



TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

JONAS KURTTO
JATKUVUUSSUUNNITTELULLA JA ICT-VALMIUDELLA
TIETOTURVALLISEMPI JA SIETOKYKYISEMPI ORGANISAATIO

Diplomityö

Tarkastaja: professori Pekka Loula
Tarkastaja ja aihe hyväksyty
Talouden ja rakentamisen
tiedekuntaneuvoston kokouksessa
9. joulukuuta 2015

TIIVISTELMÄ

JONAS KURTTO: Jatkuvuussuunnittelulla ja ICT-valmiudella tietoturvalisempi ja sietokykyisempi organisaatio
Tampereen teknillinen yliopisto
Diplomityö, 102 sivua, 3 liitesivua
Tammikuu 2016
Tietotekniikan diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietoverkkojen hallinta ja tietoturva
Tarkastaja: professori Pekka Loula

Avainsanat: liiketoiminnan jatkuvuussuunnittelu, jatkuvuussuunnitelma, riskienhallinta, ICT-valmius, tietoturva

Työssä pyritään parantamaan kuntasektorilla toimivan tietotekniikan palvelukeskuksen Tipakkeen jatkuvuudenhallintaa. Jatkuvuussuunnittelua kehittämällä on mahdollista saavuttaa tietoturvalisempi organisaatio, joka on samalla sietokykyisempi sitä uhkaavia häiriötä ja riskejä vastaan.

Jatkuvuussuunnittelun ja jatkuvuudenhallinnan hyviä käytäntöjä tutkitaan työn teoriaosassa perehtymällä alan kirjallisuuteen ja standardeihin. Organisaation nykyinen jatkuvuudenhallinnan dokumentaatio analysoidaan työn empiirisessä osassa peilaamalla sitä teoriaan. Analyysillä pyritään havaitsemaan puutteita ja kehityskohteita nykyisessä toiminnassa. Hyväksi havaittuja toimintatapoja sovelletaan organisaation toimintaan esittämällä kehitysehdotuksia jatkuvuudenhallintatoimenpiteisiin.

Kirjallisuustutkimuksen lisäksi suoritetaan laadullinen kyselytutkimus, jonka tarkoituksena on saada organisaatiokohtaista lisätietoa kehityskohteiden havaitsemisen tehostamiseksi. Kyselytutkimuksesta saatu informaatio analysoidaan ja sen perusteella tehdään kehitysehdotuksia nykyisiin toimintatapoihin.

Suoritetun nykytilan analyysin ja kyselytutkimuksen perusteella Tipakkeen suurimmat haasteet liittyvät henkilöstön osaamiseen ja resursseihin liittyviin riskeihin varautumiseen sekä jatkuvuudenhallinnan toimenpiteiden koulutukseen ja harjoitteluun. Riskit on analysoitava ja priorisoitava rajallisten resurssien tehokkaaksi kohdentamiseksi. Jatkuvuussuunnitelmassa mainittujen toimenpiteiden koulutus henkilöstölle ja häiriötilanteiden harjoittelu etukäteen on välttämätöntä organisaation häiriösietoisuuden kasvattamiseksi.

Tipakkeen tulee varmistaa, että jatkuvuudenhallinnan toimenpiteiden koulutukseen ja harjoitteluun on saatavilla riittävät resurssit. Jatkuvuussuunnittelu on jatkuvaan parantamiseen pyrkivä jatkuva prosessi, jonka avulla Tipake voi säilyttää toimintakykynsä myös yllättävissä häiriötilanteissa.

ABSTRACT

JONAS KURTTO: Continuity planning and ICT-readiness for a more secure and resistant organization

Tampere University of Technology

Master of Science Thesis, 102 pages, 3 Appendix pages

January 2016

Master's Degree Programme in Information Technology

Major: Network Management and Information Security

Examiner: Professor Pekka Loula

Keywords: business continuity, continuity plan, risk management, ICT-readiness, information security

The aim of this thesis is to improve the continuity management of Tipake ICT service centre that operates in the public sector. By improving continuity planning it is possible to achieve a more secure organization that is also more resilient against threats and risks at the same time.

The best practices of continuity planning and continuity management are researched by studying relevant literature and standards in the theoretical part of the thesis. The organization's existing continuity management documentation is analysed in the empirical part of the thesis by mirroring it to the theory. The aim of the analysis is to notice deficiencies and potential points of development in current approaches. The best practices are applied to the organization's approaches by providing development suggestions to existing continuity management measures.

In addition to the literature research a qualitative survey is conducted to gain organization-specific information to improve the discovery of points of development. The information gained from the survey is analysed and used to suggest development points to current measures.

On the basis of the conducted analysis and the results of the survey Tipake's biggest challenges are related to the preparedness against risks related to knowledge and resources of personnel and also to the education and training of continuity management measures. Risks must be analysed to allocate limited resources effectively. The education of the measures stated in the continuity plan and training of disruptive events beforehand is essential to increase the tolerance for disruptions.

Tipake needs to make sure that there are necessary resources available for education and training of continuity management measures. Continuity planning is a continuous process that aims for continuous improvement and by which Tipake can remain functional in unexpected disruptions.

ALKUSANAT

Haluan kiittää HTL Ari Sainiota tuesta, hyvistä neuvoista ja perehtymisestä diplomityöhön sekä tutkimuksen toteuttamisen mahdollistamisesta. Kiitokset myös Liisa Dahlstedtille hänen avustaan kyselytutkimuksen toteuttamisessa.

Diplomityön tarkastaja, professori Pekka Loula ansaitsee myös kiitokset tuestaan työn eri vaiheissa.

Keravalla, 18.1.2016

Jonas Kurtto

SISÄLLYSLUETTELO

1.	JOHDANTO	1
2.	TIETOTURVALLISUUS JA RISKIENHALLINTA	2
2.1	Tieto-omaisuus	2
2.2	Tietoturvallisuuden tavoitteet.....	6
2.3	Tietoturvallisuuden osa-alueet	8
2.4	Riskienhallinnan tavoitteet ja osa-alueet.....	13
2.5	Riskien luokittelu	15
2.5.1	Tietoriskit	17
2.5.2	IT-riskit	20
3.	JATKUVUUSSUUNNITTELU	25
3.1	Jatkuvuussuunnittelun osa-alueet.....	29
3.1.1	Koordinointi, ohjeistus ja vastuutus.....	31
3.1.2	Kriittisten prosessien tunnistaminen	33
3.1.3	Riskianalyysi.....	36
3.1.4	Liiketoiminnan keskeytysvaikutusanalyysi	41
3.1.5	Riskien torjunta ja vaikutusten pienentäminen	44
3.1.6	Suunnitelman dokumentointi, testaus ja ylläpito	47
4.	ISO/IEC 27031 -STANDARDI	51
4.1	ICT-valmius	53
4.2	ICT-valmiuden suunnittelu	55
4.3	ICT-valmiuden käyttöönotto	60
4.4	ICT-valmiuden ylläpito	63
5.	ORGANISAATION NYKYTILA	69
6.	JATKUVUUDENHALLINNAN KEHITTÄMINEN	74
6.1	Tutkimusongelma ja -menetelmät.....	74
6.2	Kyselytutkimuksen suorittaminen.....	74
6.3	Nykytilan analyysi	76
6.4	Kyselytutkimuksen tulokset ja analyysi.....	78
6.4.1	Yleiset käsitykset	79
6.4.2	Tietoturvallisuus ja riskienhallinta.....	80
6.4.3	Koulutus ja harjoittelu.....	82
6.4.4	Viestintä ja tiedottaminen	85
6.4.5	Resurssit	87
6.4.6	Vastuut	88
6.5	Jatkuvuudenhallinnan kehittämisen ratkaisumalli	91
7.	YHTEENVETO	96
	LÄHTEET	98

LYHENTEET JA MERKINNÄT

BCM	engl. Business Continuity Management, liiketoiminnan jatkuvuudenhallintaprosessi
BCMS	engl. Business Continuity Management System, liiketoiminnan jatkuvuudenhallintajärjestelmä
BIA	engl. Business Impact Analysis, liiketoiminnan keskeytysvaikutusanalyysi
BYOD	engl. Bring Your Own Device, henkilökohtaisten laitteiden käyttö organisaatiossa
EMV	engl. Expected Monetary Value, odotetun rahallisen arvon analyysi
ERM	engl. Enterprise Risk Management, kokonaisvaltainen riskienhallinta
ICT	engl. Information and Communications Technology, tieto- ja viestintäteknologia
ILM	engl. Information Lifecycle Management, tiedon elinkaaren hallinta
IRBC	engl. Information Security Management System, hallintajärjestelmä riskejä ja seurauksia vastaan
ITIL	engl. Information Technology Infrastructure Library, kokoelma IT-palveluiden hallinnan ja johtamisen käytäntöjä
MBCO	engl. Minimum Business Continuity Objective, toiminnon minimipalvelutaso
MTO	engl. Maximum Tolerable Outage, keskeytyksen enimmäissieto aika
MTPD	engl. Maximum Tolerable Period of Disruption, häiriöiden sietokyvyn enimmäisaika
NIST	engl. National Institute of Standards and Technology, USA:n standardointiviranomainen
PDCA	engl. Plan, Do, Check, Act, PDCA-kehityssykli
RAID	engl. Redundant Array of Independent Disks, vikasietoisuutta ja/tai nopeutta parantava kiintolevytekniikka
RPO	engl. Recovery Point Objective, toipumispiste
RTO	engl. Recovery Time Objective, toipumisaika
SLA	engl. Service Level Agreement, palvelutasosopimus
TIPAKE	Tietotekniikan palvelukeskus -liikelaitos
UPS	engl. Uninterruptible Power Supply, varavoimalaite

1. JOHDANTO

Tässä diplomityössä käsitellään jatkuvuussuunnittelua kohdeorganisaation toiminnan jatkuvuuden parantamisen työkaluna. Kohdeorganisaatio on Keravan kaupungin tietotekniikan palvelukeskus -liikelaitos (jatkossa Tipake). Tipake toimii asiakkaittensa, Keravan ja Järvenpään kaupunkien sekä Mäntsälän kunnan IT-palveluiden tuottajana ja yhteishankintayksikkönä.

Tipake pyrkii tuottamaan kustannustehokkaita perustietotekniikan infrastruktuuriratkaisuja ja tietojärjestelmiä, mukaan lukien työasemahallinta-, konesali-, tietoliikenne- ja tietoturvapalveluita. Tipakkeen tavoitteena on tarjota kuntasektorille soveltuvaa, laadukasta IT-palvelua ja kehittää toimintaansa yhteistyössä asiakkaittensa kanssa pystyäkseen vastaamaan parhaiten laajaan palveluntarpeeseen.

Diplomityön tavoitteena on selvittää kirjallisuudessa, tieteellisissä artikkeleissa ja standardeissa esitettyjen, hyväksi havaittujen toimintatapojen soveltamista Tipakkeen toimintaan sekä kehittää Tipakkeen jatkuvuudenhallintaa.

Työn teoriaosassa käydään läpi jatkuvuussuunnitteluprosessi siihen liittyvine kokonaisuuksineen. Teoriaosan luvuissa 2 ja 3 käsitellään tieto-omaisuutta, tietoturvallisuutta, riskienhallintaa ja jatkuvuussuunnittelua kirjallisuuteen ja tieteellisiin artikkeleihin pohjautuen. Teoriaosan luvussa 4 käsitellään ICT-varautumista koskevaa ISO/IEC 27031 -standardia.

Työn empiirisessä osassa tutkitaan organisaatiota ja kuvataan tutkimusongelma sekä ongelman selvittämiseksi laadittu tutkimus johtopäätöksineen. Empiirisen osan luvussa 5 kuvataan Tipakkeen jatkuvuudenhallinnan nykytila. Empiirisen osan luvussa 6 kuvataan tutkimusongelma ja käydään lävitse Tipakkeen henkilöstölle laaditun kyselytutkimuksen suorittaminen. Luvussa 6 esitetään lisäksi nykytilassa havaitut kehittämiskohteet toimenpide-ehdotuksineen ja kyselytutkimuksen tulokset analysoituna. Nykytilaa ja kyselystä saatuja vastauksia analysoimalla pyritään kehittämään Tipakkeen jatkuvuudenhallintaa teoriaosassa esitettyjen käytäntöjen ja toimintatapojen mukaisesti.

Diplomityössä tutkittavaa aluetta on rajattu siten, että erinäisiä jatkuvuudenhallinnassa käytettäviä teknisiä menetelmiä, kuten varmistus- ja varavoimajärjestelmiä ei käsitellä kuin yleisellä tasolla eikä niiden teknisiin toimintaperiaatteisiin perehdytä tarkemmin. Tämän lisäksi jatkuvuudenhallintaa pyritään kehittämään ensisijaisesti parantamalla olemassa olevia jatkuvuudenhallintatoimenpiteitä teoriaosassa esitettyjen asioiden osalta.

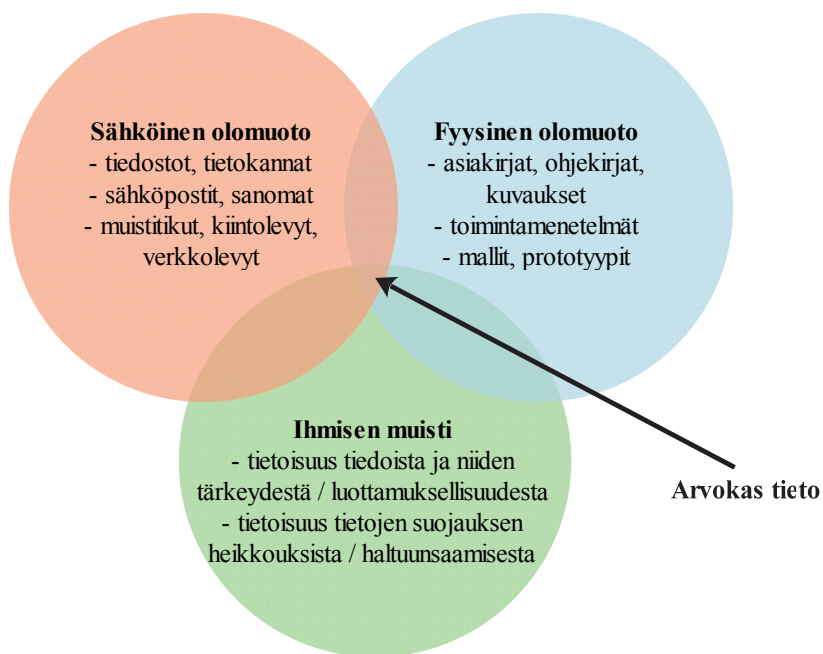
2. TIETOTURVALLISUUS JA RISKIENHALLINTA

Käsite *tieto* voidaan ymmärtää monilla eri tavoilla. Kurosen (1998, s. 8) määritelmän mukaan tieto koostuu datasta ja informaatiosta: Data on vaihteleva kokoelma merkkejä, numeroita, koodeja, pulsseja tai signaaleita, joihin ei välttämättä liity mitään merkitystä ja jotka eivät välttämättä ole tulkittavissa tai omaksuttavissa tiedoksi. Informaatio on dataa, johon on liitettävissä merkitys tai tulkinta. Tieto on puolestaan ymmärrettävissä ja omaksuttavissa olevaa informaatiota. Esimerkkinä datasta esitetään television kohina eli ”lumisade” ja informaatiosta fysiikan alaan kuuluvat Maxwellin yhtälöt, jotka muuttuvat ymmärrettäväksi tiedoksi riittäväillä matematiikan ja fysiikan opinnoilla.

Laihonen et. al. (2013, s. 17-18) puolestaan määrittelevät tiedolle 3 eri tasoa ja määritelmää. Data määritellään rakenteettomiksi tosiasioiksi. Informaatio määritellään rakenteelliseksi dataksi, joka on käytettävissä analyyseissä. Tietämys määritellään inhimilliseksi, usein kokemukseen perustuvaksi tiedoksi. Tämän lisäksi tieto erotellaan kahteen tasoon: Kokemuksen kautta henkilölle kertyneeseen hiljaiseen tietoon, jota voidaan kuvata intuition ja osaamisena sekä usein kirjalliseen muotoon puettuun, helposti tallennettavaan ja siirrettävään eksplisiittiseen tietoon, kuten matemaattisiin ilmaisuihin.

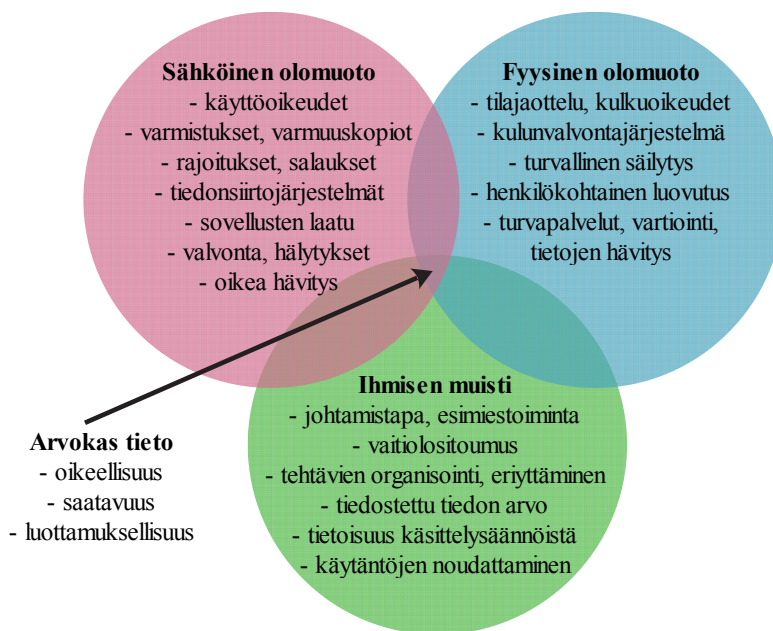
2.1 Tieto-omaisuus

Organisaation henkilöstö käsittelee työssään monesti organisaation liiketoimintaan ja asiakkaisiin liittyviä tietoja erilaisin välinein ja ohjelmistoin. Tärkeän tiedon suojaaminen vaatii tiedon olemassa olon tunnistamisen. Tiedon suojaaminen edellyttää organisaation henkilöstöltä kykyä tiedon tunnistamiseen, luokitteluun ja käsittelyyn. Sähköisessä muodossa olevaa tietoa suojataan teknisillä menetelmillä ja suojauskeinoilla. Fyysisen suojauksen, kuten kulunvalvonnan osuus tietojen suojaamisessa on myös oleellista. Tiedon merkityksen ja arvon selvittämiseksi sekä tiedon suojaamisen tarpeen arvioimiseksi on tunnistettava tiedon eri olomuodot. Tärkeä ja arvokas tieto voi olla missä tahansa olomuodossa. On tärkeää tunnistaa, että tiedon eri olomuotojen suojausmenetelmät riippuvat tiedon käsittelyketjusta. (Kyrölä 2001, s. 24). Tiedon ja sen käsittelyketjun eri olomuodot on esitetty kuvassa 1.



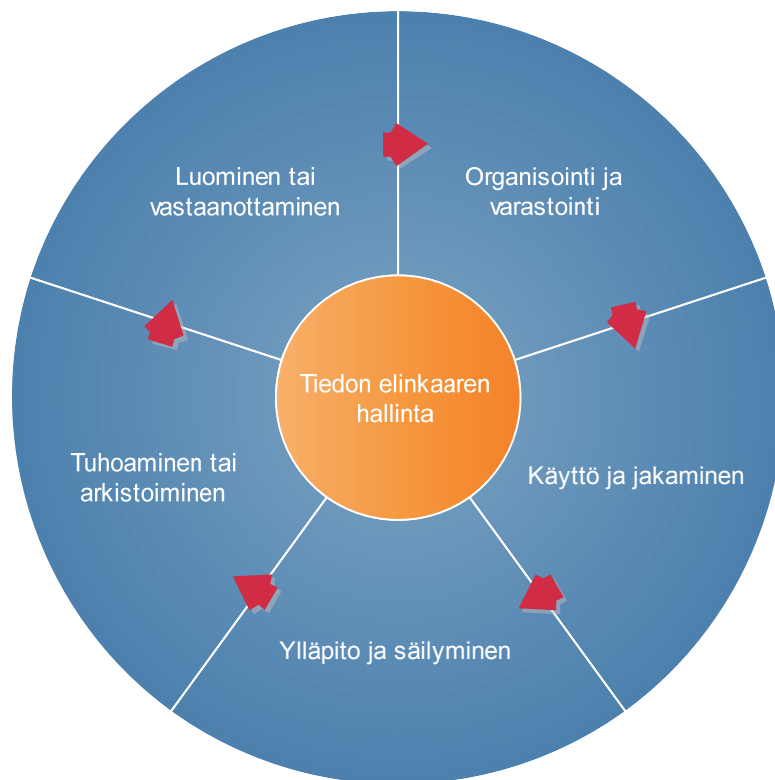
Kuva 1. Tiedon ja sen käsittelyketjun erilaiset olomuodot (mukaellen Kyrölä 2001 s. 25).

Tietoturvallisuustyön ja tietoriskien hallinnan perusvaatimusten mukaisesti tiedolle määritetään oikeellisuus-, käytettävyys- ja luottamuksellisuusvaatimukset. Näiden vaatimusten mukaisesti luodaan menettelyt ja keinot, joilla varmistetaan tärkeiden tietojen saatavuus ja järjestelmien käyttö, tietojen oikeellisuus ja eheys sekä järjestelmien toiminnan oikeellisuus ja ajantasaisuus sekä tietojen luottamuksellinen käsittely ja järjestelmien rajattu käyttö. (Kyrölä 2001, s. 24). Tiedon suojauskeinot olomuodoittain on esitetty kuvassa 2.



Kuva 2. Tiedon suojauskeinot olomuodoittain (mukaellen Kyrölä 2001, s. 127).

Tiedolla on elinkaari, joka alkaa tiedon luomisesta tai vastaanottamisesta. Elinkaari jatkuu organisoinnilla ja varastoinnilla, käytöllä ja jakamisella, ylläpidolla ja säilymisellä ja päättyy tiedon poistamiseen. Poistaminen voi tarkoittaa pysyvän tuhoamisen lisäksi myös pysyvää säilyttämistä, arkistointia. (Dederer & Dmytrenko 2015, s. 32). Tiedon arvo vaihtelee elinkaaren eri vaiheissa, mutta tietoturvallisuus on tärkeää elinkaaren vaiheesta riippumatta (Siponen 2014). Tiedon elinkaaren vaiheet on esitetty kuvassa 3.



Kuva 3. Tiedon elinkaaren vaiheet (mukaillen Dederer & Dmytrenko 2015, s. 33).

Tiedon elinkaaren hallinnan (engl. Information Lifecycle Management, ILM) avulla pyritään lisäämään tiedon saatavuutta, vähentämään riskejä ja kustannuksia sekä lisäämään liiketoiminnan taloudellisuutta. ILM sisältää määritelmät mitä tietoa organisaatiolla on, missä sitä säilytetään, kuka on tiedon omistaja ja tiedosta vastuullinen taho, miksi tietoa säilytetään, kuinka nopeasti ja helposti tietoa voidaan käyttää, kuinka tiedon muutoksia seurataan sekä kuinka kauan tietoa on säilytettävä. (Dederer & Dmytrenko 2015, s. 32).

Dederer ja Dmytrenko (2015, s. 33-35) määrittelevät parhaiden käytäntöjen menetelmän tiedon elinkaaren hallintaan, joka sisältää 8 vaihetta:

1. *Informaatiosta oppiminen*: On selvítettävä, mitä informaatiota on olemassa, missä informaatio sijaitsee, kuka omistaa informaation, miksi informaatiota säilytetään, koska informaatio voidaan poistaa ja kuinka informaatiota varastoidaan.

2. *Johdon tuen saaminen*: Tiedon elinkaaren hallinnasta suoriutuminen työntekijätasolla edellyttää organisaation johdon halukkuutta. Johtotason on varmistettava, että ILM tukee organisaation tavoitteita, korostettava toiminnan noudattamisen merkitystä, määriteltävä roolit ja vastuut sekä osoitettava esimerkkiä.
3. *Yhteistyön tekeminen*: Organisaatio saavuttaa suurempia tuloksia yhteistyöllä. Yhteistyöhön tulisi osallistua ainakin laki- ja IT-osaamista omaavat tahot sekä riskienhallinnan ja liiketoiminnan osaajat, tarvittaessa organisaation ulkopuolelta.
4. *Työryhmän luominen*: Työryhmään tulisi kuulua organisaation johdon lisäksi myös henkilöitä, jotka ymmärtävät tiedon merkityksen liiketoiminnallisten tavoitteiden saavuttamisessa oman yksikkönsä työssä. Työryhmä voi myös vaikuttaa muutosten onnistumiseen ja varmistaa, että tehdyt toimet edustavat organisaation tarpeita.
5. *Sääntöjen ja menetelmien luominen*: Henkilöstöä on koulutettava jatkuvasti ja tehty dokumentaatio on oltava helposti saatavilla. Säännöt ja sanktiot on oltava selkeästi määriteltyjä. Sääntöjä ja menetelmiä laadittaessa on huomioitava organisaation riskinsietokyky esimerkiksi tiedon arkistoinen tai lopullisen hävittämisen suhteen. Säännöt ja menetelmät on päivitettävä säännöllisesti ja informoitava henkilöstölle johdon ja työryhmän toimesta.
6. *Uusien järjestelmien huomioiminen*: Uusien käyttöön otettavien järjestelmien on mukauduttava tiedon hävittämisen ja arkistoinen aiheuttamiin vaatimuksiin. Järjestelmän käyttöönoton jälkeen on myös päivitettävä organisaation tiedon sijaintikartta.
7. *Kaikkien järjestelmien valvonta*: Tieto on luokiteltava poistamiskäytäntöjen noudattamiseksi. Tiedon elinkaaren viimeisen vaiheen toteuttaminen edellyttää yhteistyötä päätösvalan omaavan tahon kanssa.
8. *Dokumentaation tekeminen*: Tehdyt toimenpiteet on dokumentoitava ongelmatilanteiden varalta. Jotta dokumentaatio pysyy ajantasaisena, se on katselmoitava ja päivitettävä vähintään vuosittain.

Organisaatio ei voi hallita tietoa, jota se ei tiedä omaavansa. Tietoa saadaan monista eri lähteistä ja kaikki nämä lähteet on tunnistettava tiedon määrän selvittämiseksi. Tieto voi myös sijaita eri paikoissa, kuten organisaation omissa palvelintiloissa tai pilvessä. Tiedon olinpaikkojen kartoittamiseen voidaan käyttää tietokarttaa, josta selviää tietojen fyysiset sijaintipaikat. Vaikka organisaation IT-osasto on vastuullinen tietojärjestelmien ja tietotekniikan toimivuudesta, se ei omista niissä sijaitsevia tietoja. Tiedon omistajan määrittämiseksi on tiedettävä tietojärjestelmiä käyttävät tahot, kuten liiketoimintayksiköt. Omistajan lisäksi on määriteltävä, millaisia käyttöoikeuksia tietoon eri tahoilla tulee olla. Kaikkea tietoa ei kannata myöskään säilyttää pysyvästi. Tietoja hävittäessä on selvitettävä tiedon ikä, omistaja, liiketoiminnallinen arvo ja käyttötarkoitus sekä mahdolliset lakiin liittyvät tekijät. (Dederer & Dmytrenko 2015, s. 33).

2.2 Tietoturvallisuuden tavoitteet

Tietoturvallisuudella pyritään kolmeen tavoitteeseen, jotka ovat luottamuksellisuus (engl. confidentiality), eheys (engl. integrity) ja saatavuus (engl. availability). Tieto on luottamuksellista, kun siihen pääsy on rajoitettu oikeutetuille tahoille. Tiedon eheys tarkoittaa, että tietoon saa kohdistua ainoastaan oikeutettuja muutoksia käsittelyn ja käytön aikana. Saatavuudella tarkoitetaan tiedon saatavilla oloa, koneiden käytettävyyttä ja palvelujen toimivuutta. (Järvinen 2012, s. 10). Jokaisen tietoturvallisuuden osa-alueen tärkeys vaihtelee järjestelmittäin ja organisaatioittain. Joissakin tietojärjestelmissä voi olla informaatiota, jonka luottamuksellisuus on kriittisempää kuin saatavuus. (Lehtinen et. al. 2006, s. 9).

Lehtinen et. al. (2006, s. 9) puolestaan määrittelevät tietoturvallisuuden tavoitteet seuraavasti: Tieto on luottamuksellista, kun se on tuntematonta kaikille muille paitsi oikeutetuille tahoille. Tieto on eheää, kun se ei ole muuttunut viimeisimmän sallitun muutoksen jälkeen. Tieto on saatavilla, kun se on oikeutettujen tahojen käytettävissä sopivassa muodossa ja kohtuullisessa ajassa.

Fåk (2010, s. 149) mainitsee, että on olemassa kolme päätapaa, joissa voi syntyä virheitä:

1. Tarvittavaa dataa ei kyetä toimittamaan (saatavuus)
2. Toimitettu data on virheellistä (eheys)
3. Data toimitetaan asiattomalle taholle (luottamuksellisuus)

Tiedon luottamuksellisuus voidaan toteuttaa salaamisella, pääsynvalvonnalla, todennuksella, valtuutuksella ja fyysisen turvallisuuden avulla. Tiedon eheys voidaan varmistaa varmuuskopioimalla, tarkistussummilla ja tietoa korjaavilla koodeilla. Tiedon saatavuus voidaan varmistaa fyysisellä suojauksella ja laitteistojen kaksinkertaistamisella, kuten RAID-tekniikalla ja varalaitteilla. (Karvi 2012). Gordonin (2002, s. 12-15) mukaan organisaatioissa käytetään monesti nauhavarmistuksia tiedon varmuuskopioimiseksi ja saatavuuden parantamiseksi. Tällöin voidaan tarvittaessa palata aikaisempaan, varmuuskopioituun tilaan, jos tietoa on hävinnyt tai korruptoitunut.

Basin et. al. (2011, s. 2) määrittelevät tietoturvallisuuteen liittyen käsitteet subjekti ja objekti. Subjektit ovat aktiivisia kokonaisuuksia, kuten käyttäjiä tai järjestelmiä, jotka toimivat käyttäjien määrittämällä tavalla. Objektit ovat passiivisia säiliöitä, jotka varastoivat informaatiota tai dataa. Esimerkkejä objekteista ovat tallenteet, tiedostot, hakemistot ja tietojärjestelmät. Basin et. al. (2011, s. 12) lisäävät tietoturvallisuuden tavoitteisiin myös tilivelvollisuuden (engl. accountability). Tämä tarkoittaa toimia, kuten tapahtumalokeja, joilla tietty tapahtuma voidaan yhdistää tiettyyn subjektiin, jota voidaan pitää tilivelvollisena tapahtumasta.

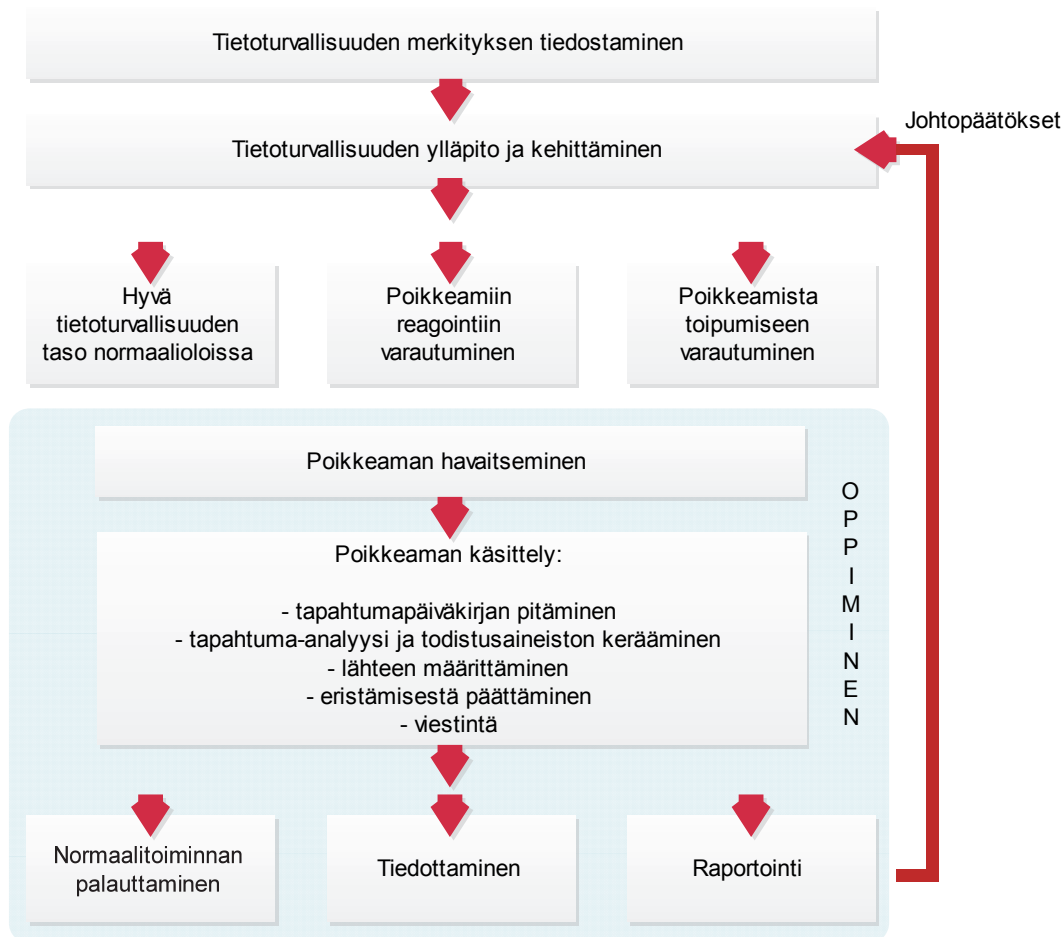
Nykyaikaisessa tietoturvatutkimuksessa ja -käytännössä käytetään lisäksi kolmea muuta käsitettä. Nämä käsitteet ovat varmuus (engl. assurance), autenttisuus (engl. authenticity) ja anonymiteetti (engl. anonymity). (Karvi 2012).

Varmuudella tarkoitetaan luottamuksen muodostamista ja ylläpitämistä tietokonesysteemeissä. Luottamus syntyy, kun ihmiset ja systeemit toimivat odotetulla tavalla. Luottamus muodostuu kolmen tekijän yhteistoiminnasta. Käytösäännöt määräävät, kuinka tulisi toimia. Oikeudet kuvaavat, mikä on sallittua. Suojaukset takaavat, ettei oikeuksia rikota tai väärinkäytetä. (Karvi 2012).

Autenttisuudella tarkoitetaan menetelmiä, joilla varmistetaan käskyjen, politiikkojen ja käyttöoikeuksien tuleminen oikeilta tahoilta. Kiistämättömyys kuuluu autenttisuuteen ja sillä tarkoitetaan, että määräyksen antaja tai tehtävän hyväksyjä ei voi jälkikäteen kiistää antaneensa määräystä tai hyväksyneensä tehtävää. Julkisen avaimen salauksen avulla toteutetulla digitaalisella allekirjoituksella saadaan aikaan autenttisuus ja kiistämättömyys. Digitaalinen allekirjoitus takaa myös eheyden eli dokumentin muuttumattomuuden. (Karvi 2012).

Anonymiteettiä tarvitaan yksilön suojan parantamiseksi. Toimittaessa todellisen identiteetin varassa, digitaalisessa maailmassa on helppoa yhdistää erilaisia tietoja yksilön suojan murentamiseksi. Organisaatio voi lisätä anonymiteettiä koosteen, sekoituksen, välimuistin ja pseudonyymien avulla. Koosteessa tietoja kerätään useista yksilöistä ja tiedoista julkaistaan esimerkiksi keskiarvoja tai summia. Sekoituksessa tapahtumia, tietoja ja yhteyksiä sekoitetaan siten, että tietue ei ole yhdistettävissä yksilöön - tiedot on kuitenkin voitava koota paljastamatta yksilön identiteettiä. Välimuisti suorittaa tehtäviä yksilön puolesta paljastamatta yksilöä. Pseudonyymit ovat kuvitteellisia identiteettejä, joita voidaan käyttää identiteetin salaamiseksi. (Karvi 2012).

Tietoturvallisuuden poikkeamiin johtavat erilaiset tilanteet voivat olla tahallisia tai tahattomia. Organisaatio voi varautua suurimpiin riskeihin ennalta suunnittelemalla korjaavat toimenpiteet, toipumisen ja kriisiviestinnän. Organisaation tulee pyrkiä ennaltaehkäisemään tietoturvapoikkeaminen syntymistä ja myös varmistaa kykynsä havaita erilaisia poikkeamia sekä reagoida niihin. (Valtiovarainministeriö 2007, s. 77). Tietoturvapoikkeamien hallintaprosessi on esitetty kuvassa 4.



Kuva 4. Tietoturvapoikkeamien hallintaprosessi (mukaellen Valtiovarainministeriö 2007, s. 78).

Solmsin (2011, s. 215-216) mukaan on tunnustettu tosiasia, että tietoturvallisuuden strateginen tehtävä tunnustetaan organisaatioissa vasta sitten, kun organisaation ylin johto antaa siihen täyden tukensa ja sitoumuksensa. Tietoturvallisuus on teknisten asioiden lisäksi myös hallinnollinen asia, eikä johtotaso voi delegoida tietoturvallisuuden hoitamista yksin organisaation IT-yksikön hoidettavaksi.

Viestintäviraston (2015) mukaan tietoturva ei ole ainoastaan tietotekniikkaa. Suojattavat kohteet ja niitä uhkaavat riskit on tunnistettava ja määriteltävä. Organisaation ulkoinen ja sisäinen ympäristö ovat jatkuvassa muutoksessa, joten organisaation tietoturvatarpeetkin muuttuvat. Tietoturvatarpeiden arviointi on jatkuva prosessi.

2.3 Tietoturvallisuuden osa-alueet

VAHTI eli valtionhallinnon tietoturvallisuuden johtoryhmä on laatinut vuonna 2007 ohje- ja suositusmateriaalin tietoturvallisuutta koskien. Materiaali jaottelee tietoturvallisuuden 8 osa-alueeseen: tietoaineistoturvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikennepalveluiden turvallisuus, laitteistoturvallisuus,

käyttöturvallisuus, ohjelmisto- ja ohjelmistokehityksen turvallisuus sekä jatkuvuuden ja erityistilanteiden hallinta.

Tietoaineistoturvallisuus koskee eri tallennusmuotojen, kuten paperisten asiakirjojen, optisten ja magneettisten muistivälineiden, mikrofilmien, äänitteiden ja vastaavien teknisten laitteiden sisältämien tietojen suojausta. Tietoaineiston käsittelyyn suositetaan organisaatiokohtaisia ohjeita tietoaineiston synnystä sen tuhoamiseen asti, joskin viranomaisille on määräykset lainsäädännön huomioimiseen ja tiedon luokitteluun sekä luokittelun vaatimiin suojaustoimenpiteisiin. Henkilöstön perehdyttäminen tietoaineistojen käsittelyohjeisiin on organisaation johdon vastuulla. (Valtiovarainministeriö 2007, s. 55).

Snedakerin (2007, s. 6) mukaan 80 % kaikesta menetetystä tiedosta häviää ihmisperäisistä syistä. Fåk (2010, s. 151) mainitsee, että suurimmat tietoturvariskit aiheutuvat ihmisen ja tietotekniikan välisessä yhteydessä sekä laitteiden välisessä kommunikaatiossa. Inhimilliset virheet, kuten näppäilyvirheet voivat johtaa helposti esimerkiksi luottamuksellisen tiedon välittymiseen asiattomille tahoille. Laitteiden väliset kommunikaatioyhteydet ovat puolestaan herkkiä ulkoisille häiriöille.

Henkilöstöturvallisuus tarkoittaa henkilöstöstä aiheutuvien riskien hallintaa. Sen perustana on osaava ja sitoutunut henkilöstö sekä toimenkuvissa selkeästi kuvatut tietoturvavastuut- ja tehtävät, tämän lisäksi henkilöstöhallinnon prosessit on oltava määritelty riittävällä tasolla avainhenkilöriskien välttämiseksi. Henkilöstöturvallisuuden keskiössä ovat rekrytointiin, toimenkuvien muutoksiin ja palvelussuhteiden loppumiseen liittyvät prosessit, joista on oltava sovitut toimintamallit. Rekrytoitavan henkilön tausta, sopivuus ja osaaminen on voitava selvittää tehtävän vaatimusten ja luottamuksellisuuden edellyttämällä tavalla. Avainhenkilöt on tunnistettava ja heidän käytettävyytensä on varmistettava avainhenkilöriskien hallitsemiseksi. Toiminnassa on otettava huomioon henkilöstön lomat, poissaolot, työnkierto ja väliaikaisjärjestelyt sekä henkilöstön valmentaminen poikkeusolojen varalta. Organisaation toiminnan suojaksi rakennettujen menetelmien kiertäminen tulee estää tunnistamalla ja poistamalla vaaralliset työyhdistelmät. Henkilöstön määrän, työtyytyväisyyden ja motivaation riittävä taso vaikuttaa myös tietoturvallisuuden toteutumiseen. Poikkeusoloja koskevassa suunnittelussa voidaan tarvittaessa varata henkilöstöä riittävien henkilöstöressurssien varmistamiseksi poikkeusoloissa. (Valtiovarainministeriö 2007, s. 57). Wilbanks et. al. (2014, s. 21) huomauttavat, että organisaatiomuutokset, kuten fuusiot vaikuttavat henkilöstöön, asiakkaisiin ja tieto-omaisuuteen. Organisaatiomuutoksiin liittyvät yhdenmukaistamiset luovat tietoon, järjestelmiin, ohjelmistoihin ja laitteisiin liittyviä riskejä, jotka tulee huomioida kaikkien osapuolten kannalta.

Fyysinen turvallisuus pyrkii turvaamaan organisaation häiriöttömän toiminnan olosuhteista riippumatta. Organisaatiot ovat itse vastuussa fyysisestä suojauksestaan. Tämä osa-alue sisältää kulunvalvonnan, kamera- ja muun teknisen valvonnan, vartiointin

sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan. Alueeseen, rakennukseen, tilaryhmään tai tilaan kohdistuvat turvallisuustarpeet määräävät vähimmäisvaatimukset turvallisuutta parantaville toimille ja järjestelmille. Tilojen suojaus toteutetaan tai sitä parannetaan turvallisuusluokituksen mukaisesti uutta rakennusta rakentaessa tai vanhaa peruskorjattaessa. Rakennuksen omistaja tai kiinteistöhallinto on vastuussa tilojen hallinnasta ja turvallisuusjärjestelyjen toteutuksesta. Tiloja käyttävän organisaation johto tuntee kuitenkin käyttämänsä tietotekniikan turvallisuustarpeet parhaiten ja päättää turvallisuusratkaisuista. Mahdolliset kehittämistarpeet toimitilaturvallisuudessa on huomioitava vuosisuunnitelmien laadinnassa. (Valtiovarainministeriö 2007, s. 59).

Tietoliikennepalveluiden turvallisuus sisältää muun muassa tietoliikennelaitteistojen kokoonpanon, luetteloinnin, ylläpidon ja muutosten hallinnan, ongelmatilanteiden kirjauksen, käytön valvonnan, verkon hallinnan, viestinnän salauksen ja varmistamisen, merkittävien tietoturvapoikkeamien tarkkailun, kirjauksen ja selvittämisen sekä tietoliikennesovellusten testauksen ja hyväksymisen. Uhkiin tulee varautua suunnittelemalla ja rakentamalla organisaation tietoliikennetoiminnot ja niitä toteuttavat verkkojärjestelmät siten, että valittu arkkitehtuuri tukee varautumista. (Valtiovarainministeriö 2007, s. 61).

Laitteistoturvallisuus käsittää laitteistojen suojauksen, asennuksen, ylläpidon ja poiston sekä niihin liittyvän hallinnoinnin, jossa määritellään laitteelle omistaja, turvaluokka, valvonta sekä kapasiteetin suunnittelu. Tarkoituksena on turvata laitteiston elinkaari asennuksesta turvalliseen poistoon elinkaaren lopussa, sisältäen takuun, ylläpidon ja erilaiset tukipalvelut ja -sopimukset. Tietoturvatason ylläpitoon ja tietoturvapoikkeamien reagointiin voidaan vaikuttaa suuresti sopimalla palvelun tasoa määrittelevät rajat ja vasteajat. Vasteaikojen muutoksilla voidaan vähentää varalaitteiden varastoinnin tarvetta, mutta tämä kasvattaa riippuvuutta toimittajan kyvystä toimia vasteaikojen mukaisesti. Jos kokonainen palvelu tai osa organisaation laitteista sijaitsee toisen osapuolen tiloissa, on kiinnitettävä huomiota fyysisen turvallisuuden järjestämiseen ja tilojen pääsynhallintaan sopimuksissa. Jos palvelun on oltava jatkuvasti asiakkaiden käytössä, on sopimukset ulotettava koko järjestelmään ja vaadittava riittävät selvitykset verkkoyhteyksistä ja fyysisestä pääsystä järjestelmään kaikkina aikoina. Laitteistojen käyttöjärjestelmistä, ohjelmistoista ja niiden asetuksista sekä sisältämästä operatiivisesta tiedosta on oltava varmuuskopiot, jotta kaikki tiedot laitteista voidaan palauttaa toipumistilanteessa. Järjestelmän laitteita on voitava valvoa ohjelmallisesti ja niiden käyttöasteita on pystyttävä seuraamaan säännöllisesti. Järjestelmän tietoturvapäivityksiin on oltava ohjeet ja päivitykset on testattava ennen tuotantoon ajamista, tarvittaessa päivitykset on voitava peruuttaa ongelmatilanteissa. (Valtiovarainministeriö 2007, s. 63).

Käyttöturvallisuus tarkoittaa tietotekniikan turvallisen käytön vaatimia toimintaolosuhteita. Tähän pyritään toimivuuden valvonnalla, käyttöoikeuksien hallinnalla, käytön ja lokien valvonnalla, ohjelmistotuella, ylläpitoon, kehittämiseen ja

huoltotoimintoihin liittyvillä turvallisuustoimenpiteillä, varmuuskopioinnilla sekä häiriöraportoinnilla. Tietojärjestelmien suojaaminen haittaohjelmilta ja viruksilta kuuluu myös käyttöturvallisuuteen. Käyttöturvallisuustaso perustuu järjestelmän sisältämien tietojen luokitukseen. Tietoturvallisuutta parannetaan pitämällä järjestelmät päivitettyinä ja tuntemalla normaalista poikkeavat tilat. Hyvä ylläpitokäytäntö on suunnitelmallista, vastuullista ja ammattitaitoista sekä selkeästi ohjeistettua ja vastuutettua. Järjestelmät ja niihin liittyvät menettelytavat ja toimenpiteet tulee olla dokumentoituna, jota päivitetään tarvittaessa. Järjestelmän omistajalla ja ylläpitäjällä tulee olla sopimus vastuista ja ylläpitopalvelun palvelutasosta sekä vasteajoista. Ulkoistettujen ylläpito- ja tietoturvapalveluiden sisällön tulee olla tarkasti määriteltyjä eri tilanteiden vasteaikojen, eskaloinnin sekä toiminnan häiriö- ja poikkeustilanteiden osalta. (Valtiovarainministeriö 2007, s. 65-68).

Basinin et. al. (2011, s. 6-7) mukaan kaikkia käyttöoikeuksia tulisi olla aina niin vähän, kuin työtehtävien hoitamisen kannalta on välttämätöntä. Tällä tarkoitetaan tietoteknisten käyttöoikeuksien lisäksi myös fyysisiä käyttöoikeuksia, kuten avaimia ja ovikoodeja. Tietoturvallisuudessa määritettyjen subjektien tulisi olla oikeutettuja objekteihin vain minimaalisella tasolla. Kaikkia objekteja tulisi myös valvoa ja hallita. Käyttöoikeuksia voidaan rajoittaa myös ajallisesti esimerkiksi organisaation yleisiin toiminta-aikoihin.

Organisaatiolla tulee olla etätyötä koskevat tietoturvaohjeet, joissa huomioidaan myös työvälineet ja tietoliikenneverkot. Etätyössä on huomioitava etätyöpisteen fyysisen turvallisuuden valvomisen hankaluus sekä laitteiden ja tiedon katoaminen ja varkaudet. Järjestelmien tilaa ja käyttöä voidaan valvoa reaaliaikaisesti tai jälkikäteen lokien perusteella. Valvonta toteutetaan tietojen luokituksen ja palveluiden kriittisyyden edellyttämällä tavalla siten, että esimerkiksi kriittisiksi luokitellut palvelut ovat ympärivuorokautisessa valvonnassa. Lokit kerätään ja tallennetaan siten, etteivät ne ole muutettavissa tai poistettavissa tietomurron yhteydessä. Lokeissa oleviin tietoihin voi kuulua luottamuksellisia tietoja ja ne suojataan tällöin valtuuttamattomalta käsittelyltä. Henkilöstön toiminnan valvonta ja valvontatiedon käsittely on laissa säädetty ja työntekijöiden valvonnasta sovitaan yhteistoimintamenettelyssä. Toimintaohjeet määrittelevät seurattavat tietoturvahkista tiedottavat tahot. Järjestelmien käyttäjien työroolit määrittelevät käyttöoikeudet ja -valtuudet, joilla varmistetaan käyttäjien työtehtävien ja vastuiden edellyttämät pääsyoikeudet. (Valtiovarainministeriö 2007, s. 65-68).

Viestintäviraston (2015) mukaan etätyön tietoturvallisuutta ei voida välttämättä edistää samoilla tavoilla kuin kiinteässä toimipisteessä, jossa voidaan olettaa tietoverkon olevan luotettava, koska se on fyysisesti eristetty sekä itse hallittu ja valvottu. Etätyössä tarvittaviin vaihtoehtoisin verkkoyhteyksiin liittyvät tietoturvahat on arvioitava yhtä huolellisesti kuin kiinteän toimipisteen. Etätyön tietoturvallisuuteen kohdistuu myös erilaisia uhkia kuin kiinteässä toimipisteessä, kuten fyysisen kulunvalvonnan puute ja omien laitteiden käyttö. Wilbanks et. al. (2014, s. 20-21) mainitsevat, että henkilöstön

käyttäessä omia laitteitaan BYOD-tyyppisesti (engl. Bring Your Own Device) työnsä tekemiseen on riskinä, että laitteille voidaan asentaa riskialttiita ohjelmistoja tai vierailla haitallista sisältöä sisältävillä sivustoilla. Laitteille saattaa päätyä myös organisaation arkaluonteista tietoa, kuten asiakastietoja. Organisaatiolla on vähän tai ei ollenkaan hallintaa henkilöstönsä omistamiin laitteisiin.

Ohjelmisto- ja ohjelmistokehityksen turvallisuus tarkoittaa käyttöjärjestelmien, ohjelmistojen ja sovellusten tunnistamis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen ylläpitoon ja päivityksiin liittyviä turvallisuustoimenpiteitä. Ohjelmistokehityksessä käytettävät prosessit, käyttöjärjestelmän ja ohjelmistojen asetukset sekä käyttäjien koulutus ja ohjeistus vaikuttavat ohjelmistojen turvallisuuteen. Teknisillä turvakeinoilla, kuten rajoittamalla käyttäjien ja muiden ohjelmien pääsyä ohjelman sisältämään tietoon tai turvapäivityksiä ja -ohjelmia asentamalla sekä järjestelmien turvaominaisuuksia käyttämällä voidaan myös vaikuttaa ohjelmistoturvallisuuteen. Turvallinen sähköinen asiointi edellyttää sähköisten palveluiden tuottamisessa käytettyjen ohjelmistojen turvallisuutta. Tietojärjestelmähankkeissa on varmistettava tietoturvallisuuden huomioiminen hankkeessa ja uudessa tietojärjestelmässä, myös järjestelmien muutoksissa ja kehittämisessä koko elinkaaren ajan. Tärkeysluokitus, turvallisuustarpeet ja -taso sekä tietoturvavaatimukset määritetään tietojärjestelmän esitutkimusvaiheessa. Järjestelmän testaus tulee suunnitella hallinnolliselta ja tekniseltä kannalta. Testaus voidaan kohdistaa kertaluontoisesti koko järjestelmään tai osaan siitä tai säännöllisesti tuotantoympäristöön, jolloin vähitellen tapahtuvia pieniäkin muutoksia voidaan testata. Hallinnollisia tietoturvatarkastuksia ovat vaatimusmäärittely- ja suunnitelmakatselmoinnit sekä ratkaisujen varmistamiset tietoturva-asiantuntijoiden toimesta. Teknisiä tietoturvatarkastuksia ovat koodikatselmuksien ohjelmistojen kriittisiin toimintoihin. (Valtiovarainministeriö 2007, s. 69-71).

Basinin et. al. (2011, s. 3-4) mukaan järjestelmät tulisi luoda mahdollisimman yksinkertaisiksi, eriytetyiksi ja avoimiksi. Yksinkertaiset järjestelmät ovat helpommin käytettäviä ja ylläpidettäviä toiminnan ja tietoturvamekanismien osalta. Yksinkertaiset järjestelmät sisältävät myös todennäköisesti vähemmän virheitä kuin monimutkaisemmat järjestelmät. Eriyttämisellä tarkoitetaan kokonaisuusien jakamista pienempiin osiin siten, että järjestelmän eri osat eristetään toisistaan, jotta niiden välistä tiedonvaihtoa voidaan kontrolloida paremmin. Eriyttämistä voidaan käyttää sovelluksissa esimerkiksi siten, että sovellusta käytetään palvelimelta paikallisen kiintolevyn sijaan. Järjestelmän tietoturvallisuuden ei tulisi perustua sen suojausmekanismien toiminnan salaamiseen vaan helpommin suojattaviin asioihin, kuten avaimiin tai salasanoihin. Avoin sovellus on laajemmin tutkittavissa ja arvioitavissa, jolloin se on myös tietoturvalisempi. Salaisuuksia on vaikeaa suojella, koska ne on säilytettävä tietoturvalisesti jossakin muodossa, kuten ihmisen muistissa tai tallennusmedioissa. Tästä syystä salaisten tietojen määrä tulisi pyrkiä pitämään mahdollisimman pienenä järjestelmiä suunniteltaessa.

Jatkuvuuden ja erityistilanteiden hallinta käsittelee organisaation toimintaa poikkeavissa olosuhteissa ja toiminnan jatkuvuuden varmistamista (Valtiovarainministeriö 2007, s. 73). Tätä kokonaisuutta käsitellään tarkemmin luvussa 3: Jatkuvuussuunnittelu.

2.4 Riskienhallinnan tavoitteet ja osa-alueet

Aven (2010, s. 175) määrittelee riskienhallinnan tavoitteeksi riittävien keinojen varmistamisen asian suojaamiseksi tehtävien toimien mahdollisilta haitallisilta seurauksilta sekä riskien ja kustannusten tasapainottamisen. Riskienhallinnalla pyritään lisäämään ymmärrystä riskejä koskevien päätösten ja toimenpiteiden tekemistä varten (Ilmonen et. al. 2010, s. 156). Riskienhallintaan liitetään tyypillisesti käsitteet riski, uhka, todennäköisyys, haavoittuvuus ja vaikutus (Iivari & Laaksonen 2009, s. 118). Riskienhallintaan liittyvät käsitteet on esitetty taulukossa 1.

Taulukko 1. Riskienhallintaan liittyvät käsitteet (mukaillen Iivari & Laaksonen 2009, s. 118).

KÄSITE	Riski	Uhka	Todennäköisyys	Haavoittuvuus	Vaikutus
TARCOITUS	Uhan vaikutuksen ja toteutumisen todennäköisyyden tulo	Jokin ei-toivottu tapahtuma	Uhan realisoinnin todennäköisyys	Tarkastellun kohteen piirre, joka mahdollistaa uhan aiheuttaman negatiivisen vaikutuksen	Uhan toteutumisesta seuraava negatiivinen vaikutus

Kokonaisvaltaisen riskienhallinnan tavoitteena on ensin pyrkiä tunnistamaan organisaation tavoitteiden saavuttamista uhkaavat riskit. Tämän jälkeen tunnistetut riskit arvioidaan, analysoidaan ja priorisoidaan, jotta saadaan selville mitkä riskit ovat merkittäviä ja kuinka rajalliset hallintaresurssit tulisi kohdistaa. (Ilmonen et. al. 2010, s. 70). Jos organisaatiolla on riskienhallintayksikkö, jolla on vastuullaan riskienhallinta kokonaisvaltaisesti, puhutaan ERM-toiminnasta (engl. Enterprise Risk Management). Organisaation riskienhallintayksikön vastuulla on 3 riskienhallinnan prosessia, jotka ovat riskien analysointi, riskien pienentäminen sekä jäännösriskien arviointi. (Iivari & Laaksonen 2009, s. 100-101). Kliem & Richie (2015, s. 80) määrittelevät jäännösriskin olevan ”se osa riskiä, joka jää jäljelle riskiin vastaamisen jälkeen”.

Riskien tunnistaminen, riskien vaikutusten analysoiminen ja riskejä vähentävien toimenpiteiden ehdottaminen kuuluvat riskien analysointiin. Riskkejä vähentävät toimet käsittävät riskien priorisoinnin, riskejä pienentävien toimenpiteiden käyttöönoton ja ylläpidon. Riskien arviointi on riskienhallinnasta vastaavan tahon tekemää jäännösriskien arviointia ja riskejä vähentävien toimien riittävyyden arviointia. Riskienhallinnasta vastaava taho vastaa organisaation lain ja vaatimusten mukaisuudesta käytännön tasolla ja on suositeltavaa, että tämä taho toimii yhteistyössä jatkuvuudenhallinnasta vastaavan tahon kanssa jatkuvuuden turvaamiseen liittyvissä tehtävissä. (Iivari & Laaksonen 2009, s. 100-101).

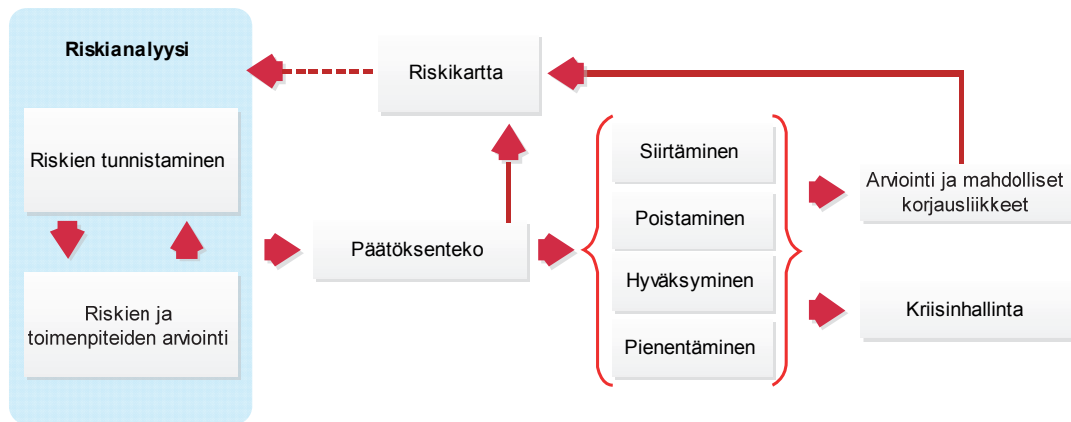
Avenin (2010, s. 175-176) mukaan riskienhallinta kattaa menetelmät riskien todennäköisyyksien vähentämiseen ja niiden potentiaalisten vaikutusten vähentämiseen. Kun riski ei ole poistettavissa, se tulee hallita. Riskienhallinnalla voidaan saavuttaa riittävä tasapaino mahdollisuuksien ja menetysten suhteen ja se voi johtaa jatkuvaan parantamiseen päätöksenteossa ja toiminnassa.

Ainoastaan havaittujen riskien hallinta on mahdollista. Riskienhallinnasta vastaavien tahojen haasteena on kerätä mahdollisimman paljon informaatiota ja riittävän monimuotoinen ryhmä kohteen tai toiminnon riskien arvioimiseen. Tehokas riskien havaitseminen vaatii sekä kohteen tai toiminnon substanssiosaamista, että menetelmien hallintaa. Jotta mahdollisia syy-seuraussuhteita voidaan havaita tehokkaasti, tarvitaan eri asiantuntijoiden ryhmätyötä. Henkilö ei aina ole oman työnsä tai osaamisalueensa paras riskien havaitsija, sillä ihmisillä on taipumusta tottua riskeihin, jolloin ne jäävät huomaamatta. (Flink et. al. 2007, s. 125).

Avenin (2010, s. 177) mukaan organisaation johdon täytyy osallistua riskienhallintaan, jos sen halutaan onnistuvan. Ehdotettuja hyväksi havaittuja johdon toimia onnistumisen varmistamiseksi ovat:

- Riskienhallintastrategian luominen, pyritäänkö organisaatiossa täyttämään vain säädetyt minimivaatimukset vai pyritäänkö luokkansa parhaaksi
- Riskienhallintaprosessin luominen, muodolliset prosessit ja rutiinit, joita organisaatiossa noudatetaan
- Hallinnon, rakenteiden, roolien ja vastuiden perustaminen siten, että riskienhallintaprosessi muodostuu osaksi organisaatiota
- Analyysien ja tukijärjestelmien toteuttaminen, kuten riskianalyysi ja erilaisten tapahtumien ja esiintymien kirjaaminen
- Riskienhallintakulttuurin viestintä, koulutus ja kehitys siten, että organisaation kompetenssi, ymmärrys ja motivaatio lisääntyvät

Riskienhallintaprosessin osa-alueet on esitetty kuvassa 5.



Kuva 5. Riskienhallintaprosessin osa-alueet (mukaellen Flink et. al. 2007, s. 131).

2.5 Riskien luokittelu

Riskien luokittelun avulla riskit saadaan yhteismitallisemmiksi ja vertailukelpoisiksi keskenään. Luokittelu parantaa organisaation riskitietoisuutta ja lisää ymmärrystä riskien välisistä suhteista. Luokittelu on riippuvaista arvioivasta yksilöstä, toimialasta, ajankohdasta ja kontekstista. Luokittelun avulla voidaan myös pyrkiä varmistamaan kaikkien olennaisten riskien tunnistaminen organisaatiossa. Yksi vakiintuneimmista tavoista on luokitella riskit 4 riskilajiin: *strategisiin*, *operatiivisiin*, *taloudellisiin* ja *vahinkoriskeihin*. Tällöin riskit luokitellaan lähteen ja tyyppin mukaan. (Ilmonen et. al. 2010, s. 70). Aven (2010, s. 176) puolestaan luokittelee riskit samoihin riskilajeihin ilman vahinkoriskejä.

Strategiset riskit liittyvät organisaation pidemmän aikavälin strategisiin tavoitteisiin. Nämä riskit liittyvät strategisen päätöksenteon epävarmuustekijöihin esimerkiksi viiden vuoden ajanjaksolla. Pitkä tarkasteltava ajanjakso voi sisältää useita sisäisiä ja ulkoisia epävarmuustekijöitä, jotka voivat aiheuttaa organisaation tavoitteiden saavuttamattomuuden. Ulkoiset tekijät liittyvät esimerkiksi kilpailijoiden, liiketoimintaympäristön, asiakaskäyttäytymisen tai -tarpeiden tai alaa koskeviin ennakoimattomiin muutoksiin, kuten lainsäädäntöön, uusiin teknologioihin, makrotalouden negatiivisiin muutoksiin tai raaka-aineiden ja hyödykkeiden suuriin hinnanmuutoksiin. Sisäiset tekijät liittyvät esimerkiksi strategian toimeenpanon epäonnistumiseen. Organisaation kehitysportfolio, tuote- tai palveluvalikoima eivät välttämättä vastaa strategisten tavoitteiden tarpeita tai kehityshankkeet epäonnistuvat. On mahdollista, ettei organisaatiolla ole riittävää kompetenssia strategisesti tärkeimmillä osa-alueilla tai kompetenssivajetta ei tunnisteta, esimerkiksi toimintaa ei kyetä suuntaamaan asiakkaiden tarpeiden suuntaisesti. Yritysten väliset fuusiot, toiminnan ulkoistaminen tai tietojärjestelmien integrointi voivat myös epäonnistua. (Ilmonen et. al. 2010, s. 71-72).

Aven (2010, s. 176-177) määrittelee strategisiksi riskeiksi näkökulmat ja tekijät, jotka ovat tärkeitä organisaation pitkän tähtäimen suunnittelussa. Esimerkkejä tällaisista riskeistä ovat:

- Fuusiot ja yritysostot
- Teknologia
- Kilpailu
- Poliittiset olosuhteet
- Lainsäädäntö ja sääntely
- Työmarkkinat

Organisaation päivittäisiin toimintoihin, välittömiin tai välillisiin vahinkoihin tai maineeseen liittyvät riskit ovat *operatiivisia riskejä*. Riittämättömät tai epäonnistuneet sisäiset prosessit, henkilöstö, järjestelmät tai ulkoiset tapahtumat voivat johtaa operatiivisiin riskeihin. Sisäiset operatiiviset riskit voivat liittyä organisaatioon ja sen johtamiseen, esimerkiksi epäonnistuminen prosessien johtamisessa tai kehittämisessä, heikko päätöksentekoprosessi tai päätöksentekokyky, kykenemättömyys päätösten suunnitteluun, konkreettisten tavoitteiden asettamiseen, päätösten toimeenpanoon tai intressiristiriidoista aiheutuvat epäonnistumiset. Merkittävimmät operatiiviset riskit voivat toteutuessaan keskeyttää liiketoiminnan esimerkiksi tietoliikennekatkoksen tai ulkopuolisen palveluntarjoajan konkurssin takia. Myös sopimukseen ja vakuutuksiin liittyvät riskit, kuten vastuiden epäselvyydet tai sopimusten tulkintaerimielisyydet kuuluvat operatiivisiin riskeihin. Operatiivisiin riskeihin voidaan varautua laatimalla toimintasuunnitelmia kriisitilanteiden varalle. Jos organisaation varautuminen kriisitilanteisiin on puutteellista, tilanteet voivat eskaloitua alkuperäistä tilannetta huomattavasti vakavammiksi. Esimerkiksi lisävahingot organisaation maineelle syntyvät, jos kriisitilanteen huono johtaminen näkyy organisaation ulkopuolelle kaaosmaisena toimintana. Viestinnän merkitys on tällaisissa tilanteissa suuri, sillä esimerkiksi tapahtumasta ulkopuolisille annettujen lausuntojen ristiriitaisuus pahentaa kriisiä ennestään. (Ilmonen et. al. 2010, s. 72-74).

Aven (2010, s. 177) määrittelee operatiivisiksi riskeiksi normaaliin toimintatilaan vaikuttavat tekijät. Tällaisia riskejä ovat esimerkiksi:

- Vahingot, epäonnistumiset, virheet, laatupoikkeamat, luonnonkatastrofit
- Tarkoitukselliset toimet, sabotaasi, tyytymättömät työntekijät
- Kompetenssin menettäminen, avainhenkilöt
- Oikeudelliset olosuhteet, puutteelliset sopimukset, vastuuvakuutukset

Taloudelliset riskit voivat liittyä organisaation rahaprosessia uhkaaviin riskeihin, kuten maksuvalmiuteen, valuutan ja korkojen vaihteluun tai sopimusten osapuolien kykenemättömyyteen hoitaa velvoitteitaan sopimuksissa. Osa maariskeistä luetaan taloudellisiin riskeihin, esimerkiksi vieraan valtion lainsäädännön ennakoimattomista

muutoksista seuraavat negatiivisesti organisaation verokohteluun tai pääomavaatimuksiin liittyvät riskit. (Ilmonen et. al. 2010, s. 74-75).

Aven (2010 s. 177) määrittelee taloudellisiksi riskeiksi organisaation taloudelliseen tilanteeseen liittyvät riskit. Esimerkkejä tällaisista riskeistä ovat:

- Markkinariskit, tavaroiden ja palveluiden hinnat, valuuttakurssit, arvopaperit
- Luottoriskit, velallisen velvollisuuksien laiminlyönnit
- Likviditeettiriskit, puutteelliset käteisvarat, ajalliset myyntivaikeudet

Tyypilliset *vahinkoriskit* ovat henkilöstöön liittyviä, kuten työkyvyttömyyteen, työkykyyn tai työtapaturmiin liittyvät riskit. Henkilöturvallisuuteen, kuten työvoiman saatavuuden tai kompetenssin riittämättömyyteen, henkilöstön poissaoloihin, matkustamiseen, avainhenkilöiden menettämiseen tai työperäisiin sairauksiin ja vaarallisten aineiden käsittelyyn liittyvät riskit ovat myös vahinkoriskejä. (Ilmonen et. al. 2010, s. 75).

Riskejä voidaan luokitella myös muilla tavoin, kuten vakuutettaviin ja ei-vakuutettaviin, tietoiisiin ja tiedostamattomiin tai välittömiin ja välillisiin riskeihin. Vakuutettavat ja ei-vakuutettavat riskit ovat usein synonyymejä vahinko- ja liikeriskeille. Vahinkoriski tuottaa organisaatiolle aina aineellista menetystä, kun taas liikeriskeissä on mahdollisuus liiketoimen onnistumiseen. Liikeriski voi vaihdella huomattavasti muun muassa suhdanteiden vaikutuksesta, eikä näihin riskeihin ole saatavilla vakuutuksia riskin vaihtelevan luonteen ja ennustamattomuuden vuoksi. Tietoiset riskit kuuluvat liiketoimintaan, sillä liiketoiminta itsessään edellyttää riskien ottamista. Riskien jako välittömiin ja välillisiin tarkoittaa, vaikuttaako riskin toteutuminen toimintaan suorasti vai esimerkiksi pidemmän ajan kuluessa monimutkaisten syy-seuraussuhteiden kautta. (Ilmonen et. al. 2010, s. 75-76).

2.5.1 Tietoriskit

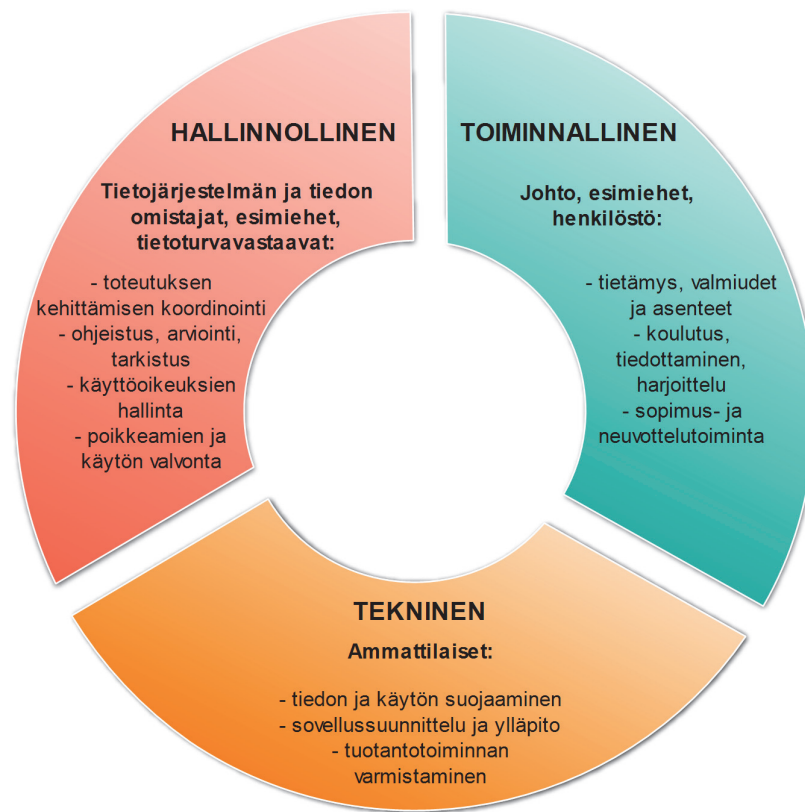
Tietoriski on organisaation toiminnassa tapahtuva tilanne, jossa tarvittava tieto, tietojärjestelmä tai osa siitä ei ole käytettävissä tai käytettävissä oleva tieto on muuttunut, vääristynyt, hävinnyt tai joutunut asiattoman tahon käyttöön. Tällöin tiedon luottamuksellisuus, eheys tai saatavuus on uhattuna ja tilanne haittaa tai estää työntekijän tai prosessin toimintaa tai johtaa väärin toimenpiteisiin tai tuloksiin. (Kyrölä 2001, s. 25). Tietoriskit ovat pääosin operatiivisia, osittain strategisia riskejä.

Kyrölä (2001, s. 26) määrittelee tietoriskeiksi esimerkiksi seuraavat tilanteet:

- Käyttäjätunnus tai salasana paperille kirjoitettuna työhuoneessa
- Huolimaton asiakirjojen säilyttäminen, asiakirjan päätyminen asiattomalle
- Uniikin tiedon häviäminen tai tuhoutuminen

- Tiedostojen luvaton lähettäminen organisaation ulkopuolelle
- Tiedottomuus tiedon merkityksellisyydestä tai luottamuksellisuudesta
- Vaitiolositoumuksen alaisten asioiden levittäminen asiattomille
- Viestien ja asiakirjojen kopioiminen tai ohjautuminen väärin
- Tietokonevirus tai ohjelmavirhe estää toiminnan tai muuttaa tietoa
- Tietovälineiden katoaminen tai tuhoutuminen
- Käytöstä poistettujen tietovälineiden huolimaton käsittely
- Sovelluksen huolimaton ylläpito

Organisaation tietoriskit tulee hallita monella organisaatiotasolla. Organisaation johdon tulee tuntea organisaatiota uhkaavat sisäiset ja ulkoiset riskit, myös tietoriskit, ja tehdä päätökset tiedon suojaamisen tahdosta. Esimiesten tulee hallita jokapäiväisessä työssä tapahtuvat yllätykselliset tilanteet. Henkilöstön tulee ymmärtää tiedon merkitys omassa työssään. Tekniset asiantuntijat huolehtivat omalta osaltaan tietoliikenneverkon toimivuudesta, laitteiden käytettävyydestä sekä sähköisessä muodossa olevan tiedon varmistuksesta. Riskienhallinnasta ja turvallisuudesta vastaavat tahot huolehtivat puolestaan tietoisuuden parantamisesta ja toimintamenetelmien, tietojen sekä käyttöomaisuuden suojausmenetelmien riittävydestä. (Kyrölä 2001, s. 28-29). Liiketoiminnan jatkuvuuteen ja tieto-omaisuuden suojaamiseen kuuluvat tehtävät on esitetty kuvassa 6.



Kuva 6. Tietoriskien hallinnan tehtäväalueet (mukaellen Kyrölä 2001, s. 29).

Järveläisen (2013, s. 583) mukaan organisaatio voi menettää asiakkaita ja huonontaa mainettaan sekä markkina-asemaansa tilanteissa, joissa tarvittava tieto ei ole käytettävissä. Tiedon saatavuuden varmistaminen tulee olla yksi organisaation tärkeimmistä prioriteeteista.

Valtiokonttorin (2012, s. 4) määritelmän mukaan tietoriskien hallintaan osallistuvat tai siihen liittyvät osapuolet ovat:

- Ylin-, operatiivinen-, tietohallinto- ja tietoturva-johto
- Tietoturva-asiantuntijat
- Toiminnasta vastaavat eli prosessien ja tietojärjestelmien omistajat
- Tietojärjestelmien pääkäyttäjät ja loppukäyttäjät

Tieto-omaisuuteen liittyvät riskit tulee arvioida johdonmukaisesti luottamuksellisuuden, eheyden, saatavuuden ja lainmukaisuuden suhteen. Tieto tulee tunnistaa ja sille tulee määrittää omistaja. Riskit arvioidaan vähintään neliportaisella asteikolla vaikutusten mukaan. (Jordan & Silcock 2006, s. 177-178). Esimerkki riskitasoista on esitetty taulukossa 2.

Taulukko 2. Riskitasot vaikutusten ja toimenpiteiden mukaan (mukaellen Jordan & Silcock 2006 s. 178).

RISKITASO	VAIKUTUS ORGANISAATION TOIMINTAAN, TUOTTAVUUTEEN, MAINEESEEN TAI TURVALLISUUTEEN	TARVITTAVAT TOIMENPITEET TILANTEESTA PALAUTUMISEEN
Matala	Vähäinen	Minimaaliset
Kohtalainen	Rajoitettu	Normaalit
Korkea	Merkittävä	Laajat
Erittäin korkea	Vakava tai katastrofaalinen	Äärimmäiset

2.5.2 IT-riskit

Informaatiotekniikkaan liittyviä sisäisiä operatiivisia riskejä ovat esimerkiksi teknologioiden valintaan ja integrointiin liittyvät riskit. Liiketoimintatarpeita vastaamattomat teknologiat, niiden heikko skaalautuvuus tarpeiden mukaisesti sekä järjestelmien riippuvuudet ovat esimerkkejä sisäisistä operatiivisista IT-riskeistä. Ulkoisten palveluntarjoajien ja toimittajien riittämätön osaamistaso ja kyvyttömyys osaamisen kehittämiseen ja johtamiseen ovat osittain sisäisiä ja osittain ulkoisia riskejä. Tietoturvallisuuteen liittyviä operatiivisia riskejä ovat tiedon saatavuuteen, luottamuksellisuuteen, eheyteen sekä tiedon laatuun liittyvät riskit. (Ilmonen et. al. 2010, s. 72-73).

IT-riskit voivat vaikuttaa organisaation tavoitteisiin suoraan tai välillisesti ja niiden vaikutukset vaihtelevat pienestä haitasta katastrofiin (Jordan & Silcock 2006, s. 71). Fåk (2010, s. 144-146) mainitsee, että tietotekniikan käyttökohteiden määrä ja järjestelmien monimutkaisuus aiheuttavat sen, että IT-riskejä arvioidaan usein joko pahimman mahdollisen tilanteen mukaan tai arvioijan omiin kokemuksiin perustuen. IT-järjestelmien monimutkaisuus ja vaihtelevuus tekevät IT-riskien vaikutusten varman arvioimisen mahdottomaksi. IT-riskeistä aiheutuvat taloudelliset seuraukset ovat myös vaikeita arvioida esimerkiksi palvelunestohyökkäyksen kohdistuessa verkkoliiketoimintaan. Asiakkaiden käyttäytymisen muutos palvelun toimimattomuuden takia voi siirtää asiakkaat kilpailevan organisaation asiakkaiksi, jolloin taloudelliset seuraukset eivät jää ainoastaan IT-riskin korjaamiseen käytettyihin resursseihin.

Fåk (2010, s. 146) määrittelee vakaviksi IT-riskeiksi tilanteet, joissa riski vaikuttaa jonkin kriittisen järjestelmän automaattiseen toimintaan tai joissa henkilöt tekevät kriittisiä päätöksiä virheen vaikutuksesta. Henkilöt saattavat tehdä katastrofaalisia päätöksiä IT-riskien aiheuttamien, selkeästi virheellisten tietojen perusteella joko laiskuudesta, välinpitämättömyydestä tai resurssien puutteesta johtuen.

Jordan & Silcock (2006, s. 60) jaottelevat IT-riskit 7 luokkaan sen mukaan, kuinka tietotekniikka voi epäonnistua ja vaikuttaa negatiivisesti organisaation liiketoimintaan:

Projektit, jotka eivät valmistu tai valmistuvat erilaisina kuin on suunniteltu -riskiluokka koskee epäonnistuvia IT-projekteja sekä liiketoimintaprojekteja, joissa on merkittävänä osana jokin IT-komponentti. Uusien järjestelmien toteuttamiseksi, olemassa olevien järjestelmien laajentamiseksi tai järjestelmien käyttötapojen tehostamiseksi aloitettujen projektien epäonnistuessa suunniteltu päivitys tai laajennus ei toteudu oletetusti. Organisaatio ei saa niitä etuja, joita uuden järjestelmän ajateltiin tuovan mukanaan. Kolme tärkeintä aluetta, joilla projekti voi jäädä tavoitteistaan, ovat ajoitus, laatu ja laajuus. Tällöin projektit valmistuvat myöhässä, kuluttavat suunniteltua enemmän varoja tai resursseja, tarjoavat odotettua vähemmän toimintoja käyttäjille tai valmis tuote on keskeneräinen tai häiritsee liiketoimintaa käyttöönoton jälkeen. Tähän riskiluokkaan

kuuluvien riskien aktiivinen hallinta edellyttää projektinhallinnan ja tuotannon laajamittaista osaamista sekä kokemusta IT-hankinnoista ja -toteutuksista. (Jordan & Silcock 2006, s. 60).

IT-palveluiden jatkuvuus -riskiluokka liittyy IT-palveluiden katkoksiin ja liiketoimintaa häiritsevään epäluotettavuuteen. Järjestelmien tulisi toimia luotettavasti käyttäjien tarpeita palvellen. Järjestelmän ollessa poissa käytöstä järjestelmästä riippuvat liiketoimintaprosessit voivat lamaantua. Jos palvelut toimivat, mutta huonolla suorituskyvyllä, voivat kasvaneet vasteajat aiheuttaa merkittäviä seurauksia käyttäjien ja asiakkaiden tuottavuudelle. Näiden riskien hallitseminen edellyttää ongelmien, asiakastuen, IT-palveluiden ja liiketoiminnan jatkuvuudenhallinnan kokemusta sekä kykyä toipua kriisitilanteista. (Jordan & Silcock 2006, s. 61).

Kadonnut tieto-omaisuus -riskiluokka koskee erityisesti IT-järjestelmissä olevan tietomaisuuden katoamista, vahingoittumista ja väärinkäyttöä. Organisaatio ei välttämättä ole edes tietoinen kaikesta omistamastaan tiedosta. Tärkeitä tietoja voi päätyä kilpailijoille tai asiakastiedot voivat päätyä kaikkien nähtäville, jolloin organisaation asiakassuhteet ja maine kärsivät. Kadonneesta tiedosta riippuvaiset liiketoimintaprosessit voivat häiriintyä, kun tarvittava tieto ei ole saatavilla. Tämän tyyppisten riskien hallinta edellyttää organisaatiolta kokemusta tietoturvallisuudesta ja tiedonhallinnasta. (Jordan & Silcock 2006, s. 61-62).

Tietotekniikan arvoketjun katkeaminen on yksi riskiluokista. IT-palveluntarjoajat ja IT-toimittajat ovat nykyään oleellisessa roolissa organisaation IT-projektien toteuttamisessa ja päivittäisessä toiminnassa. Jos organisaatio ei saa mitään sille luvataan, voi syntyä välittömiä seurauksia ja häiriöitä järjestelmissä ja palveluissa. Jos palveluntarjoajan tai toimittajan käyttämä teknologia ei ole ajantasaista, se vaikuttaa organisaation kokonaistehokkuuteen. Myyjien kanssa toimimisen, ulkoistamisen ja sopimusten hallinnan kokemus auttaa hallitsemaan näitä riskejä. (Jordan & Silcock 2006, s. 62).

Hajoavat sovellukset ja järjestelmät -riskiluokka liittyy sovellusvirheisiin. Sovellusten toimimattomuudesta aiheutuvat seuraukset vaihtelevat käyttäjän lievästä ärsyyntymisestä suureen katastrofiin. Vaikutuksiin vaikuttavat toimiala sekä järjestelmien verkottuneisuus, jossa yksittäisen sovelluksen häiriö voi vaikuttaa useiden organisaatioiden toimintaan, jos järjestelmät ovat keskenään yhteydessä. Sovelluksilla voi olla toiminnallisten puutteiden lisäksi ei-toiminnallisia piirteitä, jotka eivät ole niin selkeitä ja joiden vaikutukset tuntuvat vasta pidemmällä ajanjaksolla. Tällaisia ovat esimerkiksi järjestelmien huono ylläpidettävyys, laajennettavuus tai muokattavuus. Jos sovellus on huonosti dokumentoitu tai strukturoitu, voi vikojen korjaaminen olla haasteellista. Ohjelmiston kehittäjä voi tahtomattaan lisätä uusia, merkittäviä vikoja tehdessään ohjelmistoon pieniä muutoksia. Kokemus sovelluskehityksestä, ohjelmiston ylläpidosta, laajentamisesta, integroinnista, testaamisesta, valvonnasta ja ongelmien

seurannasta sekä versioiden ja järjestelmän asetusten hallinnasta ovat edellytyksenä näiden riskien hallinnalle. (Jordan & Silcock 2006, s. 62-63).

IT-infrastrukturi -riskiluokka keskittyy IT-infrastrukturiin eli sovellusten käyttämien keskitettyjen ja hajautettujen tietokone- ja verkkolaitteistojen sekä alustaohjelmistojen, kuten käyttöjärjestelmien ja tietokantojen hallintajärjestelmien ongelmiin. Häiriö tässä riskiluokassa voi olla pysyvä, jos esimerkiksi järjestelmän komponentti hajoaa korjauskelvottomaksi tai väliaikainen, jos esimerkiksi sähkövirta tai tietoliikenneyhteys katkeaa. Järjestelmien vikasietoisuuden taso vaikuttaa häiriöiden vakavuuteen eli onko käytettävissä esimerkiksi varalaitteita vai pysäyttääkö häiriö järjestelmän kokonaisuudessaan. Valittaessa infrastruktuuria on huomioitava uudempien mallien kanssa yhteensopimattomat järjestelmät, sillä esimerkiksi käyttöjärjestelmän uusiminen voi aiheuttaa sovelluksen toimimattomuuden. Jotta tämän tyyppisiä riskejä voidaan hallita, tarvitaan operationaalista kokemusta järjestelmien asetusten hallinnasta, järjestelmien hoidosta, valvonnasta ja kapasiteetin hallinnasta sekä pitkän tähtäimen suunnittelua ja arkkitehtuurien ymmärtämistä. (Jordan & Silcock 2006, s. 63-64). Cerullo & Cerullo (2004, s. 70) huomauttavat, että riskit liiketoiminnan katkeamiseen kasvavat suhteessa organisaation riippuvuuteen IT-infrastruktuurista.

Strategiset riskit ja tulevaisuuden uhat on seitsemäs riskiluokka. Jos tietotekniikka ei pysty täyttämään liikestrategian odotuksia, vaikutukset eivät ole välittömiä, mutta ne muodostuvat suuriksi tulevaisuudessa. Jotta organisaatio pysyisi kilpailukykyisenä, sen täytyy olla selvillä IT-alan edistyksestä löytääkseen hyväksikäytettäviä mahdollisuuksia. IT-strategiassa olevat puutteet voivat aiheuttaa suuriakin ongelmia, jos esimerkiksi IT-järjestelmän kehitys on umpikujassa. Vaikeuksien ja muutoksiin tarvittavien kulujen lisääntyminen on yleistä ja pidemmällä ajanjaksolla olemassa oleviin järjestelmiin joudutaan käyttämään enemmän kehitysresursseja kuin uusiin projekteihin. Kokemus strategioista ja suunnittelusta sekä erilaisten arkkitehtuurien ymmärtäminen ovat edellytyksenä näiden riskien hallitsemiselle. (Jordan & Silcock 2006, s. 64).

Ilmonen et. al. (2010, s. 165-166) määrittelevät IT-riskien hallinnan tavoitteeksi IT-palveluiden ja organisaation toimintaan IT:n kautta vaikuttavien riskien tunnistamisen. Organisaation tulee varmistaa, että:

- IT-palveluiden ja IT-toimintojen merkittävät riskit tunnistetaan
- Riskien liiketoiminnalliset vaikutukset arvioidaan
- Riskien todennäköisyys arvioidaan pisteytetysti, sillä IT-riskien monimutkaisuus ei tee aidon todennäköisyyden arviointia tarkoituksenmukaiseksi
- Riskien todennäköisyys ja merkittävyys viestitään liiketoimintajohdolle
- Riskit priorisoidaan esimerkiksi SLA-tasojen (engl. Service Level Agreement) vaikutusten perusteella, jolloin on mahdollista saada tietoa myös taloudellisista seurauksista
- Riskeille määritellään keinot poistoon, vähentämiseen tai siirtämiseen

- Riskien vaatimat toimenpiteet sekä riskien tunnistamisen ja hallinnoinnin prosessit ovat priorisoitavissa ja delegoitavissa linjaorganisaatiolle
- Organisaation johto ja koko henkilöstö tutustuvat toimintaansa liittyviin riskeihin ja oppivat niistä

Uudet teknologiat voivat mahdollistaa kilpailuetua organisaatiolle tai sen kilpailijoille, mutta uusimman teknologian käyttöönotto voi aiheuttaa ongelmia. Vanhentuvat teknologiat on korvattava ajallaan ja joskus on otettava käyttöön aivan uusinta teknologiaa. Tähän liittyy riskejä liiketoiminnalle aiheutuvien mahdollisuuksien ja uhkien tunnistamisen suhteen, jos teknologioiden seuraaminen on IT-henkilöstön vastuulla. IT-henkilöstö pystyy monesti havaitsemaan tulevat teknologiat, mutta niiden vaikutusta liiketoiminnalle ei osata arvioida. Liiketoiminnan kannalta merkittävien teknologioiden tunnistaminen tarvitsee tehokasta kommunikaatiota IT:n ja liikkeenjohdon välillä. Vaikka kommunikaatio olisi kunnossa, voivat olemassa olevan arkkitehtuurin joustamattomuus tai IT-henkilöstön tarvittavien valmiusten puute muodostua esteeksi uuden teknologian käyttöönotossa. (Jordan & Silcock 2006, s. 290-291).

IT-riskien hallinta on sisällytettävä määrättyjen työntekijöiden työnkuvaan sen sijaan, että heidän oletettaisiin suorittavan vaadittavia toimia omasta aloitteestaan. Roolien määrittämisen jälkeen niihin on valittava oikeat vastuuhenkilöt. Vastuurakenne voidaan laatia taulukkona, jossa luetellaan erityyppiset IT-riskit, roolit ja riskienhallinnan elinkaaren vaiheet. Laadinnassa on huomioitava, että velvollisuudet on erotettava toisistaan, jotta kutakin riskiluokkaa varten on olemassa oma riippumaton rooli valvontatoimenpiteitä varten. Asiantuntijoiden prosessi-, järjestelmä- tai erityisriskien tietämys sekä johdon kaikkia tekijöitä arvioiva päätöksenteko on kyettävä tasapainottamaan. IT-riskien hallintaroolit on sovitettava olemassa oleviin rakenteisiin, jos se onnistuu luontevasti ja uusia rooleja on luotava tarvittaessa esimerkiksi osastojen välille. Lisäksi yhteiset vastualueet tulee kohdentaa tarvittaessa, jotta jokainen osa-alue on varmasti jonkun vastuulla. (Jordan & Silcock 2006, s. 77). Esimerkki IT-riskiluokkien vastuuttamisesta on esitetty taulukossa 3.

Taulukko 3. IT-riskiluokkien vastuuttaminen riskiluokittain (mukaellen Jordan & Silcock 2006, s. 78).

Vastuu Riskiluokka	Tunnistus / havaitseminen	Arviointi / analyysi	Käsittely (toimenpiteiden määrääminen)	Valvonta ja jälkitarkastus
Projektit	Projektitiimi	Projektipäällikkö	Projektipäällikkö	IT-projektien johtaja
IT-palveluiden jatkuvuus	Liiketoiminta-prosesseihin liittyvä henkilöstö	Liiketoiminnan jatkuvuuden koordinoija, IT-palvelutuotannon päällikkö	Liiketoiminnan jatkuvuuden koordinoija, IT-palvelutuotannon päällikkö	IT-palvelutuotannon johtaja
Tieto-omaisuus	Tiedonhaltijat ja järjestelmien käyttäjät	Turvallisuus-päällikkö	Liiketoimintapäälliköt, tietohallintojohtaja	Tietohallintojohtaja
Palveluntarjoajat	Projektipäälliköt, IT-palvelutuotannon päälliköt	Ulkoistamis- ja hankintapäällikkö, sopimuksista vastaava päällikkö	Ulkoistamis- ja hankintapäällikkö	IT-palvelutuotannon johtaja
Sovellukset	Järjestelmän ylläpitäjät, käyttäjät, sovelluksen tukitiimi	Sovelluspäällikkö, hankintapäällikkö	Liiketoimintajärjestelmien omistajat	Tietohallintojohtaja
Infrastruktuuri	Järjestelmän hallinnoija, järjestelmän tukitiimi, käyttäjät	Infrastruktuuri-päällikkö, hankintapäällikkö	Infrastruktuuri-päällikkö	Tietohallintojohtaja
Strategiset ja tulevat	IT-arkkitehdit ja IT-suunnittelijat	IT-strategiasta ja suunnittelusta vastaava päällikkö	Liiketoiminnan jatkuvuuden koordinoija, IT-strategiasta ja suunnittelusta vastaava päällikkö	Yritysstrategiasta vastaava johtaja

3. JATKUVUUSSUUNNITTELU

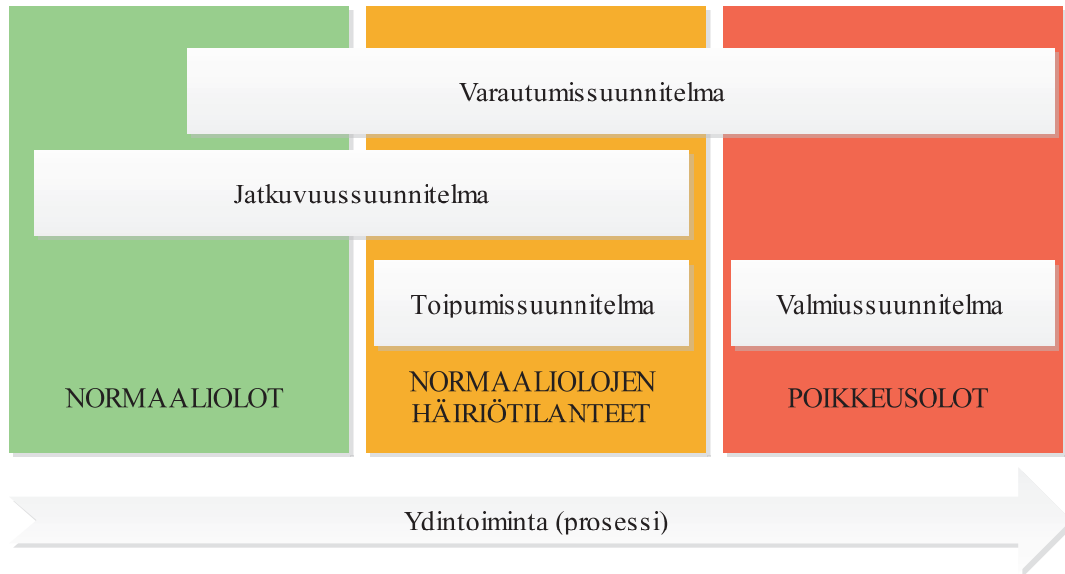
Snedaker (2007, s. 3) määrittelee jatkuvuussuunnittelun metodologiaksi, jolla luodaan ja validoidaan suunnitelma liiketoimintojen jatkuvuuden ylläpitämiseksi ennen häiriötä, niiden aikana ja jälkeen. Cerullon & Cerullon (2004, s. 70) määritelmän mukaan jatkuvuussuunnittelulla pyritään poistamaan tai vähentämään haitallisten tapahtumien vaikutusta ennen tapahtuman toteutumista. Mahdollisimman nopea palautuminen häiriötilanteista on kriittistä organisaation toimintakyvyn kannalta. Jos vakaviin häiriötilanteisiin ei varauduta ennalta, kriisit saattavat jopa pysäyttää organisaation toiminnan. Ernst & Youngin vuonna 2002 toteuttaman tietoturvaluottelun mukaan yli 75 % organisaatioista maailmanlaajuisesti oli kohdannut toiminnassaan odottamattomia keskeytyksiä (Ernst & Young LLP 2002). Tästä syystä jokainen organisaatio tarvitsee kattavan jatkuvuussuunnitelman, joka kattaa niin organisaation sisäiset kuin ulkoiset uhkatekijät.

Kliemin & Richien (2015, s. 13-14) mukaan jatkuvuussuunnittelulla pyritään saavuttamaan kolme tavoitetta:

1. Parantaa selviytymisen todennäköisyyttä
2. Vähentää haitallisten tapahtumien vaikutuksia
3. Palauttaa kriittiset prosessit toimintaan

Tunnistettuun negatiiviseen tapahtumaan varautuminen ennalta kasvattaa organisaation selviytymisen todennäköisyyttä. Jatkuvuussuunnittelun avulla organisaatio tietää, *kuka, mitä, milloin, missä ja miksi* toimitaan kun häiriötilanne tapahtuu. Valmistautumalla ymmärretään häiriön vaikutukset toimintaan ja tiedostetaan, mitä resursseja palautumiseen tarvitaan. Tietämällä jatkuvuudenhallintaa vaativat prosessit voidaan häiriöihin varautua ennalta eli jatkuvuussuunnittelu on enemmänkin valmistautumista kuin reaktiota. Organisaation kaikki prosessit eivät myöskään ole toiminnan kannalta yhtä tärkeitä. Kriittisimmät prosessit on saatava palautettua toimintaan ensimmäisinä. (Kliem & Richie 2015, s. 13-14).

Liiketoiminnan jatkuvuussuunnittelu on osa laajempaa kokonaisuutta eli varautumissuunnittelua. Tämä kokonaisuus sisältää 3 erilaista suunnitelmaa, jotka ovat jatkuvuussuunnitelma, toipumissuunnitelma ja valmiussuunnitelma. Näitä suunnitelmia käytetään erilaisissa olosuhteissa, joita nimitetään normaalioloiksi, normaaliolojen häiriötilanteiksi sekä poikkeusoloiksi. (Iivari & Laaksonen 2009, s. 18). Edellä mainittujen suunnitelmien ja olosuhteiden väliset suhteet on esitetty kuvassa 7.



Kuva 7. Suunnitelmien ja olosuhteiden väliset suhteet (mukaellen Iivari & Laaksonen 2009 s. 19).

Doughtyn (2001) mukaan onnistuneen jatkuvuussuunnittelun perusedellytyksenä on, että jatkuvuussuunnitelmille määritetään omistajat. Omistajien tulee olla ne tahot, jotka toteuttavat jatkuvuussuunnitelmia käytännössä häiriötilanteessa. Jos omistajuutta ei määritellä, laaditut suunnitelmat eivät pysy ajantasaisina. Tällöin on riskinä, että organisaatio ei kykene palautumaan häiriötilanteista määritetysti, tarvittavassa ajassa ja kustannustehokkaalla tavalla. Omistajuus voidaan määritellä esimerkiksi liiketoimintayksiköittäin, prosesseittain, toiminnoittain tai sovelluksittain. Omistajuus tulee määritellä johtotasolla ja se tulee sisällyttää organisaation jatkuvuussuunnittelupolitiikkaan. Omistajuutta määriteltäessä on huomioitava jatkuvuussuunnitelmien monimutkaisuus ja lukumäärä.

Jatkuvuussuunnittelulla pyritään takaamaan organisaation toimintojen jatkuvuus normaalioloissa, normaaliolojen häiriötilanteissa sekä poikkeustilanteissa. Normaaliolojen häiriötilanne tapahtuu, kun toteutunut poikkeama normaalioloista on lievä, eikä se vaikuta kuin häiriön kohteena olevaan organisaatioon. Poikkeustilanteilla tarkoitetaan vakavaa organisaation häiriötilannetta, kuten tuotantolaitosta, tiloja tai henkilöstöä kohdannutta onnettomuutta. Myöskään poikkeustilanteissa organisaation kannalta vakava häiriötilanne ei kosketa yhteiskuntaa laajemmin. (Iivari & Laaksonen 2009, s. 18-19).

Normaalioloissa organisaation liiketoimintaympäristö on stabiili ja toiminta on häiriötöntä. Hetkellisesti liiketoimintaa haittaavat ongelmat, kuten laiterikot tai lyhytaikaiset tietoliikennekatkokset, joista selvittää normaalein työruutiinein nopeasti, ovat normaaliolojen ongelmia. Jatkuvuussuunnitelman yhden osan tulisi kohdentua normaalitoiminnan jatkuvuutta edistäviin toimenpiteisiin sekä niiden kuvaamiseen ja

toteuttamiseen, kuten dokumentointiin, varmistusprosesseihin ja huoltosuunnitelmiin. (Iivari & Laaksonen 2009, s. 95).

Kun organisaation liiketoimintaympäristöön ilmestyy liiketoiminnan harjoittamista vaikeuttava häiriö ja toimintaa joudutaan muuttamaan, on kyseessä normaaliolojen häiriötilanne. Katastrofi koskettaa organisaatiota paikallisesti eikä vaikuta muihin toimijoihin tai yhteiskuntaan kuin välillisesti. Tällöin otetaan käyttöön jatkuvuussuunnittelussa tehty toipumissuunnitelma. Jos kriisi vaikuttaa palvelujen tuottamiseen asiakkaille, sidosryhmille tai viranomaisille, on tilanteesta tiedotettava sisäisen tiedottamisen lisäksi myös vaikutuksen alaisille tahoille vaatimusten edellyttämästi. Tiedottamisen tulee olla keskitettyä, koordinoitua ja totuudenmukaista, sillä ongelmatilanteissa toimiminen vaikuttaa organisaation maineeseen. Huono, vähättelevä tai valheellinen tiedottaminen johtaa maineen kärsimiseen, vaikka alkuperäinen ongelmatilanne olisikin ollut lievä. (Iivari & Laaksonen 2009, s. 95-96). Snedaker (2007, s. 15) lisää, että hyvin hallittu kriisitilanne saattaa jopa kasvattaa organisaation mainetta korkeammalle kuin se oli ennen kriisiä. Järveläinen (2013, s. 588) lisää, että asiakaspalvelussa työskentelevien henkilöiden tulee kyetä kommunikoimaan asiakkaille häiriötilanteista tavalla, joka ei vaikuta asiakasuskollisuuteen negatiivisesti.

Organisaation toimintaa suuresti haittaavat, vakavat yhteiskunnassa esiintyvät häiriöt ovat poikkeusoloja. Poikkeusoloilla on laajoja yhteiskunnallisia vaikutuksia ja organisaatiot joutuvat hyvin todennäköisesti supistamaan toimintaansa ja tarjoamiaan palveluja. Viranomaisten erillislainsäädännöllä tekemä toiminnan sääntely on myös tyypillistä poikkeusoloille. (Iivari & Laaksonen 2009, s. 96).

Organisaatiolla saattaa olla tärkeitä yhteiskunnallisia tehtäviä, joiden turvaaminen on erityisasemassa. Näiden yhteiskuntaa laajemmin koskettavien tapahtumien, kuten suuronnettomuuksien, luonnonmullistuksien, vakavan rikollisuuden tai sotilaallisen voiman käytön aiheuttamat erityistilanteet eli poikkeusolot on määritelty erillisessä yhteiskunnan elintärkeiden toimintojen turvaamisen strategiassa (YETTS). Näissä tilanteissa organisaation tehtävät määritellään valmiussuunnitelmassa. (Iivari & Laaksonen 2009, s. 18).

Toipumissuunnitelma on osa jatkuvuussuunnitelmaa ja se sisältää toimintaohjeet häiriöstä toipumiseen, normaaliin toimintaan palaamiseen sekä toiminnan jatkamiseen. Yksittäinen toipumissuunnitelma sisältää suunnitelmaan kuuluvien liiketoimintaprosessien ja niihin liittyvien tietojärjestelmien varajärjestelmävaatimukset, vastuut, tehtävät valmiuden luomiseksi sekä toimintaohjeet normaaliolojen häiriötilanteissa. Toipumissuunnitteluun kuuluvat olennaisesti riskien arviointi, liiketoiminnan keskeytysvaikutusanalyysi, toipumisstrategiat, harjoittelu ja testaaminen. (Iivari & Laaksonen 2009, s. 19-20).

Valmiussuunnittelu kattaa toiminnan poikkeusoloissa ja sitä käytetään erityisesti julkishallinnossa. Valmiussuunnitelma laaditaan ja ylläpidetään normaaliolojen aikana ja se sisältää kuvauksen toimenpiteistä, joilla varmistetaan organisaation toiminnan jatkuvuus vakavissa häiriötilanteissa ja poikkeusoloissa. Suunnitelmassa kuvataan toimintaperiaatteet häiriötilanteita ja poikkeusoloja varten, normaaliaikana tehtävät varautumistehtävät, toiminnot ja palvelut häiriötilanteissa ja poikkeusoloissa sekä tarvittava yhteistyö sidosryhmien kanssa. Valmiuslaki (1080/1991) liittyy keskeisesti valmiussuunnitteluun ja lain tarkoituksena on antaa viranomaisille riittävät toimivaltuudet sodan aikana ja vähäisemmissä poikkeusoloissa. Valmiuslain mukaan poikkeusolojen aikana organisaatiot voivat joutua luovuttamaan henkilöstöään, tilojaan, laitteitaan ja muita resurssejaan tilanteen vaatimalla tavalla, jos valtioneuvosto tekee päätöksen asiasta. (Iivari & Laaksonen 2009, s. 20-21).

Valtiokonttorin (2012, s. 3) mukaan valmiuslaki (1080/1991) koskee valmiussuunnittelua seuraavasti: ”*Valmiuslaki (1080/1991) 40§: Valtioneuvoston, valtion hallintaviranomaisten, valtion liikelaitosten ja muiden valtion viranomaisten sekä kuntien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muin toimenpitein varmistaa tehtäviensä mahdollisimman häiriötön hoitaminen myös poikkeusoloissa.*”.

Varautumissuunnitelma sisältää valmiussuunnitelman lisäksi toimet normaaliolojen häiriötilanteista palautumiseen. Jatkuvuussuunnittelu ja varautumissuunnittelu eroavat toisistaan siten, että jatkuvuussuunnitelmassa ei varauduta poikkeusolojen aiheuttamiin ongelmiin. Yhteiskunnan kannalta elintärkeät toiminnot, kuten valtionjohto, sotilaallinen puolustus, sisäinen turvallisuus, talouden ja yhteiskunnan toimivuus, väestön toimeentuloturva ja toimintakyky sekä kriisinsietokyky suojataan varautumissuunnittelun avulla. Tämä koskettaa yleisesti julkishallintoa ja varautumisvelvollisuuden piirissä olevia organisaatioita. (Iivari & Laaksonen 2009, s. 21-22).

Organisaation riskienhallinta, tietoturvallisuus ja toiminnan laadunvarmistus ovat osaltaan jatkuvuussuunnittelua. Jatkuvuussuunnittelu on luonteeltaan jatkuvaa ja prosessinomaista ja sen tavoitteena on varautua ennalta mahdollisesti tapahtuviin ongelmiin. Esimerkkejä tällaisista ongelmatilanteista ovat tietojärjestelmien häiriöt, inhimilliset virheet, tahalliset väärinkäytökset, katkokset tietoliikenneyhteyksissä tai sähköverkossa, tulipalot, vesivahingot, toimipisteiden käyttökeltomuus tai avainhenkilöiden menettäminen. Ongelmiin varaudutaan toipumissuunnitelmilla ja normaaliolojen aikana tehtävillä liiketoiminnan tukiprosesseilla, jotka ovat osa jatkuvuussuunnittelua. (Iivari & Laaksonen 2009, s. 18-19).

Jatkuvuussuunnittelu on yhteydessä organisaation muihin toimintoihin ja prosesseihin ja sillä on läheinen yhteys myös riskienhallintaan. Jatkuvuussuunnitteluprosessin tulisi olla jatkuva ja jatkuvaan parantamiseen tähtäävän PDCA-syklin mukainen. (Iivari & Laaksonen 2009, s. 22-23). Kliem & Richie (2015, s. 95) määrittelevät

jatkuvuussuunnitteluprosessin jatkuvaksi kehitys-, ylläpito- ja testausprosessiksi tietokyvyn kasvattamiseksi. Craig (2001) lisää, että jatkuvuussuunnitelmien laatiminen ei ole kertaluontoinen tehtävä vaan prosessi, joka edellyttää koko organisaation kattavaa sitoutumista ja yhteistyötä. Prosessin ylläpitämiseksi jatkuvuussuunnittelun on oltava määrätty tavoitteellinen toiminto. Jatkuvuussuunnittelun päätarkoituksena tulee olla organisaation selviytymiskyvyn varmistaminen.

3.1 Jatkuvuussuunnittelun osa-alueet

Ilmosen et. al. (2010, s. 162-164) mukaan jatkuvuussuunnitteluprojektin suunnittelussa ja toteuttamisessa on 5 vaihetta, jotka ovat:

1. Nykytilan arvioiminen
2. Jatkuvuussuunnitelman perustana olevien riskiskenaarioiden läpikäyminen
3. Parhaiden käytäntöjen hyödyntäminen
4. Jatkuvuussuunnitelman laadinta ja ylläpito
5. Harjoittelu ja oppiminen

Ilmonen et. al. (2010, s. 164) korostavat, että jatkuvuussuunnitelman tekeminen ja sen harjoittelu voivat vaikuttaa ”teoreettiselta puuhastelulta” ja turhalta, koska useimmat laadittavat riskiskenaariot eivät koskaan toteudu. Tällöin saattaa olla vaarana, että jatkuvuussuunnitelma laaditaan kertaluontoisena työnä, eikä sitä koskaan päivitetä tai harjoitella. Jatkuvuussuunnitelmien tekemisen, päivittämisen ja harjoittelun varmistaminen on aina organisaation johdon vastuulla. Johdon on myös varmistettava, että vastuut ovat selkeät ja suunnitelmien tekemiseen ja harjoitteluun on tarvittavat resurssit.

Suunnitelman laatimiseen ei ole yhdenmukaista tapaa, vaan suunnitelmat laaditaan käyttäen hyväksi erilaisia käytäntöjä, joita laativat ja dokumentoivat tietyt organisaatiot, kuten NIST (engl. National Institute of Standards and Technology) (Iivari & Laaksonen 2009, s. 92). Ilmonen et. al. (2010, s. 163) mainitsevat, että jatkuvuussuunnitelmien vertailu eri organisaatioiden välillä voi olla hankalaa asioiden luottamuksellisuuden takia. Koska suunnitelmien tekeminen on myös yksin haasteellista, voidaan suunnittelun apuna käyttää ulkopuolista apua. Erilaisia standardeja, kuten BS 25999 -standardia voidaan hyödyntää jatkuvuussuunnitelmien minimivaatimusten määrittämisessä sekä olemassa olevien jatkuvuussuunnitelmien tasoa ja osatekijöitä arvioitaessa. BS 25999 -standardi on korvattu vuonna 2012 ISO 22301 -standardilla, joka on sisällöltään pääpiirteittään sama, mutta siihen on lisätty muutamia uusia käsitteitä, kuten PDCA-sykli (The British Standards Institution, 2012).

NIST:n tekemän määritelmän mukaan jatkuvuussuunnitelma laaditaan seitsemässä eri vaiheessa, jotka on esitetty taulukossa 4. Suunnitelmia laaditaan tyypillisesti strategia-, prosessi- ja IT-järjestelmätasolla. Ensin on päätettävä vastuut ja suunnitelman taso, jonka

jälkeen voidaan aloittaa jatkuvuussuunnitelman laadinta ja siihen liittyvät toimet, kuten riskianalyysi ja liiketoiminnan keskeytysvaikutusanalyysi (engl. Business Impact Analysis, BIA). (Iivari & Laaksonen 2009, s. 92).

Taulukko 4. *Jatkuvuussuunnittelun vaiheet NIST:n mukaan (mukaellen Iivari & Laaksonen 2009, s. 93).*

	KOORDINOINTI, OHJEISTUS JA VASTUUTUS	KRIITTISTEN PROSESSIEN TUNNISTAMINEN	RISKIEN TUNNISTAMINEN JA ARVIOINTI
Jatkuva parantaminen 	- suunnittelun perusteet - ohjeistus - osallistajat - osallistujien vastuut	- prosessien kuvaus - apuvälineet ja mallit - riippuvuuksien tunnistaminen	- riskianalyysin menetelmät ja apuvälineet - uhkamallit - katastrofit - riskimatriisit - riskien käsittely
	SUUNNITELMAN DOKUMENTOINTI, TESTAUS JA YLLÄPITO	RISKIEN TORJUNTA JA VAIKUTUSTEN PIENENTÄMINEN	LIIKETOIMINNAN KESKEYTYS- VAIKUTUSANALYYSI
	- toipumissuunnitelmat - koulutus - testausmenetelmät - säilytys - auditointi - jatkuva parantaminen	- riskienhallintastrategiat - prosessien parantaminen - rahoitus- ja vakuutusinstrumentit	- vaikutukset liiketoiminnalle - kriittisyysluokittelu - vaikutusten arviointi

Jatkuvuussuunnittelun vaatimaan työmäärään vaikuttavat muun muassa organisaation liiketoimintamallien monimutkaisuus ja toimintaympäristö sekä tehtävän suunnitelman taso. Organisaatiossa aikaisemmin tehdyt jatkuvuutta edistävät toimenpiteet, keskeisten liiketoimintaprosessien sisältö ja riippuvuusuhheet sekä olemassa oleva dokumentaatio vaikuttavat lisäksi työmäärään. (Iivari & Laaksonen 2009, s. 93).

Suunnittelun kannalta on oleellista ymmärtää prosessien toiminta alusta loppuun, jotta prosessi voidaan tarvittaessa rakentaa uudelleen. Prosessien toiminnan ymmärtäminen normaalitilanteissa, normaaliolojen häiriötilanteissa sekä poikkeusoloissa on myös tärkeää. Prosessien välisten riippuvuuksien tunnistaminen ja IT-jatkuvuuden ollessa kyseessä myös IT-järjestelmien ja komponenttien tunnistaminen, joista prosessit ovat riippuvaisia on oleellista. Koska organisaatio ei toimi irrallaan muista toimijoista ja yhteiskunnasta, tarvitaan myös toimintaympäristön ja sidosryhmien toiminnan tuntemusta oman toiminnan tuntemuksen lisäksi. (Iivari & Laaksonen 2009, s. 94-95).

3.1.1 Koordinointi, ohjeistus ja vastuutus

Suunnittelun koordinointi- ja ohjeistusvaiheen tärkeimmät tavoitteet ovat varmistaa, että suunnitelmat tulevat riittävän yhtenäisiksi, eri suunnitelmat tukevat toisiaan ja liittyvät toisiinsa, kokonaisuus on tietyn tahon hallinnassa ja ohjauksessa, suunnitelmia tekevät tahot saavat apua ja tietävät mistä kysyä sitä. Suunnittelutyön tulee olla tehokasta ja viedä mahdollisimman vähän resursseja ja aikaa osallistujilta. Koska suunnitelmia laaditaan eri tasoilla eri ihmisten toimesta, on tärkeää koordinoita ja ohjeistaa suunnittelun toteutus suunnitelmien samankaltaistamiseksi. (Iivari & Laaksonen 2009, s. 97-98).

Tässä suunnitteluvaiheessa määritetään jatkuvuus- ja toipumissuunnitelmien rakenne ja laaditaan mallipohjat, joihin kustakin asiasta vastaavat tahot dokumentoivat suunnitelmaan sisällytettävät asiat. Dokumenttien pohjana voidaan hyödyntää standardeja tai hyväksi havaittuja malleja, joihin tulee sisällyttää taulukot ja tekstiosuudet valmiiksi yhdenmukaisuuden varmistamiseksi henkilöstä riippumatta. Suunnitteluohjeina käytetään yleisesti jotakin riskienhallinta- ja arviointimenetelmää, toipumissuunnitteluun liittyviä teknisiä ohjeistuksia eri järjestelmistä sekä jatkuvuussuunnitteluun liittyviä ohjeistuksia, kuten kirjallisuutta. (Iivari & Laaksonen 2009, s. 97). Suomessa valtiovarainministeriön ylläpitämä VAHTI-verkkosivusto tarjoaa ohjeita ja mallipohjia organisaation jatkuvuussuunnittelua varten (Vahti-ohjeet 2015).

Jatkuvuus- ja toipumissuunnittelun roolit ja vastuut jaetaan eri toiminnoissa ja tehtävissä toimiville henkilöille siten, että organisaation johto nimeää suunnitteluun koordinaattorin, joka ohjaa jatkuvuussuunnittelun käytännön työtä. Johto määrittelee suunniteltavan alueen, suojattavat liiketoiminta-alueet- ja prosessit sekä osallistuu suunnittelun keskeisiin liiketoiminnallisia päätöksiä tai analyysyjä vaativiin vaiheisiin, lisäksi jatkuvuudenhallinnan prosessin tulee olla johdon omistuksessa. Johdon tulee tunnistaa prosessien jatkuvuuden turvaamisen vaatimukset ja osoittaa tarvittavat resurssit jatkuvuuden turvaamisen edellyttämiin toimiin. Lisäksi ulkoisten vaatimusten, kuten asiakkaiden tai viranomaisten asettamien vaatimusten tunnistaminen on johdon vastuulla. Johto osallistuu myös suunnitelmien säännölliseen testaamiseen ja kehittämiseen sekä aktivoi tarvittaessa jatkuvuussuunnitelman toipumiskomponentin eli julistaa tilanteen häiriötilanteeksi, jota varten toipumissuunnittelu on tehty. Koordinoinnin eli suunnittelun käytännön vastuu voi IT-jatkuvuussuunnittelussa olla esimerkiksi organisaation IT-yksiköllä. Vastuutaho ei kuitenkaan laadi suunnitelmia tai tee asiaan liittyviä päätöksiä yksin, vaan varmistaa, että nämä asiat tehdään asianmukaisesti ja että suunnitelmat pysyvät ajantasaisina ja niiden täytäntöönpanoa harjoitellaan. (Iivari & Laaksonen 2009, s. 98-99). Doughty (2001) täydentää, että ylimmän johdon tehtäviin kuuluu lisäksi myös kriittisten rahallisten ja henkilöllisten resurssien saatavuuden jatkuva varmistaminen.

Snedaker (2007, s. 6-7) lisää, että on tärkeää tiedostaa henkilöstön moninaiset roolit ja vastuut häiriötilanteissa. Erityisesti häiriötilanteisiin koulutetut henkilöt alkavat toimimaan, ottamaan vastuuta ja hallitsemaan tapahtumia joidenkin jäädessä

toimintakyvyttömiksi. Tilanteen aiheuttama stressi voi heikentää toimintakykyä myös koulutetussa henkilöstössä. Tämä voidaan huomioida jatkuvuussuunnitelmaa laadittaessa varmemman toimintakyvyn saavuttamiseksi.

Organisaation riskienhallinnan vastuuseen kuuluu jatkuvuussuunnitteluun kuuluvien riskianalyysien suorittaminen ja riskien arviointi. Liiketoimintaa uhkaavat riskit ovat pääosin samoja kuin jatkuvuussuunnitteluun liittyvät riskit, joten on mahdollista hyödyntää aikaisemmin tehtyjen riskianalyysien tuloksia myös jatkuvuussuunnittelua tehtäessä. (Iivari & Laaksonen 2009, s. 100-101).

Tietojen, prosessien ja järjestelmien omistajat määrittävät tietojen, prosessien ja järjestelmien suojaustarpeet, toipumis- ja palautumisvaatimukset sekä liiketoiminnan keskeytymisestä aiheutuvat vaikutukset. Omistajat osallistuvat järjestelmien ja prosessien tärkeysluokitteluun sekä prosessien kuvaamiseen, mikäli prosesseista ei ole olemassa riittäviä prosessikuvauksia. Omistajat määrittelevät tavoitellun toipumisajan (engl. Recovery Time Objective, RTO) sekä toipumispisteen (engl. Recovery Point Objective, RPO). Toipumisaika määrittää ajanjakson, jonka aikana asia tai toiminto on saatava palautettua toimintaan. Toipumispiste määrittää tilan, johon toiminta, tieto tai järjestelmä palautetaan - tämä tila ei välttämättä ole juuri ongelmaa edeltänyt tila. (Iivari & Laaksonen 2009, s. 101).

Organisaation IT-osastolla on tärkeä rooli normaalitilanteiden IT-järjestelmien jatkuvuutta turvaavissa toimissa, kuten tietojen varmistuksessa, järjestelmien ylläpidossa ja teknisessä kehittämisessä. Tietojen ja prosessien omistajat määrittelevät turvattavien kohteiden riippuvuudet tietojärjestelmistä ja suojattavien kohteiden jatkuvuuden ja toipumisen vaatimukset, IT-osasto tarkastelee asiaa tietojärjestelmien osalta. On järkevää tehdä nämä tarkastelut uuden järjestelmän rakennusvaiheessa osana vaatimusmäärittelyä eikä jälkikäteen. Tavallisesti IT-osasto tai järjestelmän kehittäjä tai toimittaja laatii ja ylläpitää organisaation IT-jatkuvuus- ja toipumissuunnitelmia. (Iivari & Laaksonen 2009, s. 102).

Organisaation esimiestason tulee johtaa jatkuvuussuunnittelun toteutusta ja käyttöönottoa vastuullaan olevien asioiden osalta ja varmistaa vastuullaan olevien toimintojen tärkeät asiat. Näitä ovat prosessien ja järjestelmäympäristöjen suunnittelu huomioiden jatkuvuuden vaatimukset, dokumentointi, tietojen varmistaminen, järjestelmien ylläpito ja huolto sekä tehtävien kierto, eriyttäminen ja koulutus. Organisaation henkilöstö osallistuu koulutuksiin sekä rooliensa ja työtehtäviensä mukaisesti toimintaan esimiesten ohjeiden ja määräysten mukaisesti. Organisaation sidosryhmät tulee ottaa mukaan jatkuvuussuunnitteluun, jos ne osallistuvat osaltaan palvelun tai toiminnan tuottamiseen. Vaihtoehtoisesti sidosryhmien jatkuvuussuunnitelmat voidaan huomioida organisaation omassa jatkuvuussuunnitelmassa. Vaikka organisaation toiminta ei olisi riippuvaista sidosryhmistä, on ne huomioitava tiedotuksen, vaatimusten, toivomusten ja

viranomaisten tapauksessa määräystensä osalta jatkuvuussuunnittelussa. (Iivari & Laaksonen 2009, s. 102-103).

3.1.2 Kriittisten prosessien tunnistaminen

Analysoimalla ja tunnistamalla kriittiset prosessit voidaan turvata oikeat asiat oikeilla tavoilla. Tämä on tärkeää, sillä jatkuvuussuunnittelun tavoitteena on turvata organisaation kriittisten prosessien toiminta myös häiriötilanteissa. Kriittisten prosessien omistajan tulee pystyä määrittelemään, kuinka suuren tietomäärän menettämisen, prosessin käyttökatkoksen tai muun häiriön vaikutuksen organisaatio kestää ja millaisia seurauksia tapahtumalla on pidemmällä ajanjaksolla. (Iivari & Laaksonen 2009, s. 104). Carr & McManus (2001) täydentävät, että häiriöistä palautuminen kestää pääsääntöisesti huomattavasti kauemmin kuin itse häiriö. Liiketoiminnan keskeytyminen hetkellisestikin voi aiheuttaa mittavia taloudellisia vahinkoja pidemmällä ajanjaksolla, esimerkiksi silloin jos organisaation asiakkaat eivät voi käyttää organisaation palveluita ja siirtyvät kilpailevan organisaation asiakkaiksi. Järveläinen (2013, s. 584) lisää, että käyttökatkoksilla on merkittäviä vaikutuksia organisaation asiakkaiden uskollisuuteen. Asiakkaat eivät hyväksy mistään syistä johtuvia katkoksia. Jos organisaation palvelut ovat keskeytyksen takia poissa käytöstä, kilpailevien organisaatioiden palveluita käytetään herkästi.

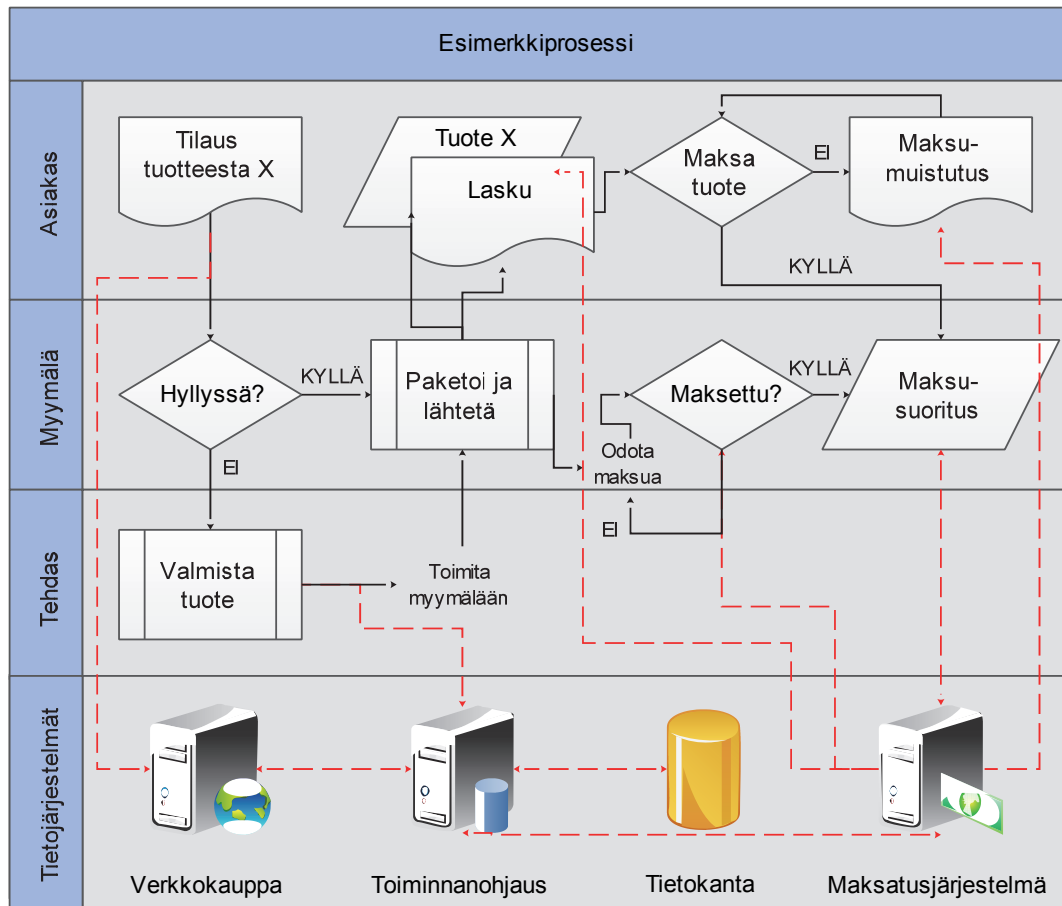
Torabi et. al. (2014, s. 310) huomauttavat, että häiriön tapahduttua organisaation resurssit voivat vähentyä niin, ettei kaikkia häiriön alaisia toimintoja voida palauttaa toimintaan samanaikaisesti. Tärkeimmät ja kriittisimmät toiminnot on palautettava ensimmäisinä toimintaan siten, että huomioidaan toiminnoille määritetty häiriöiden sietokyvyn enimmäisaika (engl. Maximum Tolerable Period of Disruption, MTPD) sekä toimintojen minimipalvelutaso (engl. Minimum Business Continuity Objective, MBCO).

Häiriöiden sietokyvyn enimmäisaika määrittää ajan, jonka kuluessa häiriön aiheuttamat haitalliset vaikutukset kasvavat niin suuriksi, ettei niitä voida enää hyväksyä. Toimintojen minimipalvelutaso on alin hyväksyttävä taso, jolla organisaatio vielä saavuttaa liiketoiminnalliset tavoitteensa häiriötilanteessa. (ISO 22301 2012, s. 5). Snedakerin (2007, s. 3) mukaan tietyt organisaatiot, kuten rahoituslaitokset, luottoyhtiöt ja suurten volyymien verkkokaupat ovat erityisen haavoittuvaisia pitkään kestäville häiriöille. Tällaisissa yhteyksissä, joissa kymmenen minuutin toimintakatkos aiheuttaa organisaatiolle miljoonan dollarin tappiot, on perusteltua investoida suuriakin summia jatkuvan toiminnan varmistaviin jatkuvuusratkaisuihin. Järveläinen (2013, s. 584) lisää, että organisaatio voi saavuttaa kilpailuetua, jos se kykenee palautumaan häiriötilanteista kilpailijoitaan nopeammin.

Onnistunut jatkuvuussuunnittelu ja liiketoiminnan jatkuvuudenhallinta edellyttää prosessien kuvaamisen, sillä ilman kokonaiskuvaa organisaation ydin- ja tukiprosesseista ei voida tietää, miten häiriöt ja poikkeustilanteet voivat vaikuttaa toimintaan. Prosessit

tulee kuvata strategisella ja operatiivisella tasoilla, joilla myös jatkuvuussuunnitelmat tehdään. Normaalit päivittäisessä toiminnassa käytetyt ja toistettavat prosessit kuvataan operatiivisella tasolla, sisältäen kaikki vaiheet ”tuotteen” valmistumiseen, kuten palvelu- tai työkuvaus. Häiriötilanteessa hyvin dokumentoidut prosessit tehostavat toiminnan palauttamista ennalleen, varalaitteille tai varahenkilöiden tehtäväksi. Strategisella tasolla huomioidaan organisaatio kokonaisuudessaan, arvioiden operatiivisten prosessien kriittisyyttä ja keskinäisiä riippuvuuksia. Strategisen tason prosessien kuvaamisen avulla tiedetään, mitkä ovat organisaation tärkeimmät, ensimmäisenä palautettavat prosessit katastrofista tai poikkeusoloista palautumiseksi. Organisaation toiminnan kannalta kriittisiin prosesseihin liittyy usein tietojärjestelmiä, joita voidaan kutsua kriittisiksi järjestelmiksi. Kriittisten prosessien ja järjestelmien tulee kestää pieniä häiriöitä ja poikkeuksellisia tapahtumia, kuten sähkökatkoksia ilman, että toiminta keskeytyy. (Iivari & Laaksonen 2009, s. 105-106). Järveläinen (2013, s. 584) lisää, että kriittisten järjestelmien tunnistaminen ja niihin keskittyminen on ratkaisevaa, joskin kaikki järjestelmät on otettava huomioon.

Prosessit tulee kuvata riittävän yksityiskohtaisesti, jotta ne ovat toistettavissa prosessikuvausten perusteella. Dokumentointi tulee tehdä prosessin kulun (engl. process flow) näkökulmasta sekä yksittäisten tehtävien (engl. tasks) osalta. Vähimmillään kuvaukseen tulisi sisältyä prosessin nimi ja versio, omistaja, kuvaus prosessin läpiviemiseksi jaettuna yksittäisiin tehtäviin, yksittäisten tehtävien kuvaukset (syöte, tuote, alaprosessi, toistuminen, keskimääräinen volyymi), vaadittavat resurssit ja riippuvuudet, ajoitus ja kesto, suorittajat sekä prioriteetti ja kriittisyys organisaation kannalta. Prosessin kulun havainnollistamiseksi voidaan käyttää vuokaaviota, joka on kaavamainen yksinkertaistus prosessin vaiheista ja tehtävistä, tämän lisäksi prosessin kulku kuvataan yleensä sanallisesti. (Iivari & Laaksonen 2009, s. 106-107). Esimerkki prosessikuvauksesta on esitetty kuvassa 8.



Kuva 8. Esimerkki prosessikuvauksesta (mukaellen Iivari & Laaksonen 2009, s. 107).

Prosessien väliset riippuvuussuhteet on tärkeää huomioida, koska prosessin ongelmat voivat heijastua välittömästi tai viiveellä myös toiseen prosessiin. Jos kriittistä tekijää ei tunnisteta, ei sen ylläpitoon ole varauduttu eikä sitä pystytä toipumistilanteessa palauttamaan riittävän nopeasti tai välttämättä ollenkaan. Erilaisten palveluiden, kuten julkisten palveluiden tai tuotantohyödykkeiden jatkuvaan saatavuuteen liittyvät keskeytykset ovat uhkia, joiden syyt tulee selvittää osana prosessien kuvausta ja riskien analysointia. Tarkastelu kohdistetaan erilaisten ja erimittaisten keskeytysten häiriövaikutuksiin ja varautumismahdollisuuksiin, joissakin tilanteissa varautuminen keskeytyksiin on helppoa ja kustannustehokasta. Tyypilliset keskeytykset koskevat esimerkiksi sähkön, kaasun, veden, polttoaineiden, tietoliikenteen tai raaka-aineiden saatavuutta. (Iivari & Laaksonen 2009, s. 109).

Sähkö-energian saatavuuteen liittyvät ongelmat ovat keskeisiä uhkia tietojärjestelmille ja -verkoille. Esimerkiksi hajautetuissa järjestelmissä tietojenkäsittelyn eheys edellyttää luotettavaa sähkön saantia järjestelmän kaikkiin kriittisiin osiin eli sähkön saantia joudutaan tarkastelemaan laajasti. On tarpeen tarkastella prosessien riippuvuutta sähköstä, kuinka pitkät sähkökatkokset on siedettävissä, mitä korvaavia sähkönsaantikanavia on saatavilla ja mitä voidaan tehdä rajoitetulla sähkösaannilla tai

ilman sähköä. Tärkeät IT-järjestelmien keskuksat tulisi pyrkiä varmistamaan esimerkiksi eri muuntajapiireistä ja järjestelmien hallittu alarajo tulee varmistaa varavoimallaittein (engl. Uninterruptible Power Supply, UPS). Lyhyetkin sähkökatkokset voivat aiheuttaa laiterikkoja tai esimerkiksi tietojen korruptoitumista. On tiedostettava myös varajärjestelmien vikaantumisen mahdollisuus, mistä syystä järjestelmiä ei tulisi sijoittaa ainoastaan yhden UPS-järjestelmän taakse. (Iivari & Laaksonen 2009, s. 112).

Organisaatioihin muodostuu usein ns. avainhenkilöiden ryhmiä, joiden menettäminen aiheuttaa riskin. Avainhenkilöt on tunnistettava, jolloin riskiä voidaan pyrkiä pienentämään esimerkiksi parantamalla dokumentointia ja henkilöstöä kouluttamalla. Jos työvoima ei ole käytettävissä esimerkiksi toimitiloihin liittyvän onnettomuuden takia, voidaan käyttää erilaisia etätyöjärjestelyitä, jotka vaativat, että organisaation tietojärjestelmät ovat toimintakuntoisia ja henkilöstöllä on kotonaan käytettävissä tarvittavat laitteet. (Iivari & Laaksonen 2009, s. 112-113). Snedaker (2007, s. 6) lisää, että organisaation avainhenkilöt tulee saada mukaan jatkuvuussuunnitteluun, jotta jatkuvuussuunnitelmista saadaan luotua tukevampia ja samalla niiden käytännön toteuttamisessa oleelliset henkilöt saadaan helpommin tunnistettua.

IT-järjestelmiä voivat uhata esimerkiksi vahingot tai hyökkäykset organisaation sisä- tai ulkopuolelta. Kriittisten IT-järjestelmien haavoittuvaisuus erilaisia hyökkäyksiä kohtaan tulee selvittää kriittisten prosessien kartoituksessa, samoin kuin järjestelmien suojaamiseen ja riskialttiuteen sekä fyysisiin uhkisiin, kuten vesi- ja palovahinkoihin liittyvät asiat. Organisaation yhteistyökumppanien palvelut, kuten ulkoistettu palvelinten hallinta voivat aiheuttaa häiriintyessään katkoksia organisaation toimintaan. Jatkuvuuden parantamiseksi voidaan varautua yhteistyökumppaneista mahdollisesti aiheutuviin uhkisiin. Riski voi olla ulkoistetussa palvelussa pienempi, jos käytetään esimerkiksi isoa ulkoistettua konesalipalvelua. Organisaation itse tuottamassa toiminnassa voidaan toimintaa kuitenkin yleensä valvoa helpommin. Yhteistyökumppanien kanssa solmitut sopimukset voivat myös vaikuttaa riskien suuruuteen ja voi olla mahdollista, että riskejä voidaan pienentää ainoastaan neuvottelemalla sopimukset uudelleen. Palvelutasosopimuksissa määritellään palvelutasot, joista poikkeamisesta määritetään sanktiot. Sanktiot tulee mitoittaa jatkuvuuden keskeytyksen kustannusten mukaisiksi, jotka selvitetään keskeytysvaikutusanalyysin avulla. (Iivari & Laaksonen 2009, s. 114-117).

3.1.3 Riskianalyysi

Riskianalyysi voidaan tehdä kvantitatiivisesti eli määrällisesti käyttäen esimerkiksi uhan toteutumisen todennäköisyyttä prosentteina ja uhan vaikutuksesta seuraavia kustannuksia euromääräisesti. Tämä ei ole aina mahdollista, jolloin voidaan käyttää kvalitatiivista eli laadullista riskianalyysiä, esimerkiksi neliportaista asteikkoa: ei riskiä, matala riski, keskimääräinen riski ja korkea riski. Riskianalyysiprosessi voidaan toteuttaa vaiheittain, tunnistamalla riskit ensin yleisellä tasolla, sitten syventymällä tarkemmin haluttuihin,

esimerkiksi suuriksi arvioituihin riskeihin ja lopuksi analysoimalla niitä tarkemmin. (Iivari & Laaksonen 2009, s. 118).

Kliemin & Richien (2015, s. 82-83) mukaan määrällinen riskianalyysi on laadullista syvällisempi, numeerinen analyysi riskin vaikutuksista. Yksi tavallinen tapa määrälliseen riskianalyysiin on odotetun rahallisen arvon analyysi (engl. Expected Monetary Value, EMV). EMV määritetään kertomalla riskin todennäköisyys prosentteina sen arvioiduilla rahallisilla vaikutuksilla, jolloin saadaan tulokseksi rahamääräinen summa. Esimerkki odotetun rahallisen arvon analyysistä on esitetty taulukossa 5.

Taulukko 5. *Odotetun rahallisen arvon analyysi EMV (mukaellen Kliem & Richie 2015, s. 83).*

RISKI	TODENNÄKÖISYYS	VAIKUTUS	ODOTETTU ARVO EMV	SIJOITUS
A	0,5	100 000 €	50 000 €	2
B	0,7	50 000 €	35 000 €	3
C	0,3	70 000 €	21 000 €	4
D	0,8	150 000 €	120 000 €	1

Riskit tulee arvioida säännöllisin väliajoin, vähintään vuosittain ja aina kun toimintaympäristössä tapahtuu suuria muutoksia, kuten uusien prosessien syntyessä tai vanhojen prosessien muuttuessa. Riskianalyysiä tehtäessä on ymmärrettävä organisaation prosesseihin ja tietojärjestelmiin kohdistuvien uhkien aiheuttajat, esimerkiksi henkilöstö, ulkopuoliset toimijat, järjestelmien ja teknisten laitteiden virheet ja vaurioitumiset sekä erilaiset onnettomuudet. (Iivari & Laaksonen 2009, s. 119).

Riskianalyysijä tehtäessä on havaittu hyväksi liiketoiminnan edustajien ja IT-osaston erilaiset ryhmätyöt, työpajamenettelyt sekä valmiiden dokumenttipohjien täyttäminen. Riskianalyysin tulee keskittyä kaikkiin oleellisiin liiketoimintaprosesseihin, eikä pelkästään IT-asioihin. Liiketoiminnan prosessit ja niihin liittyvät riskit on tärkeää linkittää toisiinsa ja huomioida myös tietoturvallisuuteen liittyvät tekijät, jotta saadaan kokonaiskuva jatkuvuussuunnitteluun liittyvistä vaatimuksista. Kun kaikki toiminnot ja prosessit osallistuvat riskianalyysiin, saadaan kattavampi käsitys organisaatiota uhkaavista riskeistä, niiden todennäköisyyksistä ja vaikutuksista. Liiketoiminnan toimintojen ja prosessien välinen tärkeysjärjestys, kriittiset resurssit, katkojen vaikutukset, sallitut katkoajat ja toimintojen palautusjärjestys saadaan myös määritettyä samalla. (Iivari & Laaksonen 2009, s. 123-124). Kliemin & Richien (2015, s. 82) mukaan riskianalyysissä on myös määriteltävä riskin ”*omistajuus*” eli riskistä vastuullinen taho.

Riskianalyysissä on otettava huomioon myös organisaation johdon rooli. Riskianalyysin tulokset esitellään johdolle ja johto hyväksyy tulokset ja sitoutuu tehtäviin toimiin ja investointeihin. Jos toimiin ei ryhdytä, johto hyväksyy riskit. Hyväksymiskriteerit

määritellään kirjallisesti hyväksymisperiaatteiden tiedottamiseksi. Jos esimerkiksi suojaustoimien rakentaminen veisi ajallisesti liian pitkään, voidaan riski hyväksyä vastoin periaatteita. Tällöin riskin tietoinen hyväksyminen kirjataan ylös ja varmistetaan suojaustoimien rakentaminen sen ollessa mahdollista. (Iivari & Laaksonen 2009, s. 124). Craig (2001) lisää, että riskinottohalu ja hyväksyttävät riskit ovat täysin organisaation johdon päätettävissä. IT-osasto tunnistaa erilaiset riskit ja sen vastuulla on tuoda tunnistetut riskit johdon arvioitavaksi. ISACA:n (2009, s. 17) määritelmän mukaan riskinottohalu on sellainen riskitaso, joka ollaan valmis hyväksymään tavoitteiden saavuttamiseksi.

Riskianalyysillä pyritään tuottamaan päätöksentekijöille tietoa ja ymmärrystä tekijöistä, jotka voivat vaikuttaa toimintoihin ja lopputuotoksiin negatiivisesti, jotta he voivat päättää riskien hallintaan liittyvien toimien toteuttamisesta. Riskianalyysin vaiheet ovat riskienhallintakehikon määrittely, uhkien tunnistaminen, uhkien todennäköisyyden arviointi, riskien ja niiden vaikutusten arviointi ja riskien käsittely. (Iivari & Laaksonen 2009, s. 124-127).

Riskienhallintakehikon tarkoituksena on tehdä riskianalyysien tekemisestä mahdollisimman helppoa kaikille osapuolille ja varmistaa tulosten yhteismitallisuus. Tämä vaihe käsittää pohjien laatimisen uhkien tunnistamiselle, todennäköisyyksille ja vaikutuksille. Samalla voidaan laatia myös uhka- ja haavoittuvuusluetteloita, joita voidaan käyttää apuna riskianalyyseissä. (Iivari & Laaksonen 2009, s. 125).

Riskianalyysi alkaa uhkien tunnistamisesta eli sellaisten uhkien kartoittamisesta, jotka voivat vaikuttaa tarkasteltaviin toimintoihin tai resursseihin negatiivisesti. Tämän jälkeen arvioidaan uhkien toteutumisen todennäköisyys, jonka apuna voidaan käyttää historiatietoja sekä asiantuntijoiden arvioita. Toteutumisen todennäköisyyteen vaikuttavat tarkasteltavan kohteen haavoittuvuudet ja suojaustoimenpiteet. Aluksi voidaan analysoida tarkasteltavan kohteen haavoittuvuudet ja arvioida olemassa olevien suojaustoimenpiteiden vaikutukset, jonka jälkeen voidaan määrittää jäännösriski. (Iivari & Laaksonen 2009, s. 125-126).

Seuraavan vaiheen pyrkimyksenä on tunnistaa ja arvottaa uhkien alaisten toimintojen ja resurssien arvo, kriittisyys ja herkkyys uhille. On erityisen tärkeää tunnistaa tästä joukosta organisaation toiminnan kannalta tärkeimmät. Kun suojattavat asiat on tunnistettu ja arvoitettu, tulee arvioida mahdollisten tappioiden ja vahinkojen maksimimäärä uhkien toteutuessa. Arvion tulee sisältää toiminnan palauttamisesta aiheutuvat kustannukset. Riskien suuruuden määrittämisessä voidaan käyttää mallipohjaa, jossa otetaan kantaa uhan todennäköisyyteen, toteutumisen helppouteen ja kohteen liiketoiminnalliseen arvoon esimerkiksi numeerisilla arvoilla. (Iivari & Laaksonen 2009, s. 126-127). Esimerkki riskin suuruuden arvioinnin mallipohjasta on esitetty kuvassa 9.

UHAN TOTEUTUMISEN TODENNÄKÖISYYS									
Pieni			Kohtalainen			Suuri			
TOTEUTUMISEN HELPPOUS									
KOHTTEEN ARVO	Matala	Kohtalainen	Korkea	Matala	Kohtalainen	Korkea	Matala	Kohtalainen	Korkea
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

Kuva 9. Mallipohja riskien suuruuden arvioimiseksi asteikolla 0-8 (mukaellen Iivari & Laaksonen 2009, s. 127).

Valtiokonttorin (2012, s. 6-7) mukaan useimmat riskien arviointimallit kuvaavat riskin suuruuden uhkan todennäköisyyden ja mahdollisen vaikutuksen tulona, johon liittyy kaksi ongelmaa. Tulomalli ei huomioi, että yksittäiseen riskiin vaikuttaa monia tietyille kohteelle ominaisia uhkatekijöitä sekä yleisiä uhkatekijöitä, jotka vaikuttavat moniin kohteisiin. Lisäksi tulomalli ei huomioi riittävästi niin sanottuja rappeutumisriskejä eli varsinaisen välittömän vahingon lisäksi toipumisen kestosta aiheutuvia vahinkoja. Nämä ongelmat voidaan pyrkiä ratkaisemaan käyttämällä riski-indeksimallia, jossa

- Jokaiselle tarkastelukohteelle määritetään sen riskeihin vaikuttavat uhkatekijät
- Kunkin uhkatekijän riski-indeksi arvioidaan yksittäisistä uhkatekijöistä
- Riski-indeksejä painotetaan tarvittaessa niiden vaikutuksen suuruuden mukaan
- Kokonaisriski on yksittäisten uhkatekijöiden riski-indeksien painotettu keskiarvo

Riskien komponentit visualisoidaan eri värein ja sijoitetaan taulukkoon. Taulukon väristä voidaan päätellä nopeasti yleiskuva kokonaisriskistä. Riskeissä huomioidaan todennäköisyys, vaikutus ja toipumisaika. Lopuksi riskille lasketaan numeerinen arvo siten, että minimiriski on arvoltaan 0 ja maksimiriski on arvoltaan 100. Kokonaisriski tulkitaan riski-indeksin perusteella siten, että

- 00-20: Hyvin vähäinen riski, ei edellytä toimenpiteitä. Tarkastetaan riskiarvio, mikäli mahdollinen vaikutus on suuri.
- 21-40: Vähäinen riski, tarkkaillaan riskin kehittymistä, arvioidaan ja tunnustetaan mahdollisia korjaavia toimenpiteitä.
- 41-60: Kohtalainen riski, suunnitellaan ja aikataulutetaan korjaavat toimenpiteet.
- 61-75: Suuri riski, suunnitellaan ja käynnistetään korjaavat toimenpiteet nopeasti.
- 76-100: Kriittinen riski, käynnistetään korjaavat toimenpiteet välittömästi.

Viimeisessä vaiheessa pyritään löytämään kustannustehokkaita tapoja ja toimia riskien pienentämiseksi ja hallitsemiseksi. Näitä keinoja ovat esimerkiksi uudet käytännöt tai tekniset ja fyysiset kontrollit. Riskien hallinnassa tasapainoillaan riskien toteutumisesta aiheutuvien kustannusten, suojauskustannusten ja vaihtoehtoisten riskien välillä. Lopuksi riskien arvioinnin tulokset dokumentoidaan ja kehitetään riskien hallinnan toimintasuunnitelma. (Iivari & Laaksonen 2009, s. 127-128). Kliem & Richie (2015, s. 80) määrittelevät kontrollin ”*prosesseiksi ja menetelmiksi, joilla vähennetään kriittisiin liiketoimintoihin kohdistuvien riskien todennäköisyyttä ja vaikutusta*”.

Riskianalyysin tulokset kootaan esimerkiksi taulukkoon, johon listataan organisaation toimintaa uhkaavat riskit, niiden vaikutukset, riskien todennäköisyydet ja varautumismenetelmät. (Iivari & Laaksonen 2009, s. 135-136). Esimerkki riskitaulukosta on esitetty kuvassa 10.

RISKI	VAIKUTUS	TODENNÄKÖISYYS	TORJUNTA TOTEUTETTU	TORJUNTA MAHDOLLISTA	RISKIPISTEYTYYS
Tulipalo	Laitetila tai laitteet tuhoutuvat	Korkea	Ei	Kyllä	Korkea
Sähkökatko	Laitteet vahingoittuvat tai eivät voi toimia	Korkea	Kyllä	Kyllä	Matala
Varkaus	Laitteet vahingoittuvat tai katoavat	Kohtalainen	Osittain	Kyllä	Kohtalainen
Kriittisen komponentin hajoaminen	Laite vahingoittuu tai ei toimi	Korkea	Kyllä	Kyllä	Kohtalainen
Järjestelmien häirintä (esim. DDoS)	Ohjelmistojen toiminta estyy tai häiriintyy	Kohtalainen	Osittain	Osittain	Kohtalainen

Kuva 10. Riskitaulukko (mukaellen Iivari & Laaksonen 2009, s. 136).

Merkittävimpiä tai todennäköisimpiä riskejä voidaan käsitellä omissa taulukoissaan, joissa voidaan esittää toimenpiteet riskin käsittelyyn ja normaalitilaan palaamiseen. (Iivari & Laaksonen 2009, s. 137). Esimerkki yksittäisen riskin käsittelytaulukosta on esitetty kuvassa 11.

RISKI	Tulipalo
TODENNÄKÖISYYS	Kohtalainen
VAIKUTUS	Suuri
TODENNÄKÖINEN SKENAARIO	Laitetilassa tai laitetilän rakennuksessa syttyy tulipalo, joka vahingoittaa laitteistoa
HÄIRIINTYNYNEET TOIMINNOT	Kaikki
TOIMENPITEET NORMAALITILAAAN PALAAMISEKSI	<ol style="list-style-type: none"> 1. Esisammutus 2. Palokunnan hälyttäminen 3. Rakennuksen evakuointi jos tarpeen 4. Vahinkojen kartoitus 5. Järjestelmien palauttaminen kriittisyysluokan mukaisesti 6. Tapahtuman syyn selvittäminen ja mahdolliset parannukset
VASTUUHENKILÖ	
UHAN TORJUNTA	<ul style="list-style-type: none"> - Ensisammutusvälineet laitetilassa - Automaattinen palontorjunta - Palohälytysjärjestelmä kaikissa tiloissa - Henkilöstön koulutus hätätilanteisiin - Vakuutukset
RAJOITTEET	
RESURSSIT	

Kuva 11. Yksittäisen riskin käsittelytaulukko (mukaellen Iivari & Laaksonen 2009, s. 137).

3.1.4 Liiketoiminnan keskeytysvaikutusanalyysi

Liiketoiminnan keskeytysvaikutusanalyysillä pyritään selvittämään riskien toteutumisesta aiheutuvat liiketoiminnalliset vaikutukset, joiden perusteella valitaan jatkuvuuden turvaamisen ja toipumisen kannalta oikeat toimenpiteet. Keskeytysvaikutusanalyysissä siis tunnistetaan kriittiset liiketoiminnot sekä niiden keskeytymisestä aiheutuvat kustannukset ja vaikutukset. Keskeytysvaikutusanalyysi on prosessi, jossa kerätään tietoa haastattelemalla liiketoiminnan vastuullisia henkilöitä ja käydään läpi dokumentaatiota. Tiedon keräämisen jälkeen liiketoiminnot, niihin liittyvät tehtävät ja transaktiot sekä eri liiketoimintojen väliset riippuvuudet ja hierarkia dokumentoidaan. Tämä tehdään tyypillisesti samalla kun liiketoimintaprosessit kuvataan, jonka jälkeen liiketoiminnot ja prosessit voidaan luokitella kriittisyysluokkiin kerätyn tiedon perusteella. Liiketoimintojen kriittisyyttä luokiteltaessa on otettava huomioon liiketoiminnan sietämä enimmäiskatko aika, häiriön vaikutukset tuottavuuteen, taloudelliset vaikutukset, säädösympäristöstä johtuvat vastuut ja maine. (Iivari & Laaksonen 2009, s. 138-139).

Torabin et. al. (2014, s. 309) mukaan liiketoiminnan keskeytysvaikutusanalyysi voidaan määritellä prosessiksi, jossa analysoidaan operationaalisia toimintoja ja vaikutuksia, jotka häiriö voi niihin aiheuttaa. Pää tavoitteena on kerätä ja analysoida tietoa raportin koostamiseksi organisaation johdolle liiketoiminnan jatkuvuus suunnitelman tekemistä varten.

Snedaker (2007, s. 211) määrittelee liiketoiminnan keskeytysvaikutusanalyysin tarkoitukseksi:

- Organisaation kriittisten tavoitteiden tunnistamisen ja priorisoimisen sekä näiden palautumisajan määrittämisen
- Johdon informoimisen jokaisen toiminnon keskeytysten enimmäissietoajasta (engl. Maximum Tolerable Outage, MTO)
- Resurssitiedon tuottamisen soveltuvan palautumisstrategian valitsemiseksi
- Sisäisten ja ulkoisten riippuvuuksien esittämisen kriittisten tavoitteiden saavuttamiseksi

Doughty (2001) puolestaan määrittelee liiketoiminnan keskeytysvaikutusanalyysin tehtäväksi organisaation ydinprosessien ja niiden kriittisten riippuvuuksien tunnistamisen. Eri liiketoimintojen edustajien tulisi osallistua palautumisstrategioiden määrittämiseen, jotta palautusstrategioissa voidaan hyödyntää juuri näissä toiminnoissa työskennelleiden tahojen kokemusta. Tähän tarkoitukseen voidaan käyttää erilaisia työryhmiä.

Mawsonin (2003, s. 44) mukaan liiketoiminnan keskeytysvaikutusanalyysillä saavutetaan 3 asiaa:

- Organisaation jokaiselle toiminnolle tai resurssille määritetään arvo organisaation kokonaistoiminnan kannalta
- Luodaan perusta kriittisten resurssien ja toimintojen tunnistamiselle, joka on välttämätöntä palautumisstrategioiden luomiseksi
- Muodostetaan kriittisten kohteiden palauttamisjärjestys katastrofien varalta

Mawson (2003, s. 44) määrittelee myös keskeytysvaikutusanalyysille tavoitteet:

- Sähkökatkosten vaikutusten selvittäminen
- Liiketoimintaprosessien, toimintojen, osastojen ja työalueiden kriittisyyden selvittäminen organisaation kokonaistoiminnan kannalta
- Aikakriittisten tietojärjestelmien, tiedon ja tietoliikennepalveluiden selvittäminen
- Vaadittavan palautumisajan selvittäminen
- Liiketoimintayksikköjen keskinäisten riippuvuuksien selvittäminen
- Vaadittavien resurssien selvittäminen

Jacksonin (2001) mukaan liiketoiminnan keskeytysvaikutusanalyysillä tuotetaan lisäksi organisaation johdolle tietoa, jonka perusteella voidaan arvioida aikakriittisten resurssien ja palveluiden keskeytysten enimmäissieto aika. Useimpien organisaatioiden kannalta aikakriittisiä resursseja ja palveluita ovat:

- Henkilöstö
- Toimitilat
- Tietokonejärjestelmät
- Ohjelmistot
- Puhelin- ja tietoliikenneverkot sekä laitteet
- Tärkeät arkistot ja tieto

Keskeytysvaikutusanalyysin tekoon otetaan mukaan tiedon keräämisen kannalta tärkeimmät tahot, tyypillisesti liiketoiminnasta tietävä liiketoimintajohto sekä keskeytysten vaikutuksista tietävät liiketoimintaprosessien omistajat. Tiedon keräämisessä käytettävät menetelmät, kuten haastattelut tai kyselyt päätetään. Organisaation tärkeimmät liiketoiminnot ja niiden kriittisyysjärjestys sekä tuotantopanokset ja resurssit, joista tärkeimmät liiketoiminnot ovat riippuvaisia, tunnistetaan. On myös laskettava, kuinka kauan liiketoiminnot säilyvät toimintakykyisinä ilman tuotantopanoksia ja resursseja. Tämän jälkeen tunnistetaan liiketoimintoihin liittyvät uhat ja haavoittuvuudet sekä arvioidaan näistä aiheutuvat riskit liiketoiminnoille. Lopuksi havainnot kirjataan ylös, raportoidaan ne johdolle ja tehdään dokumentaatio liiketoiminnan jatkuvuussuunnitelmaan sekä tehdään tarvittavat päätökset riskien pienentämiseksi ja toiminnan jatkuvuuden parantamiseksi. (Iivari & Laaksonen 2009, s. 139).

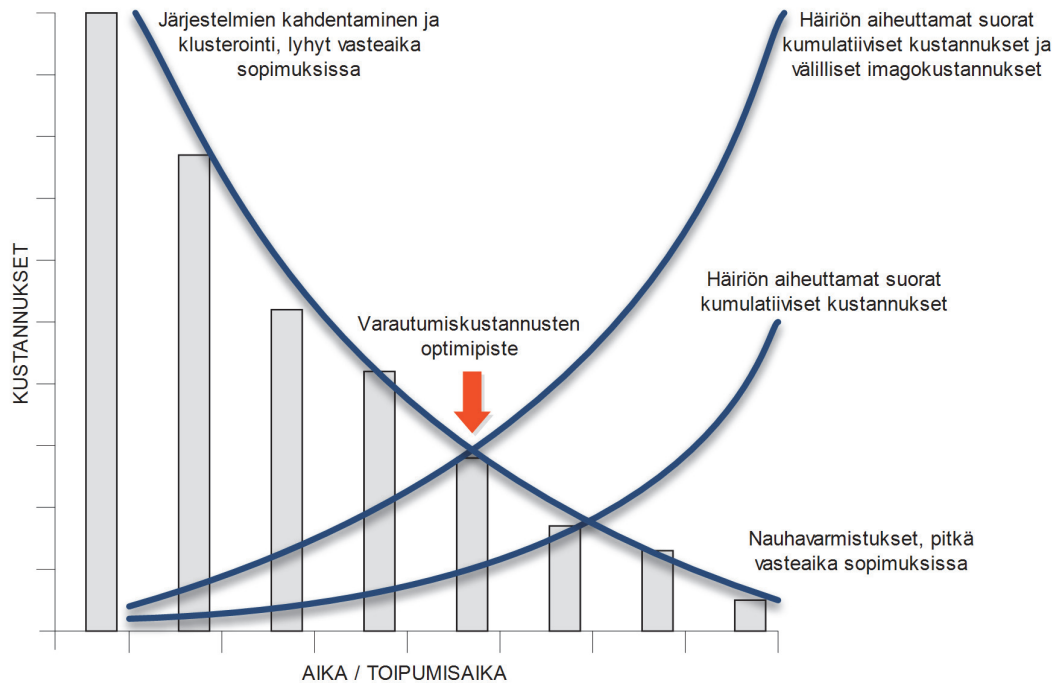
Oikeiden henkilöiden osallistuminen keskeytysvaikutusanalyysiin on tärkeää, sillä mitä paremmin siihen osallistuvat henkilöt tuntevat organisaation liiketoimintaa, sitä tarkempi analyysi saadaan. Tarkoituksena on tunnistaa, mistä asioista liiketoiminta on riippuvaista ja kohdistaa liiketoiminnot näitä asioita tukeviin järjestelmiin, laitteisiin ja muihin tuotantontekijöihin. Eri toimintojen keskinäinen tärkeysjärjestys organisaation kokonaisjatkuvuuden kannalta saadaan selvitettyä yhteisen keskustelun aikana. Keskeytysvaikutusanalyysin avulla eri toiminnot ja niiden keskeytymisestä aiheutuvat kustannukset saadaan mitattua ja arvoitettua sekä riittävä panostus ja resurssit saadaan kohdennettua keskeisimpien toimintojen turvaamiseen. Keskeytysvaikutusanalyysi eroaa riskianalyysistä siten, että siinä ei olla kiinnostuneita keskeytyksen syistä eli riskeistä vaan keskeytysten vaikutuksista toimintaan. Riskianalyysi onkin tehtävä ennen keskeytysvaikutusanalyysiä, jotta kaikki mahdolliset keskeytysten syyt havaitaan. (Iivari & Laaksonen 2009, s. 140-141).

3.1.5 Riskien torjunta ja vaikutusten pienentäminen

Keskeytysvaikutusanalyysin avulla tiedetään kriittisten komponenttien, järjestelmien ja prosessien sietokyky häiriöitä vastaan sekä suojaumisesta aiheutuvat kustannukset. Jotta tiedetään, mikä on optimaalinen riskien ehkäisyn ja vaikutusten pienentämisen taso, tarvitaan kustannusvaikutusanalyysiä. Häiriön kesto vaikuttaa kustannuksiin esimerkiksi huoltosopimusten vasteaikojen kautta ja nopeasta vasteajasta maksetaan enemmän kuin hitaasta. IT-järjestelmissä on huomioitava palvelun kriittisyys siten, että jos järjestelmän toimiminen on aina välttämätöntä, voi sen suojaaminen vaatia esimerkiksi fyysistä hajauttamista eri sijainteihin lyhyen palautumisajan varmistamiseksi. Tällaiset järjestelyt nostavat suojausten kustannuksia. (Iivari & Laaksonen 2009, s. 143-144).

Snedakerin (2007, s. 4) mukaan aina toimiva palvelu on erittäin kallis suunnitella ja toteuttaa. Joissakin organisaatioissa näin voidaan kuitenkin toimia, sillä palvelun toimimattomuus voi aiheuttaa vieläkin suurempia kustannuksia kuin jatkuvaan toimivuuteen liittyvät investoinnit. Häiriöiden sietokyky vaihtelee organisaatioittain ja se on myös riippuvaista ajasta. Organisaation toiminta-aikojen ulkopuolelle sijoittuvat toimintakatkokset eivät välttämättä vaikuta organisaatioon, jos sillä ei ole tällöin toimintaa. Avaintekijöinä suojausta valittaessa ovat organisaation kyky toimia ilman suojelettavaa kohdetta ja suojaukseen käytettävissä olevat resurssit.

Optimaalista suojauskustannusten tasoa voidaan arvioida piirtämällä häiriöstä ajan mittaan aiheutuvat kumulatiiviset kustannukset sekä palautumisesta ja suojauksesta aiheutuvat kustannukset toipumisajan kuluessa. Käyrien leikkauspiste on optimitaso, joka määrittää ajan, jonka järjestelmä voi olla pois käytöstä. Varautumisen kustannukset ovat sitä pienempiä, mitä pidempiä häiriön sieto aika ja toipumisaika voivat olla. (Iivari & Laaksonen 2009, s. 144-145). Esimerkki kustannusvaikutusanalyysistä on esitetty kuvassa 12.



Kuva 12. Esimerkki riskien torjunnan kustannusvaikutusanalyysistä (mukaellen Iivari & Laaksonen 2009, s. 144).

Iivarin & Laaksosen (2009, s. 145) mukaan ei ole järkevää luoda kaikille järjestelmille mahdollisimman nopeaa vasteaikaa, koska tällöin kustannukset kasvavat merkittävästi. Aina ei ole myöskään järkevää toteuttaa halvinta mahdollista ratkaisua, sillä liiketoiminta kärsii toiminnan palauttamisen kestäessä pitkään. Häiriöiden kustannukset voivat olla rahallisten kustannusten lisäksi myös esimerkiksi vaikeammin mitattavia imagokustannuksia. Doughty (2001) lisää, että kustannusvaikutusanalyysillä tehdään riskien ja niiden estämisestä aiheutuvien kustannusten vertailu. Tämän tarkoituksena on valita oikeat toimintatavat, joissa riskien ja kustannusten taso on tasapainossa.

Lainsäädännössä tai sopimuksissa määrättyjen tehtävien hoitamatta jättäminen voi aiheuttaa sanktioita ja asiakkaiden luottamus voidaan menettää, mistä aiheutuu välillisesti myös taloudellisia kustannuksia. Suojausten oikea ja riittävä suunnittelu ja toteutus jo järjestelmän käyttöönotto- tai tilausvaiheessa aiheuttaa murto-osan kuluja jatkuvasti muutettavaan ja korjailtavaan järjestelmään verrattuna. Tästä syystä järjestelmän käytettävyyksivaatimukset on analysoitava ennen järjestelmän vaatimusmäärittelyn tekemistä ja järjestelmän käyttöönottoa tai tilaamista toimittajalta. (Iivari & Laaksonen 2009, s. 145).

Riskienhallinnan strateginen tavoite on sovittaa mahdolliset riskien negatiiviset vaikutukset organisaation toimintaan ja riskien estämisestä aiheutuviin suoriin tai epäsuoriin kustannuksiin. Eri riskejä hallitaan eri tavoilla ja samatkin riskit voidaan hallita eri tavoilla eri toiminnoissa, joissakin prosesseissa riski voi olla hyväksyttävissä kun taas toisaalla riskiä voidaan hallita esimerkiksi vakuutuksen avulla. Riskienhallinnan

strategiat valitaan liiketoiminnan keskeytysvaikutusanalyysin tulosten avulla siten, että huomioidaan lakisääteiset velvoitteet ja normit, koska joihinkin riskeihin voi olla pakollista varautua. Organisaation havaitessa uuden, ennen huomioimattoman riskin on valittava strategia, jonka mukaan havaittu riski halutaan hallita. (Iivari & Laaksonen 2009, s. 146).

Organisaatio voi käyttää riskienhallintaan yleensä useita erilaisia keinoja. Riski voidaan välttää luopumalla riskialttiista toiminnasta, jos riskejä ei haluta ottaa. Resurssien tai laitteiden monistamisella voidaan joissakin tapauksissa saavuttaa riittävä toimintavarmuus pienelläkin investoinnilla, samoin kuin ulkoistamalla riski suurelle palveluntarjoajalle. Riskeistä aiheutuvia vaikutuksia minimoimalla, esimerkiksi varmuuskopioinnilla tai varahenkilöjärjestelyillä voidaan pyrkiä torjumaan riskin toteutumisesta aiheutuvaa haittaa. Riskin aiheuttamia taloudellisia kustannuksia voidaan myös siirtää vakuutusten avulla, mutta pääasiallisesti on suositeltavaa käyttää muita keinoja, koska vakuutukset eivät usein korvaa välillisiä vahinkoja. Näitä vahinkoja vastaan on olemassa erillisiä keskeytysvakuutuksia, joilla voidaan kattaa myös välillisiä vahinkoja ainakin osittain. Riski voidaan myös hyväksyä, jos se on riittävän pieni. Tähän vaikuttaa organisaation koko, toimiala ja riskinottohalu. Riski voi olla pieni silloin, jos se on vaikutuksiltaan tai todennäköisyydeltään tai molemmilta osin pieni. (Iivari & Laaksonen 2009, s. 146-148). Kliem & Richie (2015, s. 5) suosittelevat oman riskienhallinnan ja vakuutusten yhdistelmää. Organisaation omat jatkuvuudenhallinnan toimenpiteet voivat vaikuttaa vakuutusmaksuihin alentavasti.

Prosessien jatkuvuuden parantamiseen pyrkivät toimenpiteet voivat olla joko riskejä ehkäiseviä, niitä välttäviä tai niiden vaikutuksia vähentäviä. Prosessien toiminnan turvaamiseksi voidaan hankkia varalaitteita, välineitä ja tarvikkeita varastoon, erityisesti jos toimittajan huoltovarmuuteen ei pystytä tai haluta luottaa. Organisaation prosessien kannalta tärkeät, vikaantumiselle alttiit laitteet on voitava korjata tai vaihtaa uusiin nopeasti. Varmuuskopioimalla säännöllisesti organisaation käsittelemä tieto ja tietojärjestelmät vähennetään häiriöistä aiheutuvaa työmäärää ja aikaa. Henkilöstön osaamiseen panostamalla voidaan myös parantaa prosessien jatkuvuutta, jotta henkilöstö tiedostaa organisaation jatkuvuuden kannalta tärkeät asiat, prosessit, laitteet ja työvälineet. Koulutus parantaa lisäksi henkilöstön reagointinopeutta ja toipumissuunnitelmien skenaarioiden harjoittelu harjaannuttaa toimimaan vastaavissa tilanteissa. Prosessien jatkuvuutta parantavien kontrollien parannuksien lisäksi tulee arvioida olemassa olevien kontrollien toimintaa ja tehokkuutta, eikä vanhentunutta tai turhaa kontrollia tule käyttää organisaation riskienhallinnassa tavan vuoksi. Kontrolli on korvattava uudella, jos se on helposti saatavilla, perusteltavissa ja kustannustehokas. (Iivari & Laaksonen 2009, s. 148-149).

Riskien vaikutuksia voidaan rajoittaa ja jakaa vakuutuksilla, joskaan riski ei ole koskaan täysin siirrettävissä. Jos riski on organisaation kannalta liian suuri yksin kannettavaksi, eikä sitä voida muilla tavoin välttää riittävästi tai hyväksyä, voi vakuuttaminen olla

järkevää. Organisaatio tarvitsee usein vapaaehtoisia vakuutuksia toiminnan keskeytysten ja häiriöiden varalta lakisääteisten vakuutusten, kuten henkilöstön tapaturma- ja työeläkevakuutusten lisäksi. Vakuutukset auttavat organisaatiota kattamaan häiriöistä ja katastrofeista aiheutuneita taloudellisia kustannuksia, mutta vakuutuksilla ei voida estää vahinkojen syntymistä. (Iivari & Laaksonen 2009, s. 150). Kliemin & Richien (2015, s. 6) mukaan tietyt toiminnan osa-alueet, kuten henkilöstöresurssit ovat erityisen alttiita oikeustoimille. Jatkuvuussuunnittelussa tulee huomioida myös lakiteknisten asioiden aiheuttamat riskit.

3.1.6 Suunnitelman dokumentointi, testaus ja ylläpito

Jatkuvuussuunnittelun dokumentointivaiheessa on huomioitava suunnittelun tasot, strateginen ja operatiivinen taso. Strategisen tason suunnitelma toimii perustana operatiivisen tason suunnitelmille. Organisaatiolla tulee olla jatkuvuussuunnitelmat kaikista sen strategisesti merkittävistä toiminta-alueista eli niistä toiminnoista, jotka on määriteltävä tärkeiksi strategisen tason jatkuvuussuunnitelmassa. On tiedettävä, mitä operatiivisen tason jatkuvuussuunnitelmia ruvetaan mahdollisesti vähentyneillä resursseilla toteuttamaan ja mitä toimintoja palauttamaan, jos katastrofitilanne tapahtuu. (Iivari & Laaksonen 2009, s. 152-153).

Suunnitelmien tulisi noudattaa yhteistä rakennetta ja tätä varten suunnitelmille laaditaan mallirunko. Rungon tulisi sisältää tietyt perusasiat, jotka ovat versionhallinta, tavoite ja rajaukset, riskienhallinta, liiketoiminnan keskeytysvaikutusanalyysi, jatkuvuuden turvaaminen, toipumissuunnitelmat, toipumisryhmien vastuut ja tehtävät, yhteystiedot, jatkuvuussuunnitelman testaaminen, koulutus sekä jatkuvuussuunnitelman ylläpito. (Iivari & Laaksonen 2009, s. 153-156).

Versionhallintaosioista tulisi selvittää, koska jatkuvuussuunnitelmaa on viimeksi päivitetty ja kenen toimesta päivitys tehtiin ja mitä muutoksia tehtiin. Versionhallinta antaa myös sisäisille tai ulkoisille auditoijille kuvan siitä, milloin ylläpito on tehty. Tavoitteessa ja rajauksissa kerrotaan, minkä takia ja mihin tavoitteeseen tai tarkoitukseen dokumentti on tehty. Rajaus kertoo, onko kyseessä strategisen vai operatiivisen tason suunnitelma ja määrittelee, keitä suunnitelma koskee. Riskienhallinta on pakollinen osuus, jossa luetellaan kaikki riskianalyysivaiheessa tunnistetut riskit, niihin varautuminen, todennäköisyys ja luokittelu. Riskienhallintaosassa on hyvä esittää strategiset vaihtoehdot riskien hallintaan ja toimenpiteet, joilla riskienhallintaa toteutetaan käytännössä. Keskeytysvaikutusanalyysiosassa esitetään analyysin tulokset ja se on myös pakollinen osio. Tässä osiossa luetellaan kriittiset toiminnot, jotka organisaatio tai tarkastettava prosessi tarvitsee toimiakseen. Jatkuvuudenturvaamisosiossa esitetään muun muassa normaalitilanteissa tehtävät huoltotoimenpiteet aikatauluineen ja tekijöineen. Osiossa käsitellään myös IT-järjestelmien varmistukseen liittyvät asiat ja yleistä toiminnan jatkuvuutta parantavat tekijät, kuten varahenkilöjärjestelyt. (Iivari & Laaksonen 2009, s. 153-154).

Toipumissuunnitelmia käsittelevä osiossa esitetään toimet, kuinka palataan vakavasta häiriötilanteesta tai poikkeusoloista normaaliin tilaan ja kuinka toipumisryhmä menettelee häiriötilanteissa. Toipumistoimenpiteiden sisältö ja vastuut, toipumishenkilöiden määrä, yhteystiedot, resurssit, roolit ja vastuut toipumisen toteuttamiseen esitetään myös tässä osiossa. Tähän osioon on hyvä sisällyttää myös ennalta mahdollisesti mietityt palautuspolut ja eri toimintojen ja järjestelmien palautusjärjestys sekä tiedotusjärjestelyt jatkuvuuden ollessa uhattuna. Yhteystieto-osioon kerätään organisaation toipumisryhmän, varajäsenten ja toipumisen kannalta tärkeiden ulkopuolisten tahojen, kuten yhteistyökumppanien, laitetoimittajien ja tietoliikenneoperaattorien yhteystiedot. Testausosiossa esitetään käytetyt testausmenetelmät, testausprosessi ja testausaikataulu. Koulutusta koskevat asiat, kuten koulutussuunnitelma, koulutuksen vastuuhenkilöt sekä koulutuksen sisältö esitetään koulutusosiossa. Ylläpito-osio kertoo, kuinka jatkuvuussuunnitelmaa ylläpidetään, kenen vastuulla ylläpito on ja millä aikataululla suunnitelma on käytävä läpi ja muutokset on tehtävä. Tässä osiossa kerrotaan myös, missä ja miten suunnitelmaa säilytetään. (Iivari & Laaksonen 2009, s. 154-155).

Ilmosen et. al. (2010, s. 164) mukaan jatkuvuussuunnitelman testaamisen tehtävänä on lisäarvon tuottaminen ja toiminnan kehittäminen, ei henkilöiden syyllistäminen tai vajavaisen valmiuden osoittaminen. Testaamisessa voidaan käyttää tarkkailijaa, joka raportoi testauksen etenemisen. Raportissa arvioidaan kunnossa olevat ja kehittämistä vaativat asiat sekä tärkeimmät vaaratekijät ja korjaavat toimenpiteet vastuuhenkilöineen. Testauksen päätyttyä järjestetään yhteenvetotilaisuus, johon kaikki testaukseen osallistuneet osallistuvat. Raportissa voidaan myös arvioida, kuinka suuria vahinkoja olisi vastaavassa tositilanteessa odotettavissa.

Cerullon & Cerullon (2004, s. 77) mukaan jatkuvuussuunnitelman testaaminen ja harjoittelu tärkeä osa jatkuvuussuunnittelua. Jatkuvuussuunnitelma tulee testata kattavasti ja henkilöstöä on harjoitettava, sillä IT-riippuvaisten organisaatioiden kyky selviytyä vakavista häiriötilanteista paranee testaamisen ja harjoittelun myötä. Organisaatioiden on myös arvioitava testausmenetelmiään, jotta ne ovat käytännöllisiä, kustannustehokkaita ja sopivia. Kattavalla testaamisella saavutetaan varmuutta toiminnassa sekä varmistetaan palautumiskyky tositilanteessa.

Lam (2002, s. 23) määrittelee neljä syytä testata jatkuvuussuunnitelmia:

- Selvitetään jatkuvuussuunnitelmien kyky ylläpitää asetettuja palvelutasoja
- Tunnistetaan jatkuvuussuunnitelmien mahdolliset puutteet aikaisessa vaiheessa
- Arvioidaan ovatko asetetut palvelutasot realistiset ja saavutettavissa olemassa olevilla resursseilla
- Kasvatetaan johdon ja henkilöstön luottamusta jatkuvuussuunnitelmiin

Jatkuvuussuunnitelman harjoittelu ja testaaminen käsittävät testausmenetelmien luomisen, häiriöistä vastaavan henkilöstön samanaikaisen testauksen ja harjoittelun sekä jatkuvuussuunnitelman arvioimisen ja uudelleentestauksen. Testaaminen on välttämätöntä, jotta voidaan selvittää jatkuvuussuunnitelman kyky vastata kriittisiin riskeihin. Tämän lisäksi testaamisella varmistetaan, että häiriöistä vastaava henkilöstö tietää, kuinka sen tulee toimia realistisissa tilanteissa. Harjoittelu kasvattaa myös henkilöstön itseluottamusta ja vähentää hätäntymistä tositilanteessa. Ylimmän johdon tuki testaamiselle ja harjoittelulle varmistaa organisaation sitoutumisen ja tarvittavat resurssit. (Cerullo & Cerullo 2004, s. 71). Dey (2011, s. 231) lisää, että jatkuvuussuunnitelman testaamisessa on huomioitava kaiken tyyppiset riskit pahimpien mahdollisten vaikutusten mukaan.

Morwoodin (1998, s. 28) mukaan jatkuvuussuunnitelmista hyödytään ainoastaan silloin, kun niitä voidaan toteuttaa käytännössä. Organisaation kyky hyödyntää jatkuvuussuunnitelmia riippuu merkittävästi henkilöstön tietoisuudesta ja kyvystä suorittaa jatkuvuussuunnitelmissa määritettyjä asioita. Jatkuvuussuunnitelmiin ei voida perehtyä ensimmäistä kertaa silloin, kun häiriö on jo tapahtunut. Pelkkä jatkuvuussuunnitelmien lukeminen ei myöskään riitä, vaan tarvitaan harjoittelua ennen häiriöiden toteutumista. Wrobel (2001) lisää, että jatkuvuussuunnitelman toiminnan testaaminen ja arvioiminen on yhtä oleellinen osa jatkuvuussuunnittelua kuin palautumistoimien kuvaaminen. Testaamisessa suositellaan käytettäväksi dokumentointia, johon harjoitukseen osallistuneet kirjaavat harjoituksessa oppimiaan asioita ja mahdollisia muutostarpeita seuraavaa testausta ajatellen. Dokumentointi tulee myös käydä lävitse organisaation johdon kanssa. Testaustilannetta tulee ajatella oppimistapahtumana ja eri tilanteita voidaan harjoitella sulkemalla tarkoituksella tiettyjä avainhenkilöitä harjoituksen ulkopuolelle.

Morwood (1998, s. 28) suosittaa, että henkilöstöä harjoitettaisiin ensin, jonka jälkeen harjoiteltuja asioita testattaisiin käytännössä. Tällöin voidaan varmistua, että harjoitellut asiat vastaavat käytännön tilanteissa tarvittavaa osaamista. Henkilöstöä tulee harjoittaa ensin tilanteisiin, joista heidän tulee suoriutua. Harjoittelu ja testaaminen eroavat toisistaan ainoastaan tavoitekriteerien osalta. Testaamisessa tavoitekriteerit ovat harjoittelua korkeampia, todellisen vaadittavan tason mukaisia.

Morwood (1998, s. 29) jakaa jatkuvuussuunnitelmien harjoittelun kahteen tyyppiin:

- Tietoisuutta lisäävä koulutus
- Skenaarioiden harjoittelu

Tietoisuuden lisäämisen tarkoituksena on luoda koko henkilöstölle ymmärrys jatkuvuussuunnitelmien sisältämisestä asioista. Tällainen koulutus toteutetaan eri tavoin riippuen siitä, osallistuuko kohteena oleva henkilöstö jatkuvuudenhallintaan epäsuorasti vai suorasti. Epäsuorasti jatkuvuudenhallintaa toteuttava henkilöstö käsittää käytännössä

koko organisaation henkilöstön, jolloin riittää yleisluontoinen luennointi, jossa käsitellään organisaation vastuita, ryhmiä ja tehtäviä ja toimintaa yleisesti häiriötilanteissa. Jatkuvuudenhallintaa suorasti toteuttava henkilöstö tarvitsee yksityiskohtaisempaa koulutusta. Koulutuksen sisältö on pääsääntöisesti samaa kuin koko henkilöstölle, mutta tarkemmassa mittakaavassa. Koulutuksessa tulee käydä lävitse erityisesti osallistujien roolit ja vastuut tehtävineen. Koulutus tulee järjestää myös organisaatioon uusina henkilöinä rekrytoituille sekä tehtäviään organisaation sisällä vaihtaneille henkilöille. Koulutusta tarvitaan myös tilanteissa, joissa olemassa oleviin jatkuvuussuunnitelmiin tehdään suurempia muutoksia. (Morwood 1998, s. 29-30).

Skenaarioiden harjoittelu tulee toteuttaa tietoisuuden lisäämisen jälkeen. Harjoitusten tulee vastata kohderyhmän häiriöiden aikaisten tehtävien tasoa ja eri henkilöstöryhmiä harjoitetaan tehtäviensä mukaisissa asioissa. Harjoituksilla voidaan varmistaa henkilöstön osaaminen jatkuvuussuunnitelmissa määritettyjen alueiden osalta sekä kasvattaa osaamista tarvittavissa taidoissa. Harjoitukset voivat lisäksi tuoda esiin jatkuvuussuunnitelmissa olevia puutteita ja kehittää sitä entisestään. Tyypillinen koulutus- ja harjoitusohjelma sisältää esimerkiksi neljännesvuosittain järjestettävät tietoisuutta lisäävät koulutukset uusille ja tehtäviään vaihtaneille henkilöille, neljännesvuosittain tai puolivuositain järjestettävät teoreettiset harjoitukset, joissa henkilöstö pohtii reagoimistaan ja toimintaansa kuvitteellisissa tilanteissa sekä vuosittain järjestettävät käytännön operatiiviset harjoitukset. (Morwood 1998, s. 30-31).

Deyn (2011, s. 232) mukaan on hyvin tärkeää, että henkilöstö ymmärtää jatkuvuussuunnittelun käytön ja siihen osallistumisen tärkeyden. Henkilöstöä koskevien jatkuvuudenhallintapolitiikkojen, -menetelmien ja -ohjeistuksien ymmärtäminen tulee varmistaa tietoisuutta lisäämällä. Dokumentoinnin on oltava riittävää jatkuvuudenhallinnan kaikissa vaiheissa. Ylimmän johdon merkitys motivoivana tahona on suuri alusta lähtien. Lam (2002, s. 25) lisää, että sitoutumista jatkuvuudenhallintaan voidaan kasvattaa käyttämällä varoittavina esimerkkeinä sattuneita katastrofeja, joiden seurauksiin olisi voitu vaikuttaa jatkuvuussuunnitelmien avulla. Henkilöstön tietoisuutta voidaan lisätä ryhmätyöskentelyllä, jolloin voidaan tarvittaessa kutsua myös organisaation ulkopuolisia asiantuntijoita luennoimaan. Koulutusta tulee antaa sekä tekniselle henkilöstölle että organisaation johdolle.

Jatkuvuussuunnitelma tulisi säilyttää ainakin kahdessa fyysisesti erillään olevassa paikassa, esimerkiksi organisaation päätoimitiloissa, jossakin varatilassa ja mahdollisessa varmuuskopioiden erillisessä säilytystilassa tai arkistossa. Säilytys tulisi tehdä sekä paperisessa että sähköisessä muodossa ja päivitysten yhteydessä tulisi päivittää myös kaikki suunnitelmasta tehdyt kopiot. (Iivari & Laaksonen 2009, s. 157-158).

4. ISO/IEC 27031 -STANDARDI

ICT-valmius liiketoiminnan jatkuvuudenhallintaan (engl. ICT Readiness for Business Continuity, IRBC, jatkossa ICT-valmius) on hallintajärjestelmä, jonka avulla organisaatio voi vastata jatkuvasti muuttuviin riskeihin, varmistaa kriittisten ICT:n tukemien liiketoimien jatkuvuuden, olla valmiudessa reagoimaan ICT-palveluiden katkeamiseen sekä palautua häiriöistä ja katastrofeista. ICT-valmius on osa liiketoiminnan jatkuvuudenhallintaprosessia. (ISO/IEC 27031 2011, s. 3-4). Deyn (2011, s. 229) mukaan ICT-valmiudella voidaan taata IT-palveluiden luottamuksellisuus, eheys ja saatavuus kaikissa tilanteissa ja se on täten merkittävässä roolissa liiketoiminnan jatkuvuuden ylläpidossa.

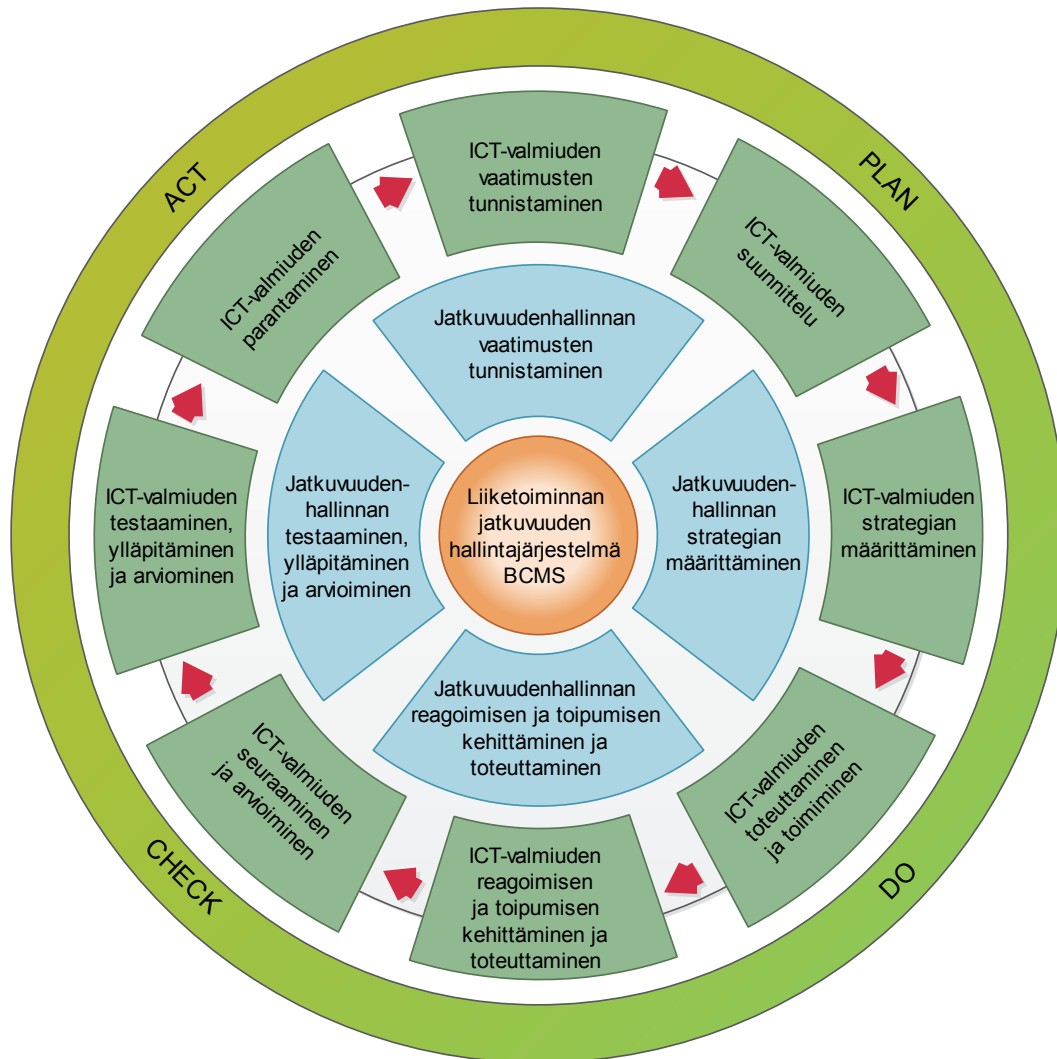
ISO/IEC 27031 -standardi tarjoaa ohjeistuksen tapahtumienhallintaan (engl. incident management), tietoturvallisuushkiin reagoimiseen sekä keskeytysten pienentämiseen. Standardi auttaa organisaatiota varautumaan ja reagoimaan tietoturvallisuuden vaarantumiseen sekä vähentämään liiketoimintaan kohdistuvia keskeytyksiä. Se tarjoaa viitekehyksen kaikkien osa-alueiden tunnistamiseen ja määrittelemiseen organisaation ICT-valmiutta koskien. Standardia voidaan hyödyntää kaiken kokoisissa organisaatioissa, joissa rakennetaan ICT-valmiutta ja joissa vaaditaan ICT-palveluiden ja -infrastruktuurin toimintaa liiketoimintojen varmistamiseksi keskeytysten aikana. Standardin avulla voidaan myös mitata ICT-valmiuden toimivuutta johdonmukaisella ja tunnistetulla tavalla. (Humphreys 2012, s. 19).

Liiketoiminnan jatkuvuudenhallinta (engl. Business Continuity Management, BCM) on hallintaprosessi, jolla tunnistetaan uhkien potentiaalisia vaikutuksia organisaatioiden liiketoimintaan. Se tarjoaa viitekehyksen sietokykyä ja suojautumista varten organisaation toiminnan keskeytyksiä vastaan. (ISO/IEC 27031 2011, s. 3-4).

Torabi et. al. (2014, s. 309) määrittelevät liiketoiminnan jatkuvuudenhallinnan prosessiksi, jolla luodaan puitteet organisaation häiriönsiedolle ja jolla pyritään tunnistamaan sisäisiä ja ulkoisia uhkia ja riskejä sekä selvittämään niiden vaikutuksia liiketoimintaprosesseihin. Tuckerin (2015, s. 33) mukaan liiketoiminnan jatkuvuudenhallinta käsittää riskien tunnistamisen ja vaiheet riskien käsittelyyn tavalla, jotka tekevät organisaatiosta sietokykyisen häiriöitä aiheuttaville tapahtumille ja tilanteille. Tarkoituksena on luoda strategiat toimintojen ylläpitämiseen ja valmistella henkilöstö toteuttamaan laadittuja strategioita sekä varmistaa tarvittavien resurssien olemassaolo niitä tarvittaessa.

Organisaation täytyy ottaa käyttöön järjestelmällinen prosessi estääkseen, ennustaakseen ja hallitakseen IT:n häiriöt, jotka voivat potentiaalisesti katkaista IT-palveluiden toiminnan. Tämä voidaan parhaiten saavuttaa soveltamalla PDCA-syklin mukaista

toimintaa ICT-valmiuden hallinnassa. Tällä tavoin ICT-valmius tukee liiketoiminnan jatkuvuudenhallintaprosessia varmistamalla, että IT-palvelut ovat mahdollisimman häiriösietoisia ja ne voidaan palauttaa toimintaan sovitusti ennalta määrätyillä tavoilla ja ennalta määrätyssä ajassa. (ISO/IEC 27031 2011, s. VI). ICT-valmiuden ja liiketoiminnan jatkuvuudenhallinnan integraatio on esitetty kuvassa 13.

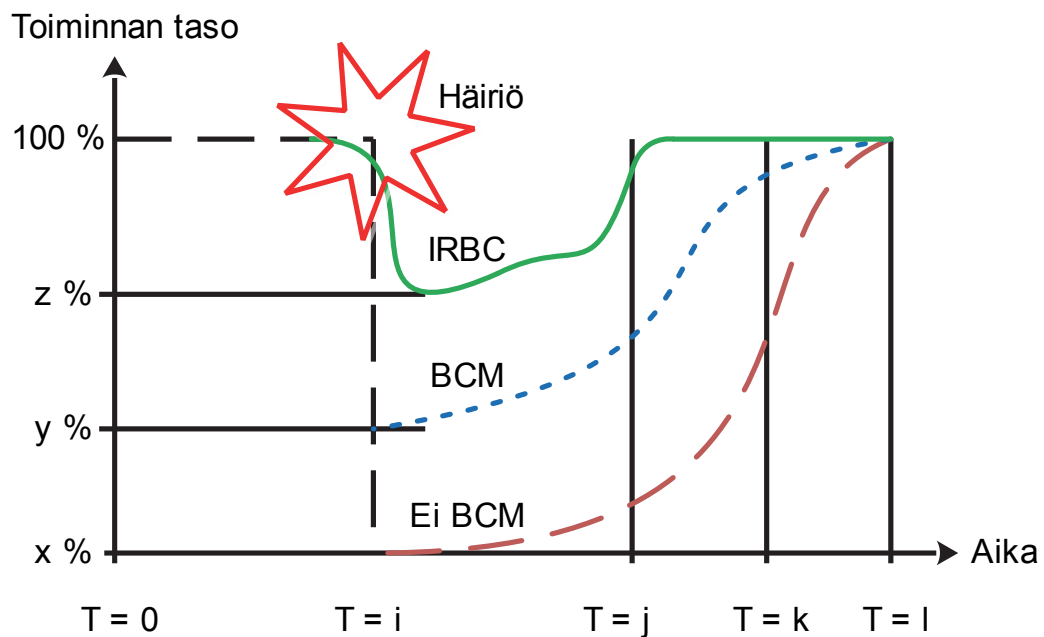


Kuva 13. ICT-valmiuden ja liiketoiminnan jatkuvuudenhallinnan integraatio (mukaillen ISO/IEC 27031 2011, s. VII).

Humphreysin (2012, s. 20) mukaan ICT-valmiudella voidaan täydentää ja tukea organisaation liiketoiminnan jatkuvuudenhallintaa sekä tietoturvaluutta:

- Reagoimalla jatkuvasti muuttuvaan riskiympäristöön
- Varmistamalla kriittisten liiketoimintojen jatkuvuus
- Valmistautumalla toimimaan ja reagoimaan ICT-palveluiden katkoksiin ennen niiden tapahtumista
- Reagoimalla häiriöihin ja katastrofeihin sekä palautumalla niistä

Humphreys (2012, s. 20-21) lisää, että organisaatio voi vähentää liiketoiminnan katkeamisia ja niistä palautumiseen kuluva-aikaa ottamalla käyttöön ISO/IEC 27031 -standardin mukaiset aikaisen varoituksen, havainnoinnin ja ennakoimisen prosessit. Tällöin organisaation ICT-infrastruktuuri ja -järjestelmät ovat sietokykyisempiä ja tukevampia liiketoiminnan jatkuvuuden kannalta ja toiminnan tason aleneminen on asteittaista häiriön tapahtuessa äkillisen ja suuren romahduksen sijaan. Toiminnan taso ei myöskään laske niin alas kuin ilman varautumistoimenpiteitä. Häiriötilanteet tulee dokumentoida, analysoida ja katselmoida, jotta niistä voidaan oppia vastaavia tulevaisuuden tilanteita varten. Tällöin organisaatio on paremmin valmistautunut häiriöihin, tapahtumat ovat paremmin hallittavissa ja aikaisemmin tehdyt virheet voidaan jättää toistamatta. Esimerkki ICT-valmiuden ja liiketoiminnan jatkuvuudenhallinnan vaikutuksista häiriötilanteesta palautumiseen on esitetty kuvassa 14.



Kuva 14. ICT-valmiuden ja liiketoiminnan jatkuvuudenhallinnan vaikutukset toiminnan palautumiseen häiriötilanteessa (mukaillen Humphreys 2012, s. 20).

4.1 ICT-valmius

ISO/IEC 27031 -standardin (2011, s. 5). määritelmän mukaan ICT-valmius perustuu viiteen pääperiaatteeseen:

- *Haitallisten tapahtumien estäminen:* ICT-palveluiden suojaaminen uhkilta on kriittistä organisaation järjestelmien toiminnan riittävän tason varmistamiseksi
- *Haitallisten tapahtumien havaitseminen:* Tapahtumien havaitseminen aikaisimmassa mahdollisessa vaiheessa vähentää niiden vaikutuksia palveluihin, palautumiseen vaadittavia resursseja ja varmistaa riittävän palvelun laatutason

- *Reagoiminen*: Tapahtumaan parhaiten sopiva reagoimistapa johtaa tehokkaampaan palautumiseen ja vähentää toimintakatkosten kestoa, väärä reagoimistapa voi aiheuttaa pienen ongelman muuttumisen katastrofiksi
- *Palautuminen*: Oikean palautumisstrategian tunnistaminen ja käyttöönotto varmistaa nopean palautumisen ja vähentää katkosaikaa, palautusprioriteettien avulla kriittisimmät palvelut saadaan palautettua toimintaan ennen vähemmän tärkeitä palveluja
- *Parantaminen*: Kaikkien tapahtumien dokumentoinnin, analysoinnin ja katselmoinnin avulla organisaatio voi varautua paremmin tuleviin tapahtumiin sekä hallita ja välttää häiriöitä

ISO/IEC 27031 -standardissa (2011, s. 6) määritellään ICT-valmiuden pääelementit 7 luokkaan:

- *Henkilöstö*: Asiantuntijat ja varahenkilöt, joilla on tarvittava osaaminen
- *Toimintaympäristö*: Fyysinen ympäristö, jossa ICT-resurssit sijaitsevat
- *Teknologia*: Laitteet (kuten palvelimet, tallennusjärjestelmät, nauhavarmistukset), verkko (kuten datayhteydet, kytkimet, reitittimet) ja ohjelmistot (kuten käyttöjärjestelmät ja sovellukset sekä ohjelmistojen väliset rajapinnat)
- *Data*: Sovellus- ja muun tyyppinen data
- *Prosessit*: Toiminnan varmistaminen, palauttaminen ja ylläpito sekä ICT-resurssit kuvaava dokumentaatio
- *Toimittajat*: Esimerkiksi tele- ja internet-operaattorit

ISO/IEC 27031 -standardin (2011, s. 7) mukaisella ICT-valmiudella organisaatiossa voidaan:

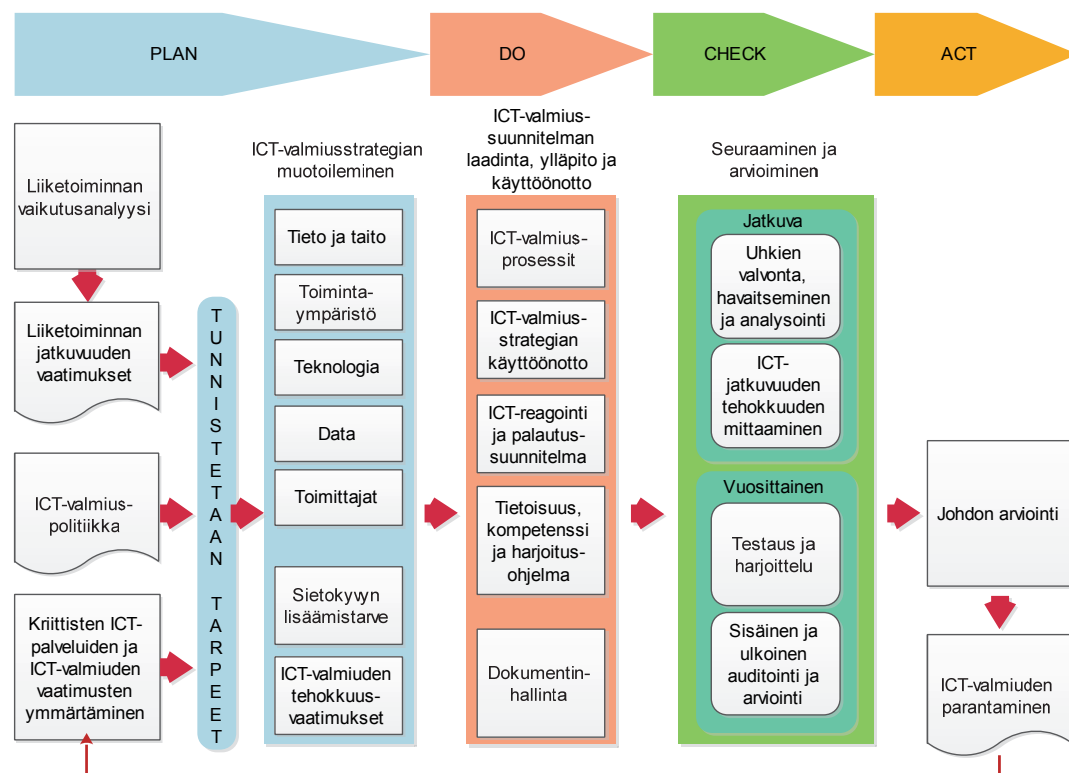
- Selvittää ICT-palveluiden jatkuvuuden riskit sekä heikkoudet
- Tunnistaa ICT-palveluiden häiriöiden potentiaaliset vaikutukset
- Edistää sisäisen ja ulkoisen liiketoimintajohdon ja ICT-palveluntarjoajien yhteistyötä
- Kehittää ICT-henkilöstön kompetenssia harjoittelemalla oikeita toimintatapoja ICT-jatkuvuussuunnitelmien mukaisesti ja testaamalla ICT-valmiutta
- Luoda varmuus, että ICT-palveluiden ennalta määrättyyn toimintatasoon, tuen saamiseen ja riittävään viestintään häiriötilanteissa voidaan luottaa
- Varmistaa, että tietoturvallisuus (luottamuksellisuus, eheys ja saatavuus) säilytetään tietoturvallisuuspolitiikan mukaisesti
- Lisätä luottamusta liiketoiminnan jatkuvuusstrategiaan, yhdistämällä IT-ratkaisuihin kuluvat resurssit saavutettaviin liiketoiminnallisiin hyötyihin
- Hyödyntää kustannustehokkaita, sopivasti mitoitettuja ICT-palveluita, joiden tärkeys on määritelty palveluittain
- Kasvattaa mainetta huolellisena ja tehokkaana organisaationa

- Saavuttaa mahdollista kilpailuetua osoittamalla kykyä toimittaa tuotteita ja palveluita sovitusti myös häiriöiden aikana
- Ymmärtää ja dokumentoida sidosryhmien odotukset ICT-palveluita kohtaan

4.2 ICT-valmiuden suunnittelu

ICT-valmius saadaan toteutettua tehokkaammin ja kustannustehokkaammin, kun se suunnitellaan ja rakennetaan ICT-palveluihin jo alkuvaiheessa osana ICT-valmiusstrategiaa, joka tukee organisaation liiketoiminnan jatkuvuuden tavoitteita. Tällä tavoin ICT-palvelut ovat paremmin rakennettuja ja ymmärrettyjä sekä sietokykyisempiä. Jälkikäteen tehtynä muutokset ovat monimutkaisempia ja kalliimpia ja niistä voi aiheutua häiriöitä. (ISO/IEC 27031 2011, s. 7).

Organisaation tulee kehittää, ottaa käyttöön ja ylläpitää sekä jatkuvasti parantaa ICT-valmiutta tukevia dokumentoituja prosesseja. Näillä prosesseilla varmistetaan, että ICT-valmiuden tavoitteet ovat selkeästi määriteltyjä, ymmärrettyjä ja viestittyjä sekä johdon sitoutuminen ICT-valmiuteen on havainnollistettua. (ISO/IEC 27031 2011, s. 7). ICT-valmiuden vaiheittaiset tehtävät on esitetty kuvassa 15.



Kuva 15. ICT-valmiuden vaiheittaiset tehtävät (mukaillen ISO/IEC 27031 2011, s. 8).

ICT-valmiuden prosessi on PDCA-syklin mukainen ja se tulisi integroida organisaation johtamistoimiin siten, että sitä johdetaan organisaation ylimmän johdon toimesta ja

edistetään esimiesten toimesta. ICT-valmiuteen erikoistunutta henkilöstöä voidaan tarvita tukemaan ja hallitsemaan ICT-valmiusohjelmaa monilta osastoilta. Tarvittavien resurssien määrä on riippuvainen organisaation koosta ja monimutkaisuudesta. (ISO/IEC 27031 2011, s. 8).

Organisaatiolla tulee olla dokumentoitu ICT-valmiuspolitiikka, joka voi olla aluksi pääpiirteinen. Sitä voidaan hienosäätää ja parantaa ICT-valmiuden prosessin kypsyessä ja sitä tulee seurata ja päivittää säännöllisesti organisaation tarpeiden ja liiketoiminnan jatkuvuudenhallinnan tavoitteiden mukaisesti. ICT-valmiuspolitiikan tulee muodostaa organisaatiolle dokumentoidut periaatteet, joita se tavoittelee ja jonka perusteella ICT-valmiuden tehokkuutta voidaan mitata. (ISO/IEC 27031 2011, s. 8-9). ICT-valmiuspolitiikan tulee ISO/IEC 27031 -standardin (2011, s. 9) mukaan:

- Osoittaa ja demonstroida ylimmän johdon sitoutumista ICT-valmiusohjelmaan
- Sisältää tai viitataan organisaation ICT-valmiuden tavoitteisiin
- Määrittää ICT-valmiuden laajuus sekä rajoitukset
- Olla ylimmän johdon hyväksymä ja allekirjoittama
- Olla viestitty oleellisille sisäisille ja ulkoisille sidosryhmille
- Tunnistaa ja tuottaa oleellisille tahoille ICT-valmiuden vaatimat resurssit, kuten budjetti ja tarvittava henkilöstö ICT-valmiuspolitiikan toteuttamiseksi
- Katselmoida suunnitellusti ja tarvittaessa suurten muutosten tapahtuessa

ICT-valmiuden suunnitteluvaiheen tarkoituksena on asettaa organisaation ICT-valmiuden tavoitteet. Tämä sisältää ICT-valmiusstrategian ja -suunnitelman, jotka käsittävät liiketoiminnan tukemisen, lain ja säännösten vaatimukset sekä organisaation liiketoiminnan jatkuvuuden päämäärät ja tavoitteet. Lisäksi suunnitteluvaiheessa asetetaan suorituskykykriteerit, joita organisaatio tarkkailee päämäärien ja tavoitteiden saavuttamiseksi. (ISO/IEC 27031 2011, s. 9).

Organisaation tulee määrittellä ICT-valmiusohjelman tarve osana liiketoiminnan jatkuvuudenhallinnan tavoitteita sekä määrittellä ja tarjota tarvittavat resurssit ICT-valmiusohjelman luomiseen, käyttöönottoon ja ylläpitoon. ICT-valmiuden roolit, vastuut, kompetenssit ja määräysvalta tulee myös määrittellä ja dokumentoida. Ylimmän johdon tulee nimittää riittävän kokenut ja määräysvaltainen henkilö vastuulliseksi ICT-valmiudesta ja sen käyttöönotosta. Lisäksi tulee nimittää yksi tai useampi osaava henkilö, jotka käyttöönottavat ja ylläpitävät ICT-valmiudenhallintajärjestelmää standardin mukaisesti. Organisaation tulee varmistaa, että ICT-valmiudesta vastuulliset henkilöt ovat riittävän osaavia tehtäviinsä. (ISO/IEC 27031 2011, s. 9).

Osana liiketoiminnan jatkuvuudenhallintaa organisaatio kategorisoi toimintonsa prioriteetin perusteella liiketoiminnan keskeytysvaikutusanalyysin mukaisesti. Nämä määritelmät muodostavat toipumisaikatavoitteet, toipumispisteet sekä minimipalvelutasot tuotteittain, palveluittain ja toimittain. Kaikilla kriittisiksi

priorisoiduilla asioilla tulee olla oma dokumentoitu toipumisaikatavoite, toipumispiste ja minimipalvelutaso. Organisaation tulee tunnistaa ja dokumentoida kriittiset ICT-palvelut sekä nimetä ja kuvata ne siten, että nimet ja kuvaukset ovat ymmärrettäviä, jotta varmistetaan yhteisymmärrys liiketoiminnan ja ICT-henkilöstön välillä. (ISO/IEC 27031 2011, s. 10).

Jokainen kriittinen ICT-palvelu tulee linkittää organisaation tuotteeseen ja palveluun, jota se tukee. Lisäksi jokaisen tunnistetun ja sovitun kriittisen ICT-palvelun kaikki ICT-komponentit tulee kuvata ja dokumentoida, jotta niiden kokoonpano ja yhdistyminen palvelun muodostumiseen selviää. Sekä normaali ICT-palveluntuotantoympäristö että ICT-jatkuvuuden tuotantoympäristö on kuvattava kokoonpanotasolla. Jokaisen kriittisen ICT-palvelun nykyinen jatkuvuustaso tulee tarkastella ehkäisyerspektiivistä palvelun keskeyttävien ja palvelua alentavien riskien arvioimiseksi. Pyrkimyksenä tulee olla ICT-palveluiden sietokyvyn kasvattaminen ja siten häiriöiden todennäköisyyden ja vaikutuksen vähentäminen, lisäksi voidaan havaita mahdollisuuksia häiriöiden varhaiselle havaitsemiselle ja reagoinnille. Organisaatio voi päättää sijoittaa resursseja mahdollisuuksiin palvelun sietokyvyn kasvattamiseksi. (ISO/IEC 27031 2011, s. 10).

Käytössä olevia ICT-jatkuvuuden järjestelyjä, kuten estäminen, valvonta, havaitseminen, reagoiminen ja palautuminen tulee verrata liiketoiminnan jatkuvuuden vaatimukseen jokaisen kriittisen ICT-palvelun osalta ja havaitut eroavaisuudet tulee dokumentoida. Ylintä johtoa tulee informoida havaituista eroavaisuuksista kriittisen ICT-valmiuden tason ja liiketoiminnan jatkuvuuden vaatimusten välillä. Tällaiset eroavaisuudet voivat osoittaa riskejä ja tarvetta paremmalle sietokyvyille ja lisäresursseille, kuten henkilöstölle ja osaamiselle, ICT-tilojen varustelulle, teknologioille, ohjelmistoille ja tietokannoille, rahoitukselle tai lisäbudjetoinnille sekä ulkoisille palveluille tai toimittajille. Ylimmän johdon tulee hyväksyä ICT-palvelukuvaukset ja kriittisten ICT-palveluiden listaus, jossa ICT-valmiuden tason ja liiketoiminnan jatkuvuuden vaatimusten eroavaisuuksista aiheutuvat riskit on dokumentoitu. Vaihtoehdot eroavaisuuksien ja riskien käsittelyyn tulee tutkia määrittelemällä ICT-valmiusstrategiaa. (ISO/IEC 27031 2011, s. 10-11).

ICT-valmiusstrategian tulee määrittää lähestymistavat vaadittavan sietokyvyn toteuttamiseksi, jotta häiriöiden estämisen, havaitsemisen, reagoimisen, palauttamisen ja palautumisen periaatteet otetaan käyttöön. ICT-valmiusstrategiavaihtoehdot tulee arvioida laajasti ja valittujen strategioiden tulee kyetä tukemaan organisaation liiketoiminnan jatkuvuuden vaatimuksia. Organisaation tulee huomioida resurssivaatimukset strategian kehittämisessä. Ulkoisia toimijoita voidaan käyttää apuna tarvittaessa strategian luomisessa. Strategian tulee olla joustava ja siinä tulee ottaa huomioon sisäiset rajoitukset ja tekijät, kuten budjetti, saatavilla olevat resurssit, potentiaaliset hyödyt ja haitat, teknologiset rajoitteet, organisaation riskinottohalu, olemassa oleva ICT-valmiussuunnitelma sekä säädöksistä aiheutuvat velvoitteet. (ISO/IEC 27031 2011, s. 11).

Organisaation tulee huomioida eri vaihtoehdot kriittisten ICT-palveluiden häiriövalmiudessa, kuten suojauksen ja sietokyvyn kasvattaminen, palautumisjärjestelyt sekä sisäiset järjestelyt ja kolmannen osapuolen tarjoamat palvelut. Kriittisten ICT-palveluiden vaatimien komponenttien jatkuvuus ja palauttaminen on myös otettava huomioon. Tarvittavien avaintietojen ja -taitojen ylläpitäminen tulee ottaa huomioon strategiaa suunniteltaessa. Tähän voidaan käyttää ulkopuolisia tahoja, joilla on käytettävissään erikoistunutta ICT-osaamista. Tarvittavia tietoja ja taitoja voidaan suojata ja hankkia dokumentoimalla kriittisten ICT-palveluiden rakenteet, kouluttamalla ICT-henkilöstöä osaamisen lisäämiseksi, eriyttämällä tärkeää osaamista useille henkilöille riskien kasaantumisen vähentämiseksi sekä tiedonhallinnalla ja tietojohdamisella. (ISO/IEC 27031 2011, s. 11-12).

ISO/IEC 27031 -standardin (2011, s. 12) mukaan toimintaympäristöön liittyvien tunnistettujen riskien vaikutuksia voidaan pyrkiä vähentämään:

- Luomalla vaihtoehtoisia tiloja organisaatiossa ja hajauttamalla toimintaa, joko organisaation sisällä tai ulkoisille tahoille
- Etätyöjärjestelyjen avulla
- Korvaavilla tiloilla, joita voidaan käyttää häiriötilanteessa

Organisaation toimintaympäristöön liittyvät strategiat voivat vaihdella merkittävästi ja useita toimintavaihtoehtoja voi olla saatavilla. Häiriön laatu ja organisaation koko, toiminnan laajuus, sijainti, käytössä oleva teknologia ja budjetti vaikuttavat toimintavaihtoehtoihin. Käytettäessä muita tiloja on otettava huomioon tilojen turvallisuus, henkilöstön kulkuoikeudet, etäisyys olemassa oleviin tiloihin sekä tilojen saatavuus. (ISO/IEC 27031 2011, s. 12).

ICT-palvelut, joista kriittiset liiketoiminnot ovat riippuvaisia, tulisivat olla saatavilla ennen kriittisiä liiketoimintoja. Tästä syystä palveluiden saaminen toimintaan on varmistettava tietyllä aikavälillä määritetyn toipumisajan mukaisesti. Teknologian ja ohjelmistojen toipumisajat tulee määritellä organisaation kokonaisvaatimusten mukaisesti. Kriittisiä ICT-palveluita tukevat teknologiat vaativat usein monimutkaisia järjestelyjä toimiakseen jatkuvuuden edellyttämällä tavalla. (ISO/IEC 27031 2011, s. 12). ISO/IEC 27031 -standardin (2011, s. 12-13) mukaan tästä syystä on huomioitava ICT-valmiusstrategioita suunniteltaessa:

- Liiketoiminnan jatkuvuudenhallintaohjelmassa tunnistettujen kriittisiä toimintoja tukevien ICT-palveluiden toipumisaika ja toipumispiste
- Teknologian sijainti ja etäisyys toisistaan
- Teknologian sijaintien lukumäärä
- Etäyhteydet järjestelmiin
- Jäähdytys- ja sähkövaatimukset
- Miehitettävien sijaintien käyttö

- Tietoliikenneyhteydet ja vaihtoehtoiset reitit
- Turvajärjestelyjen automaattisuus ja automaation tason tarve
- Teknologian vanhentuneisuus
- Ulkoistettujen palveluntarjoajien yhteydet ja muut ulkoiset yhteydet

Kriittiset liiketoiminnot voivat riippuvaisia (lähes) ajantasaisesta datasta. Datan jatkuvuusratkaisut tulee suunnitella vastaamaan organisaation kriittisten liiketoimintojen palautuspisteitä siltä osin, kun ne liittyvät kriittisiin liiketoimintoihin. Valittujen ICT-valmiustoimien tulee varmistaa kriittisiä liiketoimintoja tukevan datan jatkuva luottamuksellisuus, eheys ja saatavuus. Datan varastoinnin ja ICT-valmiusstrategioiden tulee vastata organisaation liiketoiminnan jatkuvuusvaatimuksia. Tällöin on huomioitava palautuspisteiden vaatimukset, kuinka data säilytetään turvallisesti ja on varmuuskopioitavissa ja palautettavissa sekä missä tietoa säilytetään huomioiden tiedon määrä ja palautukseen kuluvan ajan vaatimukset. On tärkeää ymmärtää datan käyttö organisaatiossa kokonaisvaltaisesti ja tietoa datan käytöstä voidaan kerätä kolmansien osapuolien osaamista hyödyntäen. On tärkeää huomioida myös datan luonteen, muodon ja arvon vaihtelevuus organisaatiosta riippuen. (ISO/IEC 27031 2011, s. 13).

Valittaessa ICT-valmiusstrategiaa organisaation on tiedostettava strategian toteuttamiskelpoisuuteen vaikuttavat prosessit, mukaan lukien häiriöiden estämisen, havaitsemisen, reagoimisen ja palautumisen prosessit. Organisaation on myös tunnistettava kaikki tarvittavat tekijät, jotka ovat edellytyksenä yksittäisten prosessien käyttöönottoon, kuten osaamistekijät, kriittinen data, oleelliset teknologiat ja välttämättömät laitteet ja toimitilat. (ISO/IEC 27031 2011, s. 13).

Organisaation tulee tunnistaa ja dokumentoida ulkoiset riippuvuudet, jotka koskevat ICT-palveluiden järjestämistä ja ryhtyä riittäviin toimiin, jotta toimittajat voivat toimittaa kriittiset laitteet ja palvelut sovitussa aikatauluissa. Organisaation tulee sisällyttää yhteistyökumppaniensa kanssa tehtyihin sopimuksiin ICT:n ja liiketoiminnan jatkuvuudenhallinnan vaatimukset. Sopimuksissa tulee huomioida osapuolten velvollisuudet, sovitut palvelutasot ja -ajat, kustannustenjako sekä toimintatavat vakavissa häiriötilanteissa. (ISO/IEC 27031 2011, s. 14). ISO/IEC 27031 -standardin (2011, s. 14) mukaan strategiassa tulee huomioida:

- Ylimääräisten laitteiden ja ohjelmistokopioiden varastoiminen toisessa sijainnissa
- Korvaavien laitteiden nopeiden toimitusten sopiminen toimittajien kanssa
- Lyhyen vasteajan korjauspalvelut tai laitteiden korvaaminen häiriötilanteessa
- Sähkölähteiden ja tietoliikenneyhteyksien kahdentaminen
- Varavoimageneraattorit
- Ylimääräisten tai vaihtoehtoisten toimittajien tunnistaminen

ICT-valmiusstrategiassa valitut toimintatavat tulee esitellä organisaation ylimmälle johdolle päätösehdotuksineen perustuen riskinottohaluun ja kustannuksiin. Ylintä johtoa

tulee tiedottaa myös, jos valitut strategiavaihtoehdot eivät vastaa liiketoiminnan jatkuvuuden vaatimuksia, jolloin voidaan tiedottaa myös nykyisestä toimintatasosta. Ylimmän johdon tulee valita ICT-valmiusstrategiat esitellyistä vaihtoehdoista ja hyväksyä tai hylätä dokumentoidut vaihtoehdot, jotta kaikki vaihtoehdot on käyty lävitse ja niiden sopivuus liiketoiminnan jatkuvuuden vaatimuksiin varmistetaan. Valittujen ICT-valmiusstrategiavaihtoehtojen tulisi ottaa huomioon todennäköiset riskit ja häiriöiden vaikutukset, yhtyä organisaation valitsemiin liiketoiminnan jatkuvuusstrategioihin sekä olla soveltuvia organisaation yleisiin tavoitteisiin huomioiden riskinottohalu. (ISO/IEC 27031 2011, s. 14).

Organisaation tulee sisällyttää korkean tason ICT-valmiusstrategiaansa ja suunnitelmiinsa viittaukset ICT-valmiuskykyä parannuksiin. Tällaiset parannukset saavutetaan estävillä ja korjaavilla toimilla sekä prosesseilla ja menetelmillä, jotka ovat tarkoituksenmukaisia organisaation liiketoiminnan keskeytysvaikutusanalyysi ja riskinottohalu huomioiden. Organisaation tulee kyetä valvomaan uhkia ja arvioimaan ICT-valmiusjärjestelmän kykyä vastata ongelmiin. ICT-valmiuden tehokkuudelle on määritettävä kriteerit, joita voidaan käyttää toiminnan laadun määrittämiseen. Kriteerit tulee määrittellä ICT-valmiuden vaatimusten ja yleisten liiketoiminnan jatkuvuudenhallinnan tavoitteiden mukaisesti. (ISO/IEC 27031 2011, s. 14-15).

4.3 ICT-valmiuden käyttöönotto

ICT-valmiusstrategiat tulee ottaa käyttöön kun organisaation ylin johto on antanut hyväksyntänsä. Tämä aloittaa käyttöönottovaiheen, jossa huomioidaan suositukset organisaation valitsemaan ICT-valmiusstrategiaan sekä organisaation rakenne, suunnitelmat ja menettelyt, joilla tuetaan käyttöönottoa. Organisaation tulee hallita resurssinsa, menetelmänsä ja ICT-valmiuden toiminta sekä käynnistää koulutusohjelmat ja lisätä tietoisuutta. Käyttöönotto tulee toteuttaa projektina organisaation normaalin muutoksenhallintaprosessin ja liiketoiminnan jatkuvuudenhallinnan mukaisesti hallinnan ja raportoinnin toimivuuden varmistamiseksi. (ISO/IEC 27031 2011, s. 15).

Yleinen tietoisuus ICT-palveluiden jatkuvuselementeistä on kriittistä hallintotavan ja johtamisjärjestelmän tuen saamiseksi. (ISO/IEC 27031 2011, s. 15). ISO/IEC 27031 -standardin (2011, s. 15) mukaan organisaation tulee:

- Lisätä, tehostaa ja ylläpitää tietoisuutta oleellisessa henkilöstössä jatkuvalla koulutus- ja viestintäohjelmalla ja aloittaa prosessi tietoisuuden lisäämisen tehokkuuden selvittämiseksi
- Varmistaa, että henkilöstö on tietoinen työpanoksensa merkityksestä ICT-valmiuden tavoitteiden saavuttamisessa

ISO/IEC 27031 -standardin (2011, s. 16) mukaan organisaation tulee varmistaa, että ICT-valmiuden hallintaan allokoitu vastuuhenkilöstö on riittävän kyvykästä suoriutumaan vaadittavista tehtävistä:

- Määrittämällä henkilöstöä koskevat osaamisvaatimukset
- Suorittamalla koulutustarpeiden selvitys ja tarjoamalla tarvittavaa koulutusta
- Varmistamalla, että vaadittu osaaminen on saavutettu
- Ylläpitämällä tietoja koulutuksesta, osaamisesta, taidoista, kokemuksesta ja pätevyyksistä

ICT-palautusjärjestelmät ja kriittinen data tulee mahdollisuuksien mukaan erottaa fyysisesti tuotantoympäristöstä, jotta mahdolliset häiriöt eivät vaikuta molempiin samanaikaisesti. Tuotantoympäristö voidaan erottaa loogisesti harjoittelu- ja asennusympäristöstä, jotta näitä voidaan käyttää tuotantoympäristö palauttamiseen häiriötilanteessa. Eri käyttöönottopojen skaalautuvuus, hallittavuus, tuettavuus, tehokkuus ja kustannusominaisuudet tulee selvittää sopivimman käyttöönototavan tunnistamiseksi. (ISO/IEC 27031 2011, s. 16).

ISO/IEC 27031 -standardin (2011, s. 16) mukaan ICT-teknologiastrategiat tulee myös ottaa käyttöön ja ne voivat sisältää järjestelyjä:

- ”*Hot standby*” -menetelmä, jossa ICT-infrastruktuuri replikoidaan kahden sijainnin välillä
- ”*Warm standby*” -menetelmä, jossa palautus toteutetaan vaihtoehtoisesta sijainnista, jossa ICT-infrastruktuuria valmistellaan
- ”*Cold standby*” -menetelmä, jossa infrastruktuuri rakennetaan tai konfiguroidaan alusta asti vaihtoehtoisessa sijainnissa
- Toimitusjärjestelyt, joissa ulkoinen palveluntarjoaja toimittaa laitteistoa
- Yhdistelmä yllä mainittuja strategioita

Järjestelyt datan saatavuuden varmistamiseksi tulee yhdenmukaistaa ICT-valmiusstrategioiden mukaisiksi. Datan saatavuutta voidaan lisätä ylimääräisillä sijainneilla datan säilyttämiselle, joko fyysisessä tai virtuaalisessa muodossa siten, että tietoturvallisuus säilytetään. Jos dataa säilytetään ulkopuolisilla tahoilla, datan omistajien tulee hyväksyä käytettävät hallintamekanismit. (ISO/IEC 27031 2011, s. 16).

ICT-valmiusprosessit tulee dokumentoida selkeästi ja riittävällä tarkkuudella, jotta henkilöstö voi suorittaa niitä. Organisaation menettelytavat voivat muuttua tilanteen mukaisesti ja niihin voidaan joutua sopeutumaan organisaation toiminnan prioriteettien ja sidosryhmien vaatimusten mukaisesti. (ISO/IEC 27031 2011, s. 17).

Organisaation on varmistettava, että kriittiset toimittajat pystyvät tukemaan organisaation tarpeita. Toimittajien omat dokumentoidut ja testatut liiketoiminnan jatkuvuus- ja ICT-

valmiussuunnitelmat on oltava riittäviä, jotta organisaatio saa tarvitsemansa tuen. Organisaation tulee arvioida toimittajien kyky ja kapasiteetti ennen palveluiden hankintaa sekä seurata jatkuvasti toimittajien toimintaa palveluiden hankinnan jälkeen. (ISO/IEC 27031 2011, s. 17).

Kaikille ICT-häiriöille tulee olla reaktio, joka määrittää häiriön laadun ja laajuuden, ottaa tilanteen hallintaan, käsittelee häiriön ja kommunikoi sidosryhmien kanssa. Häiriötä seuraavan reaktion tulee aktivoida soveltuva ICT-valmiustoimi. Tämän reaktion tulee olla yleisen liiketoiminnan jatkuvuudenhallinnan mukainen ja se voi käsittää häiriönhallintayksikön tai yksittäisen henkilön määrittämisen häiriöstä vastuulliseksi tahoksi. Organisaatiosta riippuen voidaan käyttää myös tasoittaista käsittelyä jaoteltuna esimerkiksi teknisiin ja palvelullisiin häiriöihin. Häiriöstä vastuullisilla tahoilla tulee olla suunnitelmat reaktion aktivoimiseen, toimenpiteisiin, koordinointiin ja viestintään. (ISO/IEC 27031 2011, s. 17).

Organisaatiolla tulee olla suunnitelmat potentiaalisten häiriöiden varalta, jotta ICT-palveluiden jatkuvuus- ja palautustoimet ovat toteutettavissa. Organisaation ICT-häiriönhallinta-, liiketoiminnan jatkuvuus- ja tekniset palautussuunnitelmat voidaan aktivoida peräkkäin tai samanaikaisesti. Pienellä organisaatiolla voi olla yksittäinen dokumentti, joka kattaa kaikki ICT-palveluiden palauttamiseen liittyvät aktiviteetit. Suuressa organisaatiossa dokumentit voivat olla yksittäisten ICT-palveluiden elementtien tasoisia. Reagointi- ja palautussuunnitelmien tulee olla suppeita ja niiden tulee olla kaikkien suunnitelmissa vastuutettujen tahojen saatavilla. (ISO/IEC 27031 2011, s. 17-18). ISO/IEC 27031 -standardin (2011, s. 18-19) mukaan suunnitelmien tulisi sisältää:

- Tarkoitus ja laajuus ylimmän johdon hyväksymänä ja suunnitelman toteuttavien ymmärtämänä sekä suunnitelman yhteys muihin suunnitelmiin tai dokumentteihin sekä mistä nämä ovat saatavilla ja miten
- Kaikkien häiriönhallinta-, reagointi- ja palautussuunnitelmien osalta priorisoidut tavoitteet: palautettavat kriittiset ICT-palvelut, palauttamisen aikamääreet, jokaisen kriittisen ICT-palvelun palautusvaiheet sekä missä tilanteessa mitään suunnitelmaa käytetään, tarvittaessa myös tarkistuslista
- Henkilöiden ja tiimien päätöksentekoa koskevat ja taloudelliset roolit ja vastuut
- Suunnitelman käyttöönotto, kuinka henkilö tai tiimi alkaa toimia, tapaamispaikat ja suuremmissa organisaatioissa komentokeskukset
- Olosuhteet, joissa reagointia ei tarvita, kuten palvelupisteessä hoidettavat pienemmät, vaikkakin kriittisissä palveluissa tapahtuvat häiriöt
- Dokumentaation omistaja ja ylläpitäjä sekä versionhallinta
- Yhteystiedot, myös sidosryhmien osalta

ISO/IEC 27031 -standardin (2011, s. 19-20) mukaan reagointi- ja palauttamissuunnitelmien tulee olla joustavia, käyttökelpoisia ja relevantteja sekä helppolukuisia ja helposti löydettäviä. Niiden tulee sisältää perusteet vakavien ongelmien

hallinnalle, joissa organisaatio tarvitsee ICT-valmiuden reaktiota. Dokumentaation tulee määrittellä kriittiset palvelut toipumisaikatavoitteineen ja palautuspisteineen, palauttamisen aikamääreet ja palauttamishenkilöstö vastuineen. Suunnitelmat on dokumentoitava siten, että henkilöstö voi hyödyntää niitä häiriötilanteissa. Suunnitelmien tulee sisältää:

- *Tavoitteet*: lyhyt kuvaus suunnitelmien tavoitteista
- *Laaajuus*: olennaisten palveluiden kuvaus ja kriittisyys, palveluita tukevat teknologiat sijainteineen, yleiskuva teknologioita hallitsevista tahoista sekä yleiskuva teknologian dokumentaatiosta sijainteineen
- *Saatavuusvaatimukset*: liiketoiminnan määrittämät vaatimukset palveluiden ja oleellisten teknologioiden saatavuudesta
- *Tietoturvallisuusvaatimukset*: palveluiden, järjestelmien ja datan vaatimukset luottamuksellisuuden, eheyden ja saatavuuden osalta
- *Palautustoimet*: lista toimenpiteistä verkon toiminnan, järjestelmien, sovellusten, tietokantojen jne. palauttamiseen normaalitasolle vaihtoehtoisessa ympäristössä, prosessi ICT-palveluiden palauttamiseksi, varmistustoimenpiteet, kanavat lisätietojen saamiseksi
- *Liitteet*: inventaario tietojärjestelmistä, ohjelmistoista ja tietokannoista, yleiskuva verkkoinfrastruktuurista ja palvelimista, inventaario laitteista ja sovelluksista sekä sopimukset ja sovitut palvelutasot
- *Tärkeimmät toimittajat*: normaalit toimittajat ja palautumispalveluiden toimittajat

ISO/IEC 27031 -standardin (2011, s. 21) mukaan ICT-valmiusasiakirjoja tulee hallita, jotta ne säilyvät selkeinä, helposti tunnistettavina ja saatavina sekä niiden säilytys, suojaus ja korjaaminen mahdollistetaan. ICT-valmiusdokumentaatiota hallitaan, jotta

- Dokumentit hyväksytään ja niiden sopivuus varmistetaan ennen julkaisua
- Dokumentit katselmoidaan ja päivitetään tarvittaessa uudelleen hyväksyen
- Muutokset ja nykyisen version tila tunnistetaan
- Soveltuvien dokumenttien asianmukaiset versiot ovat saatavilla
- Ulkoiset dokumentit tunnistetaan ja niiden jakelua hallitaan
- Vanhentuneiden dokumenttien käyttö estetään

4.4 ICT-valmiuden ylläpito

Muutos tuo mukanaan riskejä, epäonnistumisen riskin sekä olemassa olevien menettelytapojen ja strategioiden epävakauttamisen mahdollisuuden. Tästä syystä ICT-valmiusstrategioiden tulee olla sietokykyisiä ja mukautuvia. ICT-palveluun tehtävä muutos voi vaikuttaa ICT-valmiuden toimintaan ja siksi muutos tulee tehdä vasta kun sen vaikutukset liiketoiminnan jatkuvuuteen on arvioitu. (ISO/IEC 27031 2011, s. 21).

ISO/IEC 27031 -standardin (2011, s. 21) mukaan ICT-valmiusstrategioiden soveltuvuus organisaatioon taataan siten, että:

- Ylin johto varmistaa, että ICT-valmiusstrategiat tukevat edelleen organisaation liiketoiminnan jatkuvuudenhallinnan tavoitteita
- Muutoksenhallintaprosessi ottaa huomioon kaikki ICT-valmiusstrategioiden vastuulliset osapuolet suunnittelussa ja käyttöönotossa
- Uusien ICT-palveluiden käyttöönottoprosessi sisältää lopetusmahdollisuuden, jotta sietokykyä ei vaaranneta yksinkertaisillakaan päivityksillä tai parannuksilla
- Hankinnassa ja fuusioissa noudatetaan huolellisuutta ja arvioidaan sietokyvyn muutoksia
- ICT-komponentin käytöstä poistaminen huomioidaan asiaan kuuluvassa ICT-valmiudenhallintajärjestelmässä

ISO/IEC 27031 -standardin (2011, s. 22) mukaan organisaation tulee muodostaa prosessi ICT-uhkien muodostumisen jatkuvaan havaitsemiseen ja sen tulee huomioida:

- Henkilöstön, taitojen ja tietojen hankinta
- ICT-laitteistoa sisältävien toimitilojen hallinta
- Teknologian, laitteiden ja verkkojen muutokset
- Tietokannoissa ja sovelluksissa tapahtuvat muutokset
- Rahoitus ja budjetti
- Ulkoisten palveluiden ja toimittajien tehokkuus

Organisaation tulee harjoittaa ICT-palveluiden palauttamisen lisäksi myös suojaustaan ja sietokykyään, jotta voidaan selvittää palveluiden suojaus-, ylläpito- ja palautusmahdollisuudet riippumatta häiriöiden vakavuudesta, ICT-valmiudenhallinnan järjestelyt häiriöiden vaikutusten minimoimiseksi sekä normaaliin toimintaan palaamisen toimenpiteiden pätevyyden varmistaminen. Harjoituksia tulee tehdä eri tasoilla tutustuttamisesta sietokykyyn siten, että kaikki palvelun toimittamiseen vaadittavat osuudet harjoitellaan. Harjoituksiin voi liittyä riskejä, joiden ei tule aiheuttaa sellaisen tason riskejä, joita ei voida ottaa. Testaus- ja harjoitusohjelmassa määritellään harjoitusten tiheys, laajuus ja muoto. Harjoitusten laajuus voi vaihdella yksittäisen tiedoston palauttamisesta tietoliikenteen katkeamiseen. Harjoitusten tulee kohdistua koko ICT-ympäristöön palvelintiloista yksittäisiin tietokoneisiin. (ISO/IEC 27031 2011, s. 22-23).

ISO/IEC 27031 -standardin (2011, s. 23) mukaan harjoituksilla voidaan:

- Synnyttää luottamusta sietokyky- ja palautusstrategian kyvystä vastata liiketoiminnan tavoitteisiin
- Demonstroida, että kriittiset ICT-palvelut ovat ylläpidettävissä ja palautettavissa sovittujen palvelutasojen tai palautuspisteiden mukaisesti häiriöstä riippumatta

- Tutustuttaa henkilöstö palautusprosessiin
- Kouluttaa henkilöstöä ja varmistaa, että heillä on riittävä osaaminen ICT-valmiussuunnitelmien ja menetelmien toteuttamiseksi
- Tarkistaa, että ICT-valmius on samassa tilassa kuin ICT-infrastruktuuri
- Tunnistaa parannuksia ICT-valmiusstrategiassa, arkkitehtuurissa tai palautusprosesseissa
- Tuottaa todisteita auditointitarkoituksiin ja osoittaa kykyä organisaation palvelutasosta

Organisaation tulee harjoitella ICT-palveluiden kaikkia elementtejä kokonsa, monimutkaisuutensa ja liiketoiminnan jatkuvuudenhallinnan laajuutensa mukaisesti. Harjoittelun ei tule keskittyä ainoastaan palveluiden palauttamiseen ja jatkumiseen, vaan siihen tulee sisällyttää myös sietokyky, järjestelmien valvonta ja häiriönhallinta. (ISO/IEC 27031 2011, s. 23). ISO/IEC 27031 -standardin (2011, s. 24) mukaan harjoitettavia elementtejä ovat:

- Laittilojen fyysinen turvallisuus, tulipalo- ja vesivahinkoilmaisimet, evakointiprosessi, lämmitys-, ilmanvaihto- ja tuuletuslaitteet ja hälytysjärjestelmät
- Infrastruktuuri, kattaen tietoliikenneyhteydet ja verkon turvallisuus, virustorjunta sekä tunkeilijoiden estäminen ja havaitseminen
- Laitteistot, kuten palvelimet, verkkolaitteet ja varmuuskopiointijärjestelmät
- Ohjelmistot
- Data
- Palvelut
- Toimittajien roolit ja toiminta

Jotta harjoitukset eivät aiheuta häiriöitä tai heikennä palveluiden laatua, harjoitukset on suunniteltava huolellisesti harjoituksesta aiheutuvien riskien minimoimiseksi. Riskienhallinnan tulee olla riittävällä tasolla harjoitusta suorittaessa ja tähän voidaan pyrkiä varmistamalla, että kaikki data varmuuskopioidaan ennen harjoitusta, suorittamalla harjoitus suljetussa ympäristössä ja aikatauluttamalla harjoitukset hiljaisiin toiminta-aikoihin tai toiminta-aikojen ulkopuolelle samalla tiedottaen loppukäyttäjiä asiasta. (ISO/IEC 27031 2011, s. 24).

ISO/IEC 27031 -standardin (2011, s. 25) mukaan harjoitusten tulee olla realistisia sekä huolellisesti suunniteltuja ja sovittuja sidosryhmien kanssa, jotta liiketoimintaprosessien häiriintymisen riski on minimaalinen. Harjoituksia ei tule myöskään suorittaa häiriöiden aikana. Harjoitusten laajuus ja monimutkaisuus tulee olla organisaation palautustavoitteiden mukaista. Jokaisella harjoituksella tulee olla myös ”toimeksianto”, joka on sovittu ennalta harjoituksen järjestäjän toimesta. Se voi sisältää esimerkiksi kuvauksen, tavoitteet, laajuuden, oletukset, rajoitteet, riskit, onnistumiskriteerit, resurssit,

roolit ja vastuut, aikamääreet, harjoituksenaikaisen tiedon tallentamisen, jälkipuinnin sekä harjoituksen jälkeiset toimet, kuten raportoinnin.

Harjoituksen kulun hallintorakenne sisältää yksilöille määritellyt roolit ja vastuut. Selkeä hallintorakenne kattaa lisäksi harjoituksen johtajan, viestinnän, varmistuksen riittävästä resursseista harjoituksen suorittamiseksi turvallisesti, riittävät tarkkailijat ja huomioijat, harjoituksen virstanpylväät, harjoituksen päättämismenettelyt sekä harjoituksen lopettamisen hätätilanteessa. Harjoitukset tulee suorittaa hallintorakenteen mukaisesti, jotta varmistetaan tavoitteiden ja virstanpylväiden saavuttaminen, harjoitusmateriaalien ja tehtävien luottamuksellisuus, samanaikaisten riskien tarkkaileminen ja lievittäminen, tarkkailijoiden ja valvojien valtuuttaminen, harjoituksen etenemisen kirjaaminen sekä kaikki osapuolet kattava jälkipuinti ja palautteen saaminen. (ISO/IEC 27031 2011, s. 25-26).

Harjoituksen päätyttyä havaitut tulokset tulee katselmoida ja tutkia pikaisesti. Tällöin tulee koota tulokset ja löydökset, analysoida ne suhteessa harjoituksen tavoitteisiin ja päämääriin tunnistaa eroavaisuudet, määrittää toimintakohteet ja aikataulut sekä luoda harjoitusraportti harjoituksen järjestäjälle. (ISO/IEC 27031 2011, s. 26).

Valtiovarainministeriön (2012, s. 35) mukaan häiriötilanteiden hallinnan menettelyjen tulee olla dokumentoituja, koulutettuja ja harjoiteltuja. Selkeällä dokumentaatiolla ja harjoittelulla luodaan edellytykset toiminnalle häiriötilanteissa ja laaditut toimintamallit saadaan tarvittaessa otettua käyttöön nopeasti uuden tyyppisissä tilanteissa. Henkilöstön osaamisvaatimuksissa, koulutuksessa ja resursoinnissa on huomioitava organisaation ydintoimintojen kannalta kriittiset erityisosaamisalueet. Resurssien ja osaamisen saatavuus on varmistettava myös häiriötilanteiden aikana.

ICT-valmiuden sisäinen tarkastussuunnitelma määrittää ja dokumentoi tarkastuksen kriteerit, laajuuden, menetelmän ja suoritusajat. Tarkoituksena on varmistaa, että sisäisen tarkastuksen suorittavat ainoastaan nimetyt, asiaan perehtyneet tarkastajat. Tarkastajien valinnalla varmistetaan tarkastuksen puolueettomuus. Tarkastussuunnitelman tulee käsittää myös ulkoiset osapuolet, jolloin esimerkiksi ulkoiset toimijat tulee arvioida organisaation ICT-valmiusstrategioiden tukemiskykyä perusteella. Sisäinen tarkastus tulee tehdä, kun kriittisiin ICT-palveluihin, liiketoiminnan jatkuvuuden vaatimukseen tai ICT-valmiuden vaatimukseen tulee muutoksia. ICT-valmiuden sisäisen tarkastuksen tulokset tulee kirjata ja raportoida. Organisaation johdon tulee tarkastella laadittu raportti ja sen perusteella tehdyt korjaavat toimenpiteet. (ISO/IEC 27031 2011, s. 26).

Ylimmän johdon tulee varmistaa, että ICT-valmiuden hallintajärjestelmä arvioidaan säännöllisin väliajoin. Arviointitiedot voidaan saada sisäisistä tai ulkoisista tarkastuksista tai itse keräämällä. Arvioinnin tulee sisältää ICT-valmiuden hallinnan, menetelmien ja tavoitteiden parantamismahdollisuudet ja muutostarpeet. Tämän lisäksi ylimmän johdon tulee katselmoida vuosittain hyväksytyt ICT-valmiuden vaatimukset, ICT-palveluiden

kuvaukset, listatut kriittiset ICT-palvelut sekä niiden ja liiketoiminnallisten jatkuvuusvaatimuksien eroavaisuuksista johtuvat riskit. Katselmoinnin tulokset tulee dokumentoida selkeästi ja dokumentointia tulee ylläpitää. (ISO/IEC 27031 2011, s. 26-27). ISO/IEC 27031 -standardin (2011, s. 27) mukaan katselmoinnin tulee sisältää:

- Organisaation sisäiset palvelutasot
- Ulkoisten palveluntarjoajien kyky ylläpitää soveltuvia palvelutasoja
- Merkityksellisten sisäisten tarkastusten tulokset
- Palaute, mukaan lukien puolueettomat valvojat
- Estävien ja korjaavien toimien tilanne
- Jäännösriskien ja hyväksyttävien riskien taso
- Aikaisempien arviointien ja suositusten perusteella tehdyt toimenpiteet
- Harjoituksista ja testeistä opitut asiat ja niiden aikana sattuneet häiriöt
- Syntymässä olevat hyvät käytännöt

ISO/IEC 27031 -standardin (2011, s. 27) mukaan katselmoinnin perusteella ylimmän johdon tulee tarpeen mukaan:

- Muuttaa ICT-valmiudenhallintajärjestelmän laajuutta
- Parantaa ICT-valmiudenhallintajärjestelmän tehokkuutta
- Tarkastella ICT-valmiuden vaatimuksia, ICT-palveluiden kuvauksia ja kriittisten ICT-palveluiden listausta sekä tunnistettuja riskejä, jotka aiheutuvat ICT-valmiuden tason ja liiketoiminnan jatkuvuusvaatimusten eroavaisuuksista
- Muuttaa ICT-valmiusstrategiaa ja menetelmiä (liiketoiminnan ja sietokyvyn tavoitteet sekä hyväksyty riskitaso), jotta ICT-palveluihin vaikuttaviin sisäisiin tai ulkoisiin tilanteisiin voidaan reagoida
- Arvioida resurssitarpeita sekä rahoitus- ja budjettivaatimuksia

Organisaation tulee valvoa ja mitata ICT-valmiuttaan määrittelemiensä ICT-valmiuden tehokkuuskriteerien mukaisesti. Kriteerit voivat olla määrällisiä tai laadullisia. (ISO/IEC 27031 2011, s. 28). ISO/IEC 27031 -standardin (2011, s. 28) mukaan määrällisiä kriteereitä ovat esimerkiksi:

- Tietyn ajan kuluessa havaitsematta jääneiden häiriöiden lukumäärä
- Häiriöiden havaitsemiseen kulunut aika
- Sellaisten häiriöiden lukumäärä, joita ei voida tehokkaasti hallita vaikutusten vähentämiseksi
- Häiriöiden havaitsemisessa käytettävien datalähteiden saatavuus
- Havaittuihin häiriöihin kulunut havaitsemis- ja korjausaika

ISO/IEC 27031 -standardin (2011, s. 28) mukaan laadullisia kriteereitä ovat esimerkiksi:

- Kyselyt
- Palautteet
- Palautekeskustelujen yhteenvedot
- Ryhmätapaamiset

Organisaation tulee jatkuvasti parantaa ICT-valmiuttaan estävien ja korjaavien toimenpiteiden avulla. Nämä toimenpiteet riippuvat organisaation liiketoiminnan keskeytysvaikutusanalyysin tuloksista ja riskinottohalusta. (ISO/IEC 27031 2011, s. 28). ISO/IEC 27031 -standardin (2011, s. 28-29) mukaan organisaation tulee ryhtyä toimenpiteisiin ICT-palveluiden ja ICT-valmiuden virheiden korjaamiseksi. Korjaavien toimenpiteiden menetelmässä:

- Tunnistetaan virheet
- Selvitetään virheiden syyt
- Arvioidaan tarvittavat toimenpiteet, joilla poikkeamia ei esiinny
- Arvioidaan ja otetaan käyttöön tarvittavat korjaavat toimenpiteet
- Dokumentoidaan tehdyt toimenpiteet
- Katselmoidaan tehdyt toimenpiteet

ISO/IEC 27031 -standardin (2011, s. 29) mukaan organisaation tulee tunnistaa ICT-valmiuden elementeissä olevat potentiaaliset heikkoudet ja suorittaa toimenpiteet:

- Potentiaalisten heikkouksien tunnistamiseksi
- Virheiden syiden tunnistamiseksi
- Tarvittavien ehkäisevien toimenpiteiden määrittämiseksi ja käyttöönottamiseksi
- Tehtyjen toimenpiteiden dokumentoimiseksi ja katselmoimiseksi

Valtiovarainministeriön (2012, s. 57) mukaan jokainen häiriötilanne tulee käydä läpi jälkikäteen. Tarkoituksena on pyrkiä selvittämään, miten tilanne syntyi, mitkä sen vaikutukset olivat ja olisiko tilanteen aiheuttanut tekijä voinut aiheuttaa myös jotain muuta. Lisäksi tulee arvioida, kuinka henkilöstö suoriutui tilanteesta ja onko tarpeen muuttaa toimintaohjeistusta tai järjestää koulutusta tulevia vastaavia tilanteita varten.

Järveläinen (2013, s. 584) lisää, että katastrofien jälkeinen palautuminen ei riitä vakavien haittojen välttämiseksi, vaan tarvitaan myös estotoimenpiteitä. ISO/IEC 27031 -standardille, kuten muillekin eri standardeille on myös tyypillistä, että ne ovat liian yleisluontoisia sellaisten organisaatioiden käytettäväksi, joilla on erityisiä tarpeita.

5. ORGANISAATION NYKYTILA

Tipakkeen jatkuvuussuunnitelmien tekeminen on aloitettu toukokuussa 2015. Jatkuvuussuunnitelmien ensimmäiset versiot on laadittu kesäkauden aikana, jolloin Tipakkeen toiminta vähenee merkittävästi johtuen kesälomakaudesta. Tällöin yhteydenottojen ja häiriötilanteiden määrä on huomattavasti alhaisempi kuin muina vuodenaikoina. Luonnollisesti kesälomakausi vähentää myös Tipakkeen resursseja, mutta asiakasrakenteesta johtuen (esimerkiksi Tipaketta runsaasti työllistävät oppilaitokset ovat kiinni) Tipakkeen henkilöstöllä on eniten aikaa toiminnan kehittämiseen kesä- ja heinäkuussa. Tipakkeen jatkuvuussuunnitelmien viimeisimmät versiot on päivitetty marraskuussa 2015 ja ne ovat tällä hetkellä vielä keskeneräisiä.

Tipakkeessa kesän 2015 aikana laadittu jatkuvuussuunnitelma: ”*Tipakkeen jatkuvuussuunnitelma*”, on versioitu 0.7 ja päivätty 6.8.2015. Jatkuvuussuunnitelmaa on päivitetty tämän jälkeen siten, että viimeisin versio on 0.9, joka on päivätty 16.11.2015. Tipakkeen jatkuvuussuunnitelman tavoitteena on ”*varautua tilanteisiin, joissa ydinprosessien ja tietokonekeskuksen normaali toiminta häiriintyy vakavasti tai keskeytyy kokonaan normaaliolosuhteissa joko ulkoisen tai sisäisen riskin toteuduttua*” sekä ”*varmistaa palvelujen toimivuus palvelutasolupausten mukaisesti*” (Tipake jatkuvuussuunnitelma 2015). Dokumentissa on kuvattu toimenpiteet normaalioloissa ja normaaliolojen häiriötilanteissa. Varsinaisen jatkuvuussuunnitelman lisäksi on laadittu kaksi muuta dokumenttia: ”*Jatkuvuudenhallinnan toimenpiteet ja toipumissuunnitelmat*” sekä ”*Tipake riskiarviointi*”.

Jatkuvuussuunnitelmassa mainitaan, että riskien arviointi suoritetaan vähintään kerran vuodessa tai suuren toimintaympäristön tai toiminnan muutoksen yhteydessä. Arvioinnin suorittavat tai teettävät Tipakkeen johtoryhmään kuuluvat henkilöt. Jatkuvuussuunnitelma liitteineen ja viitteineen esitetään päivitettäväksi tarvittaessa. Vaikutuksiltaan suurimmiksi riskeiksi on arvioitu tietokonekeskuksen tilojen fyysiset riskit, kuten sähkökatkos, jäähdytinlaitteen vikaantuminen ja tulipalo. Näiden riskien toteutumisen todennäköisyys on kuitenkin arvioitu pieneksi. (Tipake jatkuvuussuunnitelma 2015). Riskien arvioinnissa mahdollisiksi arvioidut riskit on esitetty taulukossa 6.

Taulukko 6. *Mahdollisiksi arvioidut riskit (Tipake jatkuvuussuunnitelma 2015).*

- Sähkökatkos konesalissa tai seutuverkon solmupisteissä
- Jäähdytinlaitteen vikaantuminen (konesali)
- Tulipalo (konesali)
- Laiteviat
- Ulkopuolisen tunkeutuminen tiloihin

- Operointi- tai toimintavirheet
- Ilkivalta/häiriöt (palvelunesto yms.)
- Huolto-, ylläpito- ja tukisopimukset
- Osaaminen ja riittävä kapasiteetti (varamiehityksineen)
- Tietoturvan ongelmatilanteet
- Ohjelmistojen ongelmatilanteet
- Ohjeistus ja dokumentaatio

Jatkuvuussuunnitelman organisointi- ja vastuuosuudessa määritetään, että ydinprosessien luokittelu on Tipakkeen johtoryhmän vastuulla. Suunnitelman säännöllinen katselmointi, päivittäminen ja säilytys sekä suunnitelman tiedottaminen ja tarvittava kouluttaminen on määritelty Tipakkeen johtajan määräämälle henkilölle. Tietokonekeskuksen, laittilojen sekä ydinprosessien ja -palveluiden tavoitteiden mukainen toiminta on vastuutettu nimetyille prosessinomistajille tai heidän valtuuttamilleen henkilöille. (Tipake Jatkuvuussuunnitelma 2015).

Tipakkeen palvelut on luokiteltu useiden samanaikaisten vakavien häiriötilanteiden varalta toipumisjärjestykseen. Toipumisen vaatiessa samoja resursseja toipumisjärjestelyt suoritetaan ennalta määrättyssä järjestyksessä. (Tipake jatkuvuussuunnitelma 2015).

Jatkuvuussuunnitelman mukaan Tipakkeessa käytetään ITIL:n (engl. Information Technology Infrastructure Library) mukaista häiriönhallintaa, jossa laajat ja yksittäiset häiriöt erotellaan. Laaja häiriö on määritelty useita yksittäisiä erillisiä käyttäjiä tai yhtä tai useampaa kokonaista työyksikköä koskettavaksi työn estäväksi häiriöksi. Laajan häiriön selvittämisen on määritelty käynnistävän useita toiminnallisia vaiheita ja tehtäviä. (Tipake jatkuvuussuunnitelma 2015). Määritellyt vaiheet ja tehtävät laajan häiriön selvittämiseksi on esitetty taulukossa 7.

Taulukko 7. Vaiheet ja tehtävät laajan häiriön selvittämiseksi (Tipake jatkuvuussuunnitelma 2015).

- Tilanteen tunnistaminen
- Vastuuhenkilön nimeäminen
- Laajuuden tarkempi selvittäminen ja käytettävien resurssien analysointi
- Korjaavien toimenpiteiden aloittaminen
- Tiedottaminen niin sisäisesti kuin asiakkaille ja muille sidosryhmille
- Toimintojen palauttamistoimenpiteet ja toipumisprosessin etenemisen valvonta
- Toiminnan palauttaminen normaalille tasolle
- Tilanteen ja tehtyjen toimien analysointi
- Raportin laadinta ja mahdollisten kehitysehdotusten tekeminen

Laajan häiriönhallinnan prosessi on määritelty käynnistettäväksi useiden samaan kohteeseen tai toimintoon liittyvien työn estävien häiriöiden tilanteessa. Tällöin Tipakkeen palvelupisteestä (Service Desk) nimetään häiriönhallinnan koordinaattori. (Tipake jatkuvuussuunnitelma 2015). Koordinaattorin ensisijaiset tehtävät laajan häiriön toteamisvaiheessa on esitetty taulukossa 8.

Taulukko 8. Häiriönhallinnan koordinaattorin ensisijaiset tehtävät laajassa häiriötilanteessa (Tipake jatkuvuussuunnitelma 2015).

- Luoda häiriöstä päätiketti ohjeiden mukaisesti
- Eskaloida häiriönselvitys selvitettäväksi korkeimmalla prioriteetilla asiantuntijalle Tipakkeessa
- Varmistaa, että tiedottaminen häiriöstä aloitetaan
- Luoda ongelmatiketti ja informoida ongelmanselvitysmanageria, joka käynnistää tarvittaessa ongelmanselvitysprosessin
- Varmistaa, että esimiehiä tiedotetaan tilanteesta
- Varmistaa, että Service Desk:issä on tieto häiriön laajuudesta

Laajan häiriön prosessin tärkeimmäksi tehtäväksi on määritelty asiantuntijoiden osalta palvelun mahdollisimman nopea palauttaminen toimivalle tasolle. Asiantuntijoiden työrauhan varmistamiseksi on määritelty, että ainoastaan häiriönhallinnan koordinaattori, esimiehet ja ongelmanhallintaa johtava taho ovat oikeutettuja ja velvollisia selvittämään häiriön selvittämisen aikataulutusta asiantuntijan kanssa. Ongelmanhallintaa johtava taho ja asiantuntijat on määritelty velvollisiksi tiedottamaan koordinaattoria häiriön selvitystyön etenemisestä. Vaihtoehtoiset ratkaisut (work-around) on mainittu hyödynnettäväksi tarvittaessa. Häiriön aiheuttajan ollessa tuntematon, se on määritelty selvitettäväksi ongelmanhallintaprosessin avulla. Laajan häiriön yksityiskohtaiset selvittämistehtävät ja Tipakkeen häiriönhallintaprosessi on määritelty kuvattavaksi erillisessä dokumentissa ”Häiriönhallinta-prosessidokumentti”. (Tipake jatkuvuussuunnitelma 2015).

Normaaliolojen laajojen häiriötilanteiden aikainen tiedotus on määritelty tiedotusvastaavan tehtäväksi asiakkaan kanssa sovittujen toimintamallien mukaisesti. Tiedotus on määritelty aloitettavaksi välittömästi laajan häiriön ilmetyä ja tiedotteen tulee sisältää myös ajankohta, jolloin tiedotetta viimeistään päivitetään. Häiriön selvityksen pitkittyessä on määritelty riittävän usein tehtävä väliaikatiedotus. Häiriön selvittämisen jälkeen on määritelty toimitettavaksi tiedote, joka sisältää ainakin tiedon häiriön ratkaisusta, häiriön poistumisajankohdan sekä lyhyen selvityksen häiriön syystä ja lisätietojen saatavuudesta. Tarkemmat ohjeet ja toimintamallit on ilmoitettu sijaitsevan Tipakkeen intranetin viestintäosiossa, lisäksi tiedottamisesta ja tiedotteen laatimisesta sekä kaikkien osapuolten yhteystiedoista on tehty erilliset dokumentit, jotka ovat jatkuvuussuunnitelman liitteenä (”Häiriötiedote” ja ”Yhteystiedot”). (Tipake jatkuvuussuunnitelma 2015).

Jatkuvuussuunnitelman mukaan Tipakkeen jatkuvuuden turvaaminen perustuu normaaliin tietokonekeskuksen ja ICT-infrastruktuurin ylläpitoon, tietojärjestelmien operointiin, huoltotoimenpiteisiin, ohjelmistojen päivityksiin ja palvelujen tuottamiseen sekä kehittämiseen. Prosessien omistajat vastaavat osiltaan ”*Jatkuvuudenhallinnan toimenpiteet ja toipumissuunnitelmat*” -dokumentin laadinnasta, jonka Tipakkeen johtoryhmä hyväksyy. Jatkuvuudenhallinnan toteutumiselle ja havaittujen riskien pienentämiselle luodaan edellytykset normaaliolosuhteissa suoritettavilla ennakoivilla toimenpiteillä. Myös nämä toimenpiteet kuvataan edellä mainitussa dokumentissa. (Tipakkeen jatkuvuussuunnitelma 2015).

Jatkuvuussuunnitelmassa mainitaan, että jokaiselle palvelulle laaditaan omat jatkuvuudenhallintatoimenpiteet ja toipumissuunnitelmat. (Tipake jatkuvuussuunnitelma 2015). Näissä suunnitelmissa huomioitavat toipumisvaiheen tehtävät on listattu taulukossa 9.

Taulukko 9. *Huomioitavat toipumisvaiheen tehtävät (Tipake jatkuvuussuunnitelma 2015).*

- Tilanteen ja sen laajuuden tunnistaminen
- Toipumisryhmän koolle kutuminen
- Häiriön vaikutusten rajoittaminen
- Toimintaohje palauttamisen suhteen
- Palautumisprosessin etenemisen valvonta ja palautumistilan valmistelu
- Tiedottaminen kaikille osapuolille
- Raportin laadinta
- Häiriön syiden analysointi ja korjaavat toimenpiteet

Jatkuvuussuunnitelman lopussa määritellään suunnitelman ylläpito, katselmointi, päivittäminen ja säilyttäminen. Tässä suunnitelmaversiossa näiden asioiden vastuuhenkilöä ei ole määritetty. Saman henkilön vastuulle on määritelty lisäksi Tipakkeen henkilöstön ja suunnitelman muiden osapuolien suunnitelmaa koskeva tiedottaminen ja kouluttaminen sekä suunnitelman testaaminen ja harjoittelu erillisen testaussuunnitelman mukaisesti. Suunnitelman lopuksi on listattu liitteet ja viitteet. (Tipake jatkuvuussuunnitelma 2015).

Erillisessä ”*Jatkuvuudenhallinnan toimenpiteet ja toipumissuunnitelmat*” -dokumentissa on listattu yksittäisten prosessien ja palveluiden osalta tunnistetut uhat, jatkuvuudenhallinnan toimenpiteet, toipumissuunnitelmat ja kehittämiskohteet. Yksittäisen uhan käsittely sisältää uhan kuvauksen, jatkuvuudenhallinnan toimenpiteet, toipumissuunnitelman ja mahdolliset kehittämiskohteet sekä yhteystiedot. (Tipake jatkuvuudenhallinnan toimenpiteet ja toipumissuunnitelma 2015).

Tipakkeessa on tehty riskien kartoitus ja arvio niiden vaikutuksesta toimintaan kesällä 2015 pääosin ICT-päälliköistä koostuvan työryhmän toimesta. (Tipake

6. JATKUVUUDENHALLINNAN KEHITTÄMINEN

Tässä luvussa kuvataan tutkimusongelma ja käytetyt tutkimusmenetelmät sekä esitetään nykytilan analyysi ja tutkimusongelman ratkaisemiseksi laaditut toimenpide-ehdotukset sekä suoritettun kyselytutkimuksen tulokset analysoituna.

6.1 Tutkimusongelma ja -menetelmät

Tämän diplomityön tavoitteena oli parantaa Tipakkeen jatkuvuudenhallintaa kehittämällä olemassa olevaa, vielä keskeneräistä jatkuvuussuunnitelmaa

- Havaitsemalla puutteita
- Ehdottamalla toimenpiteitä puutteiden korjaamiseksi
- Lisäämällä hyviä käytäntöjä ja toimintatapoja nykytilanteeseen
- Tuomalla lisätietoa ja uusia näkemyksiä kyselytutkimuksen avulla

Jatkuvuudenhallintaa kehittämällä Tipakkeesta tulee sietokykyisempi häiriöitä vastaan. Haitallisten tapahtumien vaikutuksia voidaan poistaa tai vähentää varautumalla häiriötilanteisiin ennalta. ISO/IEC 27031 -standardin mukaisella ICT-valmiudella häiriötilanteisiin voidaan reagoida oikein, hyväksi havaitulla ja tietoturvalisellä tavalla.

Tutkimusmenetelmänä käytettiin kirjallisuustutkimusta hyvien toimintatapojen ja käytäntöjen selvittämiseksi. Tämän lisäksi suoritettiin kyselytutkimus organisaatiokohtaisen tiedon saamiseksi nykytilan analyysin syvyyden kasvattamiseksi.

Tipakkeen nykyinen jatkuvuussuunnitelma käytiin lävitse kohdittain. Kirjallisuudessa ja standardeissa esitettyjä hyviä käytäntöjä ja toimintatapoja verrattiin Tipakkeen jatkuvuudenhallinnan nykytilaan kehittämisehdotuksia esittäen. Kyselytutkimuksesta saatua informaatiota käytettiin nykytilan analyysin apuna nykytilaa syventävänä, henkilöstön kokemana toteutumistasona.

6.2 Kyselytutkimuksen suorittaminen

Laaditun kyselytutkimuksen tarkoituksena oli selvittää Tipakkeen IT-henkilöstön

- Yleisiä käsityksiä ja valmiuksia jatkuvuudenhallintaan, tietoturvalisyyteen ja riskienhallintaan liittyen
- Koulutus- ja osaamistarpeita sekä häiriötilanteiden harjoittelua ja niistä oppimista
- Häiriötilanteiden aikaisen viestinnän ja tiedottamisen riittävyttä ja selkeyttä
- Koettua resurssien riittävyttä ja dokumentointia
- Vastuiden selkeyttä sekä vara- ja avainhenkilöihin liittyviä asioita

Kyselyllä haluttiin kartoittaa mahdollisia puutteita ja riskejä nykyisissä toimintatavoissa kehittämiskohteiden havaitsemiseksi sekä saada selville lähtökohtia aloitettavalle IT-henkilöstön kouluttamiselle ja häiriötilanteiden harjoittelulle. Kysely perustui diplomityön teoriaosassa mainittuihin asioihin. Teoriaosassa käsiteltyjä hyväksi havaittuja toimintatapoja käytettiin tavoitetilana, jonka toteutumista nykytilassa kyselyllä pyrittiin mittaamaan. Kyselytutkimuksen kysymykset muotoiltiin Tipakkeen johdon kanssa käytyjen keskustelujen perusteella. Kysely luetutettiin Tipakkeen viestinnästä vastaavalla henkilöllä ennen kyselyn toteuttamista.

Kyselyssä esitettyihin väittämiin pyydettiin vastaamaan ordinaaliasteikolla 1-5, jossa vaihtoehdot oli määritelty seuraavasti:

1. Täysin eri mieltä
2. Jonkin verran eri mieltä
3. Ei samaa eikä eri mieltä
4. Jonkin verran samaa mieltä
5. Täysin samaa mieltä

Kysymyksiä oli yhteensä 40 kappaletta, jaoteltuna 6 aihepiiriin. Aihepiirit olivat:

- Yleiset käsitykset, 4 kysymystä
- Tietoturvallisuus ja riskienhallinta, 7 kysymystä
- Koulutus ja harjoittelu, 9 kysymystä
- Viestintä ja tiedottaminen, 6 kysymystä
- Resurssit, 6 kysymystä
- Vastuut, 8 kysymystä

Kaikissa aihepiireissä oli lisäksi kommenttiosio avoimia kommentteja varten. Kysely toteutettiin sähköisenä lomakekyselynä, joka laadittiin käyttäen Webropol-kyselytyökalua. Linkki kyselyyn lähetettiin kohderyhmälle sähköpostitse ja vastausaikaa annettiin kaksi viikkoa. Viikon kuluttua kyselyn aloittamisesta lähetettiin muistutus kyselyyn vastaamisesta vastausten lukumäärän maksimoimiseksi. Henkilöstöä informoitiin kyselystä myös vastausajanjaksolle osuneissa henkilöstöpalavereissa sekä Tipakkeen intranetissä kyselyn ajan.

Webropol-kyselyn pohjana käytetty kyselylomake on diplomityön liitteenä A: Kyselylomake.

6.3 Nykytilan analyysi

Tipakkeen jatkuvuussuunnitelmassa kuvataan toimenpiteet normaalioloissa ja normaaliolojen häiriötilanteissa. Jatkuvuussuunnitelmassa ei käsitellä toimintaa poikkeusoloissa