkuvuuden hallinnan teoriaan peilaten vaatimusten ja tavoitteiden tulee olla selkeitä organisaation henkilöstölle (Niemimaa & Järveläinen, 2013).

> H1: Että olisi niinku joku selkeä ohjeistus, miten se kannattaisi tehdä. Kun on niin vähän aikaa, että meidänkin firmassamme ei niinku ole käytännössä [resursseja].

> H2: Mielellään ei mitään semmoista mistä tulee vaan lisää töitä, mutta jos oikeasti antaa jotain hyvää, niin semmoisia me kyllä käytämme mielellään.

> H5: No semmoinen tietynlainen helppous, että siitä olisi helppo löytää asioita. Helppo löytää esimerkiksi nyt vaikka sähköpostin kanssa, että mitä siinä kannattaisi huomioida ja mikä olisi sitten se varasuunnitelma, että jos sähköposti ei toimi. Minkälaisia suosituksia olisi sitten, että mihinkä sitä lähtee sitten tavallaan työstämään sitä varautumissuunnitelmaa?

6.3.2 Suunnitelman pohjana olevan mallin kattavuus ja sovellettavuus

Kaikissa kolmessa tässä tutkielmassa aiemmin esitellyissä jatkuvuuden hallinnan malleissa jatkuvuuden hallinnan kattavuutta arvioidaan ennen kaikkea asiakkaan toimesta: tehtävät toimenpiteet pohjautuvat omien toimintojen ja heikkouksien tunnistamiseen, sekä niihin kohdistuvien riskien arviointiin ja tarvittavien toimien toteuttamiseen (Niemimaa & Järveläinen, 2013; SFS, 2023; Valtiovarainministeriö, 2022). Kaikki haastateltavat kertoivat kuitenkin haastattelussa olevansa kiireisiä liiketoimintaan liittyvien päätehtävien hoitamisessa ja siksi jatkuvuuden hallinnan edellytettiin olevan mahdollisimman helppoa, mutta samalla myös kattavaa. Osa haastateltavista totesi, että jatkuvuuden suunnittelua on haasteellista toteuttaa täysin tyhjältä pohjalta ja toisaalta heillä ei myöskään ole tarkkaa tietoa millaisia asioita jatkuvuuden hallinnassa tulisi ottaa huomioon. Tästä voidaan johtaa johtopäätös, että haastatteluissa esiinnousseella kattavuudella haastateltavat tarkoittivat ennen kaikkea sitä, että mallia noudattamalla pilvipalveluihin liittyvä jatkuvuus olisi hallinnassa. Mallin tulisi olla riittävän yksityiskohtainen, jotta sen ehdottamien toimien tarpeellisuutta voitaisiin arvioida ja mallin pohjalta laadittava jatkuvuussuunnitelma olisi helppo toteuttaa.

> H1: Jos olisi enemmän aikaa tehdä niitä ja vaikka meillä on jo olemassa oleva malli, ni ehkä voisi olla helpompi vielä, jos olisi joku selkeä mallidokumentti tai pohja mitä ei tarvitsisi yhtään suunnitella vaan tietäisi varmuudella, että siinä on kaikki tarvittava asia. Silloin täytyisi vaan varata aika sille ja seurata dokumenttia.

> H2: No ihan selkeästi, jos joku laatisi tämmöisiä valmiita pohjia tämmöiseen pilvipalveluiden hallintaan. Semmoinen aina helpottaa, kun se että sä rupeat tyhjästä vääntämään semmoista dokumenttia niin se vie ihan hirveästi aikaa ja sitten se on jostain muusta ajasta aina pois. Kaikki tämmöiset dokumentoinnit mitä jo löytyisi, niin niistä olisi huomattavaa apua.

> H5: No ehkä tietenkin semmoinen mahdollisimman laaja, josta pystyisi poimimaan ne mitkä omaa liiketoimintaa koskettaa. Niin se olisi ainakin semmoinen jollain lailla ymmärrystä lisäävä ja silmiä avaava. Kun ei osaa itse välttämättä kaikkea edes huomioida, niin siitä saisi hyvin osviittaa.

6.3.3 Ajantasaisuus ja helppo löydettävyys

Viimeisenä keskeisenä ja vastaajille yhteisenä toistuvana teemana esiin nousi toive mallin ajantasaisuudesta ja helposta löydettävyydestä. Sekä jatkuvuuden hallinnan kokonaismallit, että pilvipalveluiden jatkuvuutta käsittelevä teoria painottavat jatkuvuuden hallinnan olevan iteratiivinen prosessi, jossa tarpeellisuutta ja kattavuutta arvioidaan aika ajoin uudelleen. Kattavuutta ja tehokkuutta

voidaan harjoitella esimerkiksi erilaisilla skenaarioilla tai arvioimalla liiketoimintoja sekä toimintaympäristöä uudelleen. (ISO, 2019; Kyberturvallisuuskeskus, 2020a; Niemimaa & Järveläinen, 2013; SFS, 2023) Ajantasaisuudella haastateltavat tarkoittivat, että mallin sisältö olisi nykyaikaiseen käyttöympäristöön soveltuva, mutta myös sitä, että mallia olisi myös tulevaisuudessa helppo noudattaa ja ylläpitää. Kirjallisuuskatsauksessa kuvattuja Julkria ja ISO 22301 -standardia päivitetään niitä julkaisevien organisaatioiden toimesta, mutta Niemimaan ja Järveläisen ehdottamasta mallista ei ole saatavilla päivitettyä versiota. Yhtenä tärkeänä osana mallia tulisi olla asioiden uudelleen tarkastelu, koska se varmistaisi mallin kattavuuden ja jatkuvuuden hallinnan onnistumisen pilvipalveluiden osalta myös tulevaisuudessa. Kahden haastateltavan mukaan mallin tulisi olla helposti löydettävissä ja hyödynnettävissä esimerkiksi internet-selaimen avulla ja mallin tulisi olla luettavissa tavanomaisilla ohjelmistotyökaluilla. Kirjallisuuskatsauksessa kuvatut mallit ovatkin avattavissa ja luettavissa toimisto-ohjelmistoilla.

> H2: Valmiit mallit ja sitten semmoinen automaatti raportointi, että tulisi semmoinen automaatti raportti tietyn väliajoin. Vähän proaktiivinen asenne sen pilvipalvelun puolesta siten, että meidän ei tarvitse vähän niinku huolehtia siitä.

> H5: No tietenkin, että se olisi jossakin pilvipalvelussa helposti muokattavissa, että se ei ole mikään printattu versioon vaan se olisi niinku helposti käsillä oleva. Ja tietenkin semmoinen, että olisi sitten joku kenen vastuualueella se olisi sitten semmoisen päivittäminen samassa syklissä, kun mahdollisia muutoksia tapahtuu.

7 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa pohditaan tutkimuksen tärkeimpiä tuloksia ja yhdistellään niitä kirjallisuuskatsauksen avulla havainnoituun jatkuvuuden hallinnan teoriaan. Tuloksista ja kirjallisuuskatsauksesta saadun teorian avulla pyritään muodostamaan johtopäätöksiä. Lisäksi osiossa pohditaan saatujen tulosten laatua ja rajoituksia. Tulokset on jaoteltu tutkimuskysymysten mukaisesti, jotta vastaukset kysymyksiin voitiin muodostaa ja tutkimuksen onnistumista arvioida.

