Lauri Alppisara

JATKUVUUDEN HALLINTA IT-PALVELULIIKETOIMINNASSA: CASE TIETO OYJ

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2012

TIIVISTELMÄ

Alppisara, Lauri
Jatkuvuuden hallinta IT-palveluliiketoiminnassa: Case Tieto Oyj
Jyväskylä: Jyväskylän yliopisto, 2012, 98 s.
Tietojärjestelmätiede, pro gradu-tutkielma
Ohjaaja: Heikkilä, Marikka

Yhteiskunnan tietoteknistymisen jatkuessa vakaille IT-palveluille on yhä enemmän kysyntää. IT-palvelutoimittajien rooli asiakasyritysten liiketoiminnassa kasvaa, koska liiketoimintaprosessit ovat yhä riippuvaisempia tietojärjestelmistä ja muusta IT-infrastruktuurista. Samanaikaisesti IT-infrastruktuuri kehittyy kompleksisempaan suuntaan, siksi jatkuvuuden hallinnalla, häiriöiden sietokyvyllä ja toipumiskyvyllä on elintärkeä rooli liiketoiminnan ylläpitämisessä. Kaikkia häiriötilanteita ei voi estää, mutta riskien vaikuttavuutta liiketoimintaan voidaan vähentää varautumisen avulla, tällöin puhutaan organisationaalisen häiriönsietokyvyn kasvattamisesta.

Häiriötilanteisiin varautumisen lisäksi tutkielmassa käydään läpi jatkuvuuden hallinnan toimenpiteet kriisin aikana ja palauduttaessa kriisitilanteesta. Tutkielmassa kuvataan liiketoimintalähtöisen jatkuvuuden hallinnan kirjo: Tutkielmassa lähdetään liikkeelle organisaatioon johtotasolta ja syvennytään jatkuvuuden hallinnan ohjelman elementteihin: strategiaan, riskianalyysiin, jatkuvuussuunnitteluun, kriisinhallintaan ja toipumissuunnitteluun. Kirjallisuuden perusteella muodostetaan jatkuvuuden hallinnan teoreettinen viitekehys. Viitekehyksen ja case-tutkimuksen avulla pureudutaan IT-palveluyritys Tieto Oyj:n jatkuvuuden hallinnan järjestelyihin sen tietokonekeskuksen tasolla. Tietokonekeskuksien jatkuvuus, häiriöidensieto- ja toipumiskykyä ylläpidetään huolellisen suunnittelun ja redundanttien komponenttien avulla. Tieto Oyj:n tietokonekeskukset toimivat samanaikaisesti monen asiakasyrityksen liiketoiminnan mahdollistajana, joten jatkuvuuden varmistamisen tärkeyttä ei voi ylikorostaa.

Onnistunut jatkuvuuden hallinnan ohjelma tuottaa luottamusta niin sisäisissä, kuin ulkoisissa sidosryhmissä ja voi mahdollistaa organisaation kyvykkyyden toimia menestyksekkäästi vaikeissakin liiketoimintaympäristöissä vahvan toimitusvarmuuden ja luotettavuuden takia. Luotettavuuden kautta on organisaation mahdollista parantaa asemaansa kilpailuillakin markkinoilla. On myös muistettava, että hankitun luottamuksen voi myös menettää hyvin nopeasti. Tämän tutkielman tavoitteena on antaa selkeä kuva jatkuvuuden hallinnan merkityksestä nopeasti muuttuvassa ja nykyaikaisessa IT-palveluliiketoiminnassa, sekä tuottaa malli jatkuvuuden hallinnan kyvykkyyden kuvaamiseen.

Asiasanat: liiketoiminnan jatkuvuuden hallinta, jatkuvuuden hallinnan strategia, jatkuvuus- ja toipumissuunnittelu, häiriönsietokyky, riskianalyysi

ABSTRACT

Alppisara, Lauri
Continuity management in IT service business: Case Tieto Corporation
Jyväskylä: University of Jyväskylä, 2012, 98 p.
Information Systems Science, Master's Thesis
Supervisor: Heikkilä, Marikka

Today's society is constantly moving towards more and more information technology dependable direction. Meanwhile IT-services are increasingly on demand. The role of the IT-service provider in their client companies businesses is stronger than ever before: business processes are more and more dependent on IT-infrastructure. Simultaneously IT-infrastructure is developing more complex – that is why business continuity management, incident resilience and recovery capability play a vital role in maintaining the overall business. Every crisis cannot be prevented, even though the impacts of the risks can be mitigated through preparedness. This is about building the organizational incident resilience.

In addition to preparing, this thesis is dealing with business continuity management actions during a crisis and when recovering from it. This thesis describes the outlook of the broad range of business continuity management: it starts from the top management level and goes deeper into the elements of the business continuity management program, business continuity planning, crisis management and disaster recovery planning. Literature review provides the basis of the theoretical framework for business continuity management which is used in conjunction with case-study in getting familiar to Tieto Corporation continuity arrangements in the level of the data center services. Data center continuity, resilience and recovery capabilities are maintained through careful planning and redundant components. Tieto Corporations high security data centers simultaneously enable the business of several customer companies so its importance cannot be overemphasized.

Successfully implemented business continuity management program produces confidence in the organization for both internal and external stakeholders, and enables the organization's ability to operate successfully in difficult environments. Reliability of services improves the company's role in the competitive markets. Though the trustfulness gained can also be lost very quickly. The aim of this thesis is to provide a clear picture of the importance of business continuity management in a rapidly evolving and modern IT-service business and to develop model for evaluating business continuity maturity.

Keywords: business continuity management, business continuity management strategy, business continuity & disaster recovery planning, incident resilience, risk analysis

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Tämän tutkielma on jatkoa Jyväskylän yliopistossa, informaatioteknologian tiedekunnassa keväällä 2011 valmistuneeseen kandidaatintutkielmaani, jossa liiketoiminnan jatkuvuussuunnittelua tarkasteltiin laajasti aihetta käsitelleen kirjallisuuden avulla. Kandidaatintutkielmani keskeisenä tuloksena todettiin, että onnistunut jatkuvuussuunnittelu on kilpailukyvyn edellytys tietoteknistyvässä yhteiskunnassa. Tässä pro gradu -tutkielmassa jatkuvuussuunnittelusta siirrytään laajempaan perspektiiviin, organisaation liiketoiminnan jatkuvuuden hallintaan. Tutkielmassa esitetään jatkuvuuden hallinnan tavoite ja painopistealueet, joiden kautta jatkuvuutta pyritään hallitsemaan. Yksi näistä jatkuvuuden hallinnan mahdollistavista tekijöistä on jatkuvuussuunnittelu. Myöhemmin tutkielmassa käytetään termiä jatkuvuuden hallinta, ellei liiketoiminnan osuutta kontekstissa haluta erityisesti korostaa. Jatkuvuuden hallinta on siis yläkäsite jatkuvuussuunnittelulle.

Tässä tutkielmassa tarkastelen jatkuvuuden hallintaa Pohjois-Euroopan johtavassa informaatioteknologian palveluita tuottavassa yrityksessä, Tieto Oyj:ssä. IT-palveluyrityksen tehtävänä on tuottaa palveluja asiakasyrityksilleen erilaisten projektien muodossa. IT-palveluyrityksen toimintaan kuuluu usein myös käyttöpalvelujen tarjoaminen, jossa asiakasyritysten liiketoimintakriittisten tietojärjestelmien ylläpito hoidetaan saumattomasti palveluntarjoajan palvelukeskuksen konesaleissa kellon ympäri. Tämä tutkielma käsittelee liiketoiminnan jatkuvuuden hallintaa juuri asiakkaille tarjottavien konesalipalveluiden muodossa.

Jatkuvuuden hallintaa käsittelevän kirjallisuuden perusteella on pääteltävissä, että hyvin toteutetulla jatkuvuuden hallinnalla on positiivinen vaikutus yrityksen kilpailukykyyn. Kirjallisuudessa esitetään useita prosessimalleja jatkuvuuden hallinnan organisoimiseen. Kuitenkin monissa julkaisuissa on nähtävissä jatkuvuuden hallinnan yleinen suuntaviiva, joita yleisesti kirjallisuudessa suositellaan noudatettavan. Toisin sanoen samat elementit toistuvat jatkuvuuden hallintaa käsittelevissä julkaisuissa; jatkuvuuden hallintaa käsittelevien prosessimallien toimintaperiaatteet ovat siis samankaltaisia. Tutkielmassa luon jatkuvuuden hallinnan viitekehyksen kirjallisuuden perusteella, jota vertaan

haastattelututkimukseen pohjautuvaan käsitykseen Tiedon jatkuvuuden hallinnasta. Tutkielmassa pyritään löytämään vastauksia tutkimusongelmaan, jossa selvitetään, miten jatkuvuuden hallinnan järjestelyt on toteutettu Tieto Oyj:ssä. Tämä pääongelma voidaan muotoilla seuraavasti: **Painottaako Tieto Oyj samoja jatkuvuuden hallinnan periaatteita, kuin kirjallisuudessa on esitetty?** Pyrin löytämään yhtymäkohtia ja mahdollisia eroavaisuuksia Tiedon jatkuvuuden hallinnan ja kirjallisuudessa esitettyjen jatkuvuuden hallinnan periaatteiden välillä. Aliongelmana pyrin löytämään vastauksen kysymykseen: **Miten jatkuvuuden hallinnan tärkeys ja laajempi palvelutaso on perusteltavissa IT-palvelutoimittajan asiakkaalle?** Tutkielman teoreettisena tavoitteena on kirjallisuuden ja haastattelujen tulosten perusteella luoda jatkuvuuden hallinnan kypsyyttä kuvaava malli, joka ottaa huomioon IT-palveluliiketoiminnan tarpeet.

1.1 Tutkimusmenetelmä ja rajaukset

Tutkimuksen tarkoituksena on pyrkiä laajemmin käsittämään suuren IT-palveluyrityksen jatkuvuuden hallintaa; tutkimus on siis laadullinen (kvalitatiivinen). Hirsjärvi, Remes ja Sajavaara (2008) listaavat kvalitatiivisen tutkimuksen tyypilliseksi piirteeksi muun muassa kokonaisvaltaisen tiedonhankinnan ja aineiston kokoamisen luonnollisissa, todellisissa tilanteissa. Laadullisena tutkimusmenetelmänä on case-tutkimus eli tapaustutkimus, jossa haastatellaan kohdeorganisaation jatkuvuuden hallinnan avainhenkilöitä. Haastateltavat edustavat jatkuvuuden hallinnan osa-alueita sekä tekniseltä puolelta, eli konesalien jatkuvuuden hallinnasta vastaavia henkilöitä, että liiketoimintaprosessien johtamisesta vastuussa olevia henkilöitä. Lisäksi haastateltavana on henkilö, joka edustaa Tiedon jatkuvuuden hallinnan yleistä näkemystä ja strategisia painotuksia. Case-tutkimuksen avulla aiheen tutkiminen auttaa ymmärtämään miksi, miten, mitä ja ketä varten jatkuvuutta hallitaan ja miksi se on tärkeää.

1.2 Tiedonkeruutavat

Pyrin pitämään lähdeaineiston mahdollisimman tuoreena, koska tutkielman aihe on jatkuvasti muutoksessa: teknologia kehittyy ja toimintatavat muuttuvat. Jatkuvuuden hallinnan periaatteet ovat pysyvämpiä, mutta jatkuvuuden hallinnan ja teknologian kehittyminen tuottavat yhä uusia haasteita organisaatioille. Laadullisen tutkimuksen lähtökohtana Hirsjärven, Remeksen ja Sajavaaran (2008) mukaan on todellisen elämän kuvaaminen. Empiirinen osuus käsittelee jatkuvuuden hallintaa aidossa toimintaympäristössä, vastaavasti teoriaosuudessa täytyy pyrkiä esittämään ajankohtaisin ja relevantein tieto, jotta luotettavia havaintoja ja johtopäätöksiä voidaan tehdä.

Tutkielman teoriaosuuteen kuuluvan kirjallisuuskatsauksen muodostamisessa hyödynnettiin Nelli-tiedonhakuportaalia, Google Scholar – hakukonetta, Jyväskylän yliopiston kirjastoa ja Tieto Oyj:ltä saatua materiaalia. Nelli-tiedonhakuportaalin kautta etsittiin tietoa informaatioteknologian ja tekniikan alojen tietokannoista, sekä taloustieteen ja viestinnän tietokannoista. Lähdeaineistoa löytyi seuraavista informaatioteknologian ja tekniikan alojen tietokannoista: ACM Digital Library, Computer and Information Systems Abstracts (ProQuest), Electronics and Communications Abstracts (ProQuest), IEEE Xplore - IEEE/IEE Electronic Library, Proquest Computing (ProQuest), ScienceDirect (Elsevier), SpringerLink ja Web of Science - WoS (ISI). Taloustieteen ja viestinnän tietokannoista lähdeaineistoa tutkielmassa on Emerald Journals (Emerald), ABI/INFORM Complete (ProQuest) ja Business Source Elite (EBSCO) tietokannoista. Informaatioteknologia-alan lehtijulkaisuista haettiin konferenssijulkaisuja ja tieteellisiä artikkeleita. Google Scholar – hakukonetta käytettiin jatkuvuuden hallinnasta kertovien kirjojen selaamiseen, jonka kautta myös Jyväskylän yliopiston kirjastosta oli enemmän hyötyä; moni Google Scholarissa mainittu kirja löytyi kirjastosta painetussa muodossa. Tieto Oyj antoi myös tutkimuksen ajaksi käyttööni ajankohtaista aineistoa muun muassa tietoturvaan ja jatkuvuuden hallintaan liittyvistä standardeista.

1.3 Tutkielman rakenne

Toisessa luvussa käydään läpi teoreettisemmin jatkuvuuden hallintaa, eli miten aihetta on käsitelty kirjallisuudessa. Luvussa selvitetään jatkuvuuden hallinnan yleinen luonne, sen asema organisaatiossa, jatkuvuuden hallinnan osa-alueet ja millainen tarve jatkuvuuden hallinnalle tietoyhteiskunnassa nykyisin on. Lisäksi käydään läpi jatkuvuuden hallintaa koskevia standardeja ja hyviä käytäntöjä. Tutkielman kolmannessa luvussa luodaan katsaus IT-palveluliiketoiminnan erityispiirteisiin ja sen toimintaympäristön jatkuvuuden hallintaan. IT-palveluyrityksen toimintaympäristön keskeisessä osassa on IT-infrastruktuuri, siksi kolmas luku on tutkielman kaikkein teknisorientoitunein. Neljännessä luvussa muodostetaan kirjallisuuden perusteella jatkuvuuden hallinnan viitekehys, joka kuvaa koko jatkuvuuden hallintaprosessin riskien tunnistamisesta jatkuvuutta edistävien suunnitelmien uudelleenarviointiin. Viitekehys toimii pohjana tutkielman empiirisessä osassa tehdyille haastatteluille. Viidennessä luvussa käsitellään tutkielman empiirisen osuuden rakentamista eli case-tutkimusta, mikä on toteutettu teemahaastattelujen avulla Tieto Oyj:ssä. Luvussa käydään läpi tutkimusmetodin valintaprosessi, haastattelujen lähtökohdat, perustelut haastateltavien valinnalle ja haastattelujen rajoitukset. Kuudennessa luvussa käsitellään haastattelut neljännen luvun jatkuvuuden hallinnan viitekehyksessä muodostetuin aihepiirein ja lopuksi vedetään yhteen haastattelujen tulokset ja verrataan alustavasti tuloksia tähän jatkuvuuden hallinnan viitekehykseen. Teoreettisen viitekehyksen pohjalta ja teemahaastattelujen perusteella

on ymmärretty jatkuvuuden hallinnan tavoittelevan samoja etuja, kuin perinteisesti laatujärjestelmien käyttöönotolla on pyritty saavuttamaan. Kuudennessa luvussa esitetään jatkuvuuden hallintaprosessin eteneminen organisaatiossa ja IT-palveluliiketoiminnan jatkuvuuden hallinnan kypsyysmalli, jossa on sidottu jatkuvuuden hallinnan tavoitteet laadunhallinnasta tuttuun CMMI-kyvykkyys- ja kypsyysmalliin (engl. capability maturity model integration, CMMI). Seitsemännessä luvussa, eli pohdinnassa analysoidaan tutkimuksen tuloksia. Luvussa suhteutetaan tulokset jatkuvuuden hallinnan viitekehykseen, annetaan vastaukset asetettuihin tutkimusongelmiin ja pohditaan tutkimuksen luotettavuutta ja yleistettävyyttä. Luvussa tuon esille omat ehdotukseni jatkuvuuden hallinnan tärkeyden perustelemiseen. Kahdeksantena ja viimeisenä lukuna on yhteenveto, jossa tiivistäen esitetään vastaukset tutkimusongelmiin, kerrataan jatkuvuuden hallinnalla saavutettavat hyödyt asiakaslähtöisessä IT-palveluliiketoiminnassa ja esitetään aiheet jatkotutkimukselle.

2 LIIKETOIMINNAN JATKUVUUDEN HALLINTA

Liiketoiminnan jatkuvuuden hallinnalle (engl. business continuity management, BCM) on kirjallisuudessa monia määritelmiä. Sana jatkuvuus tarkoittaa yleisesti jotakin etenevää ja keskeytyksetöntä toimintaa. Liiketoiminnan jatkuvuuden hallinnalla tarkoitetaan siis liiketoiminnan keskeytyksetöntä jatkumista ja sen hallitsemista. International Organization for Standardization (ISO) määrittelee useassa standardissaan jatkuvuuden hallinnan tavoitteeksi liiketoimintojen keskeytyksien torjumisen ja kriittisten liiketoimintaprosessien suojaamisen suurilta häiriöiltä ja onnettomuuksilta varmistaen tietojärjestelmien käytön nopean jatkumisen (ISO 27001, 2005; ISO 27002, 2005). British Standard Institutionin vuonna 2003 julkaiseman Publicly Available Specification 56:n (PAS 56) ja sen pohjalta kolme vuotta myöhemmin British Standards Institutionin julkaiseman BS 25999-1 Code of Practice for Business Continuity Management (BS 25999-1) mukaan jatkuvuuden hallinnan tulisi olla liiketoimintalähtöinen ja -ohjattu toiminto, joka yhdistää strategiset ja operationaaliset rakenteet organisaation häiriöiden ja keskeytyksien sietokyvyn aikaan saamiseksi (PAS 56, 2003), häiriötilanteiden hallitsemiseen ja niistä toipumiseen, sekä organisaation maineen ja brändin suojelemiseen (BS 25999-1, 2006). Jatkuvuuden hallinta ei pääty jatkuvuusjärjestelyiden toteuttamiseen, vaan jatkuu esimerkiksi seurannan, koulutuksen ja arvioinnin kautta normaalina osana liiketoimintoja. Jatkuvuuden hallintaa voidaan siis pitää koko ajan käynnissä olevana prosessina (BCM Glossary, 2010).

2.1 Jatkuvuuden hallinnan suhde riskienhallintaan

Riskienhallinta (engl. risk management) on organisaation synnyttämä kulttuuri, prosessit ja rakenteet, joiden tavoitteena on pystyä tehokkaasti hallitsemaan uhkia ja haittavaikutuksia. Kaikkea riskiä ei ole mahdollista tai edes toivottavaa eliminoida, joten riskienhallinnan tavoitteena on kehittää kustannustehokkaita prosesseja, jotka vähentävät riskien vaikuttavuutta hyväksyttävälle tasolle, tor-

juvat hyväksymättömät riskit, siirtävät riskiä taloudellisin keinoin (kuten vakuutuksin) ja käsittelevät riskejä organisatorisin keinoin, kuten jatkuvuuden hallinnan avulla (BCM Glossary, 2010). Jatkuvuuden hallintastrategian rinnalla PAS 56 (2003) näkee riskienhallintaohjelman käyttöönottamisen ja kehittämisen organisaatiossa. Shaw (2005) tiivistää riskienhallinnan olevan johdon strateginen ja taktinen työkalu päätettäessä toimenpiteistä liiketoimintaa koskettavien riskien käsittelyssä. Shawn (2005) mukaan riskienhallinta on perusta laajemmalle jatkuvuuden hallinnan ohjelmalle, sekä ohjaa päätöksiä, jotka vaikuttavat kaikkiin muihin toimintoihin jatkuvuuden hallinnan ohjelman puitteissa. Blyth (2009) täsmentää riskienhallinnan olevan yhteys liiketoiminnan suojelemisen, sietokyvyn kasvattamisen ja jatkuvuuden välillä. Riskienhallinta siis vahvistaa liiketoiminnan jatkuvuutta ja toipumista - parantaen tuottavuutta ja tuottoja (Shaw, 2005). Riskienhallinnassa ja jatkuvuuden hallinnassa on tunnistettavissa hyvin samanlaisia elementtejä. Vanston (2003) huomauttaakin riskienhallinnan ja jatkuvuuden hallinnan rajojen hämärtyvän; molemmilla on sama fokus, sekä osittain samat työkalut ja tekniikat tavoitteisiinsa pääsemiseksi. Vanstonin (2003) viesti on selvä: riskienhallinnan ja jatkuvuuden hallinnan välistä synergiaa tulee hyödyntää, jotta suojautuminen liiketoiminnan keskeytyksiltä voidaan maksimoida.

2.2 Jatkuvuuden hallinnan ohjelma

Jatkuvuuden hallinnan ohjelman tarkoituksena on liiketoiminnan jatkuvuuskyvykkyyden luominen ja ylläpitäminen tarkoituksenmukaisella tavalla organisaation kokoon ja kompleksisuuteen nähden (BS 25999-1, 2006). Tehokkaan jatkuvuuden hallinnan ohjelman avulla organisaation on mahdollista proaktiivisesti tunnistaa, hallita ja pienentää sen toimintaa uhkaavia riskejä (BS 25999-1, 2006). ISF (2011) painottaa häiriöitä sietävän teknisen infrastruktuurin, kriisinhallinnan kyvykkyyden ja jatkuvuussuunnitelmien ja jatkuvuusjärjestelyiden koordinoinnin koko organisaation alueella. Jatkuvuuden hallinnan ohjelman avulla organisaatio voi tehokkaasti vastata toiminnan keskeytymiseen ja säilyttää kyvyn hallita vakuuttamattomia riskejä, kuten mainetta: osoittamalla jatkuvuuden hallinnan ohjelman uskottavuuden ja kyvykkyyden organisaation on mahdollista jopa luoda itselleen kilpailuetua esimerkiksi asiakaspalvelun, tuottavuuden ja henkilökuntansa työllistämisen ylläpidettävyyden kautta (BS 25999-1, 2006). Organisaation on kyettävä toimimaan jatkuvuussuunnitelmissa edellytetyllä tavalla, siksi henkilöstölle on toimitettava toimintaohjeet ja tehtävät kriisitilanteiden varalle dokumentoidussa muodossa (ISF, 2011).

Jatkuvuuden hallinnan tavoin jatkuvuuden hallinnan ohjelma on jatkuva prosessi. Monissa jatkuvuuden hallintaa käsittelevissä tieteellisissä teksteissä jatkuvuuden hallinta koostuu useasta elementistä tai osasta. Julkaisusta riippuen osien määrä vaihtelee sen mukaan, miten tarkasti jatkuvuuden hallinnan ohjelma kussakin julkaisussa on kuvattu. Yleisesti ottaen osat ovat kuitenkin pitkälti sisällöllisesti samoja, vaikka eri otsikoita onkin käytetty. Käyn seuraa-

vaksi läpi viisi tärkeintä ja suurinta jatkuvuuden hallinnan ohjelman vaihetta, jotka kirjallisuudessa ovat nousseet esiin.

2.2.1 Menettelytavat, periaatteet ja toimintaympäristö

Jatkuvuuden hallinnan lähtökohtana on organisaation tilan ja toimintaympäristön ymmärtäminen. Nykyajan yritykset ja organisaatiot ovat entistä riippuvaisempia tietojärjestelmien, ohjelmistojen ja verkkoyhteyksien toiminnasta, joten informaatioteknologian jatkuva- tai korkea käytettävyyden taso on elintärkeää koko liiketoiminnalle (ITIL v3, 2007). Koska organisaatioiden liiketoimintaprosessit ovat hyvin riippuvaisia tietojärjestelmien toiminnasta, ITIL v3:ssa (2007) puhutaankin liiketoiminnan jatkuvuuden hallinnan sijaan informaatioteknologian palvelujen jatkuvuuden hallinnasta, vaikka käytännössä kyse on siis samasta asiasta. Liiketoiminnan jatkuvuuden hallinta on yläkäsite IT-palvelujen jatkuvuuden hallinnalle, jolle liiketoiminnan jatkuvuuden hallinta määrittää tavoitteet, kohdealueen ja vaatimukset (ITIL v3, 2007). Menestyksekäs jatkuvuuden hallinnan implementointi organisaatiossa, eli informaatioteknologian palvelujen jatkuvuus ja korkea käytettävyys voidaan saavuttaa liiketoimintaprosesseja koskettavien riskien tunnistamisen ja niiden vähentämisen kautta, joka lähtee ylimmän johdon sitoutumisesta prosessiin, jota koko organisaation henkilöstä tukee (ITIL v3, 2007). Organisaation tulisikin luoda itselleen selkeät menettelytavat, periaate tai politiikka, joka lähtee jatkuvuuden hallinnan tavoitteista ja joka on samansuuntainen liiketoiminnan vaatimusten kanssa (BS 25999-1, 2006).

2.2.2 Jatkuvuuden hallinnan strategia

Toisena osa-alueena voidaan pitää jatkuvuuden hallinnan strategian luomista. Koko organisaation kattava jatkuvuusstrategia tulee luoda ja ylläpitää, ja sen tulee olla linjassa organisaation liiketoimintastrategian ja tietoturvastrategian kanssa (ISF, 2011). Jatkuvuuden hallinnan strategia voi olla valittavissa tuote- tai palvelukohtaisesti. Valittiinpa minkälainen strategia tahansa, kaikki tähtäävät kuitenkin siihen, että organisaatio voi jatkaa kunkin tuotteen tai palvelun toimittamista asiakkaillensa hyväksyttävällä tasolla häiriöistä riippumatta (BS 25999-1, 2006). Hyväksyttävällä tasolla tarkoitetaan ennalta sovittua palvelun tasoa.

Organisaation jatkuvuuden hallinnan strategian tulee tähdätä siihen, että liiketoimintaa koskettavia riskejä kyetään hallitsemaan, jotta tärkeiden sidosryhmien edut, organisaation maine, brändi ja kyky arvon tuottamiseen voidaan turvata (ITIL v3, 2007; PAS 56, 2003). Jatkuvuuden hallinnan strategian on oltava sidoksissa organisaation strategiaan, jotta riskejä kyetään hallitsemaan ja jatkuvuuden hallintaa voidaan parantaa organisaation strategian- ja yleisten tavoitteiden mukaisesti (BS 25999-1, 2006). Toisena perusteluna jatkuvuuden hallinnan strategian tavoitteiden yhdistämiseksi liiketoiminnan strategian tavoitteisiin on se, koska yleisesti organisaatioiden liiketoiminnan strategiat ja

päätökset perustuvat sille oletukselle, että liiketoiminta jatkuu keskeytyksettä (Australian National Audit Office, 2000).

Organisaation tulee tunnistaa rajoitteet ja uhat, jotka voivat aiheuttaa merkittäviä häiriöitä liiketoiminnalle (ISO/PAS 22399, 2007). Rajoitteet ja uhat tarkoittavat siis liiketoimintaan kohdistuvia riskejä. Liiketoimintaa koskettavien riskien havaitsemiseen ja tunnistamiseen käytetään riskianalyysiä ja vaikutusanalyysiä (Business Impact Analysis, BIA). Riskianalyysi on riskien tunnistamista, analysointia ja arviointia (BCM Glossary, 2010), samanaikaisesti arvioiden riskien vaikuttavuutta liiketoimintaan (Savage, 2002). Riskit järjestetään niiden todennäköisyyden ja vaikuttavuuden perusteella (Cerullo & Cerullo, 2004). Organisaation tulee kartoittaa vaikutusanalyysin avulla kaikki mahdolliset uhkatekijät ja riskit, jotka vaikuttavat organisaation liiketoiminnan päivittäisiin toimintoihin (La Fazia, 2004). Riskianalyysin ja vaikutusanalyysin tuloksena voidaan muodostaa jatkuvuusstrategia, joka on linjassa liiketoiminnan tarpeiden kanssa, sekä tasapainossa riskien vähentämisen ja toipumisvaihtoehtojen kanssa (ITILv3, 2007).

2.2.3 Reagointi - vastatoimien kehittäminen ja käyttöönotto

Kolmantena osana on jatkuvuusstrategian pohjalta vastata tunnistettujen riskien aiheuttamiin haasteisiin. Nämä vastineet ovat jatkuvuus- ja toipumissuunnitelmia, jotka kuvaavat yksityiskohtaisesti eri toimintojen vaiheet, jotka häiriötilanteessa ja palauduttaessa siitä tulee suorittaa (BS 25999-1, 2006). Jatkuvuussuunnitelmien (engl. business continuity plan, BCP) tehtävänä on tukea kriittisiä liiketoimintaprosesseja koko organisaatiossa (ISF, 2011). Kuten aikaisemmin todettiin, informaatioteknologialla on suuri rooli jatkuvuuden hallinnassa. Kuitenkin yleisesti ottaen jatkuvuussuunnitelmissa on sekä informaatioteknologiaa koskettavia osia ja myös niitä joissa se ei ole niin merkittävässä roolissa (Dey, 2011). Toipumissuunnitelmat (engl. disaster recovery plan, DRP) ovat jatkuvuussuunnitelmia teknisempiä ja keskittyvät tietojärjestelmien, ohjelmistojen ja verkkoyhteyksien toiminnan palauttamiseen häiriötilanteen tapahduttua. Jatkuvuussuunnitelmilla ja toipumissuunnitelmilla on myös toinen merkittävä ero: Cerullo ja Cerullo (2004) huomauttavat, että jatkuvuussuunnitelma ennaltaehkäisee ja auttaa varautumaan häiriötilanteisiin, kun toipumissuunnitelma auttaa palautumaan häiriöstä normaalitilaan ongelmien ilmenemisen jälkeen.

Suunnitelmia voi olla organisaatiolla useita, riippuen sen koosta ja toimintaympäristöstä. Pienemmällä yrityksellä voi olla vain yksi jatkuvuussuunnitelma, joka kattaa liiketoiminnan vaatimukset, kun taas isommalla yrityksellä voi olla lukuisia jatkuvuus-, toipumis-, ja hätätilasuunnitelmia (BS 25999-1, 2006) yksikkö- tai toimialatasolla. Yhteistä pienille ja suurille organisaatioille on se, että jokaisessa dokumentoidussa suunnitelmassa on määritelty sen tarkoitus ja kohdealue, roolit ja vastuut, suunnitelman käyttöönottoproseduurit sekä suunnitelmasta vastuussa oleva henkilö (BS 25999-1, 2006). Jokainen jatkuvuussuunnitelma tulee kehittää yhteistyössä liiketoiminnasta vastaavien henkilöiden

kanssa ja suunnitelman tulee pohjautua mahdollisiin kriisiskenaarioihin (ISF, 2011). Kriisiskenaario simuloi riskin toteutumista ja on eräänlainen oppimistilanne. Mahdollisia kriisiskenaarioita on voitu kehittää esimerkiksi aikaisemmin tehdyn riski- ja vaikutusanalyysin yhteydessä.

2.2.4 Sulauttaminen organisaation toimintatapoihin

Neljäntenä osana jatkuvuuden hallinnan prosessissa on jatkuvuuden hallinnan tunnettuuden lisääminen organisaation sisällä. Jatkuvuuden hallintaa tukevan kulttuurin rakentaminen, edistäminen ja liittäminen organisaation arvoihin varmistaa jatkuvuuden hallinnan prosessin tehokkaamman läpiviennin, kasvattaa organisaation häiriönsietokykyä, auttaa minimoimaan keskeytymisien vaikutuksen ja todennäköisyyden ja kehittää luottamusta eri sidosryhmissä (erityisesti henkilökunnassa ja asiakkaissa) organisaatiota kohtaan (BS 25999-1, 2006). Jatkuvuussuunnitelmien käyttäjät ovat lähes aina osa organisaation henkilökuntaa, siksi tietoisuuden lisääminen jatkuvuuden hallinnasta ja jatkuvuussuunnitelmien toiminnoista henkilökunnan keskuudessa on avainasemassa, jotta oikeassa tilanteessa jatkuvuussuunnitelmassa määrätyt toimenpiteet kyetään onnistuneesti toteuttamaan (Blyth, 2009). Työntekijöiden lisäksi myös johdon tulee ymmärtää jatkuvuuden hallinnan tavoitteet ja kyettävä suoriutumaan jatkuvuussuunnitelmien läpiviemisestä (Australian National Audit Office, 2000), useinhan juuri johtajat ovat kriisitilanteessa niissä toimintoja ohjaavissa rooleissa, jotka ovat vastuussa jatkuvuussuunnitelmien toteuttamisesta.

2.2.5 Jatkuvuuden hallinnan järjestelyiden kertaaminen

Viidentenä ja viimeisenä osana on jatkuvuuden hallinnan harjoittelu, ylläpito, auditointi ja arviointi. Jatkuvuuden hallintaprosessin läpikäyminen aika-ajoin auttaa vastaamaan muuttuneisiin tarpeisiin. Harjoittelu, ylläpito ja auditointi auttavat osoittamaan, että organisaation luomat jatkuvuuden hallinnan strategiat ja suunnitelmat ovat tehokkaita, uskottavia ja tarkoitukseen sopivia (BS 25999-1, 2006). Suunnitelmien ja järjestelyiden läpikäynnin tuloksena PAS 56 (2003) näkee toimivuuden, tehokkuuden ja ajantasaisuuden luovan hallinta-, kontrolli- ja koordinointikykyä organisaatiolle häiriötilanteiden varalle strategisella, taktisella ja operationaalisella tasolla. Jatkuvuuden hallinnan harjoittelu on osa tietoisuuden lisäämistä organisaation sisällä, mutta on kuitenkin sitä tarkemmin kohdennettua henkilöille, joilla on erityisiä vastuita jatkuvuuden hallintaan liittyen (SS 540, 2008).

Seuraavaksi käyn läpi jatkuvuuden hallinnan ohjelman vaiheiden merkittävimmät aliprosessit, eli jatkuvuus- ja toipumissuunnittelun sekä kriisinhallinnan (engl. crisis management, CM). Lisäksi täsmennän hieman syvemmin niiden rooleja, sekä niiden välisiä suhteita organisaation jatkuvuuden hallinnan ohjelmassa.

2.3 Jatkuvuussuunnittelu

Jatkuvuussuunnittelun tärkeyttä voidaan perustella samoilla syillä, kuten koko jatkuvuuden hallintaakin: Jatkuvuuden hallinnan avulla organisaation häiriön sietokykyä voidaan kasvattaa ja organisaation kriittisiä liiketoimintaprosesseja pitää tukea, jotta keskeytyksetön toiminta häiriöistä huolimatta voidaan taata ja häiriöiden vaikutukset liiketoiminnalle pystytään minimoimaan (ISF, 2011). Jos esimerkiksi jokin häiriö aiheuttaa elintärkeän tiedon häviämisen, tai tieto vahingoittuu, tuhoutuu tai on muuten saavuttamattomissa, seurauksena on katastrofi organisaation kriittisille prosesseille (Fang, 2010). Informaation häviäminen katastrofin seurauksena ei koske pelkästään koneilla olevaa dataa, vaan kaikki tieto mapeissa, kansioissa, sopimuksissa ja arkistoissa voidaan myös menettää (Hiles, 2007). Jos yrityksellä ei ole poikkeustilanteen tapahduttua pääsyä elintärkeisiin tallenteisiinsa on toipuminen poikkeustilanteesta käytännöllisesti katsoen mahdotonta toteuttaa (Botha & Von Solms, 2004), siksi datan kokonaisvaltainen suojaaminen vaatii eri tallennusmuotojen yhdistelemistä, varmuuskopiointia ja datan hajauttamista eri sijaintipaikkoihin (Hiles, 2007).

Jatkuvuussuunnitelma auttaa palautumaan häiriötilanteesta normaalitilaan nopeammin, koska organisaatio on tarkan suunnittelun avulla pystynyt varautumaan ja tekemään korjaavia toimenpiteitä jo ennen mahdollisien riskien toteutumista (BS 25999-1, 2006). On silti muistettava, että vaikka organisaatio olisi kuinka hyvin varautunut häiriötilanteisiin, voivat ne silti ylittää organisaation varautuneisuuden tason ja aiheuttaa odottamattomia vahinkoja (BS 25999-1, 2006), joiden todellinen vaikutus ja laajuus voi olla ennalta hyvin vaikeaa arvioida.

2.3.1 Riskien arviointi ja analysointi

Jatkuvuussuunnittelun ja jatkuvuussuunnitelman tarkoituksena on pienentää kriisin aiheuttamia vaikutuksia ja vähentää palautumistoimintojen kestoa (Cerullo & Cerullo, 2004). Jos riskejä ei käsitellä asianmukaisesti, ne voivat häiritä liiketoiminnan jatkuvuutta (Dey, 2011), siksi on luonnollista, että jatkuvuussuunnitteluprosessi käynnistyy riskien kartoittamisella. Jotta riskejä pystyttäisiin tunnistamaan, niiden vaikuttavuutta liiketoimintaan kyettäisiin arvioimaan ja toipumista suunnittelemaan, tulee organisaation tuntea toimintatapansa (Melton & Trahan, 2009). BCM Glossaryn (2010) ja PAS 56:n (2003) mukaan riskianalyysi on riskien tunnistamista, analysointia ja arviointia. Riski voidaan määritellä merkittäväksi tapahtumaksi, joka vaikuttaa organisaation kykyyn saavuttaa liiketoiminnan tavoitteensa (Australian National Audit Office, 2000). PAS 56:n (2003) mukaan liiketoiminnan riskit ovat sisäisiä ja ulkoisia tekijöitä, jotka aiheuttavat odottamattomia tappioita. Aiemmin koetut menetykset voivat helpottaa riskien arvioimista, mutta suurimmat tappiot aiheutuvat tilanteista, joita organisaation johto ei ole pystynyt kuvittelemaan (Melton & Trahan, 2009). Jatkuvuuden hallinnan yhtenä tavoitteena ja perustana jatkuvuussuunnittelulle

on PAS 56:n (2003) mukaan jatkuva riskiprofiilien ja riskitaipumusten arviointi. Kaikkia riskejä ei voi välttää, mutta niitä voi pyrkiä hallitsemaan: hyvin riskejä hallitsevat yritykset voivat ryhtyä hankkeisiin, joita toiset yritykset pitäisivät liian riskialttiina (Siltanen, 2011). Kun kaikki kustannustehokkaat toimet on toteutettu riskin vaikutusten lieventämiseksi, jäljelle jäävää riskiä, sen todennäköisyyttä ja seurauksia kutsutaan jäännösriskiksi (engl. residual risk) (PAS 56, 2003).

2.3.2 Vaikutusanalyysi

Riskien ja uhkien arvioinnin lisäksi on huomioitava niiden todennäköisyydet ja vaikutukset (ISO/PAS 22399, 2007). Riskien todennäköisyyttä ja vaikuttavuutta arvioidaan vaikutusanalyysin (engl. business impact analysis, BIA) avulla. Vaikutusanalyysi on prosessi, joka analysoi liiketoimintoja, sekä vaikutuksia, joita häiriöillä voi olla liiketoiminnoille (BS 25999-1, 2006). Vaikutusanalyysi pyrkii tunnistamaan organisaation kriittisiin toimintoihin kohdistuvat riskit ja järjestää ne todennäköisyyden ja liiketoimintaan vaikuttavuuden perusteella (Cerullo & Cerullo, 2004). Vaikutusanalyysi auttaa myös organisaatiota arvioimaan mahdollisesti aiheutuvien tappioiden (myös ei-taloudellisten) määrän. (Savage, 2002). Näitä kriittisiä ja ei-taloudellisia objekteja organisaatiossa voivat olla henkilöstö, asiakkaat ja maine.

La Fazian (2004) mukaan vaikutusanalyysi tuottaa eniten työtä koko liiketoiminnan jatkuvuuden suunnitteluprosessissa: Vaikutusanalyysi auttaa tunnistamaan ne kriittiset toiminnot, joista yrityksen pitää suoriutua pystyäkseen toimimaan. Deyn (2011) mukaan on tärkeää luokitella ja priorisoida liiketoiminnan aikakriittiset alueet ja toiminnot. Hilesin (2007) mukaan jokaiselle toiminnolle pitää määritellä pisin hyväksyttävä ajanjakso, jonka se voi olla keskeytyneenä (engl. maximum tolerable downtime, MTD; maximum tolerable period of downtime, MTPoD). Tammineedi (2010), BCM Glossary, (2010), PAS 56 (2003), BS 25999-1 (2006), ISF (2011) lisäävät vaikutusanalyysin avulla määriteltäviin aikamääreisiin toipumispistetavoitteen (engl. recovery point objective, RPO) ja toipumisaikatavoitteen (engl. recovery time objective, RTO). Toipumispistetavoite tarkoittaa sitä, miten usein tietojen varmuuskopiointi tehdään, eli kuinka paljon dataa on varaa menettää häiriön sattuessa. Toipumisaikatavoitteella tarkoitetaan järjestelmän palautumisaikaa häiriötilanteesta normaalitilaan (BCM Glossary 2010). Jokaiselle liiketoimintaprosessille tulee arvioida kriittisyystaso, joka juontuu liiketoimintaprosessin saavuttamattomuudesta ja toipumisprioriteetista häiriötilanteen sattuessa (Tammineedi, 2010).

Vaikutusanalyysin tuloksena voidaan paremmin hahmottaa keinoja riskien välttämiseen ja lieventämiseen (Cerullo & Cerullo, 2004). Vaikutusanalyysi on lähestymistapa, joka keskittyy enemmän toteutuneiden riskien vaikutuksiin, kuin siihen mikä sai aikaan tapahtuman toteutumisen (Tammineedi, 2010). Riskien arvioinnin jälkeen tulokset tarkastetaan johtotasolla ja varmistutaan kunkin riskin (vaikuttavuuden) tasosta, joka on organisaatiolle hyväksyttävää (Lam, 2002).

2.3.3 Kriisi-, häiriö-, onnettomuus- ja poikkeustilanteet

Kriisi-, häiriö-, onnettomuus- tai poikkeustilanne voidaan määritellä tilanteeksi, joka aiheuttaa odottamattomasti liiketoiminnan keskeytymisen hyväksymättömäksi ajaksi (Reynolds, 2010). Toisaalta häiriötilanteen ei tarvitse edes olla odottamaton, kuten BS 25999-1 (2006) mainitsee, kaikkiin riskeihin ei voida täydellisesti varautua, vaikka ne ennalta tunnistettaisiinkin. Tutkielman edetessä on hyvä muistaa, että realisoitumattomia kriisejä, häiriöitä, onnettomuus- ja poikkeustilanteita käsitellään yleisesti riskeinä. Kaikkiin riskeihin ei välttämättä edes haluta varautua, vaan se riippuu nimenomaisesti riskin vaikutustasosta.

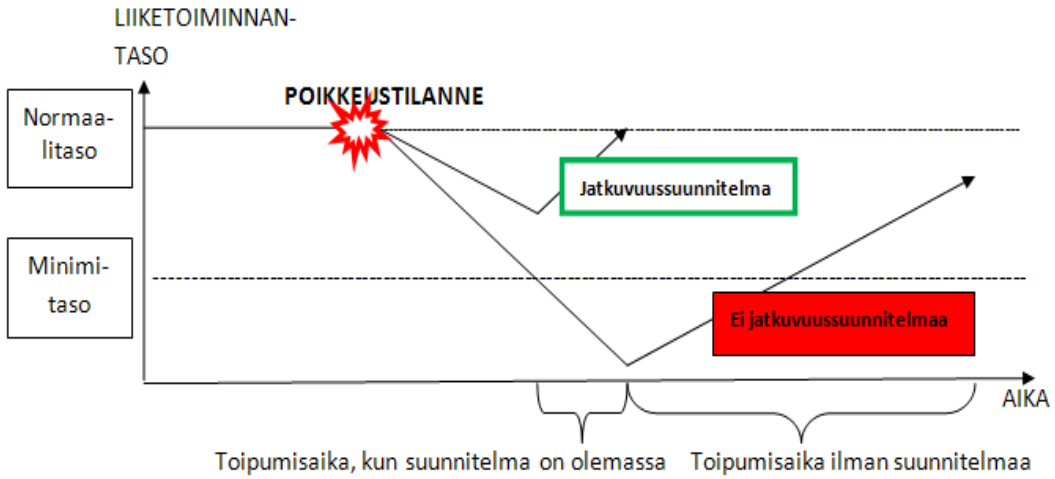
Vakavien ongelmien aiheutumiseen ei tarvita mitään maailmaa mullistavia sotia tai terrori-iskuja; jo pienet, jopa arkipäiväiset häiriöt, kuten tulipalot tai ihmisten huolimattomuus riittävät poikkeustilanteen aiheutumiseen (Ollikainen, 2009). Poikkeustilanteet voidaan jakaa kahteen pääkategoriaan: luonnon aiheuttamiin ja ihmisten aiheuttamiin poikkeustilanteisiin (La Fazia, 2004). Luonnonkatastrofeista liiketoiminnalle on aiheutunut ongelmia hurrikaanien, tulvien, maanjäristysten ja viimeisimpänä katastrofina tsunamien muodossa.

Suomea koskettavia luonnonkatastrofeja ovat lähinnä metsäpalot ja rajut myrskyt, jotka voivat aiheuttaa tuhoa sähköverkoille ja rakennuksille. Ihmisten aiheuttamiksi poikkeustilanteiksi Bocij, Greasley ja Hickie (2008) määrittelevät sabotaasin, varkaudet, vandalismin, hakkeroinnin, sekä virukset ja haittaohjelmat. ISO 27005 (2008) tietoturvan riskienhallinnan standardissa ihmisten aiheuttamat riskit jaetaan tahallisiin ja tahattomiin; standardissa mainitaan myös terrorismi, vieraan valtion tekemä vakoilu ja organisaation omien työntekijöiden tahallisesti tai tahattomasti aiheuttamat uhat. Reynolds (2008) listaa luonnon ja ihmisten aiheuttamien vahinkojen lisäksi lukuisia yksittäistapauksia. Reynolds (2008) viittaa tapauksilla tulipaloihin, sähkökatkoihin, avainhenkilöiden kuolemiin tai kommunikaatioyhteyksien katkeamiseen.

2.3.4 Jatkuvuussuunnittelun tavoite ja hyödyt

Etukäteen tehtävä varautumisen ja valmistautumisen suunnittelu auttaa organisaatiota selviämään toteutuneen riskin aiheuttamasta tilanteesta nopeammin pienemmin vahingoin, kuin ilman minkäänlaista ennakoivaa suunnittelua. Kun jatkuvuudensuunnitteluprosessi sisältäen vaikutusanalyysin on saatu päätökseen, voidaan suunnittelun pohjalta aloittaa jatkuvuussuunnitelman koostaminen (La Fazia, 2004). Cerullo ja Cerullo (2004) muistuttavat, että ei ole olemassa tiettyä valmista jatkuvuussuunnitelman rakennetta joka sopisi monen organisaation tarpeisiin, vaan jokaisen organisaation tulee työstää oma suunnitelmansa sen omaan tilanteeseen sopivaksi. ISO/PAS 22399 (2007) standardissa julkaistiin kuvio häiriöihin varautumisen ja toiminnan jatkuvuuden hallinnan (engl. Incident Preparedness and Operational Continuity Management, IPOCM) hyödyistä verrattuna varautumattomuuteen. Jatkuvuussuunnittelun hyötyä organisaatiolle voidaan kuvata samoin perustein. Tämä on kuvattu seuraavassa

kuviossa Suunnittelun ja suunnittelemattomuuden ero poikkeustilanteesta palauduttaessa (kuvio 1).



KUVIO 1 Suunnittelun ja suunnittelemattomuuden ero

Kuviosta 1 havaitaan, että toimivan jatkuvuussuunnitelman avulla häiriöstä palautuminen kohti normaalitilaa on nopeampaa ja häiriön aiheuttamat vaikutukset ovat pienempiä. Kuvio on toki vain esimerkki, eikä mitattuja lukuja toiminnan jatkuvuuden paremmuudesta ole esittää, on kuitenkin perusteltua olettaa, että näin asia on. Jatkuvuussuunnitelma on opas häiriötilanteisiin vastaamiseksi, niistä palautumiseksi ja toiminnan korjaamiseksi (Novoselnik, 2007), Australian National Audit Office (2000) lisää, että jatkuvuussuunnitelma on tarkoitettu käsittelemään niitä seurauksia, jotka ilmenevät riskien toteutuessa, kun ennaltaehkäisevät toiminnot pettävät.

Jatkuvuussuunnitelmien sisältö voi tietysti vaihdella suunniteltavan kohteen mukaan, mutta ISF (2011) antaa jokaiselle jatkuvuussuunnitelmalle tavoitteeksi olla liiketoimintalähtöinen, olla todellisia kriisitilanteita varten, roolitettu ja sen tulee olla jaettu kaikille sitä oikeassa tilanteessa tarvitseville henkilöille. Jatkuvuussuunnitelman tulee kattaa myös henkilöstön hyvinvoinnin tarpeet: Suunnitelmien tulee ottaa huomioon niiden ihmisten tarpeet, jotka suunnitelman toiminnot suorittavat (Sturdevant, 2011). Edelleen jatkuvuussuunnitelman tulee määritellä selkeästi palautettavat aktiviteetit, palvelut ja informaatio, myös aktiviteettien ja palveluiden aikarajat jossa ne tulee olla palautettuna normaalitilaan, sekä niiden keskinäinen normaalitilaan palauttamisjärjestys (ISF, 2011). Jatkuvuussuunnitelma on tulos jatkuvuussuunnittelusta (Savage, 2002), eikä se automaattisesti tuota organisaatiolle jatkuvuuden hallinnan osaamista ja kyvykkyyttä (PAS 56, 2003). Jatkuvuussuunnitelma edustaa kuitenkin tärkeää osaa jatkuvuuden hallinnan ohjelmassa, ja toimii vastineena tunnistetuille liiketoiminnan jatkuvuutta koetteleville tapahtumille (PAS 56, 2003).

2.3.5 Jatkuvuussuunnitelman keskeinen sisältö

Koska liiketoiminnan jatkuvuussuunnittelu on koko ajan käynnissä oleva prosessi (Kepenach, 2007), ja jatkuvuussuunnitelman menestyksellinen ylläpitäminen vaatii avaindokumenttien säilyttämistä (Savage, 2002). Kepenachin (2007) mukaan on tärkeää dokumentoida jatkuvuussuunnitelmaan kaikki kriittiset yhteystiedot, erityisesti hätänumerot ja vastuuhenkilöiden puhelinnumerot. Savagen (2002) tutkimuksen, Kepenachin (2007), ISF:n (2011) suositusten, ISO 27005 (2008) standardin, sekä PAS 56 (2003) ja BS 25999-1 (2006) standardien mukaisesti taulukkoon on kerätty organisaation jatkuvuussuunnitelman kannalta relevantti informaatio, joka tulisi suunnitelmaan sisällyttää (taulukko 1).

TAULUKKO 1 Jatkuvuussuunnitelmien suositeltu sisältö

Dokumentti	**Sisältö**
Jatkuvuussuunnitelman metatiedot	Ohjeet jatkuvuussuunnitelman käyttöönottoa varten, tarkat palautumistoimenpiteet aikamääreineen, tuki-informaatio, muut jatkuvuutta tukevat järjestelyt, jatkuvuussuunnitelmasta vastuussa olevat henkilöt ja viimeisimpien muutosten ajankohdat (testaus, ylläpito, harjoitukset)
Organisaatiokaavio	Nimet ja asemat organisaatiossa, vastuut ja roolit häiriötilanteissa, erityisesti vastuuhenkilöt hätätilanteessa
Yhteystiedot avainhenkilöille hätätilanteessa	Erityisesti toipumisryhmän puhelinnumerot; päätöksenteosta vastuussa olevat henkilöt, tärkeiden laitteistojen, ohjelmistojen ja järjestelmien käyttäjät ja niiden huoltohenkilöstö; liiketoimintasovellusten kehittäjät
Hätänumerot	Yleinen hätänumero, poliisin ja palokunnan numerot
Toimittaja- ja asiakasyritysten yhteystiedot	Puhelinnumerot, osoitteet, yhteyshenkilöt
Kartat ja pohjapiirrokset	Kartat ja pohjapiirrokset kaikista yrityksen toimitiloista
Teknisen infrastruktuurin kaaviot	Identiteetin- ja kulunvalvontajärjestelmät, spesifikaatio tärkeimmistä tietojärjestelmistä ja varmuuskopio- ja palautustoiminnoista; tiedot tärkeimmistä liiketoimintaprosesseja tukevista laitteistoista ja ohjelmistoista, tietoverkoista ja palvelimista; kaapeloinnista ja ilmastointilaitteista
Sopimukset	Kopiot ylläpito, vakuutus- ja palvelutasosopimuksista, toimittajaorganisaatioiden ja sidosryhmien tiedot, erityisesti asiakasorganisaatioiden tiedot

(jatkuu)

Taulukko 1 (jatkuu)

Pelastautumissuunnitelma	Evakuointisuunnitelma ja paloturvallisuusohjeet, logistiikka
Varatoimitilojen, järjestelmien ja palveluiden tiedot	Yksityiskohtaiset tiedot mahdollisista varatoimitiloista (koko, resurssit, infrastruktuuri), tiedot käytettävissä olevista palveluista ja järjestelmistä mukaan lukien ulkopuolisten osapuolten tarjoamat resurssit
Yrityksen omat säännökset ja resurssit	Tiedot toiminnan tavoitteista, suuntaviivoista ja normeista, henkilöstön hyvinvoinnin tarpeet, hätätilasta koituvat kulut
Viestintäpolitiikka	Toimintaohjeet sisäistä ja ulkoista viestintää varten, tarkat säännöt tiedottamiseen sidosryhmille, tiedotusvälineille ja medialle

ISF (2011) suosittaa jokaisen jatkuvuussuunnitelman arvioimista säännöllisesti yhteistyössä liiketoiminnan edustajien, IT-henkilöstön ja tietoturva-asiantuntijoiden kanssa. Liiketoiminnan edustajan tulee hyväksyä jatkuvuussuunnitelma ja se tulee testata säännöllisin väliajoin.

Jatkuvuussuunnitelmat on päivitettävä, jos liiketoimintaprosesseissa tapahtuu merkittäviä muutoksia, testattaessa havaitaan ongelmia tai myös silloin jos jatkuvuussuunnitelma joudutaan ottamaan käyttöön (ISF, 2011). Oikeassa kriisitilanteessa saadaan arvokasta informaatiota jatkuvuussuunnitelman edelleen kehittämistä varten, jota ei muuten testaus- tai arviointivaiheessa tulisi ilmi. Lamin (2002) mukaan jatkuvuussuunnitelmien uudelleenarviointiin ja päivittämiseen johtavia muutoksia organisaatiossa ovat myös tietojärjestelmien ja operaatioiden ulkoistaminen tai fyysinen uudelleensijoittaminen, muutokset IT-budjetissa, IT-infrastruktuurin kehittyminen (uudet ohjelmistot ja laitteet), sekä lakimuutokset ja merkittävät maailmanlaajuiset tapahtumat, kuten sodat ja terrori-iskut. Muutokset organisaatioiden toiminnassa ja toimintaympäristöissä tuottavatkin haasteet jatkuvuussuunnitelmien ajantasaisuudelle. Organisaatioiden toiminta ja palvelut eivät ole staattisia järjestelmiä, vaan dynaamisia, jotka ovat jatkuvassa muutoksessa kokoonpanonsa osalta (La Fazia, 2004). Jotta voidaan varmistua jatkuvuussuunnitelman ajantasaisuudesta, se on päivitettävä jokaisen muutoksen yhteydessä (La Fazia, 2004). Kaikkia muutoksia on harkittava ja arvioitava sen osalta, miten ne vaikuttavat jatkuvuussuunnitelmiin (ITIL v3, 2007).

2.4 Kriisinhallinta

PAS 56 (2003) standardin mukaan jatkuvuuden hallinnan ei tulisi rajoittua pelkästään informaatioteknologian toipumiseen. Shaw (2005) muistuttaa kriisinhallinnan ja jatkuvuuden hallinnan, sekä niiden tukitoimintojen integraation

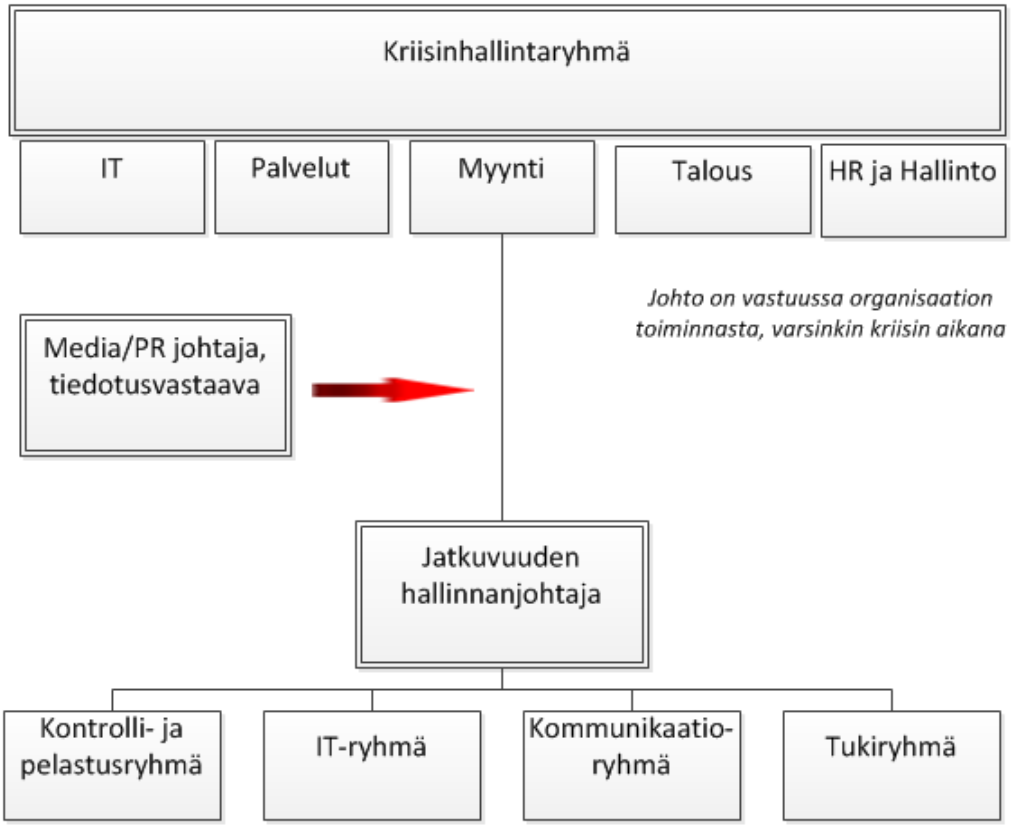
tärkeydestä koko organisaation liiketoimintojen hallinnassa. Kriisinhallintaa on käsitelty kirjallisuudessa myös sanoin hätätilan-, katastrofin- ja onnettomuuksienhallinta (NFPA, 2007). Jotta kriisejä kyettäisiin hallitsemaan, ensin täytyy määritellä, minkälainen tilanne kriisi oikein on. NFPA:n (2007) määritelmä kriisille, hätätilalle, katastrofille tai onnettomuudelle on seuraava: tapaus, joka uhkaa ihmishenkiä, omaisuutta, toimintaa tai ympäristöä. Tammineedi (2010) täsmentää kriisin olevan tapahtuma, joka uhkaa yksilön tai organisaation eheyttä, mainetta tai eloonjäämistä. Colemanin (2004) mukaan kriisi on tapaus, joka hallitsemattomasti laajenemalla aiheuttaa vahinkoa organisaation suorituskyvylle, omaisuudelle ja maineelle. Kriisinhallinta on prosessi, jolla organisaatio hallitsee onnettomuuksien laajempaa vaikutusta, kunnes onnettomuus on hallinnassa (PAS 56, 2003). Qayoumi (2002) määritteleekin kriisinhallinnan suunnitelman työkaluna organisaatioille resurssien koordinoimiseksi, jotta ihmishenkiä ja omaisuutta kyettäisiin suojelemaan heti onnettomuuden tapahduttua. Kriisit, onnettomuudet, häiriöt ja erilaiset poikkeustilanteet aiheuttavat aina vakavan riskin liiketoiminnan jatkuvuudelle.

Kriisit ovat paljon vakavampia tilanteita kuin tavalliset häiriöt ja poikkeustilanteet. Tehokkaan kriisinhallinnan ja liiketoiminnan jatkuvuuden saavuttaminen onnettomuus- tai katastrofitilanteessa vaatii vahvaa johtajuutta ja toiminnan koordinointia; organisaation kriisinhallinnan kyvykkyyden kriittisenä aspektina on kriisinhallintaryhmän osaaminen (PAS 56, 2003). Myös Hiles (2007), Reynolds (2008), Lam (2002), Savage (2002) ja Lindström, Samuelsson ja Hägerfors (2010) ovat yhtä mieltä siitä, että on järkevää perustaa kriisinhallintaryhmiä kriisin varalle. Schaafstalin, Johnstonin ja Randallin (2001) mukaan kriisinhallintaryhmän päämääränä on minimoida kriisin aiheuttamat negatiiviset vaikutukset; erilaisia kriisinhallintaryhmiä voi olla useita.

Organisaation suorituskyvystä, omaisuudesta ja henkilöstöstä on vastuussa ylin johto, heidän tukensa ja osallistumisensa on kriittisessä asemassa turvattaessa liiketoiminnan jatkuvuuden hallintaa (Tammineedi, 2010). Organisaation ylin johto toimii kriisitilanteessa kriisinhallintaryhmänä tuoden johtajuutta päätöksiin koskien jatkuvuussuunnitelmien käyttöönottoa, estäen vaurioita ja onnettomuutta laajenemasta ja turvaten organisaation kriittisten operaatioiden jatkuvuuden (Tammineedi, 2010). Suuremmissa kriiseissä kriisinhallintatiimeiltä vaaditaan nopeaa päätöksentekoa stressaavissa tilanteissa; tilanteet vaativat usein ei-rutiininomaista, monimutkaista ongelmien ratkaisutaitoa (Schaafstal, Johnstonin & Randall, 2001). Tammineedi (2010) jatkaa, että kriisinhallintaryhmän tavoitteena on koordinoida toimintojen palautumista kriisitilanteesta kohti normaalitilaa.

Kriisitilanteessa aiheutuu usein vahinkoa organisaatiolle eri muodoissa. Kriisinhallinnan tulee kattaa organisaation käyttämät toimitilat, ja sen tulee määritellä komentokeskus, jota se ensisijaisesti käyttää kriisitilanteen hallitsemiseen (BS 25999-1, 2006). Suuremmilla katastrofeilla on kapasiteettia tuhota myös fyysistä omaisuutta, kuten rakennuksia (Duncan ym., 2010). Vahinkojen laajuuden selvittämiseksi tarvitaan kontrolli- ja pelastusryhmä. Tämä ryhmä on ensimmäinen paikalle saapuva ryhmä, joka tekee tilannearvion jatkuvuuden

hallintajohtajalle (engl. business continuity manager) ja kriisinhallintaryhmälle (Tammineedi, 2010). Kontrolli- ja pelastusryhmän tehtävänä on siis selvittää aiheutuneet vahingot vielä tilanteen ollessa akuutti, pelastaa vielä pelastettavissa oleva laitteisto ja data (Tammineedi, 2010). Ryhmän vastuulla on tehdä ensimmäinen arvio siitä, milloin liiketoimintaa kyetään mahdollisesti jatkamaan normaalisti ja raportoida tilanteesta edelleen kriisinhallintaryhmälle (Hiles, 2007). Tammineedin (2010) mukaan voi olla myös tarpeellista perustaa omat ryhmät IT-infrastruktuurin ja kommunikaatioyhteyksien palauttamista varten, sekä tukiryhmä tilojen ja henkilöstöresurssien kartoittamista ja rahoituksen hankkimista varten. Tyypillinen organisaation kokoonpano ja rakenne on esitetty Tammineedin (2010) julkaisemassa kuviossa tyypillinen jatkuvuuden hallintaa tukeva kriisiorganisaatio (kuvio 2).



KUVIO 2 Tyypillinen jatkuvuuden hallintaa tukeva kriisiorganisaatio

Kuviosta on havaittavissa jatkuvuuden hallinnan liiketoimintalähtöisyys. Kuten moni muukin lähde, myös Tammineedin (2010) mukaan jatkuvuuden tulee olla liiketoimintalähtöistä; jatkuvuuden hallintaa edistävissä ryhmissä tulee olla henkilöitä, jotka tuntevat organisaation liiketoimintaa, prosesseja, teknologiaa ja myös organisaation toimintaan vaikuttavia riskejä.

Kun päivittäistä työtä tehdään asiakasyrityksille, on yleensä osoitettavissa kunkin projektin tai prosessin tärkeimmät henkilöt, joita voi olla joko yksi tai

useita. Avainhenkilöiden pidempiaikaiset sairastumiset tai jopa kuolemat voivat aiheuttaa ongelman kyseisen projektin etenemiselle, ja sitä kautta koko liiketoimintaprosessin jatkuvuudelle. Jatkuvuuden hallinnan kautta on varauduttava tilanteeseen, jossa henkilö, tai pahemmassa tapauksessa useita henkilöitä ei ole käytettävissä. Tilannetta, jossa monia työntekijöitä on poissa, voidaan kutsua jo kriisiksi. Yhtenä huomioitavana asiana kriisinhallinnassa on siis henkilöstöresurssit. Reynoldsin (2008) mukaan henkilöitä avaintehtäviin tulee kouluttaa enemmän, kuin on tarpeellista. Samasta syystä henkilöiden kouluttaminen toistensa työtehtäviin ainakin osittain on Reynoldsin (2008) mukaan suositeltavaa.

Kriisiviestintä on kriisinhallinnan tukitoiminto. Kriisiviestinnän tehtävänä on organisaation maineen suojeleminen ja puolustaminen julkisuuden tuottamalta haasteelta (BCM Glossary, 2010). Kommunikaation organisaation sisällä ja sisältä ulos on säilyttävä, jos kriisitilanteesta aiotaan selvitä (Duncan ym., 2010). Organisaation toimintojen maantieteellinen hajautuminen aiheuttaa kasvavaa painetta kommunikaation toimivuudelle. Kepenach (2007) näkee yhtenä suurimpana uhkana luonnonkatastrofien sattuessa kommunikaatioyhteyksien katkeamisen. Yhtälailla verkkoyhteyksien katkeaminen vaikkapa sähkökatkon takia aiheuttaa yrityksen viestinnälle suuria ongelmia. Duncanin ym. (2010) mukaan luotettavimpia kommunikaatiomuotoja onkin yllättäen tavallinen paperille kirjoittaminen; elektroninen kommunikaatio on hyvin sähköverkkojen toiminnasta riippuvaista, ja verbaalisen kommunikaation luotettavuus kärsii huhuista ja muista epäluotettavista viesteistä.

Liiketoiminnasta onkin tullut yhä liikkuvampaa ja paikasta riippumatonta; yhä vähemmän toimitaan kasvokkain asiakasyrityksen edustajan kanssa, vaan tietojärjestelmiä hyödynnetään viestinnän välineenä niin sähköpostissa, videokonferensseissa, Voice Over IP -puheluissa ja pikaviestimissä. Lamin (2002) mukaan yhteyttä sidosryhmiin pitää asiakasvastaava, jonka tulee kommunikoida asiakkaiden kanssa pitäen heidät informoituna tilanteen kehittymisestä. PR-toiminnot ovat niin kriittisiä (organisaation maineelle) kriisitilanteessa, että julkisena tiedottajana voi toimia vain journalistiikka-alan kokemusta omaava henkilö, muita työntekijöitä tulee ohjeistaa olla puhumatta kriisitilanteesta julkisuuteen tai muille ulkopuolisille tahoille kriisitilanteessa (Tammineedi, 2010). BS 25999-1 (2006) pitää organisaation tiedottamista medialle erityisen kriittisenä tehtävänä kriisitilanteessa: kriisinhallinnan suunnitelmissa tulee määritellä organisaation käyttämä tiedotuskanava (lähdekirjallisuudessa puhutaan mediarajapinnasta), sekä luonnostella julkilausuma kriisitilanteesta. Benoit (1997) täsmentää, että organisaation tulee tunnistaa yleisönsä: organisaatiot voivat viestiä osakkeenomistajilleen, työntekijöilleen, paikallisille asukkaille, poliitikoille tai viranomaisille - jokaisella yleisöllä on erilaiset edut, tavoitteet ja huolet.

2.5 Toipumissuunnittelu

Toipumissuunnittelu on nimensä mukaisesti häiriötilanteista normaalitilaan palautumiseen tähtäävää toimintaa. Kirjallisuudessa on yleisesti vallalla käsitys,

että toipumissuunnittelulla ja toipumissuunnitelmalla on enemmän tekninen aspekti jatkuvuuden hallinnassa. Esimerkiksi Dey (2011) määrittelee toipumissuunnittelun olevan informaatioteknologian palveluiden palauttamista ja enimmäkseen luonteeltaan teknistä toimintaa. ITIL v3 (2007) suosittaa IT-palveluiden toipumissuunnitelmien tukevan liiketoiminnan jatkuvuussuunnitelmia ja toisin päin, jatkuvuuden hallinnan ja liiketoiminnan jatkuvuussuunnitelmien tulisi edistää IT-palveluiden toipumissuunnittelua. Toipumissuunnittelun ja -suunnitelman tarkoituksena on yksityiskohtaisesti määritellä toimenpiteet liiketoimintaoperaatioiden palauttamiseksi ennalta suunnitellulle suoritustasolle annettujen aikamääreiden puitteissa (Winkler ym, 2010).

Toipumissuunnittelu eroaa jatkuvuussuunnittelusta siinä, että se on reaktiivista toimintaa, vaikka suunnittelua tehdäänkin etukäteen: käytännön toimenpiteet käynnistyvät vasta ongelmien ilmettyä, toisin kuin jatkuvuussuunnittelu pyrkii vaikuttamaan riskeihin ennen niiden toteutumista (Cerullo & Cerullo, 2004). Savagen (2002) ja La Fazian (2004) artikkeleissa muistutetaan useampaan kertaan, että jatkuvuussuunnittelulla ja toipumissuunnittelulla on eronsa. La Fazia (2004) muistuttaa, että ensimmäinen askel kohti parempaa (jatkuvuuden hallinnan) suunnitelmallisuutta on vaihtaa ajattelutapaa toipumissuunnittelusta liiketoiminnan jatkuvuuteen. Ilmeisesti aikaisemmin jatkuvuuden käsite on ollut enemmän sidoksissa tekniikkaan ja tietojärjestelmien toimivuuteen ja toipumisen parantamiseen, kuin ennaltaehkäisevään ja proaktiiviseen toimintaan. Joka tapauksessa Savagen (2002) mukaan IT-infrastruktuurilla on oma, tärkeä paikkansa jatkuvuussuunnittelussa laaja-alaisuutensa vuoksi. Herbanen, Elliotin ja Swartzin (2004) mielestä tieto- ja viestintäteknologialla on kasvava asema liiketoiminnan jatkuvuuden hallinnassa. Toipumissuunnittelu varmistaa, että IT-palvelujen toipumisjärjestelyt ovat linjassa liiketoiminnan vaatimusten kanssa (ITIL v3, 2007).

Toipumissuunnitteluun liittyy myös työpisteiden toipuminen (engl. work area recovery, WAR). Tällä tarkoitetaan sisäisiä ja ulkoisia erikseen määriteltyjä työpisteitä, joiden tarkoituksena on tarjota kaikkein välttämättömin laitteisto ja palvelut liiketoiminnan toipumista tukevien ryhmien tarpeita varten lyhyellä varoitusajalla (PAS 56, 2003). Varatoimitilasta on tarkoitus ylläpitää toimintaa kun ensisijaiset toimitilat eivät ole käytettävissä (BCM Glossary, 2010). Tavoitteena on siis turvata työn jatkuminen poikkeustilanteesta huolimatta. PAS 56 (2003) muistuttaa, että tällainen työpiste tulisi sijoittaa niin, ettei sama häiriö pääse vaikuttamaan normaalien työpisteiden myös varatilojen toimintaan. Kirjallisuudessa on usein esitetty varatoimitilojen jako kolmeen kategoriaan niiden varustelutason mukaisesti: kylmät-, lämpimät- ja kuumat toimitilat (engl. cold site, warm site, hot site). Peterson (2009) ja Savage (2002) toteavat kuuman toimitilan kaikkein käytännöllisimmäksi vaihtoehdoksi työn jatkamiselle. Savage (2002) huomauttaa ko. järjestelyiden olevan hyvin kalliita toteuttaa ja ylläpitää. Usein paremmaksi keinoksi osoittautuukin jo olemassa olevien toimitilojen kartoittaminen, jolloin kaikkein kriittisimmät toiminnot voidaan sijoittaa vähemmän kriittisten toimintojen käyttämiin tiloihin (Savage, 2002). Tämän vaihtoeh-

don lisäksi Peterson (2009) tuo esiin työntekijöiden omien asuntojen hyödyntämisen, jonka hän näkee yllättäen jopa kaikkein suosituimpana vaihtoehtona.

2.6 Jatkuvuuden hallinnan elementtien suhteet

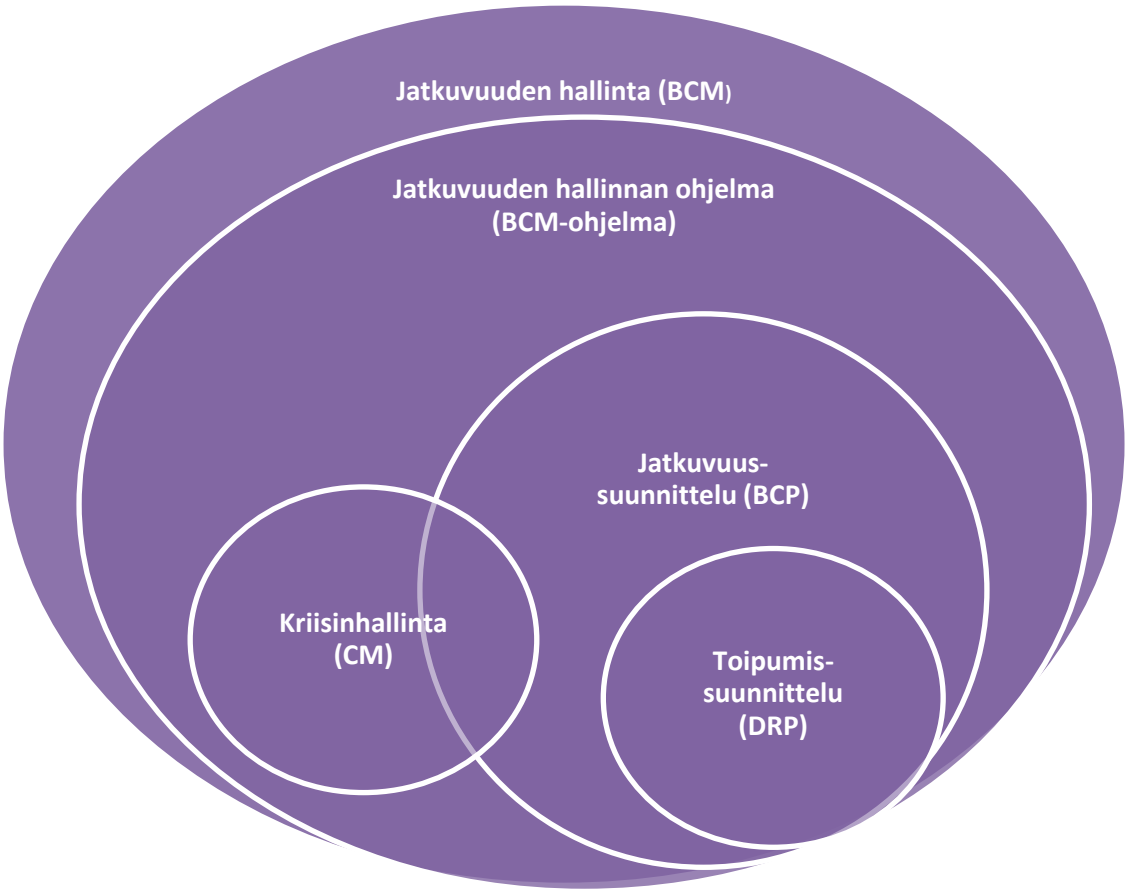
Edellä käsiteltiin jatkuvuuden hallinnan osa-alueita eli elementtejä. Kohteena olivat jatkuvuuden hallinnan yleiset piirteet, jatkuvuuden hallinnan ohjelma organisaatiossa, jatkuvuussuunnittelu, kriisinhallinta ja lopuksi toipumissuunnittelu. Täsmennän nyt taulukon ja kuvion avulla jatkuvuuden hallinnan elementtien tavoitteita ja niiden välisiä suhteita. Kirjallisuudessa jatkuvuuden hallinnalle ja sen eri osille määriteltyjen tavoitteiden mukaisesti seuraavaan taulukkoon on koottuna jatkuvuuden hallinnan osa-alueiden tavoitteet ja soveltamisalueet (taulukko 2).

TAULUKKO 2 Jatkuvuuden hallinnan elementtien soveltamisalueet

Kohde	**Tyyppi ja tavoite**	**Soveltamisalue**
Jatkuvuuden hallinta	Liiketoimintalähtöinen strategia, jonka tavoitteena on liiketoiminnan jatkuvuuden varmistaminen aiheutuvista ongelmista riippumatta	Organisaation johtotaso, ylin johto
Jatkuvuuden hallinnan ohjelma	Prosessi, jonka tavoitteena on strategiassa määriteltyjen tavoitteiden täyttäminen ja organisaation häiriönsietokyvyn kasvattaminen	Jatkuvuuden hallinnan läpiviennistä vastuulliset henkilöt ja operaatiot
Jatkuvuussuunnittelu ja -suunnitelma	Ennaltaehkäisyn ja varautumisen suunnittelu, organisaation toimiminen häiriötilanteessa	Kriittiset liiketoimintaprosessit ja funktiot
Kriisinhallinta	Katastrofit, merkittävät ongelmat ja vakavat poikkeustilanteet, organisaation toiminnan määrittely kriisitilanteessa	Ensisijaisesti kriittiset liiketoiminnot ja ydinprosessit
Toipumissuunnittelu ja -suunnitelma	Teknologian toipumissuunnittelu, teknisten osien palauttaminen häiriötilanteesta normaalitilaan	Laitteet, järjestelmät, sovellukset ja tietoverkot

Yhtenä osa-alueena jatkuvuuden hallinnan ohjelmassa oli riskeihin reagointi, eli vastatoimien kehittäminen, joita olivat jatkuvuus- ja toipumissuunnitelmat. Lisäksi käsiteltiin kriisinhallinnan ja jatkuvuuden hallinnan integraatiota organisaation liiketoimintojen hallinnassa. Herbanen, Elliotin ja Swartzin (2004) mukaan kriisinhallinnan alalla teorian painopiste on strategisessa roolissa sietää ja

palautua kriiseistä. Kriisinhallintaa voidaan pitää jatkuvuuden hallinnan juurina, koska ne muodostavat samoja ydinolettamuksia (Herbane, Elliot & Swartz, 2004). Huomion arvoista on se, että kaikki jatkuvuuden hallinnan elementit ovat koko ajan käynnissä olevia prosesseja, mutta jatkuvuussuunnittelulla, kriisinhallinnalla ja toipumissuunnittelulla on omat ajalliset riippuvuutensa: Siinä missä jatkuvuussuunnittelu ja kriisinhallinta ovat ennaltaehkäisevää ja varautuvaa toimintaa, toipumissuunnittelu kattaa vain kriisin jälkeiset palautumistoiminnot: toipumissuunnittelun lähestymistapa on vahvasti kriisin jälkeiseen toipumiseen painottuva (Herbane, Elliot & Swartz, 2004) Seuraavassa kuviossa selkiytetään jatkuvuuden hallinnan (BCM), jatkuvuussuunnittelun (BCP), kriisinhallinnan (CM) ja toipumissuunnittelun (DRP) välisiä suhteita (kuvio 3):



KUVIO 3 Jatkuvuuden hallinnan elementtien väliset suhteet

Kuviosta 3 voidaan todeta jatkuvuuden hallinnan laaja-alaisuus. Toipumissuunnittelu sisältyy jatkuvuussuunnitteluun muun muassa teknisyytensä vuoksi: tarkka spesifikaatio käytetyistä järjestelmistä ja verkoista topologioineen auttaa organisaatiota jäsentämään kriittiset toiminnallisuudet (Savage, 2002). Toipumissuunnittelu on perinteisesti painottunut informaatioteknologi-

aan, kriisinhallinta on taas ollut enemmän sukua jatkuvuuden hallinnalle, koska niissä molemmissa otetaan huomion vaiheet jo ennen kriisien ilmenemistä (Herbane, Elliot & Swartz, 2004). Jatkuvuuden hallinnan elementeistä jatkuvuussuunnittelu ja kriisinhallinta ovat lähimpänä varautumista riskeihin. Ennakkovarautuminen ja jatkuvuusjärjestelyt tähtäävät siis organisationaalisen häiriönsietokyvyn kasvattamiseen.

2.6.1 Häiriönsietokyvyn arviointi ja mittaaminen

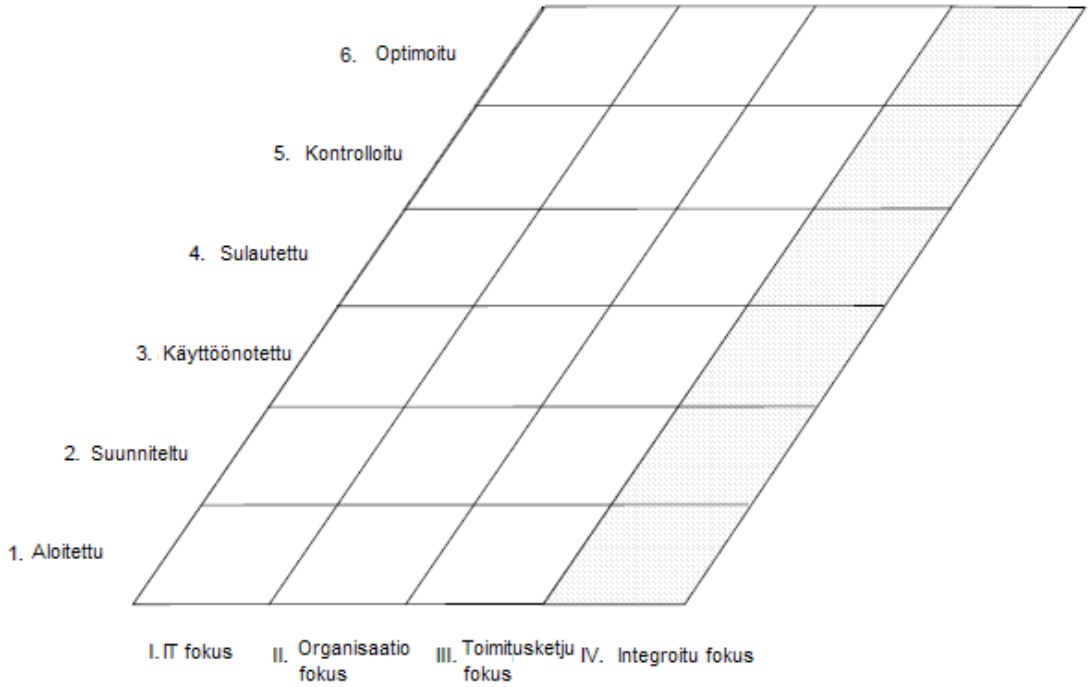
Kirjallisuudessa on esitetty muutamia malleja häiriönsietokyvyn tason mallintamiseen ja mittaamiseen. Helms, van Oorschot, Herweijer ja Plas (2006) esittivät mallin jatkuvien liiketoimintaoperaatioiden riskinsietokyvyn mittaamiseen, joka yhdistää heidän mukaansa jatkuvuutta koskevat riskialueet aikaisempaa tutkimusta paremmin. Riskikartta jaettiin kolmeen riskialueeseen, jonka avulla organisaatiot voivat tunnistaa heille parhaiten sopivan jatkuvuuden hallinnan strategian. IBM (2003) esitti julkaisussaan häiriönsietokykyisen liiketoiminnan ja infrastruktuurin analyysin, jossa esitettiin kolmen vaiheen avulla organisationaalisen häiriönsietokyvyn kasvattaminen. IBM:n julkaisussa keskityttiin sietokyvyn kuuteen kerrokseen: strategiaan, organisaatioon, prosesseihin, teknologiaan, fasiliteetteihin ja turvallisuuteen. Bhamidipaty, Lotlikar ja Banavar (2007) julkaisivat mallin, jossa IT-palveluorganisaatioiden sietokyvyn kypsyyttä arvioitiin hyvin samankaltaisesti kuin IBM:n vuonna 2003 julkaisemassa tutkimuksessa. Bhamidipatyn, Lotlikarin ja Banavarin (2007) julkaisussa keskiössä olivat fasiliteetit, teknologia, sovellukset ja data, prosessit ja ihmiset, jotka jaettiin vielä alakohtiin hierarkian muodostamiseksi. Sietokykyä arvioitiin viidellä tasolla, joiden avulla organisaation eri osille ja toiminnoille laskettiin sietokykyindeksi. Häiriönsietokyvyn tason määrittäminen auttaa organisaatiota selvittämään oman varautuneisuutensa tason. Esimerkiksi sietokykyindeksi kuvaa organisaation tiettyjen resurssien kyvyn sietää häiriöitä. Tämä on hyödyllistä jatkuvuuden hallinnan kannalta, koska hyvän häiriönsietokyvyn avulla organisaatio voi välttää riskien toteutumisesta aiheutuvia vahinkoja, erityisesti kustannuksia, koska jatkuvuus- ja toipumissuunnitelmia ei välttämättä tarvitse ottaa käyttöön.

2.6.2 Jatkuvuuden hallinnan kypsyyden ja kyvykkyyden arviointi

Lähdekirjallisuudessa on esitetty ainakin kaksi erilaista mallia organisaation jatkuvuuden hallinnan kypsyyden ja kyvykkyyden arviointiin. Ensimmäinen malli on Virtual Corporationin (2003) luoma malli, jossa organisaation kypsyyttä jatkuvuuden hallitsemisessa verrataan juoksemisessa kehittyvään ihmiseen. Malli on kuusitasoinen, jossa tärkeimmät kyvykkyydet, kuten johtajuus ja jatkuvuuden hallinnan ohjelman rakenne on määritelty kyvykkyyksiltään erittäin alhaisesta korkeaan. Mallin ongelma on siinä, että se ei ota tarpeeksi huomioon jatkuvuuden hallinnan jatkuvaa kehittämistä, eikä ulkoisia sidosryhmiä. Erityi-

sesti kilpailija- ja asiakasnäkökulma ovat puutteellisia. Mallin näkökulma onkin enemmän organisaation sisäisessä jatkuvuuden hallinnan kehittämisessä.

Toinen malli on Smitin (2005) kehittämä jatkuvuuden hallinnan kuusivaiheinen kypsyysmalli, jossa mikä tahansa organisaatio voi arvioida jatkuvuuden hallinnan kypsyyttään neljästä eri näkökulmasta. Näkökulmat ovat IT-fasiliteetti-, organisaatio-, sisäinen toimitusketju- ja integrointi-näkökulma. Erona Virtual Corporationin (2003) malliin, Smitin (2005) mallissa toiminnan jatkuva kehittäminen on huomioitu tasolla kuusi. Mallin ulkoinen näkökulma on tässäkin puutteellinen; toiminta keskittyy organisaation sisäisen kypsyyden parantamiseen. Smitin (2005) luoma jatkuvuuden hallinnan kypsyysmalli on esitetty seuraavassa kuviossa (kuvio 4).



KUVIO 4 Jatkuvuuden hallinnan kypsyysmalli

Smitin (2005) mallissa jatkuvuuden hallinnan prosessien laatu kehittyy pystyakselilla ja näkökulma vaihtuu vaaka-akselilla. Jatkuvuuden hallinnan kypsyyttä ei siis pyritä kokonaisvaltaisesti kuvaamaan, vaan se on jaettu osiin näkökulmien mukaisesti. Jatkuvuuden hallinnan kypsyyttä ja kehittyneisyyttä kuvaava malli, joka ottaisi paremmin huomioon organisaation sidosryhmät ja jatkuvuuden hallinnan jatkuvan etenemisen eli prosessiluontoisuuden on vielä kehittämättä. Tämän tutkimuksen tieteellinen tavoite on mallintaa jatkuvuuden hallinnan kehittyminen organisaatiossa palvelukeskeisesti, asiakkaat huomioiden. Tähän tavoitteeseen ja sen saavuttamiseen palataan myöhemmin tutkielmassa.

3 IT-PALVELULIIKETOIMINNAN JATKUVUUDEN HALLINTA

Tässä luvussa käsitellään jatkuvuuden hallintaa erityisesti IT-palvelutoimittajan näkökulmasta. Ensimmäisenä käydään läpi IT-palveluyrityksen toimintaympäristöä ja palveluliiketoiminnan erityispiirteitä. Seuraavana käsitellään tietokonekeskuksia, eli missä asiakkaille tarjottavia konesalipalveluita tuotetaan ja ylläpidetään. Lopuksi tehdään katsaus asiakassuhteisiin IT-palveluliiketoiminnan ja jatkuvuuden hallinnan kontekstissa.

3.1 IT-palveluyrityksen toimintaympäristö ja IT-palveluliiketoiminnan erityispiirteet

IT-palveluyrityksen liiketoimintamalliin kuuluvat asiakasyrityksille toimitettavat palvelut. Palvelujen toimittaminen edellyttää palveluliiketoiminnan hallitsemista, edelleen palveluliiketoiminnan hallitseminen ja johtaminen vaatii palvelujen tuottamisen osaamista ja hallintaa. Liiketoimintaprosessit ovat erityisen tärkeitä palvelujenhallinnan näkökulmasta: liiketoimintaprosessit käyttävät organisaation tietämystä ja kokemusta mahdollistaessaan tavoiteltujen tulosten saavuttamisen (ITIL v3, 2007). Palvelujenhallinta on joukko organisaation valmiuksia tuottaa arvoa asiakkailleen palvelujen muodossa (ITIL v3, 2007). Valmiudet ovat toimintoja ja prosesseja, joilla hallitaan tuotettuja palveluja niiden elinkaaren läpi (ITIL v3, 2007).

Palveluilla on tiettyjä erityisominaisuuksia verrattuna fyysisiin tuotteisiin. Kotler ja Armstrong (1999) kuvaavat palvelun olevan asiakkaalle tarjottava toiminto tai hyöty, joka on aineeton ja ei johda omistusoikeuteen. Grönroos (2009) lisää palvelun ominaisuuksiin prosessiluontoisuuden, ja että palveluja tuotetaan ja kulutetaan samanaikaisesti. Turnerin (1994) tukee tätä näkemystä todetessaan, että palvelua ei voida etukäteen tarkastaa, sitä ei voida säilyttää, jälleenmyydä tai palauttaa. Palvelun tuottaminen tarkoittaa erittäin läheistä suhdetta tuottajan ja kuluttajan välillä: puskuria IT-palveluyrityksen asiakasra-

japinnan ja asiakkaiden välillä on vähän tai ei ollenkaan (ITIL v3, 2007). Lämsän ja Uusitalon (2002) mukaan jo 2000-luvun alussa organisaatioiden strategioissa on ollut havaittavissa yhä enemmän omaan ydinliiketoimintaan keskittymistä, jolloin muut palvelut ostetaan toisaalta. Kovinkaan monella yrityksellä ei ole resursseja tai välttämättä edes halua ylläpitää omaa IT-infrastruktuuriaan. IT-palveluyritys tuottaa esimerkiksi konesaliensa kautta palveluja asiakasyritysten IT-infrastruktuurin hallitsemiseen. Tieto Oyj (2012a) listaa IT-infrastruktuurin ulkoistamisratkaisujen eduiksi oikean osaamisen ja sen säilyttämisen, teknologian ajantasaisuuden, hallinnan helpottumisen sekä hallintakustannusten alenemisen.

On tyypillistä, että palvelut toistetaan asiakkaalta seuraavalle, mutta muokataan kunkin asiakkaan omien odotuksien ja vaatimusten mukaisesti (Turner, 1994). Palvelun tarkoituksenmukaisuudesta tulee sopia erikseen määriteltävässä sopimuksessa, tällöin asiakkaan haluama palvelutaso määritellään erikseen osana palvelutasosopimusta. Palvelutaso ilmaisee palvelun muodon lopullisin ja mitattavin ehdoin (ITIL v3, 2007). Tarkat ehdot määritellään palvelutasosopimuksessa (engl. service level agreement, SLA). Palvelutasosopimus on palvelun tuottajan ja palvelun käyttäjän välinen sopimus, jossa määritellään tuotettavan palvelun luonne, laatu, saatavuus ja tarkoitus (BCM Glossary, 2010). Mitattavuus palvelutasosopimuksessa voidaan toteuttaa suorituskykymittareiden (engl. key performance indicator, KPI) avulla. Suorituskykymittarit mahdollistavat koko palvelun toimittamisen arvioinnin sekä liiketoiminnan, että IT:n edustajien tahoilta (BCM Glossary, 2010).

IT-palveluliiketoiminnassa konesalipalveluiden näkökulmasta jatkuvuus tarkoittaa sitä, että häiriöistä ja poikkeustilanteista huolimatta palvelu jatkaa toimintaansa tukien liiketoimintaa. Palveluntarjoaja sitoutuu ylläpitämään palvelun voimavaroja, jotka takaavat riittävät varautumis- ja toipumistasot (ITIL v3, 2007). Erilaiset järjestelmät ja prosessit huolehtivat, ettei asiakkaan vastaanottaman palvelun taso laske alle ennalta määriteltyjen rajojen alle ja sovittu palvelutaso toteutuu. Sitoutuminen palvelutasoon sisältää myös palvelun normaaliuden palauttamisen ennalta määriteltyjen aikamääreiden mukaisesti, jotta vian tai tapahtuman kokonaisvaikutusta voidaan rajoittaa. Jatkuvuus varmistetaan ensisijaisesti päällekkäisten, moninkertaisten rakenteiden ja resurssien kautta (ITIL v3, 2007). Wan ja Chan (2008) täsmentävät IT-palveluiden jatkuvuuden hallinnan olevan keskittyvän organisaation kykyyn jatkaa ennalta sovitun tasoisten IT-palvelujen tarjoamista, vähintään häiriön jälkeisien liiketoiminnan (minimi)vaatimusten mukaisesti.

ITIL v3:n (2007) huomauttaa, että juuri palvelun aineettomuus tekee saavutettavuudesta (engl. availability) tärkeimmän palvelun laatua mittaavan ja edustavan tekijän, se on ilmeisempi kuin palvelun kapasiteetti, jatkuvuus ja turvallisuus. Ei ole olemassa ainoastaan tilanteita, jolloin IT-palvelut ovat tai eivät ole käytettävissä, vaan on myös tilanteita jolloin palvelu on saavutettavissa, mutta huonolaatuisena (Wan & Chan, 2008). Palvelun käyttäjät kokevat kapasiteetin, jatkuvuuden ja turvallisuuden vaikutukset juuri saavutettavuuden kautta (ITIL v3, 2007).

3.2 Tietokonekeskus: häiriöitä sietävä IT-infrastruktuuri

Tieto Oyj (2012b) huomauttaa käyttöpalvelujen olevan erittäin laajoja kokonaisuuksia, jotka muodostuvat useiden osapuolten vastuulla olevista komponenteista. Komponentteja ovat esimerkiksi kytkimet, kaapelit, levyjärjestelmät, sekä verkko- ja tietoliikennekomponentit. Fyysisesti käyttöpalveluja tuotetaan tietokonekeskuksissa (engl. data center). Käyttöpalveluiden toimivuus on erittäin tärkeää: Wiboonratin (2008) mukaan Gartner Dataquestin (2007) julkaisemassa tutkimuksessa mainittiin yhden tunnin katkon maksavan pankkiiriliikkeille jopa 6,45 miljoonaa dollaria ja luottokorttimyynti vielä 2,6 miljoonaa dollaria lisää. Wiboonrat (2008) lisää, että aineellisten vahinkojen lisäksi myös aineettomat vahingot voivat olla tuhoisia: asiakkaiden tyytymättömyys, kolhut brändiin ja mahdollisuudet liiketoiminnalle tulevaisuudessa voivat heiketä. Tätä näkökulmaa tukee myös Harvard Research Groupin (2004) tutkimus, jonka mukaan häiriöiden todelliset kustannukset ulottuvat paljon pidemmälle kuin perinteiseen käyttäjäyhteisöön. Pattersonin (2002) mukaan myös (palveluja tuottavan) organisaation sisällä kärsitään luottamuksen ja tuottavuuden laskusta säännöllisten katkojen ilmetessä. Häiriöttömyyden varmistaminen on tärkeää erityisesti IT-palveluliiketoiminnassa, kun ollaan samanaikaisesti vastuussa usean asiakkaan liiketoiminnasta ylläpidettävien järjestelmien kautta. Tietokonekeskusten luotettavuutta voidaan parantaa kriittisten komponenttien redundanssia lisäämällä (Wiboonrat (2008).

3.2.1 Tietokonekeskusten tasoluokitus

Amerikan standardointi-instituutin ANSI:n (American National Standards Institution) valtuuttama telekommunikaatioalan yhdistys TIA (Telecommunications Industry Association) julkaisi vuonna 2005 tietokonekeskusten tasoluokituksen (engl. tier classification), johon alalla yleisesti luotetaan (Arno ym., 2010). Luokituksessa on neljä tasoa; luotettavuustaso nousee asteittain tasolta 1 kohti tasoa 4. Palvelun luotettavuus eli sen saavutettavuus on pitkänajan keskiarvo, joka kuvaa palvelun (esimerkiksi sähkönsyötön) toimivuutta ja suorituskykyä tyydyttävällä tasolla. Tunnin katko vuodessa tarkoittaisi 99,9886 % saavutettavuutta ja esimerkiksi 99,999 % saavutettavuus tarkoittaisi 5,3 minuutin katkoa vuosittain (Arno ym., 2010). Uptime Instituten (2009; 2001) luomassa ja myös Arnon ym. (2010) hieman suppeammin esittämässä taulukossa esitetään tietokonekeskusten tasoluokitusten pääpiirteet (taulukko 3).

TAULUKKO 3 Tietokonekeskusten tasoluokitusten ominaisuudet

Ominaisuus	Tier I	Tier II	Tier III	Tier IV
Päällekkäiset komponentit	N	N+1	N+1	2(N+1)
Jakelutiet	1	1	1 aktiivinen+ 1 vaihtoehtoinen	2 aktiivista
Rinnakkainen ylläpidettävyys	Ei	Ei	Kyllä	Kyllä
Jaoteltavuus	Ei	Ei	Ei	Kyllä
Saavutettavuus	99,671 %	99,749 %	99,982 %	99,995 %
Keskimääräinen vuosittainen katko	28,8 tuntia	22 tuntia	1,6 tuntia	0,4 tuntia

Päällekkäisillä komponenteilla tarkoitetaan mm. generaattoreiden ja UPS moduuleiden lukumäärää, jotka kantavat sähkönsyötön kuormaa (Arno ym., 2010), tai jäähdytysjärjestelmää (Uptime Institute, 2009). N tarkoittaa siis useasta komponentista koostuvaa kokonaisuutta, joka tuottaa tietokonekeskuksen tarvitseman virran (tai jäähdytyksen). N+1 tarkoittaa taas N:n lisäksi yhtä päällekkäistä (varalla olevaa) komponenttia, eli yhteensä kahta komponenttia, jotka tuottavat tarvittavan virran. 2(N+1) tarkoittaa, että tietokonekeskuksessa on kahden erillisen järjestelmän lisäksi kaksi päällekkäistä varajärjestelmää (Arno ym., 2010). Jakelutiet ovat virran ja jäähdytyksen jakeluun tarkoitettuja kanavia, jotka ovat siis tason 3 ja 4 tietokonekeskuksissa kahdennettuja (Uptime Institute, 2009). Rinnakkaisella ylläpidettävyydellä tarkoitetaan sitä, että kaikki tarvittavat huoltotyöt voidaan suorittaa ilman keskeytyksiä (Arno ym., 2010).

Uptime Institute (2009) määrittelee tason 4 tietokonekeskuksen yhdeksi tärkeäksi ominaisuudeksi jaoteltavuuden: kahdennetut järjestelmät ja jakelutiet tulee voida fyysisesti eristää toisistaan, jottei yksittäinen tapahtuma pysty yhtä aikaa vaikuttamaan molempiin järjestelmiin ja jakeluteihin. Muun muassa jaoteltavuuteen liittyen Arno ym. (2010) tuovat esiin palvelujen saavutettavuuteen liittyvän tärkeän käsitteen yksittäinen vikaantumispiste (engl. single point of failure, SPOF), joka tarkoittaa yhden komponentin vikaantumisen aiheuttavan koko järjestelmän toiminnan estymisen. Ensimmäinen askel luotettavuustason parantamiseen onkin yksittäisten vikaantumispisteiden eliminointi. Tasoluokitus tuottaa suuntaviivat ja asteikon tietokonekeskusten suunnitteluun (Arno ym., 2010). IBM (2011) on julkaissut tietoa myös tasojen 5 ja 6 tietokonekeskuksista. Käytännössä se tarkoittaa sitä, että kaksi tai useampi tason 3 tai tason 4 tietokonekeskusta toimii yhteistyössä antaen lisäturvaa jatkuvuudelle. IBM (2011) mainitsee näin korkeatasoisten ratkaisujen varjopuoleksi niiden korkean hinnan ja sovellusten on pystyttävä kirjoittamaan samanaikaisesti dataa paikal-

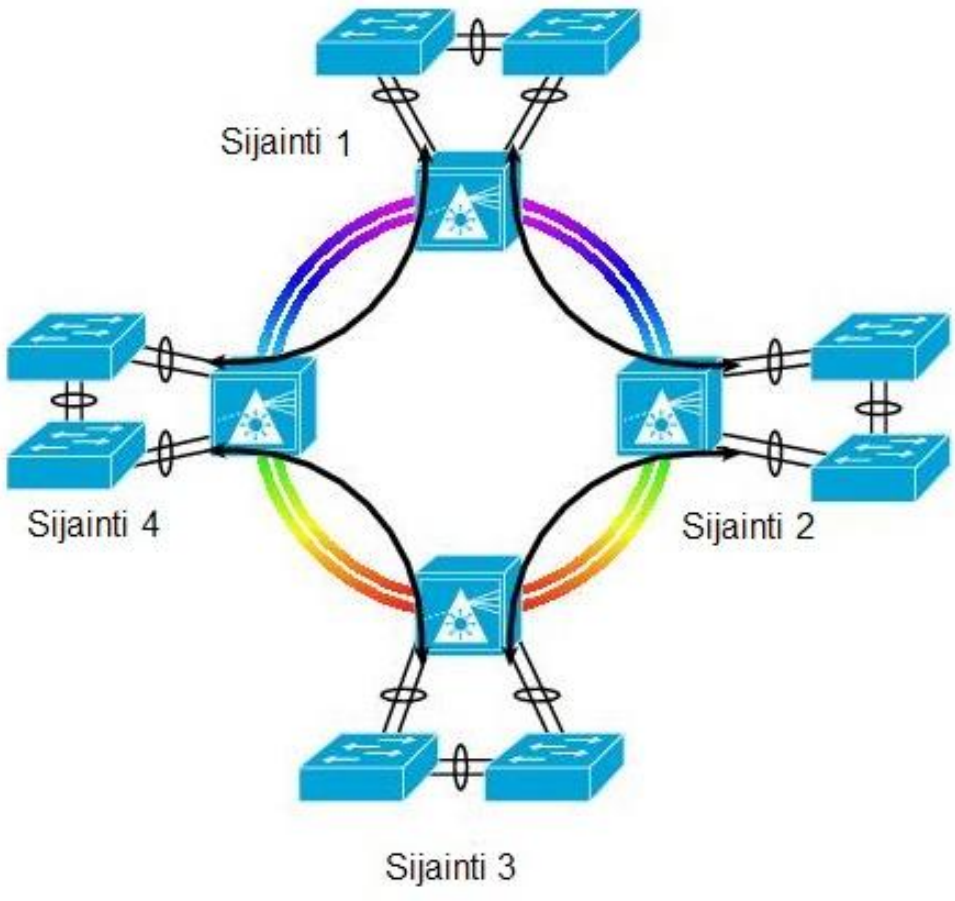
lisesti ja etäsijaintiin. Tämä taas lisää vasteaikaa, kun dataa siirretään kahden fyysisen paikan välillä.

3.2.2 Tietokonekeskusten väliset yhteydet: geoklusteri

Tietokonekeskuksessa on palvelinryppäitä, joita kutsutaan klusteriksi. Klusteri on joukko palvelimia, jotka toimivat siten kuin ne olisivat yksi tietokone (Cisco, 2011a). Palvelimet ovat usein nykyaikaisia korttipalvelimia (engl. blade server): Korttipalvelimien sanotaan olevan skaalautuvia, energiatehokkaita ja hallittavia (Cisco, 2011b), sekä kustannustehokkaita ja häiriöitä sietäviä (IBM, 2012). Cisco (2011a) määrittelee korkean saavutettavuuden klustereiden tarkoitukseksi tuottaa keskeytymätön pääsy dataan, vaikka palvelin kadottaisi yhdistettävyyden verkkoon, rikkoontuisi kokonaan tai serverin päällä toimiva sovellus ei toimisi. Klustereita käytetään yleensä palvelinfarmina yhdessä fyysisessä sijainnissa tai häiriön sietokyvyn kasvattamiseksi useissa sijainneissa eri etäisyyksillä; jälkimmäistä kutsutaan yleensä geoklusteriksi (Cisco, 2011a).

Hochmuth (2004) näki vuonna 2004 kehityksen johtavan kohti yhtenäistä verkkoalustaa, jossa tietoverkot, tietokonekeskukset ja tallennuskapasiteetti muodostavat älykkään IT-infrastruktuurin mahdollistaen informaation kulkemisen tehokkaammin sovelluksissa. Hochmuthin (2004) artikkelissa Ciscon toimitusjohtaja John Chambers kuvaili tämän kehityksen yhdistävän tietokonekeskuksen laitteet tavalla jota ei ole vielä nähty. Nyt edellä kuvatun älykkään infrastruktuurin on todettu johtaneen virtualisointiin. Virtualisoinnilla tarkoitetaan tekniikkaa joka yhdistää monia fyysisiä tallennusmuotoja loogiseen, virtuaaliseen tallennuspoolin muotoon, jota voidaan keskitetysti hallita (BCM Glossary, 2010). Tässä yhteydessä on huomattava, että myös monia muita komponentteja on virtualisoitu. Viime vuosina virtualisointi on ollut vallitseva trendi, jossa eri konesalikomponenttien virtualisoinnilla on saavutettu kustannustehokkuutta ja ketteryyttä IT-infrastruktuuria hallittaessa (Crump, 2009). Virtualisointi kerää Crumpin (2009) mukaan kiinnostuvuutta myös sen aiheuttamien haasteiden takia: Virtualisoinnin takia palvelimet tarvitsevat enemmän liitettävyyttä, koska niitä käytetään hyvin moneen tarkoitukseen, toisin kuin ennen. Haasteita tuo myös tietokonekeskuksen lisääntynyt kompleksisuus, kun on tarve hallita virtuaalisia ja fyysisiä komponentteja erikseen (Crump, 2009).

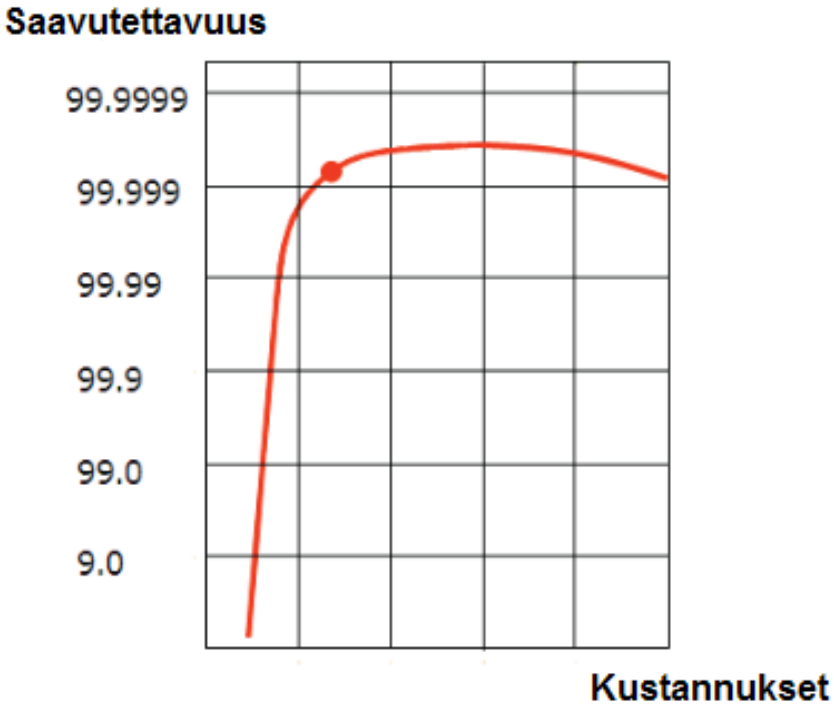
Klustereita käytetään eri sijainneissa häiriöttömyyden lisäämiseksi. Useasta tietokonekeskuksesta muodostuvan geoklusterin tarkoituksena on parantaa toipumisaikatavoitetta tekniikan avulla, ja sitä kautta parantaa organisaation liiketoiminnan jatkuvuutta (Cisco, 2011a). Seuraavassa kuviossa Cisco (2011a) esittelee hyvin häiriöitä sietävän tiheän aallonpituuden kanavointitekniikan (engl. dense wavelength division multiplexing, DWDM) perusrakenteen, eli DWDM-rengastopologian (kuvio 5).



KUVIO 5 DWDM-rengastopologia

Sijainnit kuvaavat tietokonekeskuksia, jotka ovat yhteydessä toisiinsa kahdennetulla, tai jopa monikerroksisella tekniikalla. Topologioita on olemassa useita, mutta DWDM-renkaan etuna on palvelujen korkean saavutettavuuden taso, jossa häiriöistä voidaan toipua yksi- ja kaksisuuntaisilla kytkimillä (Cisco, 2011a), joilla voidaan siirtää dataa vaihtoehtoista reittiä renkaassa myötä- ja vastapäivään häiriötilanteen sattuessa. Yhteyden katketessa dataa voidaan siis siirtää aina vaihtoehtoista reittiä.

Monen informaatioteknologia-alan yrityksen ongelmana on se, että asiakkaat vaativat luotettavampia järjestelmiä, mutta eivät ole välttämättä valmiita maksamaan korkeampaa hintaa korkeamman luotettavuuden omaavista järjestelyistä, syynä tähän on, että tarkkoja laskelmia hyödyistä on hankalaa tehdä (Patterson, 2002). Kuitenkin saavutettavuuden parantamisen ja kustannuksien välinen suhde on kuitenkin melko selkeä. Saavutettavuuden ja kustannusten suhde esitetään Arnon ym. (2010) esittämässä kuviossa (kuvio 6).



KUVIO 6 Saavutettavuuden ja kustannusten suhde

Force10 Networksin (2007) mukaan on selvää, että 99,99 % saavutettavuustaso tuottaa selvästi enemmän arvoa, kuin 99 % saavutettavuustaso. Kuinka paljon arvokkaampi lisätty saavutettavuudentaso on, riippuu liiketoiminnasta ja organisaatiosta (Force10 Networks, 2007). Palveluliiketoiminnassa suuri saavutettavuus on perusteltua, kun käsitellään monen asiakkaan IT-infrastruktuuria. Erittäin usein myös asiakkaan suunnasta varmistetumman palvelun hankkiminen on ilmeistä, koska myös heidän liiketoimintansa on täysin riippuvaista IT-infrastruktuurin toiminnasta. Kun tietokonekeskuksen palvelujen saavutettavuudessa on päästy riittävälle tasolle (kirjallisuudessa riittävällä tarkoitetaan 99,999 % ajasta), lisätyt redundantit komponentit eivät enää lisääkään varmuutta, vaan ainoastaan kustannuksia (Arno ym., 2010). Tason 4 tietokonekeskus oli saavutettavissa 99,995 % ajasta (Uptime Institute, 2009), joten tämä riittävä taso ei vielä ole tullut vastaan.

3.3 Asiakassuhteet palveluliiketoiminnassa ja jatkuvuuden hallinnan kontekstissa

Palveluliiketoiminnassa pätevät samat lainalaisuudet, kuten missä tahansa muussakin liiketoiminnassa: tuotteita kehitetään, myydään ja kulutetaan. Palveluliiketoiminnassa yrityksen tuotteena ovat palvelut, joita asiakkaat kuluttavat. Prosessit ovat strateginen voimavara, kun ne tuottavat markkinadifferentiaatiota ja sen kautta kilpailuetua; tuloksena liiketoimintaprosessit määrittelevät mo-

net niistä haasteista, joita palvelunhallinnassa kohdataan (ITIL v3, 2007). Palvelunhallinnan tavoitteena on tehdä asiakkaalle tarjottavat kyvyt ja resurssit hyödyllisiksi hyväksyttävällä laadun, kustannusten ja riskin tasolla. ITIL v3:n (2007) mukaan palveluntarjoajat auttavat asiakkaita helpottamaan erityisten resurssien omistussuhteesta ja hallinnasta koituvia rajoitteita. IT-palveluiden tehokas hallintarakenne on Tiedon (2012c) mukaan suurin yksittäinen lisäarvoa asiakkaalle tuottava tekijä.

3.3.1 Onnistuneet asiakassuhteet

Toimivat kumppanuussuhteet ITIL v3:n (2007) mukaan muodostetaan organisaatioiden johtotasolla ja ne ovat riippuvaisia strategisen informaation vaihdannasta osapuolien välillä; kumppanuussuhteen tavoitteena on, että molemmat osapuolet hyötyvät suhteesta. Palvelujen suunnittelu ei rajoitu vain uusiin palveluihin, vaan se sisältää tarvittavat muutokset ja parannukset joilla ylläpidetään tai lisätään asiakkaan kokemaa arvoa palvelujen elinkaarien, palvelujen jatkuvuuden, palvelutason saavuttamisen ja määräyksien ja normien noudattamisen kautta (ITIL v3, 2007). Avaintekijät onnistuneeseen asiakassuhteeseen ITIL v3:n (2007) mukaan on listattu seuraavaan taulukkoon (taulukko 4).

TAULUKKO 4 Avaintekijät onnistuneeseen asiakassuhteeseen

Avaintekijä	**Edellytys**
Liiketoimintastrategia	Hyvä organisaatiokulttuuri, arvot ja tavoitteet linjassa
Integraation taso	Läheisyys palveluja tuottavan organisaation ja sen asiakkaan välillä
Informaation vaihdanta	Ymmärryksen lisääminen hyvän kommunikaation ja tiedon vaihdon seurauksena
Luottamus	Luottamuksen kasvattaminen organisaatioiden ja työntekijöiden välillä
Avoimuus	Palvelujen suorituskyvyn, kustannuksien ja riskien raportointi
Vastuullisuus	Kollektiivinen vastuu nykyisestä tehokkuudesta ja palvelujen kehittämisestä
Jaettu riski ja tuotto	Investointikustannuksien jakaminen ja sitä kautta syntyneiden etujen ja tuottojen jakaminen

Herbane, Elliot ja Swartz (2004) määrittelevät asiakkaan kokeman arvon säilyttämisen keinoiksi organisaation kyvyn vastustaa kriisejä, toipua nopeasti ja minimoida tappiot. Arvon säilyttäminen on taustatoiminto (koostuen jatkuvuuden mahdollistavista resursseista, prosesseista, rutiineista ja tietämyksestä). Jatkuvuuden hallinta tukee arvon säilyttämistä ja tarjoaa paremman toiminnan vakauden, jotta kilpailuetua voitaisiin strategisten aloitteiden avulla muodostaa (Herbane, Elliot & Swartz, 2004). Herbane, Elliot ja Swartz (2004) antavat kilpailuedusta esimerkin: kun monet organisaatiot kärsivät samasta häiriöstä, ne joilla on tehokkaammat palautumistoiminnot kehittävät itselleen (kilpailu)etua, eikä ainoastaan toipumisnopeuden osalta, vaan myös taistelevat maineen heikentymistä vastaan.

3.3.2 Kriittiset menestystekijät

ITIL v3:n (2007) mukaan kaikilla markkinoilla on olemassa omat kriittiset menestystekijänsä (engl. critical success factor, CSF), joihin vaikuttavat asiakkaiden tarpeet, liiketoiminnan trendit, kilpailutilanne, lainsäädäntö, toimittajaorganisaatiot, sekä standardit ja hyvät käytännöt. Kriittiset menestystekijät määrittelevät palvelustrategian onnistumisen tai epäonnistumisen; ne voidaan määritellä kyvykkyyksinä ja resursseina, jotka kuvaavat hyvin toimialan johtavien organisaatioiden ominaisuuksia (ITIL v3, 2007). Yhä vahvemmin on nähtävissä käsitys siitä, että jatkuvuuden hallinta tulee olemaan IT-palveluliiketoiminnassa yksi tärkeimmistä kriittisistä menestystekijöistä. ITIL v3 (2007) painottaa, että prosessoitaessa suurta määrää reaaliaikaista dataa (kuten finanssisektorin data) palveluntuottajien on omattava suuria tietojärjestelmiä, luotettava verkkoinfrastruktuuri, turvalliset toimitilat, tietämystä alan lainsäädännöstä ja erittäin korkean tasoinen toiminnan jatkuvuus. Blyth (2009) lisää, että jatkuvuuden hallinnan tuloksena synnytetyt suunnitelmat tuottavat markkinadifferentiaatiota tehokkuuden, ketteryyden ja yleisen kilpailukyvyn muodossa. Parantuneen kilpailukyvyn ansiosta organisaatio pystyy toimimaan sellaisissa liiketoimintaympäristöissä, joissa se ei normaalisti saisi (tai pystyisi) toimia (Blyth, 2009). Tällaisia liiketoimintaympäristöjä voisivat olla erittäin tiukasti säännelty finanssiala tai viranomaistoiminta, esimerkiksi yhteiskunnan huoltovarmuuteen liittyvät tehtävät.

4 JATKUVUUDEN HALLINNAN VIITEKEHYS

Tässä luvussa käsitellään jatkuvuuden hallinnan viitekehystä. Viitekehyksen tehtävänä tässä tutkielmassa on yhdistää ja tiivistää jatkuvuuden hallinnan tutkimus ja tieteellinen keskustelu yhdeksi malliksi, joka vastaa vallalla olevaa teoreettista käsitystä liiketoiminnan jatkuvuuden hallinnasta.

4.1 Viitekehyksen luominen, huomautukset ja taustaolettamukset

Viitekehys on muodostettu tutkimani jatkuvuuden hallintaa ja sen osa-alueita käsittelevien kirjojen, standardien, konferenssijulkaisujen, artikkeleiden ja muiden tieteellisten julkaisujen pohjalta. Kyseessä on siis Järvisen ja Järvisen (2004) mainitsema deduktiivinen tapa jäsentää ja johtaa teoreettisista olettamuksista malli jatkuvuuden hallinnan selittämiseen ja kuvaamiseen. Viitekehystä on käytetty hyödyksi haastatteluihin valmistauduttaessa kysymyksiä aseteltaessa ja aihepiirejä valittaessa. Viitekehyksen avulla saadaan muodostettua kuva jatkuvuuden hallinnan tärkeimmistä elementeistä, jotta empiirisen osuuden casetutkimuksen teemahaastatteluissa voidaan suunnata painopiste tärkeimpiin asioihin.

Käsitteet on pyritty sijoittamaan viitekehyksen strategisessa ja operationaalisessa osassa niiden ajallisten riippuvuuksien mukaisesti. Vasemmalla olevat käsitteet ilmentävät ennen kriisiä tapahtuvaa toimintaa, keskellä olevat käsitteet kriisinaikana tapahtuvaa toimintaa, ja oikealla olevat kriisin ilmettyä tapahtuvaa toimintaa. Taktisessa osassa ajallisella riippuvuudella ei ole merkitystä, koska toiminnot ovat olemassa koko toiminnan elinkaaren ajan. Ensimmäinen osa viitekehyksessä on jatkuvuuden hallinnan strateginen taso, se on esitelty taulukossa 5. Strateginen taso kuvaa organisaation ylimmän johdon hallintatapaa ja visiota jatkuvuuden hallinnan hyödyntämisestä. Strategisella tasolla tehdään päätökset suuntaviivoista ja tavoitteista, joita jatkuvuuden hallinnalla halutaan saavuttaa. Toisena osana viitekehyksessä on jatkuvuuden hallinnan

operationaalinen taso, eli työkalut, joita ovat erilaiset suunnitelmat ja menetelmät, kuten taulukossa 6 on esitetty. Suunnitelmia ovat esimerkiksi jatkuvuussuunnitelmat, kriisinhallinnan suunnitelmat ja toipumissuunnitelmat. Menetelminä suunnitelmien luomisessa ovat yleisesti tunnustetut riski- ja vaikutusanalyysi, sekä testaaminen (taulukko 6). Kolmantena osana on jatkuvuuden hallinnan taktinen taso, joka sisältää organisaation resurssit ja tärkeimmät sidosryhmät (taulukko 7). Organisaation resursseja ovat esimerkiksi sen henkilöstö, tilat ja teknologia. Kriittisten liiketoimintaprosessien toiminta on kiinni näiden resurssien saatavuudesta. IT-palvelutoimittajan konesalien kautta jatkuvuuden hallinta ja häiriöiden sietokyky on ympärivuorokautisesti suurennuslasin alla, siksi organisaation ulkopuoliset sidosryhmät ovat tärkeitä. Asiakassuhteiden, viestinnän ja joskus myös median yhteispelin toimivuudella on luottamuksen ja brändin kannalta jopa kriittinen merkitys. Seuraavaksi esittelemäni jatkuvuuden hallinnan viitekehys koostuu kolmesta osiosta, jotka liittyvät erittäin vahvasti toisiinsa. Jako kolmeen erilliseen osaan on tehty, jotta viitekehys pysyy selkeämpänä ja vahvimmin toisiinsa liittyvät käsitteet pystytään erottamaan koko jatkuvuuden hallinnan laajasta skaalasta. On totta, että osa käsitteistä voisi aivan hyvin olla useassa viitekehyksen osassa, mutta viitekehyksen tarkoituksena ei ole olla tyhjentävä, vaan suuntaa antava ja tutkimusta ohjaava.

4.2 Jatkuvuuden hallinnan strateginen taso

Taulukosta 5 voidaan huomata, että strategisella tasolla olevat jatkuvuuden hallinnan elementit ovat laajoja kokonaisuuksia, jotka ohjaavat organisaation jatkuvuuskäytänteitä ennen ja jälkeen poikkeustilanteen, mutta myös poikkeustilanteiden aikana. Yhteistä on myös hyvä hallintotapa: strategisella tasolla määritellään johdon sitoutuminen jatkuvuuden hallinnan toimenpiteisiin ja käytännön toteuttamiseen, joka heijastuu koko organisaatioon ja myös sen ulkopuolelle asiakassuhteisiin.

TAULUKKO 5 Jatkuvuuden hallinnan strateginen taso: visio, missio ja strategia

Ennen häiriötä: varautuminen ja ennakkosuunnittelu	Häiriön aikana: tilanteen hallitseminen	Häiriön jälkeinen aika: palautuminen ja toipuminen
Jatkuvuuden hallinta ja jatkuvuuden hallinnan ohjelma		
Jatkuvuusstrategia		
Jatkuvuuden hallinnan sulauttaminen organisaation toimintatapoihin		
Jatkuvuusjärjestelyiden läpikäynti, harjoittelu ja auditointi		

Jatkuvuuden hallinnan strategisella tasolla määrätään se, millaiseen jatkuvuuden hallinnan tavoitetasoon pyritään, ja kuinka paljon organisaatio on valmis panostamaan jatkuvuuden hallinnan kehittämiseen.

4.3 Jatkuvuuden hallinnan operationaalinen taso

Operationaalisella tasolla olevat käsitteet ovat osa reagointia tunnistettuja riskejä kohtaan. Kuten toisessa luvussa mainittiin, jatkuvuus- ja toipumissuunnitelmat ovat vastauksia tunnistettuihin riskeihin ja niiden tehtävänä on kriittisten liiketoimintaprosessien tukeminen. Jatkuvuus-, toipumis-, ja kriisinhallinnan suunnitelmien elinkaareen kuuluu olennaisena osana suunnitelmien arviointi, suunnitelmissa määriteltyjen toimenpiteiden harjoittelu ja testaaminen esimerkiksi erilaisten skenaarioiden avulla.

TAULUKKO 6 Jatkuvuuden hallinnan operationaalinen taso: menetelmät ja suunnitelmat

<table>
<tr><td>Ennen häiriötä: varautuminen ja ennakkosuunnittelu</td><td>Häiriön aikana: tilanteen hallitseminen</td><td>Häiriön jälkeinen aika: palautuminen ja toipuminen</td></tr>
<tr><td colspan="2">Jatkuvuussuunnittelu ja kriisinhallinta</td><td>Toipumissuunnittelu</td></tr>
<tr><td colspan="2">Riski- ja vaikutusanalyysi</td><td></td></tr>
<tr><td>Jatkuvuussuunnitelma</td><td>Kriisinhallinnan suunnitelma</td><td>Toipumissuunnitelma</td></tr>
<tr><td colspan="3">Suunnitelmien arviointi, harjoittelu ja testaaminen</td></tr>
</table>

Operationaalisen tasolla käsitteet ovat sekä proaktiivisia, että reaktiivisia. Pitää pystyä ennaltaehkäisemään ja varautumaan uhkiin (jatkuvuussuunnittelu), toimimaan reaktiivisesti kriisitilanteessa (kriisinhallinta), sekä palautumaan normaalitilaan (toipumissuunnittelu).

4.4 Jatkuvuuden hallinnan taktinen taso

Jatkuvuuden hallinnan taktisen tasoon kuuluvat käsitteet ovat ominaisuuksiltaan resursseja ja sidosryhmien toimintaa tukevia. Taktisen tasoon kuuluvat asiat ovat tärkeitä häiriönsietokyvyn kannalta, esimerkiksi teknologiaresurssien, kuten tietokonekeskusten ja muun IT-infrastruktuurin merkitys organisationaalisen sietokyvyn kasvattamisessa ja sitä kautta liiketoiminnan ylläpitämisessä on valtava. IT-palveluliiketoiminnassa koko muu jatkuvuuden hallinta ja sen aliprosessit tähtäävät juuri IT-infrastruktuurin häiriöttömyyteen, koska ydinliiketoiminta on täysin riippuvaista sen jatkuvasta toimintakyvystä.

TAULUKKO 7 Jatkuvuuden hallinnan taktinen taso: resurssit ja sidosryhmät

Liiketoimintaresurssit	Sidosryhmät	IT-infrastruktuuri
Liiketoimintaprosessit, kriittiset menestystekijät, osakkeenomistajat ja rahoittajat	Sisäiset: Henkilöstöresurssit: Kontrolli- ja pelastusryhmä, toipumisryhmä, muut työntekijät Ulkoiset: Viranomaiset, kilpailijat, toimintaympäristö, yhteistyökumppanit, asiakkaat	Tietokonekeskukset, tietojärjestelmät, sovellukset, tietoverkot
Kriisinhallintaryhmä		
Viestintä, media ja asiakassuhteet		

4.5 Teorian painopisteet: tunnistetusta riskistä valmiiseen suunnitelmaan

Jatkuvuuden hallintaa kuvattiin edellä kolmitasoisena mallina, jossa oli strateginen, operationaalinen ja taktinen taso. Kukin taso kuvastaa organisaation eri osien toimintaa jatkuvuuden parantamiseksi. Kyse oli eräänlaisesta poikkileikkauksesta, joka oli mahdollista muodostaa tutkitun kirjallisuuden pohjalta. Nyt täsmennän vielä niitä kirjallisuudessa tunnistettuja painopisteitä, joiden avulla koko jatkuvuuden hallintaprosessi viedään läpi siihen vaiheeseen, kunnes jat-

kuvuusjärjestelyt, sekä jatkuvuus-, kriisinhallinnan- ja toipumissuunnitelmat tulee taas arvioida ja kerrata.

Tutkielman toisessa luvussa todettiin, riskienhallinta on läheistä sukua jatkuvuuden hallinnalle. Ensin on siis lähdettävä liikkeelle riskien tunnistamisesta. Strategisella tasolla tehdään selväksi jatkuvuuden hallinnan periaatteet ja tavoitteet. Periaatteet voidaan ottaa esimerkiksi standardeista tai muista tunnetuista, hyviksi havaituista julkaisuista. Tärkeää on se, että sidotaan jatkuvuuden hallinta osaksi liiketoiminnan tavoitteita ja määritellään mitä sillä halutaan saavuttaa. Kun prosessi on saatu käynnistettyä, samanaikaisesti strategisella tasolla tehtyjen päätösten ja vaatimusten mukaisesti alkaa operationaalisella tasolla käytännön työ. Tämä tarkoittaa organisaation toimintaa koskevien riskien ja uhkien kartoittamista. Riskejä arvioitaessa yritetään ymmärtää, kuinka todennäköistä on, että jokin uhka toteutuu. Vaikutusanalyysillä pyritään arvioimaan, millaiset vaikutukset kullakin riskillä liiketoiminnalle on. Riskin ollessa riittävän todennäköinen ja vaikuttava, siirrytään operationaalisella tasolla seuraavaan vaiheeseen, erilaisten suunnitelmien kehittämiseen riskien toteutumisen varalle.

Kun kriittisiä liiketoimintaprosesseja uhkaavat riskit organisaatiossa on tunnistettu, voidaan aloittaa varautumisen suunnittelu. Jatkuvuussuunnittelun avulla voidaan operationaalisella tasolla varautua tunnistettujen riskien aiheuttamiin häiriöihin. Tämä on ennaltaehkäisevää toimintaa, joka auttaa jatkamaan liiketoimintaa normaalisti jonkin riskin toteutuessa. Jatkuvuussuunnitelmien lisäksi osana varautumista ovat myös kriisinhallinnan suunnitelmat ja toipumissuunnitelmat. Kriisinhallinnan suunnitelma auttaa organisaatiota toimimaan kriisitilanteessa oikein, jotta kriisin eskaloitumiselta vältyttäisiin tai maineen menettämiseltä säästyttäisiin. Toipumissuunnitelma taas keskittyy organisaation toimintoja ylläpitävän infrastruktuurin palauttamiseen, jossa erittäin tärkeässä osassa on informaatioteknologia; palveluliiketoiminnassa informaatioteknologian palautumisella on ylivoimaisesti suurin merkitys.

Taktisen tason tehtävänä on tukea operationaalisella tasolla olevia toimintoja. Moni taktisen tason tehtävistä kuuluu suoraan kriisinhallinnan tehtäviin. Tähän kuuluu esimerkiksi varautuminen kriisitilannetta varten sisäisen ja ulkoisen viestinnän varmistamiseen, sekä media- ja asiakassuhteiden ylläpitämiseen roolittamisen ja vastuiden jakamisen avulla. Taktiselta tasolta lähtien organisaation toiminnan mahdollistajat, eli kriittiset menestystekijät pitää olla tunnistettu. Taktisella tasolla jatkuvuuden hallinnan sosiaalis-tekninen luonne näkyy parhaiten: IT-palveluliiketoiminnassa tarvitaan häiriöttömään palvelujen tuottamiseen ja toimittamiseen henkilöstöresurssien avulla toimivia liiketoimintaprosesseja, jotka ovat erittäin riippuvaisia palvelutoimittajan IT-infrastruktuurin toimintakyvystä. Jatkuvuuskyvykkyyden saavuttamiseksi ja ylläpitämiseksi tarvitaan näitä kaikkia kolmea resurssia.

Tässä vaiheessa jatkuvuuden hallintaprosessi palaa takaisin strategiselle tasolle. Strategisella tasolla määritellään luotujen suunnitelmien harjoitteluun, opiskeluun, testaamiseen ja arviointiin liittyvät asiat, kuten auditoinnit, koulutus ja tietoisuuden lisääminen. Lisäksi päätetään systemaattisesta riskien seu-

raamisesta, koska esimerkiksi teknologiaan liittyvä kehitys tuo mukanaan uusia uhkia. Luodut suunnitelmat ja muut jatkuvuuden hallinnan järjestelyt tuodaan henkilöstön tietoon. Operationaalisella tasolla tämä näkyy suunnitelmien käytännön harjoitteluna ja kertaamisena.

Prosessi jatkuu edelleen ja opittua täytyy edelleen harjoitella säännöllisin väliajoin, sekä tuloksia pitää arvioida toiminnan parantamiseksi. Toimintaympäristön muuttuminen, muutokset organisaation sisällä, teknologian uudistuminen ja myös asiakasvaatimukset edellyttävät kaikki jatkuvuusjärjestelyiden päivittämistä. Näin jatkuvuuden hallinnasta tulee osa organisaation toimintakulttuuria. Vaikkei yhtään suurempaa kriisiä olisi vielä koettu, tässä vaiheessa jatkuvuuden hallinnan edut tulevat viimeistään esiin. Harkitseva, suunnitelmallinen ja häiriönsietokykyinen organisaatio kasvattaa luotettavuuttaan asiakkaiden ja muiden sidosryhmien keskuudessa. Jatkuvuuden hallintaprosessin myötä organisaation jatkuvuuden hallittavuus kasvaa ja organisaatio pystyy tuottamaan yhä häiriöttömämpiä palveluja asiakkailleen. Asiakkaan näkökulmasta ajateltuna voidaan pitää itsestään selvänä, että palvelut joita he hankkivat ovat saatavissa koko ajan, vaikka tietyt rajat palvelutasosopimuksissa katkoille määriteltäisiinkin. Jatkuvuutta ja sietokykyä pitää vaalia ja edelleen kehittää, koska hankittua luottamusta ei haluta menettää – etenkään sen takia, että olisi laiminlyöty riskien kehittymisen ja muuttumisen seuraaminen.

4.6 Yhteenveto

Tätä viitekehystä käytetään yhteenvetona tutkielman teoreettisesta osuudesta. Tutkielmassa on tähän asti käsitelty jatkuvuuden hallintaa eri näkökulmista ja eri organisaation tasoilta katsottuna. Tutkielmassa on kuvattu kirjallisuuden perusteella jatkuvuuden hallinnan laajuus, määritelty tärkeimmät käsitteet, tehty katsaus jatkuvuuden hallinnan sisältöön ja perusteltu jatkuvuuden hallinnan tärkeys. Luotiin katsaus myös IT-palveluliiketoiminnan toimintaympäristöön ja kuvattiin jatkuvuuden hallinnan ominaisuudet tässä kontekstissa. Todettiin myös IT-infrastruktuurin olevan merkittävässä osassa palvelutoimittajan kyvyssä pyrkiä turvaamaan häiriötön asiakkaiden- ja samalla myös oma liiketoiminta.

Ennen pohdinta- ja yhteenveto-osuutta on jäljellä jatkuvuuden hallinnan kuvaaminen reaalimaailman olosuhteissa. Seuraavaksi siirrytään kohti empiiristä osuutta, jota ensin pohjustetaan tutkimusmenetelmien valinnalla. Tätä viitekehystä käytetään hyödyksi tutkielman empiirisessä osuudessa: esimerkiksi haastattelujen teemat ovat muodostettu viitekehyksessä mainittujen tasojen pohjalta. Myös haastattelurungot ovat luotu tämän viitekehyksen avulla.

5 TUTKIMUSMETODI

Tässä luvussa kuvataan tutkielman empiiristä osuutta. Empiirisenä osuutena tutkielmassa on case-tutkimus Tieto Oyj:ssä, jonka tiedonkeruu on toteutettu teemahaastattelujen avulla. Case-tutkimuksen tavoitteena on selvittää kirjallisuuden ja jatkuvuuden hallinnan viitekehyksen pohjalta jatkuvuuden hallinnan toimenpiteitä aidossa ympäristössä. Case-tutkimuksen tuloksien pohjalta vastataan tutkielman aluksi esitettyihin tutkimusongelmiin: miten jatkuvuuden hallinnan järjestelyt on toteutettu Tieto Oyj:ssä; painottaako Tieto Oyj samoja jatkuvuuden hallinnan periaatteita, kuin kirjallisuudessa on esitetty? Miten jatkuvuuden hallinnan tärkeys ja laajempi palvelutaso on perusteltavissa IT-palvelutoimittajan asiakkaalle? Ensiksi tässä luvussa käydään läpi tutkimusmenetelmän valinta, perustellaan case-tutkimuksen rajaukset, kerrotaan haastateltavien valinnasta ja taustasta, haastattelujen toteutuksesta ja haastatteluissa kerätyn aineiston analysoinnista.

5.1 Tutkimusmenetelmän valinta

Tutkimusmenetelmä on siis case-tutkimus, joka toteutettiin teemahaastatteluilla. Teemahaastattelulle tiedonkeruumenetelmänä Hirsjärven, Remeksen ja Sajavaaran (2008) mukaan on tyypillistä, että kysymysten tarkka muoto puuttuu, mutta aiheet ovat tiedossa. Riippuen hieman haastattelusta, noin 15–20 kysymystä oli etukäteen laadittu tarkasti noudattaen luvussa neljä muodostamaani teoreettista viitekehystä. Järvisen ja Järvisen (2004) mukaan case-tutkimuksessa voidaan tarkastella yhtä tai useampaa tapausta, ja tutkimus voi olla luonteeltaan kuvailevaa, teoriaa testaavaa tai teoriaa luovaa. Tässä tapauksessa case-tutkimuksessa on mukana yksi tapaus, jota tarkastellaan kvalitatiivisesti. Tutkielmassa case-tutkimus on luonteeltaan kuvailevaa, mutta myös luvussa neljä esitetyn teoreettisen viitekehystä testaavaa. Tiedonkeruumenetelmänä ovat siis teemahaastattelut. Haastattelut ovat puolistrukturoituja, joka tarkoittaa Järvisen ja Järvisen (2004) mukaan sitä, että kysymykset eivät olleet tiukasti asetettuja

ennen haastattelua. Aaltolan ja Vallin (2001) mukaan puolistrukturoidun haastattelun etuna on, että haastateltava saa vastata omin sanoin kysymyksiin ja silloin tilaa keskustelulle jää enemmän. Haastateltaviksi henkilöiksi valittiin asiasta parhaiten tietävät henkilöt, kuten Järvinen ja Järvinen (2004) kirjassaan kehottavat tekemään. Tällä tavoin pyrittiin saamaan kattavuutta tapauksen käsittelemiseen ja kuvaamaan jatkuvuuden hallinnan periaatteiden toteutuminen mahdollisimman hyvin. Haastateltavien valintaa on kuvattu tarkemmin luvussa 5.3. Aaltola ja Valli (2001) täsmentävät teemahaastattelun tapahtuvan haastattelijan aloitteesta ja ehdoilla, mutta metodi auttaa tekemään haastattelusta enemmän keskustelunomaisen. Näin on mahdollista saada enemmän aihepiiristä tietoa, joka hyödyttää tutkielman tekemistä. Aaltola ja Valli (2001) huomauttavatkin, että tietty epävirallisuus jopa lisää luottamusta haastattelijan ja haastateltavan välillä. Teemahaastattelua puolsivat myös ne seikat, joita Hirsjärvi ja Hurme (2001) listaavat: Halutaan tutkia suurelle yleisölle vielä melko tuntematonta aihetta, halutaan syventää tietoutta, halutaan sijoittaa asia laajempaan kontekstiin, sekä halutaan tutkia hyvin arkaa ja luottamuksellista aihetta. Jos halutaan verrata nyt tehtyjä haastatteluja lomakkeen avulla tehtävään kyselyyn, niin haastattelun edut ovat selvät: Hirsjärvi ja Hurme (2001) kertovat, että haastattelussa on suuremmat mahdollisuudet motivoida haastateltavaa, aiheiden järjestystä voidaan säädellä, haastattelu on joustavampi metodi sallien täsmennykset ja haastattelu sopii lomaketta paremmin arkaluontoisiin aiheisiin, joka tässä tutkimuksessa jo onkin todettu. Kyseessä on siis vahvasti kvalitatiivinen tutkimus, jossa yritetään mallintaa ja kuvata tutkittavaa kohdetta viitekehyksessä esitettyjen jatkuvuuden hallinnan elementtien mukaisesti.

5.2 Rajaukset ja rajoitukset

Tutkimus on rajattu koskemaan jatkuvuuden hallintaa Tieto Oyj:n tietokonekeskuksen tasolla. Tällöin keskiössä ovat palvelujen toimittaminen asiakkaille ja heille tarjottujen käyttöpalveluiden ylläpitäminen. Muutamat kysymykset saattavat olla aihepiiriltään laajempia, mutta edelleen niidenkin kysymysten osalta yritetään selvittää vaikutukset asiakkaalle. Hyvin useasti laajemmat ongelmat vaikuttavat siis kykyyn toimittaa palveluita asiakkaalle. Haasteet jatkuvuuden hallinnalle tietokonekeskuksen ympäristössä eivät siis aina ole tietokonekeskuksen sisäisiä asioita; useat muuttujat vaikuttavat ulkoapäin palvelutoimittajan päivittäiseen toimintaan. Itse haastatteluissa on pienenä rajoituksena se, että niitä ei turvallisuussyistä johtuen nauhoitettu. Tällöin jää aina mahdollisuus siihen, että käsitellyt asiat eivät tule täysin oikein ymmärretyksi. Asia otettiin huomioon jo haastatteluja suunniteltaessa, joten molemminpuolisen ymmärryksen lisäämiseksi muistiinpanoista puhtaaksi kirjoitetut haastattelut lähetettiin vielä samana päivänä haastateltaville kommentointia ja korjaamista varten.

5.3 Case-tutkimuksen aloitus ja haastateltavien valinta

Tutkimuksessa oltiin lokakuun lopussa 2011 sähköpostitse yhteydessä Tieto Oyj:n turvallisuusjohtajaan. Hänelle lähetettiin tutkimussuunnitelma ja saatekirje, jossa tutkielman aihepiiri ja tavoitteet selvitettiin. Tutkimuksesta keskusteltiin sähköpostitse: Aihetta rajattiin ja tutkimuksen tavoitteita täsmennettiin. Myöhemmin marraskuussa 2011 sovittiin joulukuun alussa pidettävästä tapaamisesta Tieto Oyj:n tiloissa. Tapaamisessa käytiin tarkasti läpi tutkimuksen vaiheet ja menetelmät, sekä Tieto Oyj:n jatkuvuuden hallinnan periaatteita. Yleisten tutkimusta koskevien asioiden läpikäynnin lisäksi tapaaminen toimi Hirsjärven ja Hurmeen (2001) esittämänä esihaastatteluna: tapaamisessa testattiin jo aihepiirejä, haastattelujen kohdejoukon taustaa ja voitiin täsmentää ja karsia turhia osioita tutkimuksesta. ”Tuskin kukaan tutkija pystyy menemään kentälle kysymään ”oikeita” kysymyksiä suoralta kädeltä” (Hirsjärvi & Hurme, 2001). Tieto Oyj:n normaalien käytäntöjen ja aiheen arkaluontoisuuden vuoksi ensimmäisen tapaamisen yhteydessä kirjoitettiin henkilökohtainen salassapitosopimus (engl. non-disclosure agreement, NDA), joka velvoittaa tehtävän suorittajaa olemaan paljastamatta liian yksityiskohtaisia tietoja ja luottamuksellista aineistoa tutkimuksen edetessä ja sen jälkeen.

Tapaamisessa todettiin tutkimuksen hyödyntävän molempien osapuolten intressejä, joten haastattelujen aiheista ja henkilöistä sovittiin tarkemmin. Haastateltavat valittiin niin sanotulla lumipallo-otannalla, jossa turvallisuusjohtajan esityksestä valikoitui tutkimuksen tarkempiin aihepiireihin sopivat henkilöt vastaamaan haastattelukysymyksiin. Ei pidä kuitenkaan käsittää, että vastaajat olisivat millään muotoa olleet pakotettuja vastaamaan kysymyksiin, vaan tehdyn ehdotuksen perusteella lähestyin jokaista haastateltavaa erikseen haastattelupyynnöllä ja perustelin heille aiheen tärkeyden ja hyödyn myös Tieto Oyj:n kannalta. Käytettyä lumipallo-otantaa puolsi se, että haastattelija tarvitsi mahdollisimman tarkan näkemyksen kustakin aihepiiristä, jotta case-tutkimuksen suorittaminen olisi mahdollista. Siksi muun muassa satunnaisuuteen perustuvat otannat eivät tulleet kysymykseen. Tarkoituksena oli siis löytää mahdollisimman asiantuntevat henkilöt organisaation sisältä, jotta jatkuvuuden hallinnasta Tieto Oyj:ssä saataisiin mahdollisimman tarkka kuva.

Haastateltavia oli yhteensä viisi kappaletta. Haastateltavien laadukkuutta painottaen viisi osoittautui sopivaksi määräksi: kuten Hirsjärvi ja Hurme (2001) toteavat, onkin parempi puhua harkinnanvaraisesta näytteestä, kuin otoksesta. Liian suuri haastateltavien määrä olisi johtanut turhaan toistoon ja päällekkäisyyteen vastauksissa, koska jo nyt tällä määrällä tiettyä painottuneisuutta löytyi vastausten välillä. Viisi haastateltavaa jakautui siten, että turvallisuusjohtaja vastasi kysymyksiin jatkuvuuden hallinnan strategiasta ja muista laajemmista piirteistä, kuten henkilöstöresursseista ja viestinnästä. Kaksi vastaajaa pureutui samoihin kysymyksiin tietokonekeskuksen ja IT-infrastruktuurin jatkuvuuden hallinnasta. Kaksi haastateltavaa vastasi jatkuvuuden hallintaa ja liiketoimintaa koskeviin kysymyksiin. Haastateltavat olivat poikkeuksetta johtotason henki-

löitä, jotka oman työnkuvansa kautta osasivat parhaiten vastata jatkuvuuden hallintaa ja sen laajoja osa-alueita koskeviin kysymyksiin.

5.4 Haastattelujen suunnittelu ja toteutus

Haastattelukysymysten luominen käynnistyi heti joulukuun tapaamisen jälkeen, kun yksityiskohdista päästiin sopimukseen. Kuten rajoitteissa mainittiin, aiheen arkaluontoisuuden vuoksi ja kohdeorganisaation turvallisuuspolitiikasta haastattelujen nauhoittaminen ei ollut mahdollista, joten tarkat muistiinpanot haastatteluiden aikana olivat tärkeässä asemassa. Joulukuussa lähetin sähköpostitse ensimmäiset haastattelupyynnöt turvallisuusjohtajan ehdottamille henkilöille. Kysymyspatteristoa rakennettiin samanaikaisesti tutkielman teoreettisen osuuden kanssa. Tutkielman ohjaaja antoi myös omat kommenttinsa kysymyksistä, jonka avulla kysymyksiä paranneltiin. Osa suunnitelluista vastaajista vastasi heti pyyntöön, ja loputkin hieman myöhemmin. IT-infrastruktuuria ja liiketoimintaa koskevat haastattelut sovittiin tammikuun 2012 loppuun. Tammikuun puolivälissä 2012 teoriaosuus oli jo pitkällä, ja kysymykset tarkentuivat entisestään ennen ensimmäistä haastattelua.

Kaikki haastattelut tehtiin yksittäin ja kasvokkain haastateltavan kanssa Tieto Oyj:n toimipisteissä Helsingissä, Espoossa ja Tampereella. Aaltola ja Valli (2001) muistuttavat, että haastattelupaikalla on merkitystä: Kun haastattelut tehdään sellaisessa paikassa, joka on rauhallinen, tuttu ja turvallinen haastateltavalle henkilölle, on suurempi mahdollisuus onnistua. Toki yleisesti ottaen haastattelijan kannalta ympäristö voi joissain tapauksissa olla vieraantuntuinen, mutta tässä tapauksessa haastattelutilanteet olivat täysin normaalit. Kysymyksiä ei annettu haastateltaville etukäteen, mutta haastatteluja sovittaessa täsmennettiin ko. haastattelun aihepiiri ja erityisalueet. Myös heti haastattelun aluksi kerrottiin koko tutkimuksen tavoite ja hyöty organisaation kannalta. Haastattelut olivat kestoltaan noin 1,5 tuntia, joka pystyttiin käyttämään tehokkaasti hyväksi haastattelupaikkojen monipuolisten ja häiriöttömien neuvottelutilojen vuoksi. Syvä luottamus haastateltavan ja haastattelijan välillä oli tärkeää; aiheen ollessa hyvin luottamuksellinen ja arkaluontoinen, tällä voi olla vaikutusta haastateltavien vastauksiin. Luottamusta ja samalla vastausten luotettavuutta pyrittiin parantamaan salassapitosopimuksen ja tutkielman sisällön kontrolloinnin avulla, jolloin haastattelutilanteessa keskustelut olivat avoimempia ja vähemmän varautuneita. Turvallisuusjohtaja pidettiin säännöllisesti informoituna tutkielman etenemisestä.

Haastattelujen aiheet jakaantuivat kolmeen osa-alueeseen: jatkuvuuden hallinnan kokonaisnäkymä, IT-infrastruktuuri ja liiketoiminta. Aiheet sivuavat toisiaan hyvin vahvasti, mutta haastateltavien erilaisen taustan vuoksi oli mahdollista kerätä mielenkiintoisia näkemyksiä jatkuvuuden hallinnasta yleisesti, IT-infrastruktuurista ja liiketoiminnasta. Kysymykset muodostettiin nojaten teoreettiseen viitekehykseen ja tutkimusongelmiin. Myös intuitiolle annettiin rooli haastatteluissa: Aaltola ja Valli (2001) täsmentävät, että teemahaastattelun

luonteeseen kuuluu, että myös luova, lennossa tapahtuva ideointi on paikallaan. Muutamia lisäkysymyksiä syntyikin haastattelutilanteiden edetessä. Jokaisen kolmen osa-alueen haastattelurungot ovat tutkielman liitteenä: IT-infrastruktuuri liitteessä 1, liiketoiminta liitteessä 2 ja jatkuvuuden hallinnan kokonaisnäkymä liitteessä 3.

5.5 Aineiston analysointi

Koska nauhoittaminen ei ollut sallittua, myöskään haastatteluaineiston litterointia ei voitu tehdä. Tämä tarkoitti sitä, että muistiinpanoilla oli keskeinen rooli haastattelujen analysoinnin tekemisessä. Muistiinpanot tehtiin kannettavan tietokoneen avulla haastattelutilanteessa. Heti haastattelujen jälkeen haastateltavalle ilmoitettiin kerätyn aineiston kokoamisesta ja toimittamisesta mahdollisimman nopeasti haastateltavan arvioitavaksi. Tehdyt muistiinpanot kirjoitettiin kokonaisiksi lauseiksi ja lähetettiin haastateltaville korjattavaksi, täydennettäväksi ja kommentoitavaksi. Sain haastattelujen jälkeen sähköpostitse palautetta, että yleisesti ottaen kerätyn aineiston sisältö oli ymmärretty ja kirjoitettu luettavaan muotoon erittäin hyvällä tasolla. Toki pieniä korjauksia ja täydennyksiä tuli lähes jokaisessa haastattelussa, mutta paljon vähemmän kuin etukäteen oli odotettavissa. Haastattelut sujuivat suunnitellusti ja ennalta asetettuihin tavoitteisiin päästiin. Tavoitteiden saavuttamisen syiksi voidaan laskea kattava etukäteisperehtyminen aiheeseen, sekä ensimmäisessä tapaamisessa saatu käsitys yleisistä Tieto Oyj:n toimintatavoista IT-palveluliiketoiminnassa.

Aaltolan ja Vallin (2001) ja Hirsjärven ja Hurmeen (2001) mukaan teemahaastattelu aineistolle on tyypillistä, että sitä analysoidaan teemoittain. Ideana on siis se, että jokaisen haastattelijan kommentit kustakin teemasta ovat vierekkäin, jolloin niitä on helpompi vertailla. Tämä oli helppo toteuttaa nykyaikaisella tekstinkäsittelyohjelmalla. Viitekehyksen perusteella kaikki kysymykset jaettiin pääkäsitteisiin. Pääkäsitteet muodostettiin organisaation jatkuvuuden hallinnan ohjelman etenemisen mukaisesti. Haastateltavien vastaukset sijoitettiin peräkkäin pääkäsitteiden alle, jotta vertailua oli helpompi tehdä. Hirsjärvi, Remes ja Sajavaara (2008) määrittelee aineiston järjestämisen tärkeäksi vaiheeksi tiedon tallennusta ja analyysejä varten.

Hirsjärvi ja Hurme (2001) toteavat, että useassa oppaassa esitetään aineiston analysoinnin menettelytavaksi se, että aineistoa analysoidaan samanaikaisesti aineiston keruun, tulkinnan ja narratiivisen raportoinnin kanssa. Tämä pätee myös tähän tutkimukseen, koska haastattelujen aineisto purettiin heti haastattelujen päättymisen jälkeen ja käytettiin haastateltavalla tarkastettavana. Lisäksi jo haastattelujen aikana kiinnitettiin huomiota tulkintaan: Monen kysymyksen jälkeen esitin lyhyen tiivistyksen omin sanoin kerrottuna, jolloin haastateltava sai todeta, vahvistaako hän tämän tulkinnan ko. asiasta. Tämä lähestymistapa aineiston analysointiin on kuvattu Hirsjärven ja Hurmeen (2001) kirjassa. Edellä kuvattu analysointiprosessi tuotti kahden ensimmäisen haastatte-

lun jälkeen muutamia tarkentavia kysymyksiä jäljellä oleviin haastatteluihin, jotka myöhemmin tarkasteltuna osoittautuivat erittäin hyväksi lisäksi tutkimuksen empiiriseen osuuteen.

Hirsjärven, Remeksen ja Sajavaaran (2008) mukaan ymmärtämiseen ja selittämiseen pyrkivässä lähestymistavassa käytetään päätelmien tekoa. Lisäksi kun kyseessä on laadullinen tutkimus, käytetään laadullista analyysiä, joka on tässä tapauksessa aiheiden teemoittelu ja käsitteiden tyypittely.

6 CASE-TUTKIMUS: TIETO OYJ:N PALVELUKESKUKSEN JATKUVUUDEN HALLINTA

Seuraavaksi käsitellään tutkielman empiiristä osuutta, teemahaastatteluin toteutettua case-tutkimusta Tieto Oyj:n palvelukeskuksen jatkuvuuden hallinnasta. Palvelukeskuksella tarkoitetaan usean tietokonekeskuksen tai konesalin muodostamaa infrastruktuuria, joissa asiakkaiden tietojärjestelmiä ylläpidetään. Palvelukeskuksen toiminnot ovat maantieteellisesti hajautettu eri sijainteihin. Palvelukeskuksen IT-infrastruktuurin operointi tapahtuu myös fyysisesti eri paikoissa, eli itse konesaleissa ei työntekijöitä juurikaan ole. Kyseessä on käyttöpalveluita tarjoava IT-palveluyritys, jonka konesalien toiminnasta monet kansainväliset ja suomalaiset, sekä yksityisen sektorin ja julkisen sektorin yritykset ovat riippuvaisia. Ensimmäiseksi käydään läpi kuvaus kohdeyritys Tieto Oyj:stä IT-palvelutoimittajana sekä haastateltavien taustat. Seuraavaksi kuvataan Tieto Oyj:n jatkuvuuden hallintaprosessi, kuvataan jatkuvuuden hallinnalla tavoiteltavat asiat ja pureudutaan tulevaisuuden haasteisiin jatkuvuuden hallinnassa. Tutkimuksen tulokset ja niiden analysointi esitetään seuraavassa luvussa Pohdinta ja tulokset (luku 7), jossa yhdistetään pohdintaan myös teoriaosuuden pohjalta tehtyjä huomioita.

6.1 Kohdeyritys Tieto Oyj:n ja haastateltavien tausta

Case-tutkimuksen kohteena oleva Tieto Oyj on suomalainen tietotekniikan palveluyhtiö, joka tarjoaa tietotekniikkaratkaisuja ja –palveluja niin kotimaassa, kuin kansainvälisestikin (Tieto, 2012d). Tiedon palveluksessa on maailmanlaajuisesti noin 18 000 henkilöä (Tieto, 2012d). Yksi Tiedon tarjoama palvelumuoto on konesalipalvelut, joihin tämä tutkielmakin keskittyy. Strategiassaan Tieto muotoilee, että Tiedon kilpailukyky perustuu laajaan toimialaosaamiseen (Tieto, 2012e); Tiedolle tärkeitä toimialoja ovat mm. finanssipalvelut, julkinen sektori ja terveydenhuolto, teollisuus ja vähittäiskauppa, sekä energia- ja sähköntuotanto

(Tieto 2012d). Tieto pyrkii keskittymään markkinoihin, joilla se voi olla kolmen vahvimman palvelutoimittajan joukossa (Tieto, 2012e). Seuraavissa Tiedon Internet-sivuilta kootuissa sitaateissa Tieto Oyj lupaa tarjoamiensa palvelujen jatkuvaa kehittämistä ja joustavuutta:

> Parhaan mahdollisen lopputuloksen saavuttamiseksi määrittelemme yhdessä palvelutasot, kustannukset ja laatutavoitteet, jotka vastaavat liiketoimintasi edellytyksiä. Koko palvelun elinkaaren ajan arvioimme, raportoimme ja parannamme jatkuvasti palvelutoimitusta, jotta olemme aina tarpeidesi ja vaatimustesi tasolla. (Tieto, 2012a).

> Tiedon ulkoistamispalveluiden avulla varmistamme prosessiesi, henkilöstösi ja tekniikkasi yhteensopivuuden. Liiketoiminnastasi tulee joustavampaa ja voit paremmin ennakoida ympäristön muutoksia ja jopa kääntää ne kilpailueduksesi. Jättämällä päivittäisten käyttötoimintojesi hallinnan meidän huoleksemme voit itse keskittyä paremmin olennaiseen - ydinliiketoimintaasi. (Tieto, 2012a).

Tieto lupaa toimittaa laadukkaita palveluita, joiden toimitusriskit ovat vähäiset (Tieto 2012d). Toimitusriskeihin liittyen Tiedon strategiassa mainitaan, että Tiedon Jatkuvat palvelut -yksikkö tuottaa kriittisiä palveluja yhteensä noin 800 asiakkaalle (Tieto 2012e). Case-tutkimuksen kohdeyrityksenä Tieto Oyj on monipuolinen tutkimuskohde juuri toimittamiensa ja ylläpitämiensä konesalipalveluiden kriittisyyden vuoksi.

Seuraavassa taulukossa esitetään case-tutkimuksessa haastateltujen henkilöiden taustatiedot, kuten asema ja toimenkuva Tieto Oyj:n organisaatiossa (taulukko 8).

TAULUKKO 8 Case-tutkimus: haastateltavien taustatiedot

Henkilö	**Titteli ja asema**	**Toimenkuva**
H1	Riskienhallinnan johtava tarkastaja Risk manager. Corporate Lead Auditor, CAE. Risk Management Security and Internal Audit	Riskienhallinnan arviointi ja auditointi.
H2	Tietoturvapäällikkö, Data Center, Data Center Services & Storage	Palvelukeskuksen fyysinen turvallisuus, kulunvalvonta, kameravalvonta, paloturvallisuus ja riskienhallinta
H3	Tietoturvapäällikkö, Global Security Manager, Certified Information Systems Auditor (CISA)	Globaali tietoturva ja palvelukeskuksen toiminnot
H4	Tietoturvapäällikkö, Security Manager Finland	Maakohtainen tietoturva, riskien arviointi, riskienhallinta
H5	Turvallisuusjohtaja, Chief Security Officer (CSO), organisaation ylin johto	Turvallisuusstrategia, jatkuvuuden hallinnan strategia, riskienhallintastrategia, turvallisuuden hallintajärjestelmä

Haastateltavien vastausten yhteydessä käytetään haastateltavasta jatkossa lyhenteitä (esim. H1), kuten taulukon 8 Henkilö-sarakkeessa on merkitty.

6.2 Tieto Oyj:n jatkuvuuden hallintaprosessi

Kuten palveluja tuotettaessa yleensäkin, myös IT-palveluliiketoiminnassa asiakas on se osapuoli, jolle palvelu tuotetaan ja toimitetaan. H2 täsmentää, että jatkuvuuden hallinta IT-palveluliiketoiminnassa on astetta tärkeämmässä asemassa, koska asiakkaiden liiketoiminta pyörii tietojärjestelmien varassa (palveluntarjoajan) konesaleissa. IT-palveluyrityksen oma jatkuvuuden hallintaprosessi tukee myös asiakkaiden liiketoiminnan tavoitteita. H1 määrittelee jatkuvuuden hallinnan erityisesti asiakkaiden palveluiden jatkuvuuden varmistamiseksi: jatkuvuus pitää varmistaa riippumatta siitä, mikä uhka tai riski jatkuvuutta uhkaa. H2:n mukaan tulee erottaa jatkuvuus ja saatavuus: jatkuvuus tulee ymmärtää palvelujen saatavuutena. Jatkuvuus on H2:n mukaan siis toiminnan jatkamista kaikissa tilanteissa, ja jatkuvuuden hallinnalla tarkoitetaan toiminnan turvaamista kaikissa mahdollisissa olosuhteissa, eli myös poikkeusolosuhteissa. H3 määrittelee jatkuvuuden hallinnan olevan palvelun toimittamista, jonka täytyy toimia. Jatkuvuuden hallinta mahdollistaa (kaiken) liiketoiminnan, H3 jatkaa. Tieto Oyj:n liiketoiminta on palveluliiketoimintaa, jonka periaatteena on se, että palvelun täytyy jatkua. H4 täsmentää jatkuvuuden hallinnan olevan sitä, että palvelut ovat mahdollisimman hyvin käytettävissä asiakkaalle. Tähän kuuluu H4:n mukaan se tavoite, että jos jotakin sattuu, häiriöistä aiheutuvat kulut olisivat pienet ja häiriöt eivät olisi niin syviä. ”Meidän tulee ymmärtää se, että kaikki rahat, millä palkat maksetaan, tulevat asiakkailta, joten asiakkaiden ostamat palvelut eivät saa keskeytyä”. (H5, 1.3.2012). H5 tiivistää, että jatkuvuuden hallinta on osa hyvän liiketoiminnan kulttuuria.

6.2.1 Jatkuvuuden hallinnan strategia

Jatkuvuuden hallinnan strategian taustalla pitää olla tietyt periaatteet ja periaatteiden pitää määritellä ne tavoitteet mihin jatkuvuuden hallinnalla pyritään, H1 sanoo. H4 on samaa mieltä: ”Liiketoimintastrategiassa on määritelty avaintavoitteet, niiden perusteella keskitytään oikeisiin osa-alueisiin mm. riskiarvioinnissa”. H1 painottaa myös, että periaatteena pitää toimia joku tai jotkut alan standardeista, hyödynnetään siis hyviksi havaittuja käytäntöjä. Näitä hyvien käytäntöjen malleja voivat H1:n mukaan olla esimerkiksi COBIT:n, ITIL:n tai ISF:n määrittelemät kontrollit jatkuvuuden hallintaan. Standardien sisältämät suuntaviivat määrittelevät sen, miten mikäkin asia tehdään, mutta nämä suuntaviivat voidaan tarkentaa vastaamaan juuri Tieto Oyj:n tarpeisiin, esimerkiksi jonkin tilan osalta, H1 kertoo. Pyritään tekemään standardiratkaisuja, jotka on todettu toimiviksi, H2 täsmentää. Näin toimittaessa palvelujen ylläpito ja toimivuus ovat parempaa luokkaa, H2 jatkaa. H2 kertoo, että toki spesiaaliratkai-

sujakin tehdään. Näissä erityisratkaisuissa täytyy muistaa se, että yleisesti ottaen mitä enemmän erityisratkaisuja, sitä enemmän ilmenee ongelmia ja ylläpito on myös vaikeampaa, H2 kertoo. Teknologioiden osalta kannattaa pyrkiä tunnettujen ja toimivien ratkaisujen ja laitteiden käyttämiseen, myös eri valmistajien ja toimittajien käyttäminen on hyödyllistä, jatkaa H2. Tieto Oyj:n jatkuvuuden hallinnan status quo – vallitsevat tilanteet voidaan jakaa kolmeen osaan: normaaliin häiriöttömään tilaan (engl. business as usual), varasuunnitelmiin ja toipumistilaan. H1 täsmentää varasuunnitelmien olevan sitä varten, jos normaalit käytänteet eivät toimi, lisäksi toipuminen on oma osansa. Nämä tilat ja niihin liittyvät toimenpiteet ja käytettävät dokumentit on koottu seuraavaan taulukkoon (taulukko 9).

TAULUKKO 9 Status Quo – liiketoiminnan tilat jatkuvuuden hallinnan kannalta

Vallitseva tilanne	**Normaalitila** Saatavuussuunnittelu – Plan A	**Varasuunnitelma** Jatkuvuussuunnittelu – Plan B	**Toipumistila** Toipumissuunnittelu – Plan C
Toimenpiteet	Riskien monitorointi, epätoivottujen tapahtumien ennaltaehkäisy, ennakkosuunnittelu	Kun liiketoimintaa ei voida jatkaa normaalisti, Plan B on vaihtoehtoinen tapa toimia	Epätoivotun tapahtuman tapahduttua liiketoiminnan nopea palauttaminen kohti normaalitilaa
Dokumentit	Riski- ja vaikutusarviot, jatkuvuuden harjoittelun raportit, suorituskykyindikaattorit	Jatkuvuussuunnitelmat ja kriisinhallinnan suunnitelmat	Toipumissuunnitelmat

H2 kommentoi yllä olevan taulukon mukaisesti vallitsevan tilanteen mukaista jakoa:

> Suunnittelun ja suunnitelmien jako kerroksellisesti kolmeen osaan, saatavuussuunnittelu (availability planning), sitten on jatkuvuussuunnittelu (continuity planning), joka on kuin plan b, eli miten toimitaan jos jotain tapahtuu ja ei voida toimia normaalisti. Toipumissuunnittelu (recovery planning) on astetta isompi kokonaisuus, joka kattaa sen jos tapahtuu aineellisia vahinkoja. (H2, 23.1.2012).

Johdon hyväksymä politiikka tai periaate määrittelee nämä kriittiset alueet, joihin jatkuvuussuunnitelma pitää tehdä, H3 kertoo. H3 täsmentää että raportointi johdon suuntaan on myös tärkeää, koska suunnitelmia pitää päivittää: Katsotaan kokonaisuutta ja nähdään nousevia asioita, kuten virtuaalialustat ja virtualisointi, mietitään mitä tiedetään uudesta tekniikasta ja teknologioista joita ollaan ottamassa käyttöön. Jatkuvuuden hallinnan periaatteita pitää myös tarkastella: toimintaa ohjaavaa politiikkaa päivitetään myös tietyin väliajoin, H3 jatkaa. H1 on samaa mieltä, ja toteaa, että koko prosessiin kuuluu toipumisen har-

joittelu ja oppimisvaihe, opitaan tapahtumista, jotka ovat sattuneet organisaation sisällä. Erilaisia suunnitelmia on siis useita. Suunnitelmia pyritään hallitsemaan siten, että lähdetään liikkeelle ylhäältä alas, H3 kertoo. Ylhäältä alas suuntauksella tarkoitetaan fokuksen keskittämistä ensin johtotasolla käsiteltäviin jatkuvuuden hallinnan periaatteisiin, ja sitten alaspäin kohti yksittäissuunnitelmia.

> Ensin on tehty konekeskuksen kokonaissuunnitelma ja todettiin, että tämä suunnitelma voi ottaa kantaa sekä varautumiseen ja toipumiseen. Siitä generoitui tehtäviä eri ryhmille tehdä tarkempia jatkuvuussuunnitelmia. Kun raamit oli tehty kokonaissuunnitelmassa, tiedettiin mitä tehdä tarkemmissa yksittäissuunnitelmissa. Pitää miettiä miten asiakkaiden suuntaan tiedonvaihto tietyssä tilanteessa tehdään, mutta asiakas kuvaa myös itse kriittisyysasteen omista järjestelmistään, koska he tuntevat omat järjestelmänsä parhaiten. (H3, 24.1.2012)

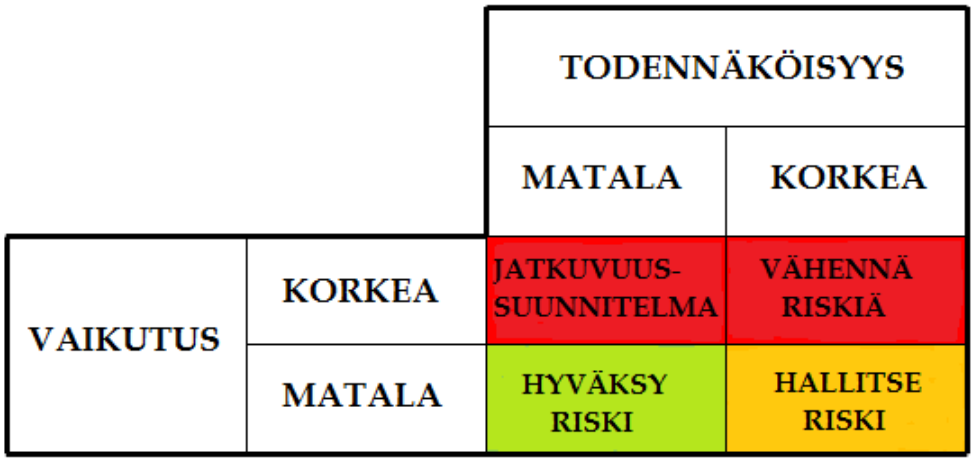
H4:n lisää, että alimmalta tasolta tulee tunnistaa riippuvuuksia ja tuoda ne seuraavalle tasolle. Riippuvuuksien tunnistamista tehdään riskiarvioinnin pohjalta, eri suunnitelmat eivät saa olla toisistaan riippumattomia, H4 sanoo.

6.2.2 Riskienhallinta, riskien ja vaikuttavuuden arviointi

Riskienhallinta on yksi riskin vähentämisen vaiheista, H1 sanoo. H2 näkee myös riskienhallinnan ja jatkuvuuden hallinnan limittyvän paljon toisiinsa. ”Riskienhallinta luo pohjan jatkuvuuden hallinnalle, koska jatkuvuutta ei voi suunnitella ellei tiedä toimintaan liittyviä riskejä”. (H2, 23.1.2012). H4:n mukaan riskiarviointi ja jatkuvuussuunnitelmat tehdään yksiköissä joissa kriittiset komponentit sijaitsevat: kokonaissuunnitelmat ovat erikseen ja komponenttitason suunnitelmat ovat erikseen. H3:n mukaan riskejä katsotaan kohteittain, lähdetään liikkeelle epätoivotusta tapahtumasta ja katsotaan syitä miksi niin voi käydä. Riskin todennäköisyyden arvioimista H3 pitää myös tärkeänä: sen avulla voidaan määritellä mikä on järkevä tarkastelutaso missäkin tilanteessa. H1:n mukaan riskianalyysi määrittelee riskit ja niiden todennäköisyydet. Riskejä pitää lähestyä myös vaikutusanalyysin kautta, H1 kertoo. Ensin pitää priorisoida suunnitelma miten riskejä käsitellään, sen jälkeen tehdään ja pohditaan erilaisia riskiskenaarioita, H1 jatkaa. Jokaiselle tunnistetulle uhkalle ja riskille pitää määritellä omistaja, joka on vastuussa riskin hallinnasta. Uhkalla H1 tarkoittaa tavoitteiden saavuttamisen estymistä jostakin syystä, silloin uhkaa voidaan käsitellä riskinä. Tavoitteet pitää olla johtotasolla selvät, H1 jatkaa. Tavoitteiden määrittelemisessä auttaa johtotasolla luotava riskipolitiikka. H1:n mukaan riskipolitiikassa pitää määritellä vaikutustasot: kun tietty vaikutustaso ylitetään, tulee luoda jatkuvuussuunnitelma. Vaikutustaso määräytyy taloudellisten vaikutusten mukaan: H1 täsmentää vaikutuksen määräytyvän usein riskin toteutuessa menetettävien eurojen mukaan. Taloudellisten asioiden lisäksi myös toipumiskyvyllä ja datan varmuuskopioiden palauttamisella on vaikutusta riskien kriittisyyteen. H1:n mukaan raha ei siis ole ainoa kriittisyyden mittari:

> Jos sulla on autoliikeyritys, sulla pitää olla vara-autoja, back-upin on joka tapauksessa toimittava, oli bisnes mitä tahansa. Rakenne voi siis olla samanlainen oli tuote tai palvelu minkälainen tahansa. Kaikki pitää pystyä palauttamaan. Mitä vaikeampaa palauttaminen on, sitä kriittisempää se on. (H1, 20.1.2012)

Joka tapauksessa kustannukset ohjaavat riskien kontrolloimista. H3 kertoo, että riskiarvioita tehtäessä ja suunniteltaessa keinoja riskien pienentämiseksi, täytyvät keinot olla järkevässä hintaluokassa. H1:n mukaan voidaan todeta, että mitä todennäköisempi riski on, sitä kriittisempi se on; viimekädessä kuitenkin riskin taloudelliset vaikutukset määräävät toimenpiteet. H3 toteaa myös, että Tieto Oyj:n jatkuvuuden hallinta ylipäätään on pysynyt hyvin liiketoiminnan määrittelemissä raameissa. Riskiskenaariot ovat tärkeässä roolissa, riskien hallitsemista harjoitellaan johto- ja palvelutasolla erikseen; riskien omistajat harjoittelevat omia skenaarioitaan, H1 huomauttaa. Tarkemmin määriteltynä strategisten liiketoimintayksiköiden johtajat joutuvat operationaalista suunnitelmaa tehdessään arvioimaan kaikki riskiluokat ja nimeämään kullekin riskille omistajan, H1 jatkaa. ”Jos riski aiheuttaa keskeytymisen, selvitetään onko siitä taloudellista haittaa itselle, asiakkaalle tai muuta haittaa, kuten haitat maineelle tai brändille”. (H1, 20.1.2012). Tieto Oyj:n mukaan jatkuvuussuunnittelun perustana on tunnistaa riskit, joiden todennäköisyys ei välttämättä ole suuri, mutta joiden potentiaaliset vaikutukset liiketoiminnalle ovat suuret. Tämä todennäköisyyden ja vaikutuksen arviointi on esitetty seuraavassa kuviossa (kuvio 7).



KUVIO 7 Riskin todennäköisyyden ja vaikutuksen arviointi

H1 kertoo, että vaikuttavuus- ja todennäköisyysmatriisissa oikea yläkulma käsitellään ensin. Oikea yläkulma tarkoittaa siis riskejä, joiden todennäköisyydet ja vaikutukset liiketoiminnalle ovat korkealla tasolla. Priorisointi auttaa vähentämään resurssien tarvetta poikkeustilanteen käsittelyssä. H3:n mukaan kriittisyyttä katsotaan komponenteittain. ”Eli mitä pitää olla, että palvelu toimisi minimitasolla. Jokin asia mikä vaikuttaa suureen osaan asiakkaita on kriittisintä”.

(H3, 24.1.2012). ”Pitää myös muistaa, että on myös olemassa tukiprosesseja, jotka ovat välttämättömiä meille, mutta joiden puuttumista asiakas ei heti huomaa, näissä rajoissa prosessien prioriteetteja voidaan siis hieman määritellä”. (H3, 24.1.2012). Kriittisintä ovat siis asiakkaisiin vaikuttavat riskit; tukiprosessien tapauksessa liikkumavaraa on hieman enemmän. H3 muistuttaa, että riskien vähentäminen varajärjestelyin ei aina poista riskiä kokonaan:

> Tiedetään että on tehty jo riskien ja uhkien varalle varajärjestelyjä, mutta tietysti valmiitkin kontrollit voivat pettää. Haasteellisinta on päästä oikeisiin euromääriin riskien vaikutuksia arvioitaessa. Tiedetään, että jokin tapahtuma voi aiheuttaa isot vahingot, mutta vahinkojen euromääräinen taso on vaikeaa määritellä. Siihen päästään rutiinien kautta. (H3, 24.1.2012).

H4 kuvaa riskien arviointia siten, että tunnistetaan omat kohteet ja omaisuus ja niiden kriittisyys, tehdään riskiarvio, ja siltä pohjalta määritetään toimenpiteet: riskien hyväksyminen tai riskien pienennys. On uhkia, jotka ovat erittäin epätodennäköisiä, mutta toteutuessaan kriittisiä ja joiden poistaminen on kallista. Niiden käsittelyyn liittyvät päätökset voivat olla vaikeita, H4 jatkaa.

> Ongelma on siinä, että järjestelmät ja palvelut tulevat yhä mutkikkaammiksi, integraatio kasvaa, uhkia ja yllättäviä riskiketjuja löytyy. Kombinaatiot on otettava huomioon, mutta se on työlästä ja jää usein vähemmälle. Tärkeää on keskeisten komponenttien huomioiminen, jotka vaikuttavat monen asiakkaan prosesseihin yhtäaikaisesti. Tämä on ylläpidon kannalta haasteellista. (H4, 30.1.2012).

Pitää pystyä arvioimaan riskin vaikutusta ja todennäköisyyttä ja verrata sitä kustannuksiin, H4 sanoo. Kustannukset ovat riskin pienentämisestä tai poistamisesta aiheutuvia kustannuksia, joita siis verrataan riskin aiheuttamiin vaikutuksiin sen toteutuessa.

6.3 Palvelukeskus ja IT-infrastruktuuri

Kriittisyyttä arvioitaessa pitää huomioida miten häiriön aiheuttama katko vaikuttaa liiketoimintaan, eli kuinka kauan liiketoiminta pärjää ilman jotain komponenttia tai järjestelmää, H4 sanoo. Silloin infrastruktuurin häiriönsietokyky ja toipuminen normaalitilaan ovat avainasemassa: ratkaisuna ovat komponenttien kahdennukset ja palautumismenettelyt, H4 kertoo. H2 täsmentää, että tietojärjestelmät voidaan jakaa kriittisiin ja erittäin kriittisiin. Jatkuvuuden varmistaminen on erittäin tärkeää, koska useilla tietojärjestelmillä on erittäin korkeat asiakasvaatimukset toimivuuden ja käytettävyyden kannalta, H2 jatkaa.

> Tavoitteena on palvelun häiriöttömän saatavuuden varmistaminen. Kokonaissuunnitelmatasolla pitää olla kaikki tieto tallessa, jotta toimintaa pystytään jatkamaan, vaikka täysin nollasta. Hinta määräytyy SLA:n perusteella. Asiakkaan pitää pystyä tunnistamaan omien järjestelmiensä kriittisyys- ja saatavuusvaatimukset, jota kautta SLA tarkemmin määräytyy. (H4, 30.1.2012).

H1 painottaa, että tekninen infrastruktuuri tulee yhä monimutkaisemmaksi, virtualisointi lisääntyy ja kaikki järjestelmät eivät pysy teknologian kehityksessä mukana. Tietokonekeskuksen valvomon kautta nähdään alueittain, millä alueella mikäkin toiminto on, H1 selventää.

> Vikojen paikallistaminen ei todellakaan saa kestää. Selvityksen täytyy tulla ASAP. Vuorokauden yli ei saada mennä missään tapauksessa. Syyn selvittämiseen menee oma aikansa, mutta korjaavat toimenpiteet ovat kriittisimpiä, jotta palvelut saadaan ylös. (H1, 20.1.2012).

H2 selvittää, että vikojen paikallistaminen voi olla erittäin haastavaa vaikeaa: tarvittaessa eri asiantuntijaryhmiä otetaan mukaan ongelmien selvittelyyn ja sitä kautta pyritään selvittämään ongelmien perimmäinen syy. Sitten katsotaan voidaanko asialle tehdä jotakin. Tämä tehdään jokaisen ongelmatilanteen yhteydessä riippuen hieman ongelman tasosta. Ulkopuolisiakin asiantuntijoita voidaan käyttää apuna, esimerkiksi laitetoimittajia tai muita asiantuntijoita, H2 kertoo. Häiriöt voidaan jakaa eri tasoihin asiakkaalle aiheutuvien vaikutuksien mukaisesti: tasolla 1 häiriöt eivät aiheuta vahinkoa asiakkaalle, tasolla 2 aiheutuu joitakin vahinkoja ja tasolla 3 aiheutuu merkittävää vahinkoa, H2 selvittää. Seuraavassa taulukossa tiivistetään palvelukeskuksen vikatilanteiden häiriötasot (taulukko 10).

TAULUKKO 10 Häiriötasot palvelukeskuksen vikatilanteissa

Häiriötaso	**Vahinkojen laajuus**	**Toimenpiteet**	**Osapuolet**
Taso 1	Ei vahinkoa asiakkaalle	Sisäinen raportti ja selvitys	Sisäiset asiantuntijat ja palvelukeskuksen henkilöstö
Taso 2	Joitakin vahinkoja asiakkaalle	Raportti sisäisesti ja asiakkaalle	Asiakkaan edustajat, sisäiset asiantuntijat, tarvittaessa laitetoimittajan asiantuntijoita
Taso 3	Merkittävää vahinkoa asiakkaalle	Virallinen loppuraportti sisäisesti ja asiakkaalle	Asiakkaan edustaja, apuna laitetoimittajat, muut asiantuntijat ja asiantuntijaryhmät

> Isoimpien ongelmien ilmetessä tehdään viralliset loppuraportit. Koko oppimisprosessia seurataan auditointeja tehtäessä ja asiakkaiden tarkastusten yhteydessä. Raportointi sovitaan asiakaskohtaisesti, jotkut vaativat järjestelmien raportointia jopa päivittäin, jotkut kuukausi- ja jotkut vuositasolla. Raporttien sisältö vaihtelee paljon. Joillekin (asiakkaille) riittää pelkät häiriöiden kestot, toisille selvitetään myös se, mikä häiriön aiheutti. (H2, 23.1.2012).

H2 jatkaa, että usein palvelutasosopimuksiin on kirjattu rahallisten sanktioiden mahdollisuus, mikäli sopimuksiin liittyvät vaatimukset eivät täyty. Lisäksi tehdään paljon yhteistyötä asiakkaan kanssa ja pyritään korjaamaan mahdolliset epäkohdat palvelun toimittamisessa. Palvelun toimivuutta seurataan eri mittareilla, jolloin on mahdollista puuttua palvelun laatuun, mikäli se lähestyy palveluvaatimusten reunaehtoja tai ei vastaa sovittua, H2 kertoo.

Isoimmilla virtuaaliympäristöjen tuottajilla on tarkat kuvaukset järjestelmistään, meillä pitää olla yhtä hyvät omistamme, H1 painottaa. Virtualisointi ja pilvipalvelut ovat ajankohtainen aihe:

> Pilvipalveluiden hinnoittelu- ja korvausmalli on erilainen kuin perinteisen data centerin. Korvaukset perustuvat usein menetettyyn päivähintaan, mikä ei ole rahallinen riski palvelun tuottajalle, mutta voi olla iso tahra maineeseen. Sellaista, mitä ei voida menettää, ei voida laittaa pilveen. (H1, 20.1.2012).

H2 kertoo, että samoja järjestelmiä pitää kahdentaa ja rakentaa kahteen eri paikkaan. Kriittiset järjestelmät tulee sijaita konesalin sisällä vähintään kahdessa eri palo-osastossa.

> Laitteiden tiedot syötetään ylös, myös fyysinen sijainti merkitään. Jos yksittäinen laite on erittäin kriittinen, varmistetaan kaavion avulla, missä yhteydessä laite on toisiin laitteisiin. Kahdennus lähtee siitä, että laitteeseen pitää olla mahdollista vetää kaksi sähkönsyöttöä ja kaksi tietoliikenneyhteyttä. Virtuaaliympäristön kriittiset elementit tai laitteet on syytä fyysisesti kahdentaa ja varmistaa, että kriittisen järjestelmän tai ohjelman varajärjestelmä on toisessa virtuaaliympäristössä, joka fyysisesti sijaitsee eri tilassa kuin varsinainen toiminto. (H2, 23.1.2012).

H2 täsmentää, että vaatimukset tulevat asiakkaalta päin, eli minkä ajan kuluessa pitää pystyä palauttamaan kukin järjestelmä. H1 tarkentaa, että kahdennuksen keskiössä on ”cost-benefit”-ajattelu, pitää pystyä toteamaan missä vaiheessa hyödyt selkeästi voittavat kustannukset. ”Sertifiointia ei tehdä sertifioinnin takia, vaan se tuo sinulle lisää asiakkaita”, H1 huomauttaa. Komponenttien kahdennustakaan ei siis tehdä vain kahdennuksen takia, korostaa H1. Sama asia toimii myös standardien kohdalla: kun tehdään standardien mukaan, se on jo eräänlainen riskivakuutus, H1 lisää. Kahdennuksesta puhuttaessa H2 huomauttaa, että kustannus riippuu täysin komponentista:

> Kaksi erillistä palvelinta eivät ole kalliita, mutta heti kun ”ketjua” viedään pidemmälle, tulee se kalliimmaksi. Esimerkiksi varavoima ketjun toisessa päässä on kalliimpaa, hot site – hot site ratkaisua voidaan pitää maksimivarmistuksena mitä kannattaa toteuttaa. (H2, 23.1.2012).

H3 kertoo, että järjestelmä voidaan kahdentaa, kolminkertaistaa ja niin edelleen. ”Se maksaa, ja asiakkaan on ymmärrettävä se, että varmennettua järjestelmää ei saa yhden hinnalla”. (H3, 24.1.2012). Täytyy nojata kokemukseen ja laitetoimittajien lupauksiin miten toimintavarmoja jotkin laitteistot ovat: mitä enemmän kompleksisuus kasvaa, sitä enemmän riskejä siihen myös vaikuttaa, H3 tiivistää. H2:n mukaan järjestelmät pyritään rakentamaan niin, jotta pysty-

tään toteuttamaan toipumispistetavoitteiden ja toipumisaikatavoitteiden vaatimukset. Toipumisen edistämisessä merkittävässä osassa ovat varmuuskopiot ja niiden palauttaminen. Peilaaminen (sama data kahteen eri paikkaan) on ensisijainen vaihtoehto, jos data on kriittistä, H1 sanoo. Tämä on kuitenkin samalla kalleinta tekniikkaa ja perinteisilläkin menetelmillä pärjätään, jos data vaihtuu harvakseltaan, kertoo H1. ”Asiakas päättää millaista turvaa haluaa ja vaatii, sen mukaan mennään”. (H1, 20.1.2012).

> SLA määrittelee sen mitä asiakas vaatii. Täytyy muistaa että, ei ole täysin varmaa keinoa varmistukseen. Tulee harjoitella. Mitä tahansa uutta, etenkin teknologiaa otetaan käyttöön tai asennetaan, sitä pitää testata riittävästi. Kuinka herkkiä ne ovat data center ympäristölle, esimerkiksi lämmityksen ja sähkönsyötön stabiilius pitää varmistaa ennen kuin laitteet otetaan käyttöön. Infra pitää tarkistaa puolen vuoden välein, tulee harjoitella puolen vuoden välein, tulee tehdä auditointi vuoden välein, sekä tiimien testaaminen pistokokein miten harjoitukset ovat menneet. Aivan kuten palolaitoskin harjoittelee. (H1, 20.1.2012).

> Pitkän aikavälin suunnitelmissa on otettava huomioon, millainen tuotantoalusta on nyt, mitkä ovat stepit sen kehittämisessä niin että redundanttisuus säilyy. Suunnitelmallista, pitkäjänteistä työtä, asiakkaat haluavat uusia ratkaisuja, ne pitää testata. (H5, 1.3.2012).

Konesaleissa pitää hallita koko kustannuspaletti – suorat ja epäsuorat vaikutukset, niitä suhteutetaan siihen kuinka paljon kannattaa sijoittaa esim. sähkökatkoihin varautumiseen, H5 kertoo. ”Ensin tehdään BIA – jos jotain oikeasta ylälaatikosta (suuri todennäköisyys, suuret häiriökustannukset) voidaan pienentää riskiä järkevässä hintaluokassa, se tehdään”. (H5, 1.3.2012). Jatkuvuuden hallinta on osa normaalia liiketoimintaa, joka tehdään siinä vaiheessa kun palvelua suunnitellaan: ei luoda ensin palvelua ja sitten mietitä jatkuvuutta, H5 täsmentää. ”Osa ohjeistuksien minivaatimuksista ei riitä meille, joten me olemme sijoittaneet varmistamiseen enemmän rahaa. Silloin kun on järkevää, varmistetaan vaatimuksien yli”. (H5, 1.3.2012).

> Asiakas tekee valinnan kustannusten perusteella, miten pitkälle varmistamisessa mennään. Nämä asiat liittyvät riskienhallintaan ja auditointeihin, joissa tulee esiin asioita joko omasta tai ulkopuolisen näkökulmasta. Asioita selviää myös ongelmatilanteiden kautta. Piilevänä voi olla montakin asiaa, mutta ne ilmenevät vasta ongelmien yhteydessä. (H2, 23.1.2012).

Erilaisia testauksia, harjoituksia, sisäisiä ja ulkopuolisten tarkastuksia tai auditointeja tehdään jatkuvasti toiminnan aikana, ja niiden yhteydessä esiin tulleet havainnot käydään läpi, tarvittaessa sitten tehdään muutoksia toimintaan, H2 kertoo. H1 täsmentää, että toipumispiste- ja toipumisaikatavoitteiden pitää ohjata toiminnan kehittämistä ja häiriöttömyyden edistämistä:

> Kun SLA päivitetään, joka on suunnittelun pohjalla, pitää tarkistaa onko asiat kunnossa. Selkeät roolit ja vastuut pitää pysyä yllä, vaikka tapahtuisi muutoksia organisaatiossa. Selkeät portfoliot joiden edistymistä seurataan. Kokoonpanon hallintajär-

> jestelmään viedään historia tapahtumista, jossa häiriölokit ovat. Se on kaikkein vaikein osasto hallita. Pilvipalveluiden vaatimukset tulee ottaa huomioon uusia järjestelmiä kehitettäessä. (H1, 20.1.2012).

Henkilökunnan ja tiimien auditoinnissa katsotaan miten monitorointi on järjestetty, tietääkö kukin roolinsa ja vastuunsa seurannassa, H1 tiivistää. Silloin työnkuvaukset ja palvelutasosopimukset katsotaan läpi, H1 jatkaa. H5:n mukaan katsotaan, että suunnitelmat ovat olemassa ja niitä harjoitellaan, etsitään single point of failure -tyyppisiä kohtia, jotka täytyy eliminoida pois. Oppiminen oikeista tapahtumista (ja niiden perimmäisen syyn selvittäminen (engl. root-cause analyysi) on tietysti myös osa arviointikokonaisuutta. Tarkempi harjoitusohjelma voidaan rakentaa seuraavasti:

> Konsernin riskienhallinta tekee ehdotuksen harjoitusaiheista, joista valitaan IMT-jäseniä eniten kiinnostavat/tärkeät. Alkuperäisellä listalla voi olla esimerkiksi 20 aihetta, joista toteutetaan viisi. Sitten harjoitellaan aiheet liiketoimintayksiköissä, jolloin pitää olla paikalla ne henkilöt, jotka oikeassakin tilanteessa osallistuisivat toimintaan. Valmiiksi kirjoitettua skenaariota eskaloidaan vaihe vaiheelta ja harjoituksen osallistuvat arvioivat miten tilanne kehittyy eteenpäin, ketä henkilöitä tai mitä resursseja tarvitaan lisää asian hoitamiseen ja kommunikointiin. Erillisiä kriisiviestintäharjoituksia pidetään myös, jolloin ulkopuolisia tahoja on myös mukana. (H5, 1.3.2012).

6.4 Liiketoiminnan näkökulma

Sertifiointi on organisaation yksi tapa vakuuttaa asiakkaat liiketoiminnan järjestelmällisyydestä: ISO-standardin mukaista sertifiointia on konsernissa tehty 90-luvun alkupuolelta lähtien, H5 sanoo. Sille on ollut myös asiakaskysyntää (sertifioitu järjestelmä on saattanut olla jopa tarjouksen jättämisen edellytys). H5 tiivistää, että sertifiointi sinänsä on suoraviivainen asia: joko täytät vaatimukset, tai on hyvä ja sertifiointielimelle kelpaava selitys miksi vaatimusta ei täytetä tai voida soveltaa. ”Standardeja rupeaa olemaan jo, mutta emme tiedä, onko DNV:llä (Det Norske Veritas) olemassa jo jatkuvuuden hallinnan sertifiointimalli, siitä voitaisiin olla kiinnostuneita”. (H5, 1.3.2012).

> Sertifiointi on verifiointi ulkopuolista standardia vastaan, eli onko huomioitu asiat riittävällä tarkkuudella. Jos sertifiointimahdollisuus on, sitä on pyritty myös hyödyntämään, koska ulkopuolisen tahon tekemä arviointi kokemuksen mukaan voi parantaa omia prosesseja. (H5, 1.3.2012).

Konsernin sisäisesti jatkuvuuden hallinnan kustannusten suhde liiketoimintaan on selvä, ne ovat täysin normaaleja kuluja, eivät ylimääräisiä menoeriä:

> Perussääntö on se, että kuka omistaa bisneksen, omistaa bisneksen jatkuvuuden hallinnan – konsernilta tulee templatet, pohjat ja se järjestää harjoitukset, vastuu toteu-

> tuksesta on yksiköillä. Jatkuvuuden hallinnasta aiheutuvat kulut ovat normaaleja liikekuluja yksiköille. (H5, 1.3.2012).

Liiketoimintayksiköiden vastuulla on teknisten yksityiskohtien katsominen, joihin tietysti kohdistetaan tarkastuksia ja pidetään harjoituksia, H5 kertoo. ”Kun siirretään virtualisointialustalle jotakin toiminnallisuutta, teknisillä asiantuntijoilla on viimekäden tieto siitä, onko tapauksessa huomioitu kaikki mahdollinen”. (H5, 1.3.2012). Asiakkaan suuntaan liiketoiminnan jatkuvuuden hallintaan liittyy olennaisesti palvelutasosopimus, jossa asiakas ja palveluntoimittaja sopivat palvelun tarkoista ehdoista. H2 tarkentaa, että palvelutasosopimuksen ehdot ohjaavat ja asettavat rajat palvelutoimittajan toiminnalle. H1 täsmentää, että tarkat ehdot on sovittu palvelutasosopimuksessa erittäin tarkkaan, palvelukatkojen kohdalla kriittisimmillään voidaan puhua jopa minuutin tarkkuudesta. Esimerkkeinä H1 nostaa esiin finanssialan ja paperiteollisuuden, jo pienikin katko maksaa paljon. ”Se maksaa myös sisäisesti, jos työtä ei pystytä tekemään”. (H1, 20.1.2012). Tarjousta mietittäessä arvioidaan vaikeusaste, tietyt palvelutasot ja tietyt vaatimukset, H4 kertoo. Palvelutasosopimuksen vaikeusasteeseen vaikuttaa H2:n mukaan tarjouspyyntövaiheessa tehty arviointi: tarjouspyyntövaiheessa tehdään arviointi, että minkälaista järjestelmää kuhunkin tilanteeseen kannattaa tarjota. ”Liiketoiminnassa tapauskohtaisesti ja aikaisempien myynticasejen avulla nähdään milloin palvelu alkaa olla liian vaikeaa toteuttaa”. (H4, 30.1.2012).

> Palvelutason ja palvelun laadun mittaaminen on erilaista. Palvelutason mittaamista tehdään prosessiauditointien kautta, jotka antavat kuvan siitä miten hyvin toimitaan. Suorituskykyindikaattorit kuvaavat prosessien toimintaa, myös jatkuvuuden hallintaprosesseille on omat mittarinsa. Selvitetään asioita kuten ovatko suunnitelmat olemassa, ovatko ne päivitetty vaatimusten mukaan jne. Käytettävyyden mittaaminen, oliko palvelu asiakkaan käytettävissä niin kuin piti. (H3, 24.1.2012).

H3 näkee jatkuvuuden hallinnan tärkeäksi asiaksi liiketoiminnan kannalta resurssien saamisen, jotta on riittävästi ihmisiä ajattelemassa asioita ja tekemässä suunnitelmia, jotta ne olisivat hyviä ja hyödyllisiä tositilanteessa. Tärkeää on myös tekninen ymmärrys, uusien ratkaisujen ja menettelytapojen löytäminen sekä teknisessä, että prosessimielessä, H3 jatkaa. Haasteena on jatkuvuuden hallinnan kustannusten perusteleminen sisäisesti:

> Liiketoiminnan kannalta jatkuvuuden turvaamisen halutaan olevan edullista. Pitäisi pystyä laskemaan ja näyttää toteen ei vain ne mahdolliset tappiot, vaan myös mahdollinen etu ja hyöty. Asioiden esittämistaito, jossa on liiketaloudellinen laskelma taustalla – siinä pitäisi pystyä parantamaan. (H3, 24.1.2012).

Myös H2:n mielestä resurssit ovat tärkeä asia. ”Pitää olla riittävästi resursseja ja ne pitää suunnata oikealla tavalla” H2 kertoo. Tärkeää on myös asiakasvaatimusten seuraaminen, jotta ne pystytään täyttämään. ”Voidaan sanoa, että kaikkein kriittisimmän järjestelmän varmistuksien toteuttaminen tuo pohjan tyyty-

väisyydelle: se kun pystytään toteuttamaan, yleensä kaikki osapuolet ovat tyytyväisiä" H2 jatkaa. IT-palveluliiketoiminnassa asiakkaan vaatimuksilla ja odotuksilla on suuri merkitys:

> Asiakkaan täytyy itse määritellä kriittisyys, asiakas yleensä tietää ja osaa sanoa mikä heille on tärkeintä. Täytyy lähteä siitä, että jos jokin järjestelmä ei ole käytettävissä 10 minuuttiin tai tuntiin, mitä tapahtuu asiakkaalle. Asiakas miettii onko olemassa jotakin vaihtoehtoista tapaa toimia. (H2, 23.1.2012).

"Jos jonkin tietojärjestelmän toimimattomuuden takia vahingot ovat tunnissa miljoonaluokkaa ja varautuminen maksaisi satatuhatta, edut ovat selvät". (H2 23.1.2012). Näkökulma jatkuvuuden hallintaan on siirtynyt välttämättömästä tehtävästä kohti markkinoilla toimimisen edellytystä:

> Fokus on siirtynyt enemmän kilpailutekijöiden puolelle. Nykyään asiakkaat osaavat kysyä enemmän ja haluavat itse tarkastaa järjestelyt. Iso kysymys on, että miten perustellaan kahdennetun järjestelmän tarpeellisuus asiakkaalle. Jos kaupan kassajärjestelmä ei toimi, sillä on välitön suora vaikutus asiakkaalle ja meille. Jos käytettävyysvaatimus on >99.99... %, sitä ei voi toteuttaa muuta kuin kahdentamalla. (H5, 1.3.2012)

H4 on samoilla linjoilla, kriittisintä on se mitä asiakas itse odottaa, ja kaikki prosessit miltä asiakas odottaa häiriöttömyyttä. Tavoitteena on asiakkaan vaatimusten täyttäminen. H2 lisää, että asiakkaan tulee määritellä järjestelmien kriittisyys ja palvelun toimittamisen reunaehdot, esimerkiksi hyväksyttävien palvelukatkojen kestot ja määrät kuukausi- tai vuositasolla. Määriteltyjen aikarajojen ylittämisestä seuraa tietysti sanktioita. H1 kertoo, että sanktiot määritellään järjestelmien alhaallaoloajan mukaisesti. Riski maksaa siis asiakkaalle vakuutuksen muodossa ja viimekädessä palvelutasosopimuksen vaikeusaste määrittelee hinnan, toki riskiä jaetaan myös vakuutusyhtiön kanssa, jatkaa H1.

Kysyttäessä liiketoimintamallien globaalistumisesta, tarkemmin määriteltynä alihankinnan ja tuotannon siirtämisestä edullisemman kustannustason maihin, H4 kertoo jatkuvuuden hallinnan kannalta keskiössä olevan etukäteen tehtävä varmistaminen. Jatkuvuusriski syntyy, jos kohdemaassa työtä ei syystä tai toisesta pystytä jatkamaan. H3 kertoo, että valvontatehtävät ovat pitkälle siirrettyjä, jos ko. maassa työnteko estyy, ongelmaa ei välttämättä havaita niin nopeasti, kuin normaalitilanteessa havaittaisiin, mutta tähänkin on varauduttu jatkuvuussuunnitelmien avulla.

> Yleensä oletetaan että tämän kaltaiset katkot ovat lyhyitä, mutta jos ne ovat pitkiä, yritetään kuljettaa henkilöstöä Suomeen. Se toimii myös toisinpäin, Suomesta muualle. Jos työntekijöiden siirtäminenkään ei onnistu, sitten pitää miettiä alihankinnan käyttämisen mahdollisuutta ja henkilöstön siirtämistä muista tehtävistä. Tämä on riski johon pitää varautua. (H3, 24.1.2012).

H3 täydentää, että jokaisessa konesalipaikassa täytyy olla tietty perusosaaminen. H4 muistuttaa myös, että on olemassa omat mallit, joiden avulla palveluita tuotetaan kauempaa. Tietoliikenne yms. olosuhteet varmistetaan etukä-

teen. ”Toiminnan hajauttaminen toimii myös etuna, palveluja pitää pystyä tuottamaan monesta paikasta”. (H4, 30.1.2012). Myös H5:n mielestä globaaliin toimitusmalliin liittyy riskejä, mutta se voi toimia tietyissä tilanteissa myös kontrollina, aivan kuten H4 huomautti:

> Kyllähän siihen liittyy, mutta globaali malli toimii riskin kontrollina – jos ollaan yhdestä toimipisteestä riippuvainen, silloin työtä ei pystytä jatkamaan. Globaalissa mallissa on mahdollista tehdä työtä muualtakin. Pitää vain varmistaa, että työn tekeminen on oikeasti mahdollista. EU rajojen ylittäminen voi aiheuttaa lakirajoitteita tiedon siirtämiseen tai sopimusrajoitteita. (H5, 1.3.2012).

Toki monikulttuurinen ympäristö vaatii tietysti oman vaivansa, kuten yhteistyön varmistamisen ja erilaisten tapojen yhdistämisen, kertoo H4. ”Eri aikavyöhykkeet mahdollistavat palvelun tuottamisen 24/7 mallilla, se helpottaa organisoimista”. (H4, 30.1.2012). ”Aikavyöhykkeitä hyödynnettäessä ihmiset voivat hoitaa tehtäviä normaalina työaikanaan, mikä parantaa työviihtyvyyttä ja työtehokkuutta. Tarkkuutta vaativa valvomotoiminta on tästä hyvä esimerkki”. (H5, 1.3.2012). Aikavyöhykkeet mahdollistavat siis työnteon normaaleina työaikoina, joka ei olisi mahdollista vain yhdellä aikavyöhykkeellä toimittaessa.

> Data pidetään siinä maassa missä asiakaskin on, jos asiakas ei muuta erityisesti halua. Asiakkaita ja konesaleja kun on monessa maassa. Valvomotoimintaa tehdään etänä asiakkaan suostumuksella. Työvoimakustannukset ovat near-shore tai off-shore – maissa edullisemmat ja pohjoismaista voi olla hankala saada syväosaajia tekemään vuorotyötä. (H5, 1.3.2012).

H3:n mukaan tuotettaessa palveluita kaukaa on muistettava varavoiman käyttö, hyvä dokumentaatio, vaihtoehtoiset toimintatavat, paikkasidonnaisuuden vähentäminen ja yhteyksien muodostaminen, jotta tiedetään mitä pitää tehdä. Alihankinnassa on nähtävissä samoja piirteitä jatkuvuuden kannalta, kuin tuotettaessa palveluja kaukaa. Toimintaa voidaan varmistaa muun muassa alihankkijoiden kanssa tehtävien sopimusten kautta, kertoo H2.

> Heidän pitää osata toimia tietyllä tavalla. Pitää olla varakomponentteja ja henkilöstöä saatavilla, ja myös kaikki pitää saada tietyssä ajassa paikanpäälle. Yrityksen tai palveluntoimittajan oma varautuminen ja suunnittelu poikkeustilanteiden varalta on tärkeää. Lisäksi täytyy huolehtia mahdollisten alihankkijoiden alihankintasopimuksiin tarpeelliset ehdot turvaamaan varautuminen poikkeusolosuhteisiin.

H2 määrittelee tarkemmiksi ehdoiksi esimerkiksi vasteajat, resurssien määrän ja varaosien saatavuuden. Jatkuvuuden hallinnan osalta alihankintaa koskevat samat lainalaisuudet, kuin emoyritystäkin: H2:n mukaan varmistukset tulee tehdä riittävän usein, palautuksien toimivuus tulee tarkistaa ja varman päälle otettaessa datan sijoittaminen fyysisesti kahteen eri paikkaan. H2 muistuttaa, että tarvittaessa dataa voidaan säilyttää myös eri muodoissa. H1 kuitenkin huomauttaa, että aina ei voi syyttää laitteistoa: ”Osittain häiriöt johtuvat inhimillisistä tekijöistä, kuten huolimattomuudesta – niitä varten on omat vakuutuksensa”. (H1, 20.1.2012). Palvelukeskuksen fyysisellä sijainnilla koetaan ole-

van merkitystä, riippuen hieman asiakaskunnasta, määrittelee H4. H3 näkee myös palvelukeskuksen sijainnilla olevan merkitystä:

> On merkitystä asiakkaiden vaatimuksissa. On tilanteita jolloin konesalin täytyy sijaita samassa maassa kuin missä asiakas toimii. Yleisesti ottaen turvallisuus luonnonilmiöitä vastaan on Suomessa hyvä, näyttää että Suomi on vakaa tässä suhteessa. Tietynlainen maantieteellinen syrjäisyys tai huomaamattomuus maailmanmittakaavassa on Suomelle myös etu. (H3, 24.1.2012).

Fyysisen sijainnin merkitys kasvaa valtionhallinnollisten järjestelmien ylläpitämisessä, kertoo H4.

6.5 Lainsäädännön vaikutukset jatkuvuuden hallintaan IT-palveluliiketoiminnassa

Lainsäädännössä velvoitetaan hoitamaan tietoturvan säilyminen, datan anonyymiys ja häviäminen ja varmuuskopiointi, H1 kertoo. H2 kertoo asiakasseurannan, ohjeistuksien ja suosituksien lisääntyvän koko ajan. Tätä kompleksisuutta ei voida pitää pelkästään huonona asiana, sillä H2:n mukaan alalla olevat pohjakriteerit asettavat palvelutoimittajat samalle viivalle.

Suoraan meidän toimintaamme vaikuttavaa lainsäädäntöä on melko vähän, mutta esimerkiksi tietokonekeskusten rakentamisvaiheessa vaikuttavia ohjeistuksia ovat rakennusmääräykset ja paloturvallisuusmääräykset, toimintaan vaikuttaa tietoliikenteeseen ja tietojenkäsittelyyn liittyvät määräykset, H2 listaa. ”Erilaisia ohjeistuksia ja suosituksia, sekä asiakaskohtaisia sopimusvaatimuksia on sitten runsaammin eri tahoilta”. (H2, 23.1.2012). H1 lisää, että huomioon on otettava myös kulunvalvonta ja yleinen turvallisuus. ”Välillinen vaikutus jatkuvuuden hallintaan on siis olemassa”. (H1, 20.1.2012). Valtionhallinnon ja vakuutusyhtiöiden ohjeistukset tulee ottaa huomioon: ohjeistukset koskevat esimerkiksi henkilörekisterien käyttöä ja edellä mainittua kulunvalvontaa, paloturvallisuutta ja rakentamismääräyksiä, selvittää H2. Yhteiskunnan huoltovarmuus näkyy vaatimuksissa: ”Valtionhallinto, finanssiala ja teollisuus ovat yhteiskunnan toimivuuden kannalta tärkeitä instansseja”. (H2, 23.1.2012). ”Palveluntoimittajana olemme sitoutuneet/sertifioineet toimintaamme erilaisia standardeja vastaan ja sitä kautta sitoutuneet tiettyihin velvoitteisiin”. (H5, 1.3.2012). Standardeista haetaan perustasoa, joista noudatetaan ainakin ISO:n ja ISF:n hyviä käytänteitä, H2 kertoo.

Välillisesti vaikuttavia ohjeistuksia on useita. Tärkeimpinä voidaan mainita finanssialan ja viestintäviraston säädökset, myös USA:n liittovaltion säätämä Sarbanes-Oxley – laki (myöh. SOx) mm. finanssidatan käsittelystä vuodelta 2002 vaikuttaa asiakasyritysten kautta palvelutoimittajaan. ”Asiakkaan puolelta toimintaa ohjaavat turvallisuuskäytänteet, asiakkaat tekevät omat suunnitelmansa ja palvelutoimittajana nivoudutaan niihin”. (H2, 23.1.2012). H3:n mukaan lainsäädäntö vaikuttaa ainakin asiakkaisiin ja välillisesti myös Tietoon, eli

miten turvataan asiakkaiden määrittelemien kriittisten palveluiden toimiminen poikkeusoloissa. Yksi kriittisistä toiminnoista on juuri mm. tilinpäätös- ja muuta finanssidataa sisältävien järjestelmien toiminta. ”SOx-lain vaikutuspiirissä olevat asiakkaat haluavat meiltä raportoinnin kontrolleista ja niiden toiminnasta”. (H3, 24.1.2012). IT-palveluliiketoimintaan sekä välittömästi, että välillisesti vaikuttava lainsäädäntö on koottu seuraavaan taulukkoon (taulukko 11).

TAULUKKO 11 IT-palveluliiketoimintaan vaikuttava lainsäädäntö

Ohjeistajataho	**Laki/ Ohjeistus**	**Kohde/vaikutusalue**	**Vaikutus**
Valtionhallinto	Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI-ohjeistus	Konesalien rakentaminen, rakennusmääräykset, paloturvallisuus	Välitön
Valtionhallinto	Kansallinen turvallisuusauditointikriteeristö, KATAKRI, ICT-varautumisen kehittämishanke eVARE, Tietoturvatasot-hanke, TTT.	Kulunvalvonta, henkilörekisterit, tietojen käsittely, huoltovarmuuskriittiset yritykset	Välitön
Vakuutusyhtiöt	Rakentamismääräykset, toimitiloja koskevat määräykset	Paloturvallisuus, yleinen turvallisuus ja suojelu	Välitön
Viestintävirasto	Tele- ja laatuvarmennetoiminta, fi-verkkotunnukset, taloudelliset määräykset sekä radioliikenne	Mobiililaitteiden tietoturva, operaattoreiden tietoliikenne	Välitön /Välillinen
USA:n liittovaltion Sarbanes-Oxley –laki (SOx)	Sisäisen valvonnan tehokkuus, taloudellisia tietoja sisältävät järjestelmät, finanssijärjestelmien varmuuskopiointi, säilytys, toipuminen, erityisesti SOx 404-pykälä	New Yorkin pörssiin listautuneet (asiakasyritykset) asiakasvaatimusten kautta	Välillinen
Finanssiala	PCI DSS (Payment Card Industry Data Security Standards)	Maksukorttialan tietoturva, (asiakasyritykset) asiakasvaatimusten kautta	Välillinen

H4:n mielestä lainsäädännön vaikutukset jatkuvuuden hallintaan ovat hyvin asiakaskohtaisia, mutta ainakin huoltovarmuuskriittisyys vaikuttaa. H3 on samaa mieltä, valtionhallinnon puolelta VAHTI-ohjeistusta noudatetaan: ”Velvoite näkyy sopimustasolla, palvelutasosopimuksien sisällössä”. (H3, 24.1.2012).

> On hyvä että ohjeistuksia on, se antaa toiminnalle raamit ja helpottaa, koska se vakioi asiakkaiden vaatimuksia, voit mitoittaa omaa toimintaasi niin, että se täyttää yleisesti vaaditut asiat. Aikaisemmin jokainen teki omat vaatimuksensa ad-hoc ja ne saattoivat olla ristiriitaisia. Ongelma on se, että valtionhallinnon VAHTI:n lisäksi löytyy eri ministeriöiden, hieman eri näkökulmasta tehtyjä ohjeistuksia. Tasojen täyttäminen ei

> ole yksinkertaista – jos täytät jonkin KATAKRI:n tason, täytätkö eVARE:n tai TTT:n tason? (H5, 1.3.2012).

EU-tasolta on tulossa tietoturvaan ja kriittiseen infrastruktuuriin vaikuttavia ohjeita jotka jossain vaiheessa vaikuttavat lainsäädäntöön myös Suomessa, H5 kertoo.

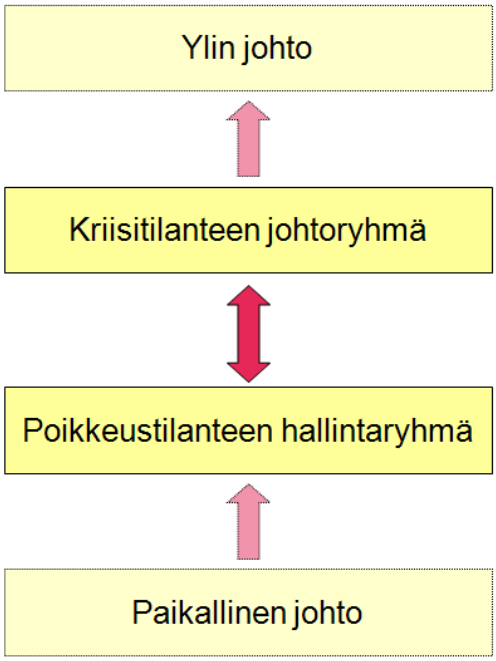
6.6 Strateginen näkökulma Tieto Oyj:n jatkuvuuden hallintaan

Kirjallisuudessa johdon tuki määriteltiin tärkeäksi osaksi jatkuvuuden hallinnan ohjelmaa ja strategian kehittämistä. Johdon määrittelemät politiikat ja periaatteet ohjaavat toimintaa myös Tieto Oyj:ssä: ”Konsernissa on BCP-policy, jossa on määritelty, että minkä tyyppisille toiminnoille pitää olla jatkuvuussuunnitelmat. Esimerkiksi konesalipalveluille pitää olla jatkuvuussuunnitelmat, sekä tarjottaville tukipalveluille”. (H5, 1.3.2012). Jatkuvuussuunnitelma tehdään myös, jos toiminnon liikevaihto ylittää tietyn kynnysarvon, tästä ääriesimerkkinä konsernin varainhallinta: ”Konserni-treasury, kun sen kautta kiertää koko konsernin liikevaihto, pitää sille olla jatkuvuussuunnitelma, vaikka henkilöstömäärä itse treasuryssä onkin pieni”. (H5, 1.3.2012). Jatkuvuussuunnitelmat tehdään myös konsernin omassa käytössä oleville järjestelmille, kun tietty käyttäjämäärä ylitetään, tai kun jossain toimipisteissä henkilömäärä ylittää tietyn raja-arvon. Isoimmilla toimipisteillä pitää olla kahdennetut kiinteistösolmut, sähkönsyöttö, tietoliikenneyhteydet. ”BCP-policyssä on BCP:n tekemiseen liittyvät käytännön ohjeet, joiden toteutumista valvotaan ja harjoitellaan”. (H5, 1.3.2012). Toimintaa ohjaavaa politiikkaa ja periaatteita muokataan standardien ja hyvien käytäntöjen avulla, joista käytetyimpiä ovat ISO-standardit, PAS 56, ISF-materiaali, sekä ITIL, kun puhutaan konesalitoiminnoista, H5 valottaa.

Jatkuvuuden hallinnan kokonaisuutta hallitaan vahvan johdon tuen kautta. Esimerkiksi konsernin riskienhallinta on julkaissut jatkuvuussuunnitteluun liittyvän aineiston ja suunnitteluohjeet, kertoo H5. ”Sisäisen tarkastuksen tehtävänä on tarkistaa, että jatkuvuussuunnitelmat ovat olemassa ja konsernin riskienhallinta järjestää jatkuvuussuunnitelmien harjoituksia vuosittain”. (H5, 1.3.2012). Johto pidetään tiiviisti informoituna jatkuvuuden hallintaan liittyvistä tapahtumista: käytännön työtä on se, että selvitetään ongelmien perimmäiset syyt (Root cause – analyysi), seurataan tapahtumia ja raportoidaan konsernin auditointi- ja riskikomitealle (Audit & Risk Committee), jossa käsitellään konsernia koskettavat riskit (engl. risk exposure), jatkaa H5. Jokaisesta vuosineljänneksestä turvallisuusjohtaja tekee tiivistelmäraportin konsernin johtoryhmälle.

Ohjeistus ja etukäteen nimetty kriisiorganisaatio määrittää vastuuhenkilöiden toiminnan kriisitilanteessa, H5 kertoo. Erikseen rakennettu käsikirja poikkeustilanteiden hoitamista varten auttaa toimimaan oikein: ”On tehty myös Incident Management Handbook, jonka mukaan toimitaan – tunnistetuille epätoivotuille tapahtumille on tässä handbookissa hallintamenettelyn kuvaukset”. (H5, 1.3.2012). Kriisitilanteessa ylintä päätöksentekovaltaa käyttää organisaation ylin

johto, mutta varsinainen tilanteen ohjaus on kriisitilanteen johtoryhmän (engl. Crisis Management Team, CMT) vastuulla, H5 selvittää. Esimerkiksi konesaliympäristössä korjaustoimia johtava osapuoli on poikkeustilanteen hallintaryhmä (engl. Incident Management Team, IMT), jolla on vastuu raportoida tilanteesta kriisintilanteen johtoryhmälle, H5 sanoo. Tiedon kriisiorganisaation kokoonpano on esitetty kuviossa 8 (kuvio 8):



KUVIO 8 Tieto Oyj:n kriisiorganisaation kokoonpano

Kuviossa tärkein vuorovaikutussuhde on kriisitilanteen johtoryhmän ja poikkeustilanteen hallintaryhmän välillä. Kriisitilanteen johtoryhmä on hallinnollinen osa kriisiorganisaatiota, joka tekee ylemmän tason linjaukset ja päätökset kriisitilanteessa, H5 valottaa. Poikkeustilanteen hallintaryhmä on enemmän operatiivinen osapuoli, joka toimeenpanee kriisitilanteen johtoryhmän tekemät päätökset tilanteen hoitamisesta, H5 kertoo. Esimerkkinä H5 mainitsee tilanteen, jossa CMT:n kaksi jäsentä voi päättää, milloin tilanne on eskaloitava kriisitilanteen hallintamalliin. ”Vaikka tilanteen hoitamiseksi perustettu paikallinen IMT ei esittäisi tilanteen eskalointia, silti CMT:llä on valtuudet tehdä päätös eskaloinnista”. (H5, 1.3.2012).

> Toimitusjohtaja antaa kasvot medialle, häntä ei oteta mukaan CMT:n, koska halutaan rauhoittaa tilanne hänen osaltaan. Nimetyille henkilöille on varahenkilöt, CMT-ryhmässä päätetään eskaloidaanko tilanne kriisitilanneohjeen mukaan hallittavaksi vai ei. (H5, 1.3.2012).

6.7 Jatkuvuuden hallinnan tärkeys ja tulevaisuus IT-palveluliiketoiminnassa

H1 näkee, että kokonaisympäristön hallinta vaikeutuu, jonka kautta riski häiriöille altistumiselle kasvaa. Hallinnassa ja monitoroinnissa roolien ja vastuiden eriyttäminen (engl. segregation of duties) ja virheistä oppiminen on H1:n mielestä tärkeää. ”Monitoroinnin auditointia pitää tehdä säännöllisesti”. (H1, 20.1.2012). H4:n mielestä IT-palveluliiketoiminnan kehitys on kohti kompleksisempaa suuntaa. ”Riskiketjuja ei käydä loppuun asti, kompleksisuus, keskinäiset riippuvuudet lisääntyvät. Arviointi on usein komponentti tai palvelukohtaista, keskinäistä vertailua pitää ottaa paremmin huomioon”. (H4, 30.1.2012).
H4 lisää, että kriittisiä menestystekijöitä pitää pystyä tunnistamaan, ja sitä kautta palvelun laatua pitää pystyä parantamaan. H3 on samoilla linjoilla, eri liiketoimintaprosesseille on paljon yhteisiä tekijöitä, esimerkiksi ITIL:n keskeisiä prosesseja noudatetaan, joita ovat tapahtumien käsittely ja hallinta (incident management), muutoksen hallinta (change management) ja ongelmien hallinta (problem management). H3:n mukaan tärkeässä asemassa ovat uudet teknologiat ja riippuvuuksien lisääntymisen huomioon ottaminen asiakkaiden järjestelmiä, sekä sisäisiä järjestelmiä ylläpidettäessä. Myös internetin olemassaolosta ollaan hyvin riippuvaisia:

> Sisäisetkin järjestelmät ovat riippuvaisia toisistaan. Yleisemmällä tasolla internetin käytettävyys, miten sillä puolella asiat toimivat – on oletettu että kyllähän se toimii, sitä pitäisi ajatella enemmän kuin tähän asti. (H3, 24.1.2012).

H4 mainitsee uusimmista teknologioista pilvipalveluiden kehittymisen, esimerkiksi virtualisointi, infrastruktuurin toimittaminen palveluna (engl. infrastructure as a servise, IaaS) ja alustan toimittaminen palveluna (engl. platform as a service, PaaS). H1:n mukaan datan keskittymisen, datan määrän kasvamisen ja virtualisoinnin seurauksena häiriöiden vaikutukset ovat suurempia ja osin vielä kartoittamattomia.

> Asiakas rakentaa alustan päälle toiminnallisuutta, josta toimittaja ja ei välttämättä tiedä mitään – tässä tilanteessa jatkuvuuden kehittäminen ja joko ketjun testaaminen on haaste. Mobiililaitteidenkaan varmennusmenetelmät ja suojausmenetelmät kuten virustorjuntaohjelmistot ja niiden hallinta on aika puutteellista yritysten näkökulmasta. (H4, 30.1.2012).

H5 ottaa kantaa myös H4:n mainitsemaan virtuaalialustojen haasteeseen: ”Osa käyttökatkoista aiheutuu teknisistä vioista osa siitä että käyttäjä tekee jotain väärin. Administraatio-oikeudet tarjoamissamme järjestelmissä pitää säilyä myös meillä, jotta voimme taata palvelun käytettävyyden”. (H5, 1.3.2012). ”Vastuukysymykset, eli vaikkapa tilanne, jossa jotain laitonta pyöritettäisiin meidän tarjoaman alustan päällä, ovat myös vähintään mielenkiintoisia”. (H5 1.3.2012)

> Datan määrä lisääntyy, hallittavan tiedon määrä lisääntyy. Virtualisointi ylipäänsä on haaste. Virtuaaliympäristön hallintajärjestelmällä hallitaan laajoja monien asiakkaiden käytössä olevia kokonaisuuksia, jotka voivat sisältää palvelimia ja tietoliikennelaitteita ja on näin ollen kriittinen komponentti. Pilvipalvelut ovat usein sijoitettuna kahdessa paikassa saatavuuden parantamiseksi. Samalla raudalla voi olla monia palveluita monille asiakkaille, voi virtuaaliympäristössä rautatason vika aiheuttaa laajan ongelman asiakaskunnalle. Eritasoiset palveluvaatimukset aiheuttavat sen, että eri järjestelmiä ei voida välttämättä laittaa samaan pilveen. (H4, 30.1.2012).

H1 on samaa mieltä ja nostaa esiin virtualisoinnin ja pilvipalveluiden kehittämisen. ”Nopeasti liikkuvalla osa-alueella taidoista ja kyvyistä tulee kilpailua. Capability, competence, skills. Kyvyt kehittää palvelua ja pysyä aallonharjalla”. (H1, 20.1.2012). Fokuksena tulee olemaan myös asiantuntemuksen kasvattaminen laajalti tietokonekeskuksen hallinnan osalta, mutta myös hyvin spesifit taidot ovat H1:n mukaan tärkeitä. Teknologian kehityksen mukana kasvavat myös riskit: ”Riskienhallinta vaikeutuu ja riskit kasvavat. Strateginen päätös, jos lähdet bisnekseen, siihen on mentävät täysillä, tämä kehitys on jatkuvaa. Tässä kasvuvaiheessa pitää pysyä mukana.”. (H1, 20.1.2012). H2 mielestä tietoliikenne on iso haaste. ”Se tuntuu olevan hankala asia. Siinä on mukana aina monta osapuolta”. (H2, 23.1.2012).

> Yleensä tietoliikenteellä on iso osuus ongelmien aiheuttamisessa. Toimintatavat eroavat operaattoreiden ja laitevalmistajien välillä. Tuotantoa tukevan infran pitäminen ajan tasalla, varavoimakoneiden vaihtaminen, kiinteistöjen ja tilojen uusiminen on hankalaa kun järjestelmät ovat toiminnassa. Tämä samanaikainen ylläpito onnistuu uusimmissa data centereissä. Jo laitteiden ja järjestelmien oma tekniikka mahdollistaa usein tämän. (H2, 23.1.2012).

Kompleksisuuden ja keskinäisten riippuvuuksien lisäksi H4 nostaa esiin tiedon ajantasaisuuden ja saatavuuden: ”Tieto pitää olla saatavilla koko ajan, enemmän ja enemmän ollaan menossa siihen, että ei saa tulla katkoksia”. (H4, 30.1.2012). Esimerkiksi verkon komponentit ovat sellaisia, joita käyttää monta asiakasta. Huoltoajankohtien järjestäminen on tällöin hankalaa, H4 kertoo.

Maailmalla tapahtuneet kriisit ovat herättäneet jonkin verran keskustelua, H3 kertoo. ”Silti nämä tsunamit yms. luonnonkatastrofit tuntuvat kaukaisilta. Enemmän nämä läheisemmät myrskyasiat aiheuttavat keskustelua.” (H3, 24.1.2012). Myrskyjen aiheuttamia sähkökatkoja H3 ei näe uhkana Tiedon jatkuvuudelle. ”Ei, koska esimerkiksi sähkönsyöttöön on varauduttu todella hyvin”. (H3, 24.1.2012). H4 lisää, että sähkön- ja voimantuotossa puhetta jatkuvuusasioista voi aiheutua lähinnä pidempiaikaisten ongelmien yhteydessä. Muutoin ulkopuolisena esimerkkinä toimivat H3:n mukaan paremmin lakot ja lakon uhat, pandemiat ja pandemian uhat, jotka antavat aihetta tarkistaa omia jatkuvuussuunnitelmia.

> Verkkohyökkäyksien ilmaantuminen ja lisääntyminen on myös esimerkki tällaisesta ulkopuolisesta tekijästä. Arvion tekee kukin jatkuvuussuunnitteluun osallistuvista tahollaan ja voi ottaa tapahtuman esille, mutta kaikkia tapahtumia ei oteta kokouksi-

> en aihelistalle. Jos asiakkaat kysyvät meidän suunnitelmista vastaavien kriisien varalta, laaditaan myös muodollinen kannanotto. (H3, 24.1.2012).

Useimmat maailmalla esiintyneet kriisit ovat myös sen luonteisia, että niihin on järkevää reagoida Tieto -tasolla, ei yksittäisellä liiketoiminta-alueella, kertoo H3. H4 täsmentää myös, että esimerkiksi tietovuodot aiheuttavat sen, että jatkuvuusasiat ovat keskustelun alla ja suunnitelmia tarkennetaan.

Jatkuvuuden hallinta on vastaajien mukaan paremmin perusteltavissa, kuin viisi vuotta sitten: ”Liiketoiminnan merkitys on kasvanut. Jatkuvuuden hallinta koskee myös johtoa, eikä ole vain muutaman konesali-ihmisen vastuulla. Meillä jatkuvuuden hallinta on jo perinteisesti ollut tärkeä asia”. (H3, 24.1.2012). H5:n mukaan jatkuvuuden hallinta on liiketoiminnan perusedellytys: ”jos siitä ei huolehdita, ei jonkin alan kuluttua ole liiketoimintaakaan”. (H5, 1.3.2012). Audit & Risk Committee (konsernin auditointi- ja riskikomitea) on ollut kiinnostunut asiasta enemmän kuin aikaisemmin, ylimmälle johdolle raportointi tehdään tiheämmin kuin aikaisemmin, jatkaa H5. H4 lisää, että asiakkaan liiketoiminnalle palvelujen jatkuvuus on tärkeämpää: ”Koko ajan enemmän tietoa viedään järjestelmiin ja tietoa käsitellään järjestelmissä entistä enemmän”. (H4, 30.1.2012).

> Mitään ei synny ilman kustannuksia. Jatkuvuuden hallintaan täytyy panostaa ja resursoida. Jatkuvuuden hallinnan pitää olla osa bisnestä. Jatkuvuuden hallinta ei pidä nähdä erillisenä osana, vaan yhtenäisenä osana liiketoimintaa. Ratkaisut mitä tehdään, pitää tehdä analyysin perusteella, ei sen mukaan, mikä on helppoa, hauskaa tai halpaa. (H5, 1.3.2012).

H5:n mukaan jatkuvuuden hallinnan sulauttaminen osaksi organisaation toimintakulttuuria on tärkeää. Se tapahtuu koulutuksen, tietoisuuden lisäämisen, asenteisiin vaikuttamisen, harjoittelun, sekä uusien ihmisien palkkaamisen yhteydessä koulutuksen ja sparraamisen avulla, H5 tiivistää. Kysyttäessä jokaiselta haastateltavalta jatkuvuuden hallintaan liittyvistä tärkeimmistä käsitteistä, nousivat riskienhallinta, toimintavarmuus ja häiriöttömyys tärkeimmiksi aiheiksi. Muita mainittuja käsitteitä olivat kokonaisvaltaisuus, perusedellytys, bisnestavoitteet, nopea toipuminen, seuranta, uskottavuus, analyysiin perustuva, saatavuus ja vaatimustenmukaisuus.

7 POHDINTA JA TULOKSET

Tässä luvussa arvioidaan tutkielman empiirisen osuuden tuloksia ja verrataan niitä jatkuvuuden hallinnan teoreettiseen viitekehykseen. Teoreettisen viitekehyksen strateginen, operationaalinen ja taktinen taso esitetään empirian valossa. Tässä luvussa esitetään myös tutkimuksen teoreettisen ongelman ratkaisu eli organisaation jatkuvuuden hallinnan kypsyyttä kuvaava malli, joka ottaa huomioon IT-palveluliiketoiminnan tarpeet. Lisäksi esitetään johtopäätökset, annetaan myös vastaukset tutkimusongelmiin, sekä arvioidaan tutkimuksen luotettavuutta, pätevyyttä ja onnistuneisuutta.

7.1 Tutkimuksen tuloksien suhde teoreettiseen viitekehykseen

Keskeiset tulokset suhteutetaan luvussa 4 muodostettuun teoreettiseen viitekehykseen jatkuvuuden hallinnasta. Tässä käsiteltävä järjestys on sama, kuin viitekehyksessäkin: Ensin käydään läpi strateginen taso, sitten operationaalinen taso, ja lopuksi taktinen taso.

7.1.1 Strateginen taso

Lähdetään liikkeelle teoreettisen viitekehyksen strategisesta osuudesta. Jatkuvuuden hallinnan teoreettisessa viitekehyksessä todettiin strategisen tason olevan ylimmän johdon periaatteiden ja politiikan, mission ja vision luomista jatkuvuuden hallinnan tavoitteisiin liittyen. Näin Tieto Oyj:ssäkin on toimittu. Haastatteluissa selvisi johdon määrittelevän ne periaatteet, joiden mukaan jatkuvuutta hallitaan. Periaatteet koskivat riskien tunnistamista ja vaikuttavuuden arviointia, jatkuvuus- ja toipumissuunnittelua ja ylipäänsä kaikkea jatkuvuuden hallintaan liittyvää toimintaa. Jatkuvuuden hallintaa todettiin ohjaavan erilaiset toimivaksi todetut standardit ja hyvät käytännöt. Haastatteluissa standardit ja

hyvät käytännöt todettiin toimivaksi keinoksi jatkuvuuden hallinnan tavoitteiden määrittelemiseen.

IT-palveluliiketoiminnassa jatkuvuuden hallinnalla todettiin olevan suurempi merkitys kuin perinteisemmässä liiketoiminnassa, koska hyvin toteutettu jatkuvuuden hallinta on IT-palveluliiketoiminnassa markkinoilla toimimisen edellytys. Jatkuvuuden ja häiriöttömyyden varmistaminen koettiin elintärkeäksi IT-palvelutoimittajan kannalta. Tieto Oyj:n ylläpitäessä samanaikaisesti usean asiakkaan liiketoimintoja pyörittäviä järjestelmiä, vakaviin häiriöihin ei yksinkertaisesti nähty olevan varaa. Painopiste on siis vakavissa häiriöissä, koska palvelutasosopimuksessa on määritelty aikarajoin, mikä häiriö on vakava ja mikä ei. Haastatteluissa ja tutkielman teoriaosuudessa todettiin myös jatkuvuuden olevan myös saatavuutta. Tieto Oyj:n asiakkaiden käyttämät konesalipalvelut on oltava saatavilla koko ajan. Siksi jatkuvuus tarkoittaa toiminnan jatkamista kaikissa tilanteissa ja jatkuvuuden hallinnalla tarkoitettiin toiminnan turvaamista kaikissa mahdollisissa olosuhteissa. Osassa haastatteluja täsmennettiin jatkuvuuden hallinnan tärkeimpänä asiana olevan erityisesti asiakkaiden palvelujen turvaaminen, riippumatta toimintaan kohdistuvista riskeistä. Haastateltavien vastaukset jatkuvuuden hallinnasta tukevat liiketoiminnan jatkuvuuden hallinta – käsitteen määritelmiä, yleisesti ottaen käsite kuvasi liiketoiminnan keskeytyksetöntä jatkamista, kuten tutkielman toisessa luvussa määriteltiin.

7.1.2 Operationaalinen taso

Operationaaliselle tasolle kuuluivat käytännön toimet jatkuvuuden turvaamiseksi. Toimet käsittivät riskien tunnistamisen, niiden vaikuttavuuden arvioinnin vaikutusanalyysin avulla, sekä jatkuvuussuunnitelmien, toipumissuunnitelmien ja kriisinhallinnan suunnitelmien luomisen, arvioinnin ja testaamisen. Kuten kirjallisuudessa, myös haastattelujen tuloksena voidaan todeta, että riskien tunnistaminen ja niiden liiketoimintaan vaikuttavuuden arviointi on pohjana erilaisten jatkuvuutta, kriisin hallitsemista ja toipumista edistävien suunnitelmien tekemiselle. Uutta tietoa oli se, että jokaiselle riskille määrätään omistaja, joka hallitsee riskiään esimerkiksi harjoittelemalla riskiskenaarioiden avulla. Yleisesti haastatteluissa nähtiin jatkuvuuden hallinnan olevan hyvin läheistä sukua riskienhallinnalle. Jatkuvuuden hallinnan nähtiin pohjautuvan tunnistettujen riskien aiheuttamille toimenpiteille.

Ennen esimerkiksi jatkuvuussuunnitelmien luomista huomion arvoista ja teorian yleisestä linjasta poikkeavaa oli se, että riskejä pyrittiin käsittelemään, jotta riskin vaikuttavuutta liiketoimintaan voitaisiin pienentää. Haastatteluissa todettiin riskien arvioinnin pohjalla olevan palvelutasosopimuksissa tarkemmin määritellyt kriittisyys- ja saatavuusvaatimukset. Tärkeää oli huomata, että johtuivat epätoivotut tapahtumat tai poikkeustilanteet sitten inhimillisistä erehdyksistä, teknisistä vioista tai ulkoisista tekijöistä tulos on aina kuitenkin sama: epätoivotut tapahtumat ovat aina riski liiketoiminnan jatkumiselle. Resurssien ollessa rajalliset, on järkevää pyrkiä hallitsemaan tilannetta, eikä päämäärättö-

mästi luoda suunnitelmia ja varajärjestelyitä sellaisten riskien varalle, joita kyetään kontrolloimaan. Kuviossa 6 esitettiin Tieto Oyj:n riskien todennäköisyyksien ja vaikutuksien arviointi. Seuraavassa kuviossa esitetään Tieto Oyj:n strategian mukaisesti edellä mainitut jatkotoimenpiteet, kun riskien vaikutukset on tunnistettu (kuvio 9).

Tapahtuman kustannukset \ Tapahtuman todennäköisyys	Ei voi tapahtua	Tapahtuu vuosittain	Tapahtuu useammin
Suuri tai erittäin suuri	Jatkuvuussuunnitelma ja toimenpiteet	Toimenpiteitä tarvitaan riskin vähentämiseksi	Toimenpiteitä tarvitaan riskin vähentämiseksi
Keskisuuri	Toimenpiteet voidaan selvittää	Toimenpiteitä tarvitaan riskin vähentämiseksi	Toimenpiteitä tarvitaan riskin vähentämiseksi
Pieni tai ei merkitystä	Ei tehdä mitään	Toimenpiteet voidaan selvittää	Toimenpiteet selvitettävä

KUVIO 9 Epätoivotun tapahtuman todennäköisyyden ja kustannusten suhde

Kuviossa 7 tavoiteltava suunta on siis matriisin oikeasta kulmasta riskiä pienentäen saada riski matriisin osaan, jossa sitä voidaan paremmin kontrolloida, esimerkiksi jatkuvuussuunnitelman tai muiden jatkuvuusjärjestelyiden avulla. Kustannuksista haastattelujen mukaan pitää selvittää, aiheutuuko vahinkoja asiakkaalle tai itselle ja missä määrin. Huomionarvoista on se, että kaikkia riskejä ei tietenkään käsitellä ensimmäistä kertaa. Siksi kolmaskin ulottuvuus on mahdollista vielä kuvioon lisätä. Silloin otetaan huomioon myös riskin hallinnan taso, siihen vaikuttavat jo aikaisemmin tehdyt jatkuvuusjärjestelyt.

Kaikki riskit eivät siis generoidu automaattisesti jatkuvuus- ja toipumissuunnitelmiksi. Tärkeää on Tieto Oyj:n mukaan suunnitelmien kerroksellisuus: normaalisti toimittaessa pääosassa ovat edellisessä kappaleessa esitetyt kontrollit riskin vaikuttavuuden vähentämiseksi. Normaalin toiminnan ollessa estynyt, Tieto Oyj:n mukaan otetaan käyttöön vaihtoehtoisia toimintatapoja, joita voidaan kutsua nimellä *Plan-b*. Jos vaihtoehtoisetkaan toimintatavat eivät ole mahdollisia, toipumissuunnittelun tehtävänä on palauttaa organisaation häiriönsietokyky. Haastatteluissa selvisi, että liiketoimintayksiköiden johtajat määrittelevät riskien omistajat, jotka taas ovat vastuussa riskien kontrolloimisesta. Suuremmat kokonaissuunnitelmat, esimerkiksi tietokonekeskus- ja konesalitasolla pitää toki olla olemassa, ennen kuin yksittäisiin riskeihin otetaan kantaa. Opera-

tionaalisen tason toimenpiteet ovat Tieto Oyj:ssä tarkoin harkittuja, suunniteltuja, kustannukset ja hyödyt huomioivia prosesseja, jotka lähtevät liikkeelle suurimpien riskien vaikuttavuuden pienentämisestä.

7.1.3 Taktinen taso

Taktisen tason elementit, kuten IT-infrastruktuuri, sidosryhmät, viestintä ja liiketoimintaprosessien menestystekijät mahdollistavat IT-palveluliiketoiminnan, joten ilman niitä ei jatkuvuuttakaan voida hallita. Tutkielman kolmannessa luvussa tutustuttiin IT-palveluliiketoiminnan toimintaympäristöön, jossa todettiin toimivan ja häiriöttömän IT-infrastruktuurin olevan keskeisessä roolissa toiminnan mahdollistajana. Standardien kautta työskenneltäessä myös konesaliympäristössä varmistutaan toiminnan oikeellisuudesta ja laadusta.

Tietokonekeskusten häiriöttömyyden varmistaminen kulkee käsi kädessä asiakasvaatimusten kanssa. Tieto Oyj:n pitää pystyä tarjoamaan varmistustasoiltaan monenlaisia konesalipalveluja, sen mukaan mitä asiakkaiden toiveet ovat. Vähemmän kriittisiä järjestelmiä voidaan ylläpitää kolmannessa luvussa esitetyn tietokonekeskusten tasoluokituksen, eli tier-luokituksen mukaisella tier-3 tasolla, kriittisimpien järjestelmien kohdalla pitää olla hyvin lähellä tier-4 tasoa. Tietokonekeskuksen laitteistoille todettiin haastatteluissa asetettavan häiriöttömyyttä edistäviä ominaisuuksia, kuten kahdennettavat tietoliikenneyhteydet ja virransyötöt. Myös ylläpidon kannalta laitteiston huoltaminen ”lennossa” on yhä tärkeämpi ominaisuus, jotta laitteistoja ei tarvitse erikseen ajaa alas tai kytkeä pois huoltotöiden ajaksi. Kahdennus on erittäin tärkeää virtualisoitaessa konesalikomponentteja ja järjestelmiä. Virtualisoinnin todettiin olevan yksi suurimmista konesalipalveluja tarjoavan toimijan haasteista sen hallittavuuden osalta. Virtualisointi on mullistanut konesaliliiketoiminnan, mutta sen tuomien mahdollisuuksien lisäksi virtualisointi aiheuttaa alati kasvavia haasteita jatkuvuudelle. Virtuaaliympäristöjen hallitsemista, kuten monitorointia ja siirrettävyyttä pitää pystyä tarkemmin seuraamaan.

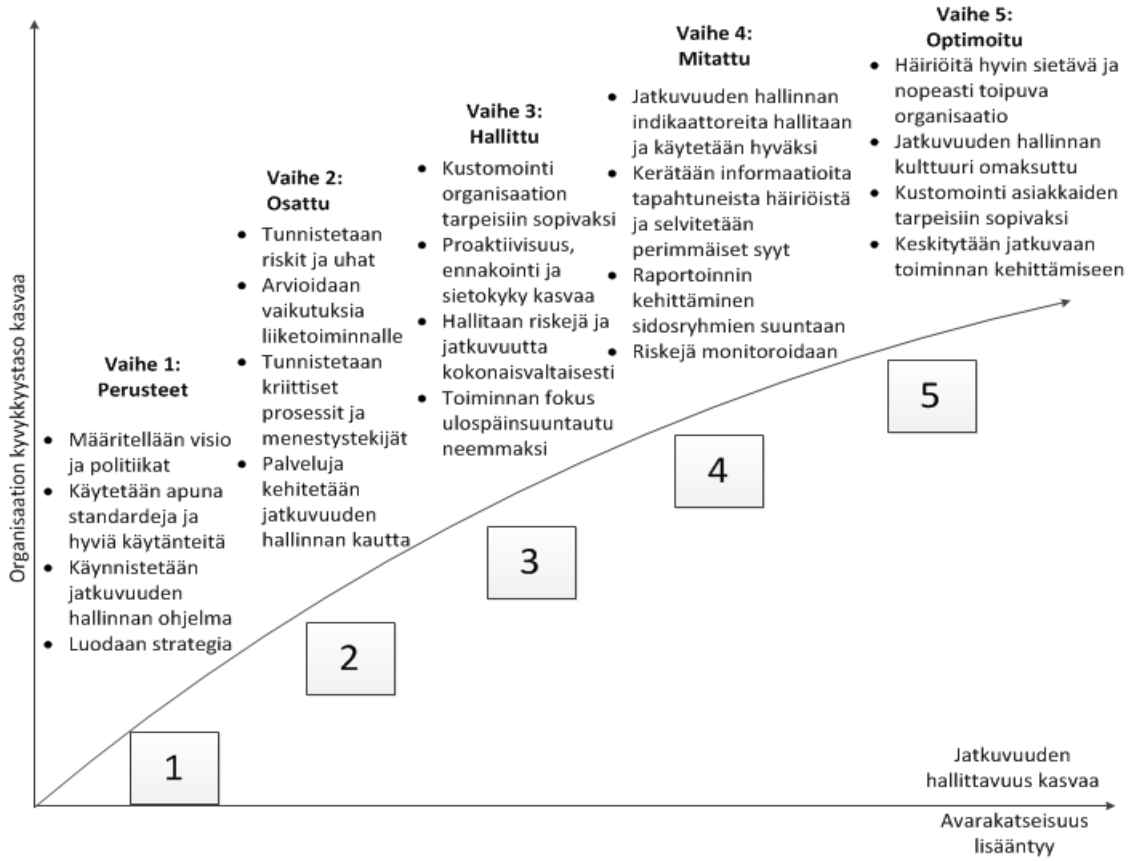
7.1.4 Jatkuvuuden hallinnan kehittäminen organisaatiossa

Tutkielman teoreettisena tavoitteena oli kehittää malli IT-palveluliiketoiminnan jatkuvuuden hallinnan kyvykkyyden arvioimiseen. Tutkielmassa jatkuvuuden hallitsemisen on todettu sekä teoriassa, että empirian osalta tuottavan luotettavuutta IT-palvelutoimittajan toimintaan. On puhuttu organisationaalisen häiriönsietokyvyn kasvattamisesta pyrkimällä luotettavaan palvelujen toimittamiseen jatkuvuuden hallinnan kautta. Kirjallisuudessa on esitetty muutamia malleja liiketoiminnan jatkuvuuden ja sietokyvyn mittaamiseen. Toisen luvun lopussa esitetyt mallit kuvasivat organisaation kyvykkyyttä tuottaa jatkuvia ja sietokykyisiä palveluja. Erityisesti niissä keskityttiin varautumisen mittaamiseen riski-indeksien kautta. Jatkuvuuden hallinnan elementtien (alaluku 2.6.2) yhteydessä esitelty Virtual Corporationin (2003) jatkuvuuden hallinnan kypsyysmalli kuvaa organisaation jatkuvuuden hallinnan kehittymistä organisaati-

on sisältä kuvattuna. Organisaatio kuvataan mallissa samalla tavalla, kuin ihminen parantaa suorituskykyään juoksussa: aluksi eteneminen tapahtuu ryömimällä, ja lopuksi kuvataan organisaatiota olympiatason urheilijana. Smitin (2005) mallissa toiminnan jatkuva kehittäminen on otettu huomioon, mutta tämäkään jatkuvuuden hallinnan kypsyyttä kuvaava malli ei ota riittävästi kantaa organisaation ulkopuolisiin sidosryhmiin, kuten kilpailijoihin, osakkeenomistajiin tai asiakkaisiin. Tämän vuoksi avarakatseisempi, sidosryhmien tarpeet paremmin huomioiva ja palvelukeskeistä ajattelua kuvaava malli jatkuvuuden hallinnan kehittyneisyyden arvioimista varten kuitenkin yhä puuttuu.

Ratkaisu tähän tutkimuksen teoreettiseen tavoitteeseen löytyi jatkuvuuden hallinnan tavoitteiden samankaltaisesta suhteesta laadun ja laadunhallintajärjestelmien tavoitteisiin. Bureau Veritas Finland (2007) toteaa ISO 9001 laadunhallintastandardin tavoittelevan hyvään liiketoimintatapaan kuuluvia asioita: asiakassuuntautuneisuus, johtajuus, työntekijöiden sitoutuminen, prosessiajattelu, järjestelmäkeskeinen johtamistapa, jatkuva toiminnan parantaminen, tosiasioihin perustuva päätöksenteko ja molemminpuolista hyötyä tuottavat suhteet toimittajiin – kaikki siis asioita, joita tässä tutkielmassa on myös liiketoiminnan jatkuvuuden hallinnalla havaittu tavoiteltavan.

IT-palveluorganisaation jatkuvuuden hallinnan kypsyysmallia suunnitellessani ajattelin, että on hyvä hyödyntää hieman jo olemassa olevaa tietoa kyvykkyyksien arvioimisesta. Huomasin, että usein esiintyvä, mutta erittäin monipuolinen laatutyössä käytetty kypsyys- ja kyvykkyysmalli CMMI rakentuu samoille periaatteille kuin jatkuvuuden hallintakin. Myös jatkuvuuden hallinnan kyvykkyyden kasvattamisen voidaan todeta istuvan laatuajattelussa tunnetun CMMI -kyvykkyys- ja kypsyysmallin tasokonseptiin. Teoriaosuudessa esille tulleet periaatteet jatkuvuuden hallinnasta saivat vahvistusta empiirisen osuuden case-tutkimuksen tuloksista. Olen koonnut tärkeimmät jatkuvuuden hallinnan periaatteet teoriaosuuden ja case-tutkimuksen tulosten pohjalta yhteen ja sijoittanut ne CMMI – viisitasomalliin (kuvio 10).



KUVIO 10 IT-palveluorganisaation viisi askelta jatkuvuuden hallitsemiseen

Kuviosta voidaan huomata jatkuvuuden hallitsemisen sulautuminen viisitasomalliin. Kuten CMMI -mallissakin, myös taso nolla on oikeastaan olemassa: jatkuvuuden hallinnan kypsyysmallissa nollataso tarkoittaa sitä, että tunnistetaan tarpeet jatkuvuuden parantamiselle organisaatiossa, mutta mitään konkreettisia toimenpiteitä tämän eteen ei ole tehty. Teoriaosuuden, teoreettisen viitekehyksen ja case-tutkimuksen kautta jäsennetyt jatkuvuuden hallinnan periaatteet näkyvät listattuna jokaisen viiden vaiheen alla. Kaikissa vaiheissa on neljä ydinkohtaa, johon IT-palveluorganisaation tulee keskittyä ottaakseen seuraavan askeleen.

Ensimmäisellä vaiheessa (tai askeleella) luodaan strategia ja tavoitteet organisaation johtotasolla, sekä käynnistetään ohjelma jatkuvuuden hallinnan tavoitteisiin pääsemiseksi. Toisella askeleella myös operationaalisella tasolla on omaksuttu jatkuvuuden hallinnan tavoitteet ja ryhdytään toimenpiteisiin, kuten toimintaympäristön riskien kartoittamiseen, niiden vaikutusten arvioimiseen ja liiketoimintaprosessien kriittisten menestystekijöiden tunnistamiseen. Tärkeää on myös kehittää olemassa olevia palveluja jatkuvuuden hallinnan kyvyt huomioiden. Kolmannella askeleella jatkuvuuden hallittavuus kasvaa ja organisaation kyvykkyys jatkuvuuden hallinnan osa-alueiden kokonaisvaltaisessa ymmärtämisessä lisääntyy. Jatkuvuuden hallinta on omaksuttu toimintakulttuuriin ja muiden sidosryhmien huomioiminen kasvaa: kolmas askel on tärkeä

avarakatseisuuden kannalta, tässä vaiheessa aletaan suunnata toiminnan fokusta kohti organisaation palveluja käyttävien sidosryhmien, kuten asiakkaiden tarpeita vastaavaksi. Neljännellä askeleella jatkuvuuden hallinnan indikaattoreita käytetään hyväksi. Tämä tarkoittaa esimerkiksi tarkentunutta raportointia kriittisten järjestelmien toipumispiste- ja toipumisaikatavoitteiden, häiriöiden aiheuttamien katkoaikojen ja asiakkaille luvattujen palvelutasojen saavuttamisesta. Tällä tasolla säännöllistä vuorovaikutusta osakkeenomistajien ja asiakkaiden suuntaan kehitetään. Viimeisenä askelmana viisitasomallissa jatkuvuuden hallinta on optimoitu, jolloin keskitytään jatkuvaan toiminnan kehittämiseen: uusien teknologioiden ja jatkuvuuden hallintaa edistävien toimintatapojen seuraamiseen ja omaksumiseen, sekä häiriönsietokyvyn kasvattamiseen. Asiakkaiden tarpeet palvelujen jatkuvuuden kannalta pystytään huomioimaan viidennellä tasolla yksilöllisemmin.

Avarakatseisuus ja asiakaskeskeisyys lisääntyvät organisaation edetessä askel askeleelta. Organisaatio ryhtyy tarkastelemaan omaa kehittymistään enemmän ulkopuolisesta näkökulmasta ja määrittelee proaktiivisesti uusia tavoitteita jatkuvuuden hallinnalle: tämä on viidennellä askeleella kuvattua toiminnan jatkuvaa kehittämistä. Jatkuvuuden hallittavuudeltaan kypsä organisaatio pystyy kehittämään tarjoamiensa palveluiden saatavuutta ja ominaisuuksia asiakastarpeita paremmin vastaaviksi.

7.2 Vastaukset tutkimusongelmiin

Seuraavaksi annetaan vastaukset tutkimusongelmiin. Ensin aloitetaan pääongelmasta, sitten annetaan vastaus aliongelmaan ja lopuksi tehdään muita huomioita case-tutkimuksessa tehtyjen havaintojen pohjalta.

7.2.1 Pääongelma: Painottaako Tieto Oyj samoja jatkuvuuden hallinnan periaatteita, kuin kirjallisuudessa on esitetty?

Pääongelmana tutkittiin painottaako Pohjois-Euroopan johtava IT-palveluyritys jatkuvuuden hallinnassaan samoja periaatteita kuin kirjallisuudessa suositellaan? Tietyin varauksin voidaan sanoa, että kyllä painottaa. Jatkuvuuden hallinta etenee strategialähtöisesti johtotasolta alkaen läpi organisaation, kuten kirjallisuudessakin on suositeltu. Tieto Oyj:n jatkuvuuden hallinnan järjestelyissä on nähtävissä selkeää määrätietoisuutta ja järjestelmällisyyttä, koska toimintaa viitekehyksessäkin esitetyllä strategisella, operationaalisella ja taktisella tasolla ohjaavat periaatteet ja politiikat. Muutenkin Tieto Oyj:n jatkuvuuden hallinnassa on nähtävissä selvä jako normaalitilanteen, sekä poikkeus- ja toipumistilanteiden välillä. Vastuuta jatkuvuussuunnitelmien luomisesta ja harjoittelusta on selkeästi jaettu liiketoimintayksiköihin. Kirjallisuudessa jatkuvuuden hallinnan toimenpiteiden eteneminen organisaatiossa on hyvin suoraviivaista, ja sopii usein paremmin pieniin kuin isoihin organisaatioihin.

Tieto Oyj:ssä riskejä pyritään tunnistamaan ja niiden vaikuttavuutta arvioimaan kuten lähdekirjallisuudessakin todettiin. Vaikutusanalyysillä on Tiedossa erittäin tärkeä rooli tehtäessä ratkaisuja riskien kontrolloimisesta. Tässä kohdassa on kuitenkin poikkeus, josta kirjallisuudessa on tietoa hyvin vähän. Kirjallisuuden perusteella on oletettavissa, että jatkuvuussuunnitelmien avulla varaudutaan jokaiseen tietyn vaikutustason ylittävään epätoivottuun tapahtumaan, jotka voisivat aiheuttaa kriittisten liiketoimintaprosessien keskeytymisen hyväksymättömäksi ajaksi. Katkojen hyväksyttävyys liittyi palvelutasosopimuksissa erikseen määriteltyihin marginaaleihin, joiden rajoissa palvelun saatavuutta voitiin tarkastella. Riskin vaikutustason perusteella tapahtuu jatkuvuussuunnitelmien luominen myös Tieto Oyj:ssä, mutta ensin riskejä yritetään kontrolloida eli pienentää. Riskien vaikuttavuutta voidaan kontrolloida toimenpiteiden avulla, jolloin vasta jäännösriskin perusteella tehdään arvio jatkuvuus- ja toipumissuunnitelmien luomisesta. Lähdekirjallisuudessa riskien vaikuttavuuden arvioimisessa käytettiin usein organisaation omaa liiketoimintaa lähtökohtana, vaikka usein myös aineettomat varat ja asiakkaatkin oli huomioitu. Tieto Oyj:n lähtökohtana IT-palveluliiketoiminnassa ovat asiakkaat, siitä kertoo esimerkiksi taulukossa 10 esitetyt häiriötasot, jossa poikkeustilanteen vakavuutta kuvaan nimenomaan häiriön vaikutus asiakkaan liiketoimintaan.

IT-infrastruktuuriin liittyvissä haastatteluissa nousivat pinnalle virtualisoinnin mahdollisuudet ja haasteet jatkuvuuden hallintaan liittyen. Lähdekirjallisuuden akateemisissa lähteissä virtualisointia oli käsitelty varsin pintapuolisesti, mutta eri yritysten tekemiä teknisiä dokumentteja asiasta kuitenkin löytyi. Tietokonekeskusten infrastruktuurista oli kirjoitettu verrattain vähän, vaikka haastattelujen perusteella voidaan sanoa häiriönsietokykyisten tietokonekeskusten olevan koko toimialan ydin. Tämä johtuu siitä, että lähdemateriaalia palveluita tarjoavan organisaation näkökulmasta ei juuri ole. Lainsäädäntö ja ohjeistukset vaikuttavat enemmän välillisesti IT-palveluorganisaation ja tietokonekeskusten toimintaan. Vaikuttavampia tekijöitä ovat asiakasyritysten vaatimukset ja toiveet Tiedon tarjoamia palveluja kohtaan.

Tiedon kriisiorganisaatio rakentuu samankaltaisesti, kuin kirjallisuudessa on esitetty. Tietysti ryhmien nimet voivat vaihdella, mutta periaate on sama: kriisitilanteessa vastuu toimenpiteistä on johdon käsissä ja toimintaa johdetaan kriisitilanteen johtoryhmän kautta. Muutoin jatkuvuuden hallinnan prosessi etenee kuten kirjallisuudessakin, suunnitelmia arvioidaan ja testataan aika ajoin, sekä organisaationaalista häiriönsietokykyä ja tietoisuutta jatkuvuuden hallinnasta vaalitaan koulutuksien, harjoittelun ja tiedottamisen avulla. Kirjallisuudessa painotetaan jatkuvuuden hallinnan ja varautumisen tulevan yhä tärkeämmäksi. Näin on myös Tieto Oyj:ssä, jokainen viidestä haastateltavasta oli sitä mieltä, että jatkuvuuden hallinnalla on tärkeämpi rooli liiketoiminnassa, kuin viisi vuotta sitten.

7.2.2 Aliongelma: Miten jatkuvuuden hallinnan tärkeys ja laajempi palvelutaso on perusteltavissa IT-palvelutoimittajan asiakkaalle?

Haastatteluiden perusteella on myös muodostettavissa vastaus aliongelmaan, jossa pyrittiin hakemaan keinoja jatkuvuuden hallinnan tärkeyden, tarpeen ja laajemman palvelutason perustelemiseen erityisesti asiakkaan kohdalla. Tähän kysymykseen vastattaessa perusteluita on löydettävissä Tieto Oyj:n jatkuvuuden hallinnan strategian kautta. Haastatteluissa ilmeni useita syitä jatkuvuuden hallinnan tarpeen perustelemiselle. Ensimmäisenä perusteluna on IT-infrastruktuurin jatkuva kehittyminen. IT-infrastruktuuri tulee kompleksisemmaksi, jolloin ydinliiketoimintaansa keskittyvien asiakkaiden kannattaa jättää kriittiset järjestelmänsä laajemmat resurssit omaavan asiantuntijayrityksen käsiin. Haastatteluissa todettiin, että asiakkaiden tulee ensisijaisesti itse arvioida omien järjestelmiensä kriittisyys, mutta toki Tieto auttaa asiakastaan kriittisyyden määrittämisessä: Tieto Oyj:n kokemus monelta toimialalta tulee näkyviin myös tässä tilanteessa, jolloin osataan tarjota parasta mahdollista vaihtoehtoa asiakkaalle ottaen huomioon aikaisemmin tehdyt ratkaisut. Tiedon jatkuvuuden hallinnan strategian pohjalla on useita standardeja ja hyviksi havaittuja käytäntöjä. Tämä tuottaa uskottavuutta ja luotettavuus palveluntarjoajana lisääntyy, kuten haastatteluissa todettiin. Haastatteluissa nousi esiin myös sertifioinnin positiivinen vaikutus; tiukoissa tarjouskilpailuissa hankitut sertifikaatit voivat olla yksi ratkaiseva tekijä.

Pitkät asiakassuhteet julkishallinnon toimijoiden kanssa auttavat Tietoa sopeutumaan jatkuvuuden hallintaa koskeviin suosituksiin ja lainsäädäntöön. Vaikka suoraan IT-palveluliiketoimintaan vaikuttavia lakeja on vain vähän, silti monet epäsuorasti vaikuttavat lait, esimerkiksi lain piirissä olevat Tiedon asiakasyritykset vaativat tiettyjen lakien ja säädösten tarkkaa noudattamista. Myös Tieto Oyj:n kotimaisuus suhteessa kilpailijoihin on etu. Erityisesti julkishallinnon palveluita ylläpidettäessä omistuspohjalla ja maantieteellisilläkin rajoilla on merkitystä, haastatteluissa selvisi. Erityisesti kyky palvelujen tuottamiseen useasta sijainnista voidaan laskea Tieto Oyj:n eduksi. Se mahdollistaa keskeytyksettömämmän palvelun toimittamisen, koska palvelun toimittamista voidaan jatkaa toisesta paikasta, jos se ei ole syystä tai toisesta mahdollista ensisijaisesta paikasta.

7.2.3 Muita havaintoja ja huomioita

Alihankinnan ja globaalien tuotanto- ja toimitusmallien (engl. offshoring) yleistyessä toimialasta riippumatta, tulee jatkuvuuskysymykset ottaa paremmin huomioon. Esimerkiksi toimintoja siirrettäessä alemman kustannustason maihin, otetaan samalla tietoinen riski normaalin toimintatason ylläpitämisessä. Kysyessäni haastatteluissa toimintojen siirtämisestä kauemmaksi jatkuvuuden hallinnan kannalta, merkittävimmäksi asiaksi nousi ennalta varmistamisen tärkeys. IT-palveluyrityksen tapauksessa toimivilla tietoliikenneyhteyksillä ja paikallisen IT-infrastruktuurin kapasiteetilla ja toimintakyvyllä on kaikkein suurin

merkitys tuotettaessa palveluja kauempaa. Myös henkilöstöpolitiikka vaikuttaa toimintojen jatkamiseen kriisitilanteessa, haastatteluissa todettiin. Toiminnan jatkumisen varmistaminen pitää onnistua sijainnista riippumatta. Tarkoitan, että ei saa tapahtua sellaista tilannetta, jossa jostain yhdestä maantieteellisestä sijainnista tulee koko organisaation toiminnan single point of failure.

Ennakkokartoituksella voidaan toki riskiä pienentää, mutta silti toiminta on mielestäni ristiriidassa jatkuvuuden hallinnan tavoitteiden kanssa, koska yleisesti ottaen ylimääräisiä riskejä ei pitäisi vapaaehtoisesti ottaa. On kuitenkin tosiasia, että jo valmiiksi erittäin kilpaillulla alalla etumatkan antaminen kilpailijoille kustannusten nousemisen kautta on pienempi paha, kuin tietoisten riskien ottaminen offshoring -liiketoiminnan takia. Toisaalta voidaan ajatella, että palvelujen tuottamisen mahdollistaminen monesta sijainnista voi olla etu siinä vaiheessa, jos jossain toimipisteessä normaaliin työntekoon ei syystä tai toisesta pystytä. Siksi kustannusten alentamista globaalien toimitusmallien avulla ei nähdä ylimääräisenä riskinä vaan välttämättömänä vaatimuksena alalla menestymiseen ja toiminnan kehittämiseen. Siispä toimintojen suuntaaminen hieman lähemmäs (engl. nearshoring) on mielestäni erittäin järkevä suuntaus liiketoiminnan jatkuvuuden hallitsemisen kannalta. Itä-Euroopan alueella kustannustason ollessa edelleen matala, sekä markkinoille pääsemisen kriteerit (tullit, byrokratia) ainakin Euroopan Unionin jäsenmaissa ovat kohtuulliset.

Yhdessä haastattelussa tulivat esiin palvelujen tuottamisen kulttuuriset esteet, esimerkiksi Aasian alueella sosiaalinen ja kulttuurinen etäisyys pohjoiseurooppalaisiin toimintatapoihin on väistämättä melko suuri. Laadukkaalla koulutuksella ja työn tukemisella voidaan tätä eroa tietysti kuroa umpeen. Joka tapauksessa poikkeustilanteessa on helpompaa kyetä palautumaan häiriöstä, kun organisaation toipumisen mahdollistavat rakenteet osaavat jo valmiiksi samanlaisen ajattelutavan. Kaukaa tuotettavien palveluiden jatkuvuuskysymykset ovat pitkälti hypoteettisia, mutta jos vakavia ongelmia syntyy lähes vuosittain Pohjoismaiden vakaalla, poliittisesti turvallisella ja stabiililla maaperällä, kukaan ei voi sulkea pois vakavien ongelmien syntymistä alihankinnan ja offshoring–liiketoiminnan seurauksena. On mielenkiintoista huomata, että organisaation toimiessa markkinoilla vahvasti liiketoiminnan ehdoilla, uusia liiketoimintaratkaisuja ja -malleja kehitettäessä otetaan yhä uusia riskejä jatkuvuuden hallinnan kannalta. Tämä on asia, johon jatkuvuuden hallinnan strategiaa kehitettäessä tulee ottaa kantaa; ratkaisuna on liiketoiminnan ja sitä tukevien resurssien yhteistyön lähentäminen ja kehittäminen.

7.3 Tutkielman arviointi

Tässä tarkastellaan tutkimuksen rajausta, luotettavuutta ja onnistuneisuutta. Tutkielman tavoitteena oli selvittää kattavat vastaukset tutkimusongelmiin ja kuvata Tieto Oyj:n jatkuvuuden hallintaa ja sen lainalaisuuksia IT-palveluliiketoiminnassa.

7.3.1 Tutkielman rajaaminen

Tutkielma oli rajattu IT-palveluyritys Tieto Oyj:n palvelukeskukseen, jossa tuotetaan konesalipalveluita asiakasyrityksille. Aluksi tutkielmaa suunniteltaessa päänvaivaa tuotti juuri rajaamisen vaikeus jatkuvuuden hallinnan laaja-alaisuuden takia. Tiedon ehdotuksen mukaisesti päätettiin rajata tutkimus koskemaan palvelukeskusta ja erityisesti asiakkaille tuotettavia palveluita. Nyt tutkimuksen loppuvaiheessa tuo rajaus tuntuu onnistuneelta. Teoriaosuudessa jatkuvuuden hallinnan ilmiö ja IT-palveluyrityksen toimintaympäristö tuli kuvattua riittävän tarkasti, jotta teoreettinen viitekehys saatiin muodostettua ja haastatteluille saatiin teoreettinen pohja. Empiirisessä osuudessa haastattelut vahvistivat rajauksen Tiedon palvelukeskukseen onnistuneen hyvin, koska kaikki aiheet tuli käsiteltyä sopivan kattavasti, eikä mitään suurempia kokonaisuuksia jäänyt käsittelemättä. Haastattelut tuottivat myös jatkuvuuden hallinnan saralta lisää mielenkiintoisia kysymyksiä, joita ei tämän tutkimuksen resurssien ja aiheiden arkaluontoisuuden vuoksi voitu tutkia. Muutamia näistä havainnoista on käsitelty tutkimuksen jatkotutkimusaiheina yhteenvetoluvussa.

7.3.2 Tutkielman luotettavuus ja pätevyys

”Tutkimuksessa pyritään välttämään virheiden syntymistä, mutta silti tulosten luotettavuus ja pätevyys vaihtelevat”. (Hirsjärvi, Remes & Sajavaara, 2008). Tämän vuoksi Hirsjärvi, Remes ja Sajavaara (2008) toteavat, että kaikissa tutkimuksissa pitää pyrkiä arvioimaan tutkimuksen luotettavuutta. Tutkielman luotettavuuteen ja yleistettävyyteen liittyy käsite reliabiliteetti. Järvisen ja Järvisen (2004) mukaan ”reliabiliteetti tarkastelee laajuutta, jolla monen samaa ilmiötä samassa tarkoituksessa tutkijan havainnot tuottavat suunnilleen samoja tuloksia” ja ”reliabiliteetti liittyy läheisesti yleisyyteen, toistettavuuteen ja falsifioitavuuteen”(Järvinen & Järvinen, 2004). Kirjallisuudessa on puhuttu saturaatiosta, jolloin tutkittavan asian löydökset alkavat toistua. Tässä tutkielmassa teoreettisen osan reliabiliteetti oli korkea, koska mitä enemmän lähdeaineistoa tutkittiin, sitä enemmän samankaltaisia malleja ja ajatuksia jatkuvuuden hallinnasta saatiin. Nämä samankaltaisuudet koostettiin luvussa neljä luotuun teoreettiseen viitekehykseen.

Empirian osalta reliabiliteetin voidaan todeta olevan hyvällä tasolla, koska haastateltavien kesken yhteneväisyyksiä vastattaessa kysymyksiin jatkuvuuden hallinnasta havaittiin. Kritiikkiä voidaan esittää siitä, että kun haastatellaan saman yrityksen henkilöitä, onkin oletettavaa, että he puhuvat samasta näkökulmasta yleisesti sovittujen periaatteiden, toimintatapojen ja päivittäisessä työssä toistuvien rutiinien mukaisesti. Tutkielman reliabiliteettiin se ei mielestäni kuitenkaan vaikuta negatiivisesti, koska yksi tutkielman tarkoitus olikin kuvata case-yrityksen toimintatapoja jatkuvuuden hallinnassa. On siis itse asiassa positiivista huomata, että organisaation eri asemassa olevat haastateltavat ovat omaksuneet samanlaisen näkökulman ja periaatteet jatkuvuuden hallintaa koh-

taan. Toinen kritiikin aihe on se, että tutkimuksen reliabiliteetti olisi todennäköisimmin sitä korkeampi, mitä enemmän haastateltavia olisi tutkimukseen otettu. Toisaalta nyt haastatellut henkilöt edustivat parhainta mahdollista tietämystä, joten tämän takia ja resurssien vallitessa reliabiliteetin voidaan todeta olevan silti hyvällä tasolla.

Toinen käsite, jota usein käytetään tutkielmaa arvioitaessa, on validiteetti (tai validius). Järvinen ja Järvinen (2004) kuvaavat validiteettia siten, miten tarkasti teoria, käsite tai malli kuvaa reaalimaailmaa. ”Havainto mittaa sitä, mitä se on tarkoitettu mittaamaan”. (Järvinen & Järvinen, 2004). Hirsjärvi, Remes ja Sajavaara (2008) täsmentävät, että kyseessä on ns. validiusongelma, joka tarkoittaa sitä mittaavatko muuttujat sitä mitä oli tarkoituskin. Validius tarkoittaa Hirsjärven, Remeksen ja Sajavaaran (2008) mukaan pätevyyttä; vastaajat ovat saattaneet ymmärtää kysymykset toisella tavalla kuin haastattelija. Hirsjärvi, Remes ja Sajavaara (2008) toteavat, että laadullisen tutkimuksen luotettavuutta voi lisätä tarkalla selostuksella tutkimuksen toteuttamisesta. Siksi tässä tutkielmassa on kiinnitetty erityistä huomiota viidennen luvun tutkimusmetodi osuuteen. Myös tulosten tulkinnan pätevyydessä auttaa, jos tulkinnat on perusteltu ja tutkimusotetta on rikastettu suorilla haastatteluotteilla (Hirsjärvi, Remes & Sajavaara, 2008). Näin tässä tutkielmassa on pyritty myös toimimaan. Vaikka äänittäminen ei ollut mahdollista, muistiinpanot mahdollistivat suorien haastatteluotteiden käyttämisen tutkielmassa. Tutkielman validiutta on myös pyritty parantamaan Hirsjärven, Remeksen ja Sajavaaran (2008) kirjassa esitellyllä Denzin teoreettisella triangulaatiolla, jossa tutkittavaa ilmiötä on lähestytty eri näkökulmista. Tässä tutkielmassa triangulaatio näkyy selvimmin liiketoiminnan, IT-infrastruktuurin ja kriisinhallinnan näkökulmissa liiketoiminnan jatkuvuuden hallintaan. Sama jako oli myös tehty haastatteluiden teemoihin, joilla empiirisen osuuden validiutta kartutettiin.

7.3.3 Onnistuneisuus

Tutkimusta voidaan pitää varsin onnistuneena, koska tutkimusongelmiin saatiin kattavat vastaukset: uutta tietoa, jota kirjallisuudessa ei vielä oltu kovinkaan paljoa käsitelty, onnistuttiin löytämään. Erityisesti jatkuvuuden hallinnan kuvaaminen Pohjois-Euroopan johtavassa IT-palveluyrityksessä ja IT-palveluorganisaation jatkuvuuden hallinnan sitominen CMMI -tasomalliin ja laatukontekstiin oli sellaista, jota ei tietoni mukaan aikaisemmin oltu vielä tehty. Tutkimusongelmien asettelua voidaan pitää onnistuneena, koska mielestäni ongelmat auttoivat avaamaan jatkuvuuden hallinnan aihepiiriä kohdeorganisaatiossa pro gradu – tutkielmaan sopivalla laajuudella. Tutkimusongelmat olivat lisäksi sopivan syvällisiä, koska aiheen arkaluontoisuuden vuoksi jatkuvuuden hallinnan tarkempi kuvaaminen ei olisi ollut mahdollista.

Tutkimukseen käytettyjen resurssien puitteissa voidaan olla varsin tyytyväisiä tutkimuksen tuloksiin. Mikäli olisin laajentanut tutkimusta lisäämällä lähdeaineistoa tai haastateltavien määrää, tutkimuksen tulokset eivät todennäköisesti olisi oleellisesti muuttuneet. Tutkimuksessa olisi ollut mielenkiintoisia

alueita, joihin olisi ollut kiintoisaa pureutua tarkemmin, mutta edellä mainitun arkaluontoisuuden huomioiden pitää olla tyytyväinen saavutettuihin tuloksiin tällä tarkkuustasolla. Tutkielmassa käsiteltiin jatkuvuuden hallintaa kuitenkin monesta perspektiivistä käyttäen teoreettisia ja empiirisiä menetelmiä. Pääasia on kuitenkin se, että tutkielmalle etukäteen määriteltyihin tavoitteisiin päästiin: tutkimusongelmiin saatiin ratkaisut jo tällä tutkimuksen laajuudella.

8 YHTEENVETO JA JATKOTUTKIMUSKOHTEET

Tässä tutkielmassa on kuvattu liiketoiminnan jatkuvuuden hallintaa IT-palveluyrityksen näkökulmasta. Tutkimusongelmana oli, painottaako Tieto Oyj:n jatkuvuuden hallinnan strategia samoja asioita, kuten kirjallisuudessa esitetyt käytänteet? Eli ovatko jatkuvuuden hallinnan järjestelyt toteutettu Tieto Oyj:ssä samalla tavalla, kuin ne on kirjallisuudessa kuvattu. Aliongelmana selvitettiin, kuinka jatkuvuuden hallinnan tärkeys, tarve ja laajempi palvelutaso tulisi perustella IT-palvelutoimittajan asiakkaalle? Vastauksia tutkimusongelmiin haettiin kirjallisuuskatsauksen, viitekehyksen ja Tieto Oyj:ssä toteutetun case-tutkimuksen avulla.

Apuna case-tutkimuksessa käytettiin siis kirjallisuuden perusteella koottua jatkuvuuden hallinnan viitekehystä, johon oli koottu jatkuvuuden hallinnan käsitteet ja painopistealueet. Kirjallisuuskatsaus käsitteli jatkuvuuden hallintaa usean julkaisun näkökulmasta, joista merkittävimpinä voidaan pitää jatkuvuuden hallintaa ja tietoturvaa koskevia standardeja. Jatkuvuuden hallintaprosessin eteneminen kuvattiin tutkielman toisessa luvussa. Luvussa käsiteltiin jatkuvuuden hallinnan strategiaa, ohjelmaa organisaatiossa, riskienhallintaa ja tunnistamista, kriisinhallintaa sekä jatkuvuus- ja toipumissuunnittelua. Kolmannessa luvussa nämä jatkuvuuden hallinnan elementit otettiin tarkasteluun IT-palveluyrityksen toimintaympäristössä. Tässä luvussa nousivat esiin erityisesti IT-palvelutoimittajan vastuu tietokonekeskuksessa tuottamiensa palveluiden häiriöttömyydestä, sekä keinot häiriöttömyyden edistämiseen konesaleissa. Tätä kautta tarkasteltiin myös asiakassuhteiden merkitystä IT-palveluliiketoiminnassa jatkuvuuden hallinnan kannalta.

Kirjallisuudessa esiin nousseet painopisteet koottiin yhteen jatkuvuuden hallinnan viitekehykseen, joka esiteltiin luvussa neljä. Viitekehyksessä muodostui koko jatkuvuuden hallintaa kuvaavat tasot: strateginen, operationaalinen ja taktinen taso. Viitekehyksen tarkoituksena oli myös yhdistää tutkielman jatkuvuuden hallinnan teoreettinen osa paremmin empiirisen osaan, eli teemahaastattelujen avulla toteutettuun case-tutkimukseen.

Empiirisen osan case-tutkimuksen teemahaastatteluissa todettiin jatkuvuuden hallinnan olevan merkittävä osa nykyaikaista IT-palveluliiketoimintaa.

Teemahaastatteluissa käsiteltiin jatkuvuuden hallinnan teoreettiseen viitekehykseen liittyviä kysymyksiä, mutta myös tilaa vapaalle keskustelulle ja kommentoinnille jätettiin. Jatkuvuuden hallinnan osa-alueista erityisesti riskien tunnistaminen ja niiden vaikuttavuuden arviointi, jatkuvuussuunnitelmat ja johtotason strategiset päätökset koskien jatkuvuuden edistämistä nousivat pääosaan. Jatkuvuuden hallinnan merkityksen todettiin kasvavan IT-infrastruktuurin kompleksisuuden, konesalikomponenttien riippuvuussuhteiden, datan määrän kasvamisen ja datan käsittelyn lisääntymisen myötä. Erityisesti pilvipalvelut ja virtualisointi nousivat esiin tämän hetken ja lähitulevaisuuden haasteellisimpina ilmiöinä jatkuvuuden hallinnassa. Myös varautumisen ja kustannusten suhdetta pidettiin haasteellisena ja yleisesti vaikeana asiana selvittää.

IT-palvelutoimittajan kyvyn toimittaa häiriöttömiä ja jatkuvia palveluja todettiin olevan markkinoilla pärjäämisen ja kilpailukyvyn edellytys. Palvelujen toimittamisen jatkuvuuteen liittyy myös ITILv3:ssä esitelty toteamus: Palveluntarjoajaa tarvitaan, koska se on erikoistunut käsittelemään ratkaisuja koskevia kustannuksia ja riskejä. Muutenhan palveluita ei tarvittaisi. (ITILv3, 2007). Sama koskee jatkuvuuden hallintaa ja toiminnan varmentamista; häiriöttömyyden varmistamiseen kannattaa panostaa, koska kun palvelu on häiriöttömämpää, maksaa se itsensä asiakkaalle takaisin vältettyjen katkojen muodossa. Hyvin organisoidut jatkuvuuden hallinnan toimenpiteet auttavat pienentämään häiriöiden aiheuttamia kustannuksia. Kaikkea liiketoimintaa koskettavaa riskiä ei voida eliminoida, mutta vaikuttavuudeltaan suurimpia riskejä pyritään hallitusti pienentämään sellaiselle tasolle, että ne voidaan hyväksyä. Tilanne, jossa asiakasyritys voi kilpailijoistaan poiketen Tieto Oyj:n jatkuvuuden varmistuksien ansiosta jatkaa toimintaansa häiriöistä huolimatta, on varsin tavoiteltava. Siitähän jatkuvuuden hallinnassa alun perin olikin kyse: liiketoiminnan jatkumisen varmistaminen häiriöistä riippumatta.

Tutkielman eri vaiheissa syntyi monta ideaa, joita olisi mahdollista jalostaa jatkotutkimuskohteiksi. Mielenkiintoinen vaihtoehto olisi tutkimus, jossa IT-palveluyrityksen potentiaalisilta asiakkailta selvitettäisiin jatkuvuuden varmistamisen tarvetta. Toisena mahdollisena aiheena jatkotutkimukselle olisi virtualisoinnin ja mobiililaitteiden jatkuvuuden hallinta. Pilvipalveluiden lisääntyessä aihetta jatkuvuutta koskeville kysymyksille on entistä enemmän. Virtualisointi todettiin jo nyt haasteeksi jatkuvuuden hallinnalle, entäpä esimerkiksi viiden vuoden päästä? Älypuhelimet ja tablet-tietokoneet lähestyvät perinteistä tietokonetta kovaa vauhtia ja nämä laitteet voivat sisältää arkaluonteista tietoa aivan yhtä paljon, kuin tietoturvaltaan paremmat perinteiset tietokoneet. Tämä tutkimus voisi asettua tietoturvan ja jatkuvuuden hallinnan rajamaastoon. Aiheita riittää siis todella paljon, myös IT-palvelutoimittajan näkökulmasta jatkuvuuden hallinnan saralla tutkittavaa riittää; teknologian kehittyessä ja riippuvuuksien kasvaessa myös jatkuvuuden hallinnalle on yhä enemmän kysyntää.

LÄHTEET

Aaltola, J. & Valli, R. (2001). *Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle.* Jyväskylä: PS-kustannus, Gummerus Kirjapaino Oy.

Arno, R.B., Friedl, A., Gross, P. & Schuerger, R. (2010). Reliability of example data center designs selected by tier classification. *HP Critical Facility Services. Industrial and Commercial Power Systems Technical Conference (I&CPS), 2010 IEEE, 9-13 May, 1 – 8*. Tallahassee, FL, USA.

Benoit, W.L. (1997). Image repair discourse and crisis communication. *Public relations review 23 (2),* 177 -186.

Bhamidipaty, A., Lotlikar, R. & Banavar, G. (2007). RMI: A Framework for Modeling and Evaluating the Resiliency Maturity of IT Service Organizations. *IEEE International Conference on Services Computing, SCC 2007, 9-13 July 2007.* Salt Lake City, UT, USA.

Blyth, M. (2009). *Business Continuity Management: Building an Effective Incident Management Plan.* John Wiley & Sons, Inc., Hoboken, New Jersey.

Bureau Veritas Finland. (2007). ISO 9001 sertifiointi – Kilpailuetua laadun avulla. Haettu 26.1.2012 osoitteesta http://www.us.bureauveritas.com/wps/wcm/connect/bv_fi/local/home/bv_com_servicesheetdetails?serviceSheetId=6881&serviceSheetName=ISO+9001+sertifiointi/.

Business Continuity Management BCM Glossary. (2010). Business Continuity Institute – BCI. Haettu 4.1.2011 osoitteesta http://www.bcmpedia.org/wiki/Business_Continuity_Management_BCM_Glossary.

Bocij, P., Greasley, A. & Hickie, S. (2008). Business information systems: technology, development and management. (4. painos). *Harlow: Pearson Education Limited.*

Botha, J. & Von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management & Computer Security 12 (4),* 328-337.

BS 25999-1. (2006). British Standards Institution. *BS 25999-1 Code of practice for business continuity management.* Draft version.

Cerullo, V. & Cerullo, M. (2004). Business continuity planning: A comprehensive approach. *Information Systems Management; Summer 2004, 21 (3),* 70-78.

Cisco Systems, Inc. (2011a). Data Center High Availability Clusters Design Guide. Haettu 12.1.2012 osoitteesta: http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/HA_Clusters/HAOver_1.html/.

Cisco Systems, Inc. (2011b). Unified Computing and Servers: Blade Servers. Haettu 27.1.2012 osoitteesta: http://www.cisco.com/en/US/products/ps10265/index.html/.

Coleman, L. (2004). The frequency and cost of corporate crises. *Journal of Contingencies and Conflict Management, 12 (1),* 2—13.

Crump, G. (2009). The Single-Fabric Data Center. *InformationWeek, 1229*, 29.

Dey, M. (2011). Business Continuity Planning (BCP) methodology — Essential for every business. *2011 GCC Conference and Exhibition (GCC), 19-22 February, 229 – 232.* Dubai: IEEE Computer Society.

Duncan, J.W, Valerie, A., Yeager, A.C. & Rucks, P.M. (2010). Surviving organizational disasters. *Business horizons. 54 (2),* 135 -142.

Fang, Z. (2010). Governments' business continuity plan for records in the electronic age. Teoksessa *Advanced Management Science (ICAMS), 2010 IEEE International Conference on Advanced Management Science, July 9-11,* 157-159. Chengdu: IEEE Computer Society.

Force10 Networks, Inc. (2007). *Benchmarking Uptime for Your Business: Methodology and Best Practices.* Haettu 16.1.2012 osoitteesta http://www.force10networks.com/whitepapers/pdf/BenchmarkingUptime.pdf./

Grönroos, C. (2009). *Palvelujen johtaminen ja markkinointi*. (3. painos). Ekonomia-sarja. Juva: WSOY.

Harvard Research Group. (2004). HRG Insight: *The Total Cost of Downtime*. Harvard, P.O. Box 297 MA, USA. Haettu 16.1.2012 osoitteesta http://www.hrgresearch.com/pdf/paper4.pdf/.

Helms, R.W., Oorschot, S.V., Herweijer, J. & Plas, M. (2006). An integral IT continuity framework for undisrupted business operations. *In Proceedings of ARES.* 240-244.

Herbane, B., Elliot, D. & Swartz, M.E. (2004). *Business Continuity Management: time for a strategic role?* Long range planning, 37 (5), 435.

Hiles, A. (2007). *The definitive handbook of business continuity management.* (2. painos). Chichester: John Wiley & sons Ltd.

Hirsjärvi, S. & Hurme, H. (2001). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö.* Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2008). *Tutki ja kirjoita*. Helsinki: Tammi.

Hochmuth, P. (2004). The network behind the new data center. *Network world, 21 (7),* 18.

IBM. (2003). *Resilient Business and Infrastructure Analysis*. Haettu 8.2.2012 osoitteesta http://www-935.ibm.com/services/us/bcrs/pdf/ss_rbia.pdf/.

IBM. (2011). *Disaster recovery - Six tiers of solutions for off-site recovery*. IBM Information Center. Haettu 23.1.2012 osoitteesta http://publib.boulder.ibm.com/infocenter/cicsts/v3r1/index.jsp?topic=%2Fcom.ibm.cics.ts31.doc%2Fdfht2%2Fdfht2ln.htm/.

IBM. (2012). *IBM BladeCenter*. Haettu 27.1.2012 osoitteesta: http://www-03.ibm.com/systems/bladecenter/index.html./

ISF. (2011). Information Security Forum. *2011 Standard of Good Practice for Information Security.*

ISO 27001. (2005). International Organization for Standardization. *Information Technology – Security techniques – Information security management systems – Requirements.*

ISO 27002. (2005). International Organization for Standardization. *Information technology – Security techniques – Code of Practice for information security management.*

ISO 27005. (2008). International Organization for Standardization. *Information technology – Security techniques – Information security risk management.*

ISO/PAS 22399. (2007). International Organization for Standardization, Publicly Available Spesification. *Societal security – Guideline for incident preparedness and operational continuity management.*

ITIL v3. (2007). Information Technology Infrastructure Library, version 3. *Service strategy, Service design – IT-service continuity management*.

Järvinen, P. & Järvinen, A. (2004). *Tutkimustyön metodeista*. Tampere: Opinpaja Oy.

Kepenach, R.J. (2007). Business Continuity Plan Design. Teoksessa *Second International Conference on Internet Monitoring and Protection San Jose, California, July 1-5.* IEEE Computer Society, 27-31.

Kotler, P. & Armstrong, G. (1999). *Principles of Marketing.* (8. painos). Upper Saddle River, NJ: Prentice Hall.

La Fazia, T. (2004). Avoid disaster through planning. *Communication news 41(11),* 20, 22, 25.

Lam, W. (2002). Ensuring business continuity. *IT Professional 4 (3),* 19.

Lindström, J., Samuelsson, S. & Hägerfors, A. (2010). Business continuity planning methodology. *Disaster Prevention and Management 19 (2),* 243 – 255.

Lämsä, A.M. & Uusitalo, O. (2002). *Palvelujen markkinointi esimiestyön haasteena.* (1-3. painos). Helsinki: Edita.

Melton, A. & Trahan, J. (2009). Business continuity planning: overcoming disaster before it happens. (Risk Essentials). *Risk Management, ProQuest Central 56 (10) 46.*

NFPA. (2007). National Fire Protection Association. *NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs.* 2007 Edition. Quincy, MA, United States of America.

Novoselnik, G. (2007). A BCP Tale: From theory to practice. *Disaster Recovery Information Exchange Central. Annual General Meeting October 19, 2007 Canada Inn Club Regent, Winnipeg, Manitoba.* Haettu 5.1.2011 osoitteesta http://www.driecentral.org/bcptale.pdf/

Ollikainen, M. (2009). Bisneksen riippuvuus tietotekniikasta kasvaa – hallitaanko riskit?. Haettu 5.1.2011 osoitteesta: http://www.tietoviikko.fi/blogit/analyytikon_ikkuna/

PAS 56. (2003). Publicly Available Spesification 56 – *Guide to Business Continuity management.*

Patterson, D.A. (2002). A Simple Way to Estimate the Cost of Downtime. *The Proceedings of LISA '02: Sixteeth Systems Administration Conference, Berkeley, CA: USENIX Association.*

Peterson, C.A. (2009). Business continuity management & guidelines. *Information Security Curriculum Development Conference - InfoSecCD '09, Kennesaw, Georgia. September 25- 26*.

Qayoumi, M.H. (2002). Mission continuity planning: strategically assessing and planning for threats to operations. *National Association of College and University Business Officials, Annapolis Junction, MD*.

Reynolds, G. (2010). *Information technology for managers.* Boston: Course Technology, Cengage learning.

Savage, M. (2002). Business continuity planning. *International Journal of Productivity and Performance Management 51 (5),* 254-261 Emerald Group Publishing Limited.

Schaafstal, A.M, Johnston, J.H & Randall O.L. (2001). Training teams for emergency management. *Computers in Human Behavior 615 – 626.*

Shaw, G.L. (2005). *Business Crisis and Continuity Management.* Disciplines, Disasters and Emergency Management Textbook. Federal Emergency Management Agency Higher Education Project.

Siltanen, M. (2011). *Tietoturvallisuuden vaatimukset ja vaikutukset liiketoimintaan sekä yhteiskuntaan.* Haettu 10.1.2011 osoitteesta http://www.tietoturvapaiva.fi/uploads/Tietoturva2011/Tietoturvallisuuden%20vaatimukset%20ja%20vaikutukset%20liiketoimintaan%20seka%20yhteiskuntaan.pdf/.

Smit, N. (2005). *Business Continuity Management. A Maturity Model.* Master's Thesis Informatics & Economics. Erasmus Universiteit Rotterdam. Haettu 28.2.2012 osoitteesta http://tbm.home.tudelft.nl/fileadmin/Faculteit/TBM/Over_de_Faculteit/Afdelingen/Afdeling_Infrastructure_Systems_and_Services/Sectie_Informatie_en_Communicatie_Technologie/medewerkers/jan_van_den_berg/news/doc/naomi.pdf/.

SS 540. (2008). *Singapore Standard 540 for Business Continuity Management (BCM)*. Head Standardisation Department SPRING Singapore.

Sturdevant, C. (2011). Updating disaster plans. *IT-management, eWeek*. Haettu 5.1.2011 osoitteesta http://www.eweek.com/c/a/IT-Management/Take-a-Realistic-Approach-to-Business-Continuity-746629/.

Tammineedi, R.L. (2010). Business Continuity Management: A Standards-Based Approach. *Information Security Journal: A Global Perspective Vol. 19, Iss. 1.*

Tieto Oyj. (2012a). *Infrastruktuurin ulkoistuspalvelut.* Haettu 11.11.2012 osoitteesta http://www.tieto.fi/palvelut/it-palvelut/infrastruktuurin-ulkoistuspalvelut/.

Tieto Oyj. (2012b). *Tiedon palvelumalli tukee Tapiola-ryhmän kasvu- ja tehokkuusvaatimuksia.* Haettu 11.11.2012 osoitteesta http://www.tieto.fi/archive/top-stories/pankki-ja-vakuutus/tapiola-ulkoisti-kayttopalvelunsa-tiedolle/.

Tieto Oyj. (2012c). *ICT-palveluiden hallinta.* Haettu 12.11.2012 osoitteesta http://www.tieto.fi/palvelut/it-palvelut/ict-palveluiden-hallinta/.

Tieto Oyj. (2012d). *Tiennäyttäjä sähköisen maailman kärkeen*. Haettu 3.5.2012 osoitteesta http://www.tieto.fi/tiedosta/.

Tieto Oyj. (2012e). *Tiedon strategia 2012-2016*. Haettu 3.5.2012 osoitteesta http://www.tieto.com/archive/materials/investors/other-investor-materials/tieto-strategy-2012-2016-presentation-fi-pdf/.

Turner, D. (1994). Redesigning the service organization. *The Journal for Quality and Participation. Vol. 17, Iss. 1,* 28.

Uptime Institute. (2009). *Data Center Site Infrastructure Tier Standard: Topology*. Haettu 16.1.2012 osoitteesta http://atd.uptimeinstitute.com/PDFs/TierStandards.pdf./

Uptime Insitute. (2001). *Industry Standard Tier Classifications Define Site Infrastructure Performance.* By W. Pitt Turner IV, PE and Kenneth G. Brill, The Uptime Institute, 2001.

Vanston, M. (2003). *Business continuity and risk management: what's the difference?*. Risk management, ZDNet.com.au. Haettu 10.1.2012 osoitteesta http://www.zdnet.com.au/business-continuity-and-risk-management-whats-the-difference-120278233.htm/.

Wan, S.C.H. & Chan, Y. (2008). Adoption of business continuity planning processes in IT service management. *3rd IEEE/IFIP International Workshop on Business-driven IT Management Salvador, Brazil*

Virtual Corporation. (2003). The Business Continuity Maturity Model® (BCMM®). Haettu 28.2.2012 osoitteesta http://virtual-corp.net/html/bcmm.html/.

Wiboonrat, M. (2008). An Optimal Data Center Availability and Investment Trade-Offs. *SNPD '08 Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, Ninth ACIS International Conference August 6-8, 712 – 719,* Phuket, Thailand.

Winkler, U., Fritzsche, M., Gilani, W. & Marshall, A. (2010). A Model-Driven Framework for Process-Centric Business Continuity Management. *QUATIC '10 Proceedings of the 2010 Seventh International Conference on the Quality of Information and Communications Technology, IEEE Computer Society, September 29 - October 2, 248 – 252,* Porto, Portugal.

LIITE 1 HAASTATTELURUNKO: IT-INFRASTRUKTUURI

Taustatiedot

H1:

- Titteli: Risk manager. Corporate Lead Auditor, CAE. Risk Management Security and Internal Audit.
- Toimenkuva: Riskienhallinnan arviointi ja auditointi.

H2:

- Titteli: Security manager. Managed Services and Transformation - Datacenter Services, Data Centers & Storage
- Toimenkuva: Fyysinen turvallisuus, kulunvalvonta, kameravalvonta, paloturvallisuus ja riskienhallinta.

Kysymykset

- Mitä sinun mielestäsi jatkuvuuden hallinnalla tarkoitetaan?
- Mikä on mielestäsi jatkuvuuden hallinnan suhde riskienhallintaan?
- Miten näet jatkuvuus- ja toipumissuunnittelun kytkeytyvän jatkuvuuden hallinnan kontekstiin?
- Miten jatkuvuuden hallinta ilmenee IT-palveluliiketoiminnassa?
- Kuinka lainsäädäntö vaikuttaa jatkuvuuden hallinnan toimenpiteisiin tietokonekeskuksessa?
- Kuinka tietojärjestelmien prioriteetit määritetään, eli mitkä järjestelmät on kyettävä palauttamaan toimintaan ensimmäisenä?
- Kuinka voidaan varmistaa järjestelmien toimivuus poikkeustilanteissa?
- Kuinka datan varmuuskopiointi pitää toteuttaa, jottei tietoa pääse häviämään poikkeustilanteen ilmetessä?
- Miten virtuaaliympäristöjä kyetään hallitsemaan ja välttämään tilanne, jossa sattuman ohjaamana ja virtuaalielementtien erinomaisen siirrettävyyden seurauksena kriittiset elementit ovat sijoitettuna samaan konesaliin?
- Kuinka pitkä aika asiakasyritysten ostaman käyttöpalvelun keskeytymiselle on vielä hyväksyttävissä?
- Kuinka kauan vikojen ja häiriöiden tunnistaminen ja ongelman laajuuden selvittäminen saa kestää?
- Kuinka viat kyetään paikallistamaan tietokonekeskuksen todella kompleksisessa ympäristössä?

- Ohjaavatko toipumispistetavoitteet (RPO), toipumisaikatavoitteet (RTO) tai pisimmät hyväksyttävät katkot (MTD) tietokonekeskuksen palveluiden kehittämistä?
- Jos palveluille asetetuista aikarajoista toistuvasti lipsutaan, mitä sanktioita siitä seuraa ja mitä keinoja on käytettävissä palvelun luotettavuuden parantamiseen?
- Tietokonekeskuksen rakentamisvaiheessa on otettu huomioon kaikki mahdolliset häiriöttömyyttä ja sietokykyä edistävät seikat, mitä asioita voidaan vielä tehdä, kun tietokonekeskus on jo käytössä?
- Kuinka suuri redundanssi komponenttien varmistamisessa on vielä kustannusten osalta mielekästä?
- Perustuuko jatkuvuuden hallinnan strategia myös teknologian osalta palvelutasosopimuksissa ja hankintasopimuksissa määriteltyihin tavoitteisiin, vastuisiin ja lupauksiin?
- Mitkä ovat kriittiset menestystekijät IT-infrastruktuurin jatkuvuuden hallinnassa?
- Miten jatkuvuuden hallinnan rooli tietokonekeskuksessa on muuttunut viimeisen viiden vuoden aikana?
- Mitkä ovat tietokonekeskuksen ja IT-infrastruktuurin jatkuvuuden hallinnan suurimmat haasteet?
- Miten kuvailisit jatkuvuuden hallintaa kolmella - viidellä sanalla?

LIITE 2 HAASTATTELURUNKO: LIIKETOIMINTA

Taustatiedot

H3:

- Titteli: Global Security Manager, Käyttöpalvelut, Certified Information Systems Auditor
- Toimenkuva: Tieto Oyj:n käyttöpalveluiden tietoturvan periaatteet ja valvonta globaalisti.

H4:

- Titteli: Security Manager Finland
- Toimenkuva: Maakohtainen tietoturva, riskien arviointi, riskienhallinta

Kysymykset

- Mikä jatkuvuuden hallinnassa on merkittävintä liiketoiminnan kannalta?
- Miten liiketoimintakriittiset prosessit voidaan erottaa ei-liiketoimintakriittisistä?
- Kuinka liiketoimintaa koskettavien uhkien tunnistaminen ja luokitteleminen tapahtuu?
- Mikä riskien vaikutusten arvioinnissa on haasteellisinta?
- Voidaanko liiketoimintakriittisten prosessien onnistumisen mahdollistavia tekijöitä tunnistaa; onko eri prosesseilla erilaiset menestystekijät?
- Ketkä määräävät jatkuvuussuunnitelmien luomisesta, millä perusteella ratkaisut tehdään?
- Miten liiketoimintalähtöisyys näkyy Tieto Oyj:n jatkuvuuden hallinnassa?
- Onko jatkuvuuden hallinnan tärkeys tällä hetkellä paremmin perusteltavissa kuin viisi vuotta sitten?
- Onko liiketoiminnan jatkuvuudesta puhuttu enemmän suurten katastrofien yhteydessä kuin normaalisti?
- Onko maailmalla tapahtuneiden kriisien perusteella tarkasteltu jatkuvuussuunnitelmia?
- Kuinka lainsäädännölliset seikat vaikuttavat liiketoiminnan jatkuvuuden hallintaan?
- Kuinka helposti palvelutasosopimusten vaikeusaste on määriteltävissä; onko olemassa selkeä käsitys kuinka häiriöttömään palvelujen toimittamiseen pystytään?
- Missä määrin ulkoistaminen ja globaalien tuotanto- ja toimitusmallien yleistyminen vaikuttaa jatkuvuuteen ja palvelujen toimittamiseen?

- Mitä keinoja on luotettavuuden ja jatkuvuuden parantamiseen ns. kustannuksiltaan sopivampien alueiden maissa, kuten esimerkiksi Intian, Baltian ja Itä-Euroopan alueilla?
- Kuinka eritasoiset jatkuvuussuunnitelmat aina tietojärjestelmätasolta tietokonekeskukseen saakka kyetään pitämään linjassa toistensa kanssa?
- Mitkä ovat mielestäsi jatkuvuuden hallinnan erityispiirteet palveluliiketoiminnassa?
- Mihin jatkuvuuden hallinnan rooli on mielestäsi kehittymässä lähitulevaisuudessa?
- Voiko tulevaisuudessa palvelukeskuksen fyysisellä sijainnilla olla vaikutusta asiakkaiden vaatimuksiin palvelujen toimittamisen jatkuvuudesta tai onko tähän kiinnitetty jo huomiota?
- Miten kuvailisit jatkuvuuden hallintaa kolmella-viidellä sanalla?

LIITE 3 HAASTATTELURUNKO: KOKONAISNÄKYMÄ

Taustatiedot

H5:

- Titteli: Chief Security Officer, CSO
- Toimenkuva: Turvallisuusjohtaja, turvallisuusstrategia, jatkuvuuden hallinnan strategia, riskienhallintastrategia, turvallisuuden hallintajärjestelmä

Kysymykset

- Miten jatkuvuuden hallinnan strategia on muodostettu?
- Mitkä standardit/ hyvät käytännöt ovat vaikuttaneet jatkuvuuden hallinnan strategian muodostamiseen?
- Miten jatkuvuuden hallinnan kokonaisuutta pyritään hallitsemaan?
- Kuinka avainhenkilöiden roolit on täsmennetty rooleissa toimiville henkilöille, osaavatko he toimia poikkeustilanteessa oikein?
- Tietävätkö avainhenkilöt, missä kokoonpanossa/ryhmässä toimivat kriisitilanteessa? Osaavatko he sanoa ketä heidän ryhmäänsä kuuluu?
- Miten kriisitilannetta pyritään käytännössä hallitsemaan?
- Kenellä on vastuu toiminnan ohjaamisesta, ja kuka päättää milloin on kriisitilanne?
- Kuinka voidaan varmistaa tietämyksen siirtyminen yksittäiseltä henkilöltä toiselle esimerkiksi vakavissa sairastapauksissa? Entä kokonaista liiketoimintayksikköä koskettavissa epidemioissa tai peräti pandemioissa?
- Liittyykö globaaleihin tuotanto- ja toimitusmalleihin ja alihankintaan jatkuvuutta koskevia riskejä?
- Miten palveluja voidaan tuottaa kaukaa liiketoiminnan jatkuvuus varmistaen?
- Kuinka eritasoiset jatkuvuus- ja toipumissuunnitelmat kyetään pitämään linjassa ja vastaamaan muuttuviin liiketoiminnan vaatimuksiin?
- Miten suunnitelmien testaaminen ja arviointi käytännössä toteutetaan ja mitä asioita niillä pyritään saavuttamaan?
- Vaihteleeko suunnitelmien testaaminen ja arviointi suunnitelman tason ja yksityiskohtaisuuden mukaan?
- Mitä vaikutuksia mahdollisesti hankittavilla jatkuvuuden hallinnan sertifikaateilla voisi olla Tiedon kilpailukyvylle?
- Kuinka lainsäädäntö tukee/rajoittaa jatkuvuuden hallinnan toimenpiteitä?

- Onko jatkuvuuden hallinnan kehittämiseen käytettävänä riittävästi resursseja?
- Miten jatkuvuuden hallinta sulautetaan käytännössä osaksi organisaation toimintakulttuuria?
- Nähdäänkö BCM välttämättömänä tehtävänä, vai mahdollisuutena kilpailukyvyn parantamiseen luotettavuuden muodossa?
- Mitä asioita voidaan tehdä jatkuvuuden hallinnan vaatimukset selkeästi ylittäen?
- Mitä taktisen tason jatkuvuutta tukevia ja tehostavia asioita pyritään tekemään?
- Mihin jatkuvuuden hallinnan rooli on mielestäsi kehittymässä lähitulevaisuudessa?
- Mitkä ovat jatkuvuuden hallinnan suurimmat haasteet?
- Miten kuvailisit jatkuvuuden hallintaa kolmella-viidellä sanalla?