7.1 Miten jatkuvuuden hallintaa toteutetaan pienissä yrityksissä ja onko siinä huomioitu pilvipalveluita?

Tutkimuksen toisena tavoitteena oli selvittää pienten yritysten jatkuvuuden hallinnan tilaa yleisellä tasolla, sekä sitä ovatko pienet yritykset pilvipalveluiden käyttäjinä huomioineet pilvipalveluiden merkitystä oman toimintansa jatkuvuuden hallinnassa. Tutkimuksen tulokset osoittavat, että yleinen jatkuvuuden hallinta ymmärretään pienyrityksissä monin eri tavoin ja siihen liittyviä toimia toteutetaan vaihtelevasti. Jatkuvuuden suunnittelu oli yrityksissä hajanaista, eikä jatkuvuuden tilaa arvioitu yhdessäkään yrityksessä säännöllisesti uudestaan. Haastateltavat pitivät jatkuvuuden suunnittelua tärkeänä, mutta kokivat haasteelliseksi resurssien riittävyyden ja puutteellisen tietotaidon asiaan liittyen. Johtopäätöksenä voidaan todeta, että yritykset eivät tarkalleen tiedä mitä onnistunut jatkuvuuden hallinta vaatii ja kuinka sitä tulisi toteuttaa. Epäselvyys toteuttamisessa ja työmäärän arvioinnin vaikeus aiheuttivat haastateltavissa yrityksissä usein sen, että jatkuvuutta ei ollut systemaattisesti arvioitu.

Haastateltavat henkilöt heräsivätkin pohtimaan yrityksensä liiketoiminnan jatkuvuutta usein haastattelun yhteydessä, jota voidaan pitää yritysten varautumisen parantamisen kannalta hyvänä asiana. Haastateltavat henkilöt tunnistivat, että jatkuvuuden hallinta on heidän henkilökohtaisella vastuullaan, mutta vastauksista oli havaittavissa, että he eivät kuitenkaan tienneet miten jatkuvuuden hallintaa tulisi käytännössä toteuttaa. Huolimatta aiheeseen liittyvästä

epätietoisuudesta, kaikki yritykset olivat kuitenkin jollain tavalla varautuneet erilaisiin liiketoiminnan häiriöihin. Yleisimmin yritykset olivat varautuneet työntekijöiden poissaoloihin tai poistumisiin, sekä työssä tarvittavien välineiden ja tarvikkeiden saatavuuksien häiriöihin. Haastateltavien vastauksista olikin havaittavissa, että liiketoiminnan jatkuvuuden suurimmaksi uhaksi koettiin myynnin vähentyminen ja siitä johtuvat taloudelliset ongelmat. Haastateltavat eivät juurikaan olleet kokeneet, että kolmansien osapuolten häiriöt, kuten logistiikkaan, lainsäädäntöön tai yhteistyökumppanien liiketoimintoihin liittyvät ongelmat olisivat vaikuttaneet vakavasti heidän liiketoimintansa jatkuvuuteen. Digitaalisen omaisuuden turvaamiseksi yritykset olivat hankkineet pilvipalveluita, jotka koettiin pääosin pelkästään jatkuvuutta parantavina tekijöinä. Jatkuvuuden hallinnan pohdinta ja suunnittelu oli näiden järjestelmien osalta usein ulkoistettu ja pohjautui luottamukselle yhteistyökumppaneihin. Tutkimuksen kirjallisuuskatsauksessa esitellyissä jatkuvuuden hallinnan malleissa järjestelmiin tulee kohdistaa erilaisia sopimuspohjaisia ja teknisiä velvoitteita, joita pienten yritysten on kuitenkin haasteellista toteuttaa.

Kirjallisia, koottuja suunnitelmia jatkuvuuden hallintaan yritykset eivät olleet yhtä lukuun ottamatta laatineet. Osassa yrityksistä oli pohdittu ja toteutettu mallien mukaisia SWOT-analyysejä yritystoiminnan analysointiin. Nämä analyysit voidaan nähdä osana jatkuvuuden hallintaa, koska ne arvioivat yritystä kohtaavia vahvuuksia, heikkouksia mahdollisuuksia ja uhkia (Suomen Riskienhallintayhdistys ry, 2023a). Epäsäännöllisesti toteutettua SWOT-analyysiä ei kuitenkaan voida kirjallisuuteen pohjautuen pitää riittävänä keinona onnistuneen jatkuvuuden hallinnan toteuttamiseen. Muut jatkuvuuden hallinnan kirjalliset ohjeet, suunnitelmat, analyysit ja dokumentit koettiin kuitenkin suuremmille organisaatioille kuuluviksi asioiksi. Toisaalta tutkielman teon aikana havaittiin, että koko organisaation jatkuvuutta parantavat mallit vaikuttavat olevan toimiensa osalta liian korkeatasoisia pienyritysten käyttöön. Pienyritykset toivoivat konkreettisia, niille kohdistettuja keinoja toteuttaa jatkuvuuden hallintaa, kun taas olemassa olevat mallit sisältävät paljon kyseisille yrityksille turhia toimenpiteitä ja työvaiheita. Ohjeita jatkuvuuden hallinnan toteuttamiseen on olemassa, ja monet niistä, kuten ISO 22301 -standardi ilmoittaa sopivansa kaikenkokoisille yrityksille toimialasta riippumatta (SFS, 2023). Soveltuvuudesta huolimatta standardia voi vain harvoin sellaisenaan hyödyntää pienyrityksessä. Tällöin standardin ostamisen lisäksi pienyritykselle jää myös toimien valitseminen ja sopeuttaminen omaan toimintaan, jotka vaativat sekä ajallisia että rahallisia resursseja. Haasteena on lisäksi se, että niukoilla resursseilla toimivan pienen yrityksen on vaikea rajata ja valita itselleen sopiva määrää toimia. Lisäksi tarkistuslistan kohtien muokkaaminen ja soveltaminen omaan käyttöön voi olla pienille yrityksille haasteellista. Tutkielman teon aikana havaittiin myös, että standardi mainitsee ”esittävänsä vaatimukset organisaation liiketoiminnan jatkuvuuden hallinnalle” (SFS, 2023). Tämänkaltaisen ilmaisun voidaan ymmärtää tarkoittavan ehdotonta listaa vaatimuksista, jotka tulee täyttää, jotta liiketoiminnan jatkuvuuden hallintaa voidaan toteuttaa. Pitkän vaatimuslistan läpikäynnin aloittaminen voi tämänkaltaisesta muotoilusta johtuen tuntua pienyrityksestä turhalta.

Toisena esimerkkinä, tutkielman kirjallisuuskatsauksessa esitetty julkisen sektorin toimijoille suunnitellun Julkri-mallin osa-alueista suurin osa on sellaisia, joiden toteuttaminen vaatisi sekä teknistä että lakeihin liittyvää asiantuntemusta. Julkrin tavoitteena onkin julkisen hallinnon tiedonhallintalain vaatimusten toteuttaminen kriteerit täyttämällä ja siksi Julkria, kuten muitakin tutkimuksessa esiteltyjä malleja voidaan noudattaa sovelletusti yksityisellä sektorilla (Valtiovarainministeriö, 2022). Tällöin omien toimintojen tunnistaminen ja analysointi on ensiarvoisen tärkeää, jotta toimet olisivat soveltamisesta huolimatta riittävän kattavia. Omien liiketoimintojen ja niihin kohdistuvien riskien tunnistaminen onkin mahdollisesti jopa tärkein vaihe jatkuvuuden hallinnassa, koska se määrittelee tulevia jatkuvuuden hallinnan toimia.

Kuten aiemmin on todettu, pilvipalvelut olivat merkittävässä roolissa haastateltujen yritysten liiketoiminnassa. Osa yrityksistä pohjasi liiketoimintansa täysin verkossa pohjautuvalle alustalle, osa taas hyödynsi pilvipalveluita keskeisten liiketoimintojensa tukitoimintoihin. Kaikki yritykset myönsivät, että liiketoiminnan toteuttaminen olisi joko mahdotonta tai erittäin haastavaa ilman käytössä olevia pilvipalveluita. Siksi pilvipalveluiden huomiointi osana jatkuvuuden hallintaa olisi tärkeää. Pilvipalveluiden ja myös muiden IT-palveluiden jatkuvuuden toteuttamiseksi havainnoitiin keinoja olemassa olevasta teoriasta ja osa keinoista olisi myös pienyritysten toteutettavissa suhteellisen pienin resurssein. Tällaisia toimia ovat esimerkiksi käytössä olevien pilvipalveluiden kartoitus ja niiden merkitys omille liiketoiminnoille, kriittisten pilvipalveluiden sopimusten tarkastelu, häiriöiden vaikutusten arviointi ja niistä palautumisen suunnittelu sekä tietoturvan huomiointi. Yritykset tunnistivat erilaisia pilvipohjaisiin järjestelmiin kohdistuvia riskejä, mutta eivät olleet juuri toteuttaneet toimia riskeiltä suojautuakseen. Yritysten vastauksista oli havaittavissa, että jatkuvuuden hallinnan yhteys pilvipalveluihin nähdään tällä hetkellä pelkästään positiivisena, eikä siihen liittyviä haasteita ollut arvioitu.

7.2 Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?

Tutkimuskysymykseen ”Millaisia ominaisuuksia on onnistuneessa pilvipalveluita koskevassa jatkuvuussuunnitelmassa pienten yritysten näkökulmasta?” etsittiin vastausta teemahaastattelun avulla. Tutkimuskysymyksen tavoitteena oli selvittää, millaisia ominaisuuksia pienet yritykset arvostavat pilvipalveluita koskevassa jatkuvuussuunnittelussa. Osana tutkimusongelman ratkaisemista haastateltavilta tiedusteltiin pilvipalveluiden merkityksestä ja käyttökohteista heidän yrityksessään. Lisäksi haastateltavia pyydettiin kertomaan, millaisiin tehtäviin he pilvipalveluita hyödyntävät. Taustakysymykset kysyttiin, koska pilvipalveluiden jatkuvuuden hallinnan perusteisiin kuuluu palvelun tarpeellisuuden ja pilvipohjaisen toteutusmahdollisuuden pohdinnan lisäksi järjestelmän hyötyjen,

vaikutusten ja riskien arviointi (Ristov ym., 2011). Tämän tutkimusongelman selvittämisen yhteydessä tehtiin havainto, jonka mukaan myös pienillä yrityksillä on haasteita järjestelmien ja tiedon hallinnassa: Käytössä olevien järjestelmien lukumäärää ja käyttötarkoituksia ei osattu vastaajien keskuudessa aina arvioida. Myöskään niihin tallennettuna olevaa tietoa ei tarkalleen osattu kuvata. Järjestelmien merkitys oman liiketoiminnan mahdollistajana tunnistettiin, mutta kysyttäessä tarkemmin mihin liiketoiminnan prosesseihin järjestelmät liittyvät, eivät haastateltavat aina olleet täysin varmoja yhteyksistä ja järjestelmillä toteutettavista liiketoiminnan osaprosesseista. Havaintoa voidaan pitää tärkeänä, koska tieto on yrityksille erittäin tärkeä omaisuuserä, ja yritysten on kyettävä suojaamaan omistamansa tieto (Bergström ym., 2020). Tietoon kohdistuu monenlaisten riskien ohella myös lainsäädännöstä johtuvia velvollisuuksia, joita yritysten tulee noudattaa. Lisäksi tiedon täysimääräinen hyödyntäminen on hankalaa, mikäli sen olemassaoloa tai sijaintia ei täysin tiedosteta.

Haastatteluiden yhteydessä pilvipalvelut miellettiin usein jatkuvuutta parantavaksi tekijäksi esimerkiksi paremman saatavuuden, skaalautuvuuden, sekä henkilöstöriskejä pienentävien ominaisuuksien ansiosta. Pilvipalvelun jatkuvuussuunnitelman sisältö ja laajuus ovat vahvasti riippuvaisia siitä, millaisia vastuita ja mahdollisuuksia yrityksellä palvelunostajana on (Kyberturvallisuuskeskus, 2020a; Ristov ym., 2011). Tässä tutkimuksessa pilvipalvelut tarkoittivat lähes poikkeuksetta SaaS-palvelumallilla tarjottavia ohjelmistoja, jolloin ohjelmistot tuotetaan ja ylläpidetään lähes täysin palveluntarjoajan toimesta, vaikkakin turvallisuuteen liittyvät vastuut jakautuvat siinäkin palveluntarjoajan ja asiakkaan välillä (Kyberturvallisuuskeskus, 2020a). Jatkuvuuden hallinta käsitteenä ei ollut pienten yritysten hallintotehtävissä toimiville tuttu, joten myöskään pilvipalveluiden merkitystä ja riskejä omalle liiketoiminnalle ei ollut pohdittu. Haastateltavat olivat usein sitä mieltä, että heidän asiantuntemuksensa ja työaikansa eivät riitä pilvipalveluiden jatkuvuuden pohdintaan, eivätkä he siksi ehdi tutkia tarkemmin sen osaprosesseja. Tästä johtuen apua esimerkiksi riskianalyysin toteuttamiseen ei ollut etsitty. Jatkuvuussuunnitelma on vain osa jatkuvuuden hallintaa, ja haastateltavat toivoivatkin pilvipalveluiden jatkuvuussuunnitelman pohjana toimivan jatkuvuuden hallinnan mallin olevan kattava mutta helppokäyttöinen. Internetissä on saatavilla sekalainen joukko pilvipalveluiden jatkuvuutta koskevia kirjoituksia, mutta niissä on tarjolla vain vähän konkreettisia keinoja pilvipohjaisia järjestelmiä koskevaan varautumiseen, eikä niistä ole helppo muodostaa kattavaa kokonaissuunnitelmaa. Lisäksi ohjeiden ajantasaisuutta ja oikeellisuutta on vaikea arvioida. Mikäli jatkuvuuden hallintaa tarkastelisi nykyisin olemassa olevien jatkuvuuden hallinnan standardien ja ohjeiden kautta, se vaatisi pieniltä yrityksiltä merkittävien lisäresurssien kohdistamista aiheeseen. Toisaalta esimerkiksi standardien tarkistuslistamainen läpikäynti ei ole pienille yrityksille tarkoituksenmukaista, koska standardien tavoitteena on usein standardointi ja sertifiointi, jotka eivät ole välttämättä pienten yritysten tavoitteena. Myös jatkuvuuden hallinnan ohjeet kuten PiTuKri ja Niemimaan ja Järveläisen laatima malli vaativat soveltamista, koska ne laajoja pienten yritysten käyttöön sellaisenaan. Soveltamisen ongelmana on kuitenkin tarpeellisten toimien

tunnistaminen ylimääräisistä. Ilman riittävää asiantuntemusta toimien valinta voi olla sattumanvaraista ja altistaa täten toiminnan häiriöille. Toisaalta ohjeiden systemaattinen noudattaminen auttaisi varmistamaan, että organisaation toiminnot ovat mahdollisimman hyvin suojattuja ja että organisaatio voi toipua mahdollisimman nopeasti häiriötilanteista. Helppokäyttöisyyden voidaankin tässä yhteydessä todeta tarkoittavan myös sitä, että malli opastaa käyttäjää järjestelmiin liittyvän jatkuvuuden hallinnan toteuttamisessa.

Vaikka tämän tutkimuskysymyksen alla tarkasteltiinkin pilvipalveluiden jatkuvuussuunnittelua, voitiin vastauksista päätellä, että haastateltavat toivoivat mallin tarjoavan laajemminkin apua jatkuvuuden hallintaan. Eräs haastateltavista totesikin, että mallin tulisi toimia vaatimuslistan sijaan enemmänkin ”ohjenuorana” jatkuvuuden hallinnan toteuttamiseen. Jatkuvuuden hallinnan määritelmissä aihe kuvataankin jatkuvana prosessina tai toimintana, jolla yrityksen liiketoiminta varmistetaan myös häiriötilanteissa, jatkuvuussuunnitelman ollessa vain osa jatkuvuuden hallintaa (Niemimaa ym., 2019; Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä, 2016; Valtiovarainministeriö, 2020). Pohdittaessa asiaa tämän näkökulman kautta, tulisi pilvipalveluita koskevan jatkuvuussuunnitelman sisältää ohjeistavaa materiaalia ja sen tulisi olla esimerkiksi vuosikelloon kytketty ohje, jonka avulla yritys varmistaa pilvipalveluiden toiminnan jatkuvuuden myös häiriötilanteissa. Mikäli yritys on laatinut jatkuvuussuunnitelmia muuhun toimintaan ja toteuttaa jatkuvuuden hallintaa sen avulla, tulisi pilvipalveluita koskeva jatkuvuussuunnitelma kytkeä osaksi sitä.

Vastauksissa nousi esiin myös suunnitelman helppo löydettävyys. Tämä voidaan ymmärtää tarkoittavan sekä jaettavan ohjeen helppoa saatavuutta, että varsinaisen toteutetun jatkuvuussuunnitelman helppoa hyödyntämistä arjessa. Tässä tutkielmassa aiemmin esitellyt jatkuvuuden hallinnan mallit ovatkin saatavilla internetissä, mutta osa niistä on maksullisia. Toisaalta yksikään niistä ei tarjoa internetissä hyödynnettävää käyttöliittymää jatkuvuussuunnitelman luomiseen. Jatkuvuussuunnitelman toteuttaminen ja huomioiminen työn ohessa voikin olla pienille yrityksille haasteellista, koska pienillä yrityksillä ei useinkaan ole varsinaista IT-palveluista vastaavaa henkilöä tai tiimiä käytettävissään. Suurin osa haastatelluista yritysten johtajista kertoikin, että heidän päivittäiseen työnkuvaansa kuuluu monipuolisesti erilaisia tehtäviä ja siksi hallinnollisen taakan lisäämistä kannattaa minimoida. Jatkuvuussuunnitelman noudattamista voisivat helpottaa esimerkiksi riittävän suoraviivainen toteutus, muistutukset sekä käytettävyys ajasta ja paikasta riippumatta.

7.3 Jatkotutkimusaiheita

Tässä tutkimuksessa tutkittiin pienten yritysten jatkuvuuden hallintaa selvittämällä ensin, miten jatkuvuuden hallintaa kirjallisuuteen pohjautuen tulisi toteuttaa, ja sen jälkeen peilaamalla sitä haastateltavien näkemyksiin oman yrityksensä jatkuvuuden hallinnasta. Kohteena olivat alle 50 henkilöä vakituisesti työllistävät yritykset, joiden vuosiliikevaihto alitti 10 miljoonaa euroa. Nämä yritykset

voidaan tilastokeskuksen mukaisesti määritellä pienyrityksiksi (Tilastokeskus, 2023). Lisäksi tutkimuksen kohteena olevien yritysten tuli hyödyntää pilvipalveluita keskeisissä liiketoiminnoissaan tai niiden tukena. Yrityksistä haastatellut henkilöt olivat poikkeuksetta johtotehtävissä toimivia henkilöitä, joten heillä oli laaja ymmärrys oman yrityksensä liiketoiminnasta ja niissä hyödynnettävistä järjestelmistä. Jatkuvuuden hallinta ja kriiseistä toipuminen ovat teemoina nousseet esiin viime vuosina esimerkiksi COVID-19 pandemian, huoltovarmuuden sekä kansainvälisten toimitusketjujen häiriöiden vuoksi. Tämän takia myös jatkuvuuden hallintaa koskevassa tutkimuksessa on viime vuosina korostunut kriiseistä selviytyminen ja pientenkin yritysten selviytymiskeinoja on tutkittu suhteellisen paljon. Aiheen ajankohtaisuudesta huolimatta tutkimuksen havaintona todettiin, että jatkuvuuden hallintaa harvoin toteutetaan pienissä yrityksissä järjestelmällisesti ja keinot sen toteuttamiseen vaihtelivat. Lisäksi kirjallisuuskatsaus osoitti, että jatkuvuuden hallinta on moninainen käsite, jonka sisältö vaihtelee hieman lähteen mukaan. Jatkotutkimus olisikin mielenkiintoista toteuttaa suurempiin yrityksiin, joissa liiketoimintojen suojaamiseen on kohdistettu enemmän resursseja ja jatkuvuuden hallintaa toteutettaisiin systemaattisesti osana yrityksen toimintaa. Suomessa julkinen sektori toteuttaa häiriöihin varautumista ja niistä toipumista osittain lain velvoittamana yhteisiä malleja hyödyntäen, mutta yksityisen sektorin jatkuvuuden suunnittelun toimintatapoja ja malleja olisi mielenkiintoista tuoda esille ja yhtenäistää: menetelmien ja hyvien käytänteiden jakaminen samankaltaisten yritysten välillä parantaisi pienten yritysten riskienhallintaa ja varautumista. Jatkuvuuden hallinnan konsultointia tarjoavia yrityksiä on niin ikään olemassa, mutta kyseisten yritysten avoimesti tarjoama tieto on usein suppeaa kaupallisten intressien vuoksi. Konsulttien ammattitaitoon pohjautuva tieto olisi tärkeä saada pienten yritysten käyttöön jatkotutkimuksen avulla. Suurempien yritysten ja konsultointiyritysten menetelmiä ja hyviä käytänteitä voitaisiin pyrkiä tuomaan sovellettuna pienten yritysten käyttöön esimerkiksi luomalla ja testaamalla malli, jota pienet yritykset voisivat hyödyntää. Myös pitkittäistutkimus edellä mainittujen menetelmien ja käytänteiden noudattamisen ja toteuttamisen hyödyistä pienissä yrityksissä olisi mielenkiintoista tutkia. Tämänkaltaista lisätutkimusta ehdottavat myös Niemimaa ja Järveläinen (2013) omassa IT-palveluiden jatkuvuuden hallintaa koskevassa tutkimuksessaan: heidän mukaansa liiketoimintoihin sidottu jatkuvuuden toteuttaminen ja sitoutuminen sen toteuttamiseen kehittyvät ajan kuluessa, ja sitä tulisi tutkia lisää.

Toisin kuin koko organisaation jatkuvuuden hallintaa koskevaa tutkimusta, pilvipalveluihin liittyvää jatkuvuuden hallintaa on tutkittu vähemmän. Kirjallisuuskatsauksessa läpikäydyissä jatkuvuuden hallinnan tutkimuksissa IT-palveluista puhutaan ainoastaan ylätason käsitteenä, eikä pilvipalveluiden erityispiirteitä aina oteta huomioon. Etenkin pienten yritysten varautumista koskevaa ohjeistusta pilvipalveluiden osalta on vaikea löytää, mitä voidaan pitää tutkimusaukkona, pilvipalveluiden ollessa yhä merkittävämmässä roolissa myös kyseisten yritysten toiminnassa. Myös tässä tutkimuksessa edellä mainittu tutkimusaukko oli havaittavissa: Pienet yritykset kaipasivat tutkimuksen mukaan konkreettisia keinoja sekä ohjeistusta jatkuvuuden hallinnan toteuttamiseen sekä

koko organisaation että pilvipalveluiden osalta. Nykyisen kaltaiset jatkuvuuden hallinnan oppaat koetaan pienille yrityksille sopimattomiksi ja turhiksi, joten suoraviivaisempi ja pienten yritysten tarpeet huomioiva lähestymistapa olisi yrityksille tarpeellinen.

Tässä tutkimuksessa SaaS-toteutusmallit korostuivat pienten yritysten tapana hyödyntää pilvipalveluita, joten tutkimusta voisi laajentaa myös kartoittamalla tarkemmin erilaisten pilvitoteutustapojen jatkuvuuden varmistamisen erityispiirteitä. Lisäksi samantyyppinen pilvipalveluihin liittyvä jatkotutkimus olisi mielenkiintoinen toteuttaa suurempiin yrityksiin, jotka omaavat erillisen IT-osaston: miten yritykset joissa vastuuhenkilöt ohjelmistoille ja varautumiselle on määritelty, ovat huomioineet pilvipalveluihin liittyvät jatkuvuusriskit?

7.4 Luotettavuus ja rajoitukset

Tämä tutkimus koostuu kirjallisuuskatsauksesta sekä empiirisestä osiosta. Tutkielman kirjallisuuskatsauksessa hyödynnettiin tieteellisiä lähteitä, alan keskeisiä standardeja ja julkaisuja, sekä viranomaisten tuottamia ohjeita. Tieteelliset lähteet etsittiin pääosin Google Scholar -palvelun avulla ja valittujen lähteiden laatu pyrittiin varmistamaan hyödyntämällä tieteellisiä julkaisuja, sekä arvioimalla viittausmääriä. Viime vuosina koetut maailmanlaajuiset kriisit, sekä pilvipalveluiden jatkuva kehitys ovat kuitenkin kasvattaneet aiheesta tehdyn tutkimuksen määrää, joten uusien artikkelien osalta viittausmääriä ei voitu hyödyntää perusteena lähteiden valinnalle. Haasteita kirjallisuuskatsauksen lähteiden valinnassa aiheutti myös vähäinen yksityistä sektoria koskevien julkaisujen määrä: julkaisut olivat usein kaupallisten toimijoiden toteuttamia eikä niitä tästä syystä hyväksytty lähteeksi kirjallisuuskatsaukseen. Puutteen takia kirjallisuuskatsauksessa hyödynnettiin myös yksityiselle sektorille sopivia viranomaisohjeita. Aineiston rajoitettu määrä ja puutteet laadun arvioinnissa otetaan huomioon tutkimuksen luotettavuutta arvioidessa.

Hiltunen (2009) on kuvannut tutkimuksen onnistumisen mittaamista validiteetin ja reliabiliteetin avulla. Validiteetti ilmaisee, miten hyvin tutkimuksessa hyödynnetty tutkimusmenetelmä mittaa juuri sitä tutkittavan ilmiön ominaisuutta jota on tarkoituskin mitata. Reliabiliteetti taas ilmaisee sen, miten luotettavasti ja toistettavasti tutkimusmenetelmä tai itse tutkimus mittaa valittua tutkimusilmiötä. Validiteetti ja reliabiliteetti ovat suhteessa keskenään: mitä alhaisempi reliabiliteetti, sitä alhaisempi validiteetti. Toisinpäin väite ei kuitenkaan pidä paikkaansa, sillä tutkimuksessa käytetty tutkimusmenetelmä voi olla hyvinkin tarkka ja toistettava, mutta mitata tutkimuksen kannalta vääriä asioita. (Hiltunen, 2009)

Hiltusen (2009) mukaan tutkimuksen validiteetti on hyvä, mikäli tutkimuksen kohderyhmä ja haastatteluissa käytetyt kysymykset ovat oikeat. Tutkimuksen tavoitteena oli selvittää miten pienet yritykset hoitavat yleistä jatkuvuuden hallintaansa, sekä oliko pilvipalveluita huomioitu osana kyseistä prosessia. Lisäksi tutkimuksessa selvitettiin, millaisia ominaisuuksia kyseiset yritykset

arvostaisivat pilvipalveluita koskevassa jatkuvuussuunnitelmissa. Tutkimuksen empiirinen osio toteutettiin laadullisena tutkimuksena, ja aineistonkeruumenetelmänä hyödynnettiin teemahaastatteluja. Haastatellut henkilöt valittiin heidän työtehtäviensä perusteella, ja he edustivat jokainen eri yritystä. Haastateltavat olivat lisäksi vastuussa yrityksensä varautumisesta, sekä pilvipalveluiden hyödyntämisestä osana liiketoimintaa. Pienissä yrityksissä vastuualueet ovat usein laajoja, ja siksi haastateltavat olivat pääosin yritysten toimitusjohtajia. Yritykset toimivat eri toimialoilla ja erilaisissa liiketoimintaympäristöissä, minkä voidaan nähdä tässä tutkimuksessa parantavan tutkimuksen validiteettia. Lisäksi tutkimuksessa haastatelluissa yrityksissä pilvipalvelut olivat keskeisessä roolissa yrityksen liiketoimintaa, joten haastatelluilla henkilöillä oli tiedossa jatkuvuuden varmistamisen merkitys myös pilvipalveluiden osalta. Tältä osin haastateltavat valittiin tutkimuksen validiteetin kannalta oikein. Lisäksi Hiltunen (2009) mainitsee, että tutkimuksen validiteettia nostaa se, että tutkimuksessa saatu tieto vastaa vallalla olevaa teoriaa tai pystyy tarkentamaan ja parantamaan sitä. Ensimmäiseen tutkimuskysymykseen vastauksena saatu jatkuvuuden hallinnan merkitys sekä suunnitelmien puute on havaittu pienyritysten jatkuvuutta koskevassa tutkimuksessa myös aiemmin (esim. Chepkoit, 2017; Fabeil ym., 2020; Kato & Charoenrat, 2018), joten ne tukevat tutkimuksen validiteettia. Toiseen tutkimuskysymykseen ei samaisesta näkökulmasta löydetty tieteellistä tutkimusta. Tutkimuksen validiteettia laskee kuitenkin haastatteluiden vähäinen määrä, minkä takia tuloksia ei voida yleistää liikaa. Lisäksi haastateltavat eivät haastatteluhetkellä pystyneet muodostamaan täydellistä kokonaiskuvaa yrityksensä jatkuvuuden hallinnasta, mikä voi vaikuttaa negatiivisesti tutkimuksen tarkkuuteen. Tätä olisi voitu parantaa täsmällisemmillä kysymyksillä, sekä tarjoamalla haastateltaville paremmat mahdollisuudet pohtia vastauksia ennakkoon.

Tutkittaville avattiin haastattelukutsussa, sekä haastattelun alussa jatkuvuuden hallinnan sekä pilvipalveluiden määritelmät, jotta haastateltavilla oli yhtenäinen ymmärrys tutkimuksessa käytettävistä käsitteistä. Tämän voidaan nähdä parantavan lopputuloksen reliabiliteettia. Lisäksi Puusa ym. (2020) toteavat, että haastatteluita on tehty laadullisessa tutkimuksessa riittävä määrä, mikäli aineisto alkaa toistaa itseään: vaikka haastattelut olivat erillisiä tilaisuuksia ja vastaajat eivät tienneet toisten haastateltavien näkemyksiä, toistuivat niissä silti samat teemat. Tältä osin haastatteluita voidaan todeta olleen riittävästi, vaikkakin tutkimuksen reliabiliteetti olisi parantunut haastateltavien määrän lisäämisellä. Tämän lisäksi tutkimuksen reliabiliteettia olisi parantanut tarkempi kohderyhmän rajaus. Etenkin toisen tutkimusongelman kannalta mittaustulosten tarkkuutta vähentää riippuvuus pilvipalvelun toteutusmallista: vastuut esimerkiksi turvallisuuteen liittyvistä asioista ovat vahvasti riippuvaisia toteutusmallista, mutta haastatteluun osallistuvien yritysten käyttämien pilvipalveluiden toteutusmalleja ei tässä tutkimuksessa rajattu. Reliabiliteettia tämän tutkimusongelman kannalta parantaa kuitenkin SaaS-toimitusmallilla toimitettavien pilvipalveluiden suuri osuus myös pienissä yrityksissä käytettävistä ohjelmistoista, sekä se, että vain yksi haastateltavista ilmoitti yrityksensä käyttävän myös muilla

toimitusmalleilla hyödynnettäviä pilvipalveluita (Statista, 2023). Näistä syistä tutkimusta ei ollut tarpeen rajata yhteen toimitusmalliin.

Kaiken kaikkiaan tutkimus vastaa tutkimuskysymyksissä esitettyihin kysymyksiin ja täyttää sille asetetut tavoitteet. Tutkimuksen kirjallisuuskatsauksessa toteutettiin katsaus siihen, mitä jatkuvuuden hallinta tarkoittaa koko organisaation, sekä pilvipalveluiden osalta. Laadullisen tutkimuksen tavoitteena on Hirsijärven (2009), sekä Puusan ja Juutin (2020) syventää ymmärrystä tutkittavasta aiheesta ja tuoda aiheeseen liittyviä subjektiivisia näkemyksiä esiin. Näihin tavoitteisiin tämä tutkimus myös vastaa: tulokset antavat lisää ja tarkempaa tietoa siitä, miten pienet yritykset toteuttavat jatkuvuuden hallintaansa ja ovatko he huomioineet pilvipalveluihin liittyviä jatkuvuusriskejä osana oman jatkuvuuden hallintansa toteuttamista. Lisäksi tutkimus tarjoaa katsauksen siihen, millaisia ominaisuuksia pienet yritykset arvostavat pilvipalveluihin liittyvässä jatkuvuussuunnittelussa. Tulosten luotettavuutta lisää myös se, että sitä ei toteutettu toimeksiantona, jolloin se tarjoaa puolueettoman näkemyksen aiheeseen.

LÄHTEET

Agarwal, A., & Agarwal, A. (2011). The Security Risks Associated with Cloud Computing. *International Journal of Computer Applications in Engineering Sciences*, *1*(SPECIAL ISSUE ON CNS), 257–259. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6bcb9009cb4548802c377951677870cbb0416756

Akello, P. (2022). *Understanding Security Threats in Cloud-Based Shadow It Work-from-Home Applications Using the General Strain Theory Lens* [väitöskirja, The University of Texas]. ProQuest. https://www.proquest.com/openview/e0e0854a32d123d6fdcec6d499faceа8/1?pq-origsite=gscholar&cbl=18750&diss=y

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

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

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/10.2307/41409971

Bergström, E., Karlsson, F., & Åhlfeldt, R-M. (2020). Developing an information classification method. *Information & Computer Security*, *29*(2), 209–239. https://doi.org/10.1108/ICS-07-2020-0110

Charoenthammachoke, K., Leelawat, N., Tang, J., & Kodaka, A. (2020). Business Continuity Management: A Preliminary Systematic Literature Review Based on ScienceDirect Database. *Journal of Disaster Research*, *15*(5), 546–555. https://doi.org/10.20965/jdr.2020.p0546

Chen, I. J., & Popovich, K. (2003). Understanding customer relationship management (CRM): People, process and technology. *Business Process Management Journal*, *9*(5), 672–688. https://doi.org/10.1108/14637150310496758

Chepkoit, B. K. (2017). *Exploring Strategic Business Continuity Planning Methods for Small Businesses in the State of Maryland* [väitöskirja, Northcentral University]. ProQuest. https://www.proquest.com/openview/065e5fdd3b3e01c45b687f9d051a3e31/1?pq-origsite=gscholar&cbl=18750

Cloud security alliance. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing*. Cloud security alliance. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Drewitt, T. (2013). *A Manager's Guide to ISO22301: A practical guide to developing and implementing a business continuity management system*. IT Governance Publishing. http://www.jstor.org/stable/j.ctt5hh683

Ercan, T. (2010). Towards virtualization: A competitive business continuity. *African Journal of Business Managemen*t, *4*(10), 2164–2173. https://academicjournals.org/article/article1380797316_Ercan.pdf

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen* (1. p.). Kustannusosakeyhtiö Vastapaino.

Eskola, J., & Suoranta, J. (2008). *Johdatus laadulliseen tutkimukseen* (8. p.). Kustannusosakeyhtiö Vastapaino.

Estall, H. (2012). *Business Continuity Management Systems: Implementation and Certification to ISO 22301*. Swindon, U.K. : BCS, The Chartered Institute for IT.

Euroopan parlamentin ja neuvoston asetus 2016/679.

Fabeil, N. F., Pazim, K. H., & Langgat, J. (2020). The Impact of Covid-19 Pandemic Crisis on Micro-Enterprises: Entrepreneurs' Perspective on Business Continuity and Recovery Strategy. *Journal of Economics and Business*, *3*(2), 837–844. https://doi.org/10.31014/aior.1992.03.02.241

Ferreira de Araújo Lima, P., Crema, M., & Verbano, C. (2020). Risk management in SMEs: A systematic literature review and future directions. *European Management Journal*, *38*(1), 78–94. https://doi.org/10.1016/j.emj.2019.06.005

Fortune Business Insights. (2023). *Cloud Computing Market Size & Share | Growth Analysis, [2030]*. Fortunebusinessinsights.com. https://www.fortunebusinessinsights.com/cloud-computing-market-102697

Gao, S. S., Sung, M. C., & Zhang, J. (2013). Risk management capability building in SMEs: A social capital perspective. *International Small Business Journal*, *31*(6), 677–700. https://doi.org/10.1177/0266242611431094

Ghaffari, F., Gharaee, H., & Forouzandehdoust, M. R. (2016). Security considerations and requirements for Cloud computing. Teoksessa *2016 8th International Symposium on Telecommunications (IST)*, 105–110. IEEE. https://doi.org/10.1109/ISTEL.2016.7881792

Gibb, F., & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, *26*(2), 128–141. https://doi.org/10.1016/j.ijinfomgt.2005.11.008

Google Scholar. (julkaisuaika tuntematon). Business continuity planning methodology. Haettu 24.11.2022a osoitteesta https://scholar.google.com/scholar?hl=fi&as_sdt=0%2C5&q=Business+continuity+planning+methodology&btnG=

Google Scholar. (julkaisuaika tuntematon). A cyclic approach to business continuity planning. Haettu 24.11.2022b osoitteesta https://scholar.google.com/scholar?hl=fi&as_sdt=0%2C5&q=A+cyclic+approach+to+business+continuity+planning&btnG=

Google Scholar. (julkaisuaika tuntematon). A framework for business continuity management. Haettu 24.11.2022c osoitteesta https://scholar.google.com/scholar?hl=fi&as_sdt=0%2C5&q=A+framework+for+business+continuity+management&btnG=

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *IEEE Security & Privacy*, *9*(2), 50–57.IEEE. https://doi.org/10.1109/MSP.2010.115

Hendre, A., & Joshi, K. P. (2015). A Semantic Approach to Cloud Security and Compliance. Teoksessa *2015 IEEE 8th International Conference on Cloud Computing*, 1081–1084. IEEE. https://doi.org/10.1109/CLOUD.2015.157

Herbane, B. (2010). The evolution of business continuity management: A historical review of practices and drivers. *Business History*, *52*(6), 978–1002. https://doi.org/10.1080/00076791.2010.511185

Herbane, B., Elliott, D., & Swartz, E. M. (2004). Business Continuity Management: Time for a strategic role? *Long Range Planning*, *37*(5), 435–457. https://doi.org/10.1016/j.lrp.2004.07.011

Hiltunen, L. (2009). *Validiteetti ja reliabiliteetti*. Jyväskylän yliopisto. http://www.mit.jyu.fi/ope/kurssit/Graduryhma/PDFt/validius_ja_reliabiliteetti.pdf

Hirsijärvi, S., & Hurme, H. (2022). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö* (2. p.). Gaudeamus. https://www.finna.fi/Record/3amk.300172

Hirsijärvi, S., Remes, P., & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi. https://www.finna.fi/Record/ekk.993788904006250?sid=3845329379

Hu, V., Iorga, M., Bao, W., Li, A., Li, Q., & Gouglidis, A. (2020). *General Access Control Guidance for Cloud Systems*. NIST Special Publication 800-210. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-210

Irsheid, A., Murad, A., AlNajdawi, M., & Qusef, A. (2022). Information security risk management models for cloud hosted systems: A comparative study. *Procedia Computer Science*, *204*, 205–217. https://doi.org/10.1016/j.procs.2022.08.025

International Organization for Standardization. (2018*). Information technology – Security techniques – Information security risk management. (ISO 27005:2018).* https://www.iso.org/standard/75281.html

International Organization for Standardization. (2019*). Security and resilience — Business continuity management systems — Requirements (ISO 22301:2019).* https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

Jyväskylän yliopisto. (19.7.2022). *Tutkimushaastattelujen tallentaminen ja käsittely*. Jyväskylän yliopisto| Intranet Uno. https://uno.jyu.fi/fi/ohjeet/turvallisuus-tietoturva-ja-tietosuoja/tietoturva/tietoturvaohjeet/tutkimushaastattelujen-tallentaminen-ja-kasittely-1/tutkimushaastattelujen-tallentaminen-ja-kasittely

Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. *International Journal of Information Management*, *33*(3), 583–590. https://doi.org/10.1016/j.ijinfomgt.2013.03.001

Järveläinen, J. (2020). Understanding the Stakeholder Roles in Business Continuity Management Practices – A Study in Public Sector. Teoksessa *Proceedings of the 53rd Hawaii International Conference on System Sciences 2020* (s. 1966–1975). HICSS. https://aisel.aisnet.org/hicss-53/dg/cybersecurity_and_government/5

Kandukuri, B. R., V., R. P., & Rakshit, A. (2009). Cloud Security Issues. Teoksessa *2009 IEEE International Conference on Services Computing* (s. 517–520). IEEE. https://doi.org/10.1109/SCC.2009.84

Kato, M., & Charoenrat, T. (2018). Business continuity management of small and medium sized enterprises: Evidence from Thailand. *International Journal of Disaster Risk Reduction*, *27*, 577–587. https://doi.org/10.1016/j.ijdrr.2017.10.002

Kaufhold, M.-A., Riebe, T., Reuter, C., Hester, J., Jeske, D., Knüver, L., & Richert, V. (2018). Business Continuity Management in Micro Enterprises: Perception, Strategies, and Use of ICT: *International Journal of Information Systems for Crisis Response and Management*, *10*(1), 1–19. https://doi.org/10.4018/IJISCRAM.2018010101

Kaur, T. (2019). Cloud Computing: A Study of the Cloud Computing Services. *International Journal for Research in Applied Science and Engineering Technology*, *7*(6), 1933–1938. https://doi.org/10.22214/ijraset.2019.6325

Kaur, T., & Kamboj, S. (2023). Descriptive Analysis of the Cloud Computing Services and Deployment Models. Teoksessa *2023 International Conference for Advancement in Technology (ICONAT)* (s. 1–6). IEEE. https://doi.org/10.1109/ICONAT57137.2023.10080749

Kowtha, S., Nolan, L. A., & Daley, R. A. (2012). Cyber security operations center characterization model and analysis. Teoksessa *2012 IEEE Conference on Technologies for Homeland Security* (s. 470–475*). IEEE.* https://doi.org/10.1109/THS.2012.6459894

Kyberturvallisuuskeskus. (2019). *Ohjeita pilvipalvelujen turvallisuudesta yksityishenkilöille, pienyhteisöille ja -yrityksille*. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/ohjeita-pilvipalvelujen-turvallisuudesta-yksityishenkiloille-pienyhteisoille-ja

Kyberturvallisuuskeskus. (2020a). *Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)*. Kyberturvallisuuskeskus. https://www.kyberturvallisuuskeskus.fi/fi/julkaisut/pilvipalveluiden-turvallisuuden-arviointikriteeristo-pitukri

Kyberturvallisuuskeskus. (9.7.2020b). *Tietoturva*. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Lambert, P. (2022). Beginner's Guide to Business Continuity – Strategies to improve every BC Program. DRJ Academy & LAMBERT Learning Institute. https://drj.com/beginners-guide-to-bc/

Leeuw, K. M. M. de, & Bergstra, J. (2007). *The History of Information Security: A Comprehensive Handbook*. Sciencedirect. https://www.sciencedirect.com/book/9780444516084/the-history-of-information-security

Lindström, J., Samuelsson, S., & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management: An International Journal*, *19*(2), 243–255. https://doi.org/10.1108/09653561011038039

Mason, R. O. (1986). Four Ethical Issues of the Information Age. *MIS Quarterly*, *10*(1), 5–12. https://doi.org/10.2307/248873

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. *Recommendations of the National Institute of Standards and Technology* (NIST SP800-145). https://csrc.nist.gov/pubs/sp/800/145/final

Moyer, J., & Novick, K. (2012). Introducing a New Resource for Water and Wastewater System Business Continuity Planning. *Journal - American Water Works Association*, *104(3)*, 37–39. https://doi.org/10.5942/jawwa.2012.104.0050

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26. https://doi.org/10.1016/j.infoandorg.2006.11.001

Niemimaa, M., & Järveläinen, J. (2013). IT Service Continuity: Achieving Embeddedness through Planning. Teoksessa *2013 International Conference on Availability, Reliability and Security* (s. 333–340). IEEE. https://doi.org/10.1109/ARES.2013.45

Niemimaa, M., Järveläinen, J., Heikkilä, M., & Heikkilä, J. (2019). Business continuity of business models: Evaluating the resilience of business

models for contingencies. *International Journal of Information Management*, *49*, 208–216. https://doi.org/10.1016/j.ijinfomgt.2019.04.010

Patel, P., & Deshpande, V. (2017). Application Of Plan-Do-Check-Act Cycle For Quality And Productivity Improvement-A Review. *International Journal for Research in Applied Science & Engineering Technology*, 5, 197–201. https://www.researchgate.net/publication/318743952_Application_Of_Plan-Do-Check-Act_Cycle_For_Quality_And_Productivity_Improvement-A_Review

Puusa, A., & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus. https://www.gaudeamus.fi/teos/laadullisen-tutkimuksen-nakokulmat-ja-menetelmat/

Rani, B., Dr, B., & Dr, A. (2015). Cloud Computing and Inter-Clouds – Types, Topologies and Research Issues. *Procedia Computer Science*, *50*, 24–29. https://doi.org/10.1016/j.procs.2015.04.006

ResearchGate. (julkaisuaika tuntematon). *Sashko Ristov.* Haettu 22.1.2024 osoitteesta https://www.researchgate.net/profile/Sashko-Ristov

Ristov, S., Gushev, M., Kostoska, M., & Kiroski, K. (2011). Business Continuity Challenges in Cloud Computing. Teoksessa *ICT Innovations 2011 Web Proceedings* (s. 149–157). Springerlink. https://proceedings.ictinnovations.org/attachment/paper/238/business-continuity-challenges-in-cloud-computing.pdf

Sahebjamnia, N., Torabi, S. A., & Mansouri, S. A. (2015). Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*, *242*(1), 261–273. https://doi.org/10.1016/j.ejor.2014.09.055

Salminen, A. (2023). Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja joihinkin hallintotieteellisiin sovelluksiin. *Vaasan yliopiston raportteja*, *40*, 7–8. https://osuva.uwasa.fi/handle/10024/15470

Sanastokeskus TSK ry. (2018). *Kyberturvallisuuden sanasto*. Huoltovarmuuskeskus. https://sanastokeskus.fi/tiedostot/pdf/Kyberturvallisuuden_sanasto.pdf

SFS. (julkaisuaika tuntematon). *ISO/IEC 27000 Tietoturvallisuuden standardisarja*. Haettu 16.11.2022 osoitteesta https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/

SFS. (julkaisuaika tuntematon). *ISO 22301 Turvallisuus ja kriisinkestävyys*. Haettu 10.1.2023 osoitteesta https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-22301-turvallisuus-ja-kriisinkestavyys/

Staalinprasannah, N., & Suriya, S. (2013). Implementation of Xenserver to ensuring business continuity through power of virtualization for cloud

computing. Teoksessa *2013 Fourth International Conference on Computing, Communications and Networking Technologies* (s. 1–6). https://doi.org/10.1109/ICCCNT.2013.6726465

Statista. (2023) *Public Cloud – Finland* [tutkimusdata]. https://www.statista.com/outlook/tmo/public-cloud/finland

Suomen Riskienhallintayhdistys ry. (julkaisuaika tuntematon). *PK-RH riskienhallinta – Nelikenttäanalyysi – SWOT*. Haettu 18.12.2023a osoitteesta https://pk-rh.fi/tools/swot.

Suomen Riskienhallintayhdistys ry. (julkaisuaika tuntematon). *PK-RH riskienhallinta – Riskien luokittelu*. Haettu 19.12.2023b osoitteesta https://pk-rh.fi/riskien-luokittelu.html

Thiel, C., & Thiel, C. (2010). Business Continuity Management für KMU. *Datenschutz und Datensicherheit - DuD*, *34*(6), 404–407. https://doi.org/10.1007/s11623-010-0114-3

Tieteen termipankki. (julkaisuaika tuntematon). *tietosuoja.* Haettu 31.1.2024 osoitteesta https://tieteentermipankki.fi/wiki/Avoin_tiede:tietosuoja.

Kallio, A. (2021). Litterointi. Teoksessa Jaana Vuori (toim.), *Laadullisen tutkimuksen verkkokäsikirja*. Tietoarkisto. https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/laadullisen-tutkimuksen-prosessi/litterointi/

Tilastokeskus. (20.12.2022). *Pilvipalveluita käytti 81 % yrityksistä vuonna 2022. [tutkimusdata]. Stat.fi.* https://www.stat.fi/julkaisu/cktvztyy82z790b55dz6j23q3

Tilastokeskus. (julkaisuaika tuntematon). *Pienet ja keskisuuret yritykset*. Haettu 10.11.2023 osoitteesta https://www2.stat.fi/meta/kas/pienet_ja_keski.html

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

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. (2016). *VAHTI 2/2016 Toiminnan jatkuvuuden hallinta*.

Valtiovarainministeriö. (2020). Julkisen hallinnon digitaalinen turvallisuus. *Valtiovarainministeriön julkaisuja*, *2020*(23). https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf

Valtiovarainministeriö. (2022). Julkisen hallinnon tietoturvallisuuden arviointikriteeristö (Julkri) – Suositus ja kriteeristö. *Valtiovarainministeriön julkaisuja*, *2022*(43). https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164183/VM_2022_43.pdf?sequence=8&isAllowed=y

Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1533

Verbano, C., & Venturini, K. (2013). Managing Risks in SMEs: A Literature Review and Research Agenda. *Journal of technology management & innovation*, *8*(3), 186–197. https://doi.org/10.4067/S0718-27242013000400017

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

LIITE 1 HAASTATTELURUNKO

Taustakysymykset

- Haastateltavan toimenkuva ja titteli
- Yrityksen toimiala
- Yrityksen koko

Jatkuvuuden hallinta/ jatkuvuussuunnittelu

- Mitä jatkuvuuden hallinta/jatkuvuussuunnittelu tarkoittaa sinulle tai yritykselle yleisesti ottaen?
- Kenen vastuulla jatkuvuuden hallinta on yrityksessänne?
- Miten olette toteuttaneet yrityksessänne jatkuvuuden hallintaa/jatkuvuussuunnittelua yleisesti ottaen?
- Millaisia haasteita olette kohdanneet toimintojenne jatkuvuuden hallinnassa/ jatkuvuussuunnitelman luomisessa?
- Millaiset tekijät helpottavaisivat jatkuvuuden hallintaa/ jatkuvuussuunnitelman laatimista?
- Oletteko hyödyntäneet mitään olemassa olevaa ohjetta/mallia/viitekehystä jatkuvuuden hallinnan toteuttamiseen?
- Jos olette,
    - Millaisia haasteita kohtasitte jatkuvuuden hallintaan käytettyjen ohjeiden/mallien /standardien/viitekehysten etsinnässä?
    - Millaisia haasteita kohtasitte jatkuvuuden hallintaan käytettyjen ohjeiden/ mallien /standardien/viitekehysten käyttöönotossa?
    - Millaisia haasteita olette kohdanneet jatkuvuuden hallintaan käytettävien ohjeiden/mallien /standardien/viitekehysten mukaan toteutetun jatkuvuuden hallinnan ylläpidossa?
    - Millaisilla ohjeen/mallin/standardin/viitekehyksen asioilla/ominaisuuksilla olisi positiivinen vaikutus jatkuvuuden hallintaan yrityksessänne?
- Oletteko laatineet jatkuvuussuunnitelman?
    - Milloin jatkuvuussuunnitelma on laadittu?
    - Kuinka usein jatkuvuussuunnitelman ajantasaisuutta/toimivuutta tarkastellaan?
    - Miten varmistatte jatkuvuussuunnitelman toimivuuden ja ajantasaisuuden?

Pilvipalvelut

- Mitä pilvipalvelut tarkoittavat yrityksellenne?
- Millaisissa tehtävissä pilvipalveluita organisaatiossanne käytetään?
- Millaisia haasteita pyritte pilvipalveluilla ratkaisemaan?

- Kuinka merkittävässä roolissa pilvipalvelut ovat organisaationne liiketoiminnan kannalta?
- Miten pilvipalveluiden merkitys on muuttunut organisaatiossanne viimeisten vuosien aikana?

Pilvipalveluiden jatkuvuuden hallinta

- Millaisia riskejä pilvipalveluihinne mielestänne kohdistuu?
- Miten olette määrittäneet riskit?
- Miten olette huomioineet pilvipalveluiden ulkoistetun luonteen?
- Miten pilvipalveluita hankittaessa huomioitte jatkuvuuteen vaikuttavat asiat?
- Oletteko käyneet toimittajan kanssa keskustelua pilvipalveluiden turvallisuuteen ja jatkuvuuteen liittyvistä vastuista?
- Mitkä pilvipalveluiden turvallisuuteen liittyvistä asioista ovat mielestänne teidän, mitkä organisaationne ulkopuolisten toimijoiden vastuulla?
- Millaisia haasteita olette kohdanneet pilvipalveluihin liittyvässä jatkuvuuden hallinnassa/ jatkuvuussuunnitelman luomisessa?
- Millaiset tekijät helpottavaisivat pilvipalveluihin liittyvää jatkuvuuden hallintaa/ jatkuvuussuunnitelman laatimista?
- Millaiset tekijät helpottavaisivat pilvipalveluihin liittyvää jatkuvuuden hallintaa/ jatkuvuussuunnitelman ylläpitoa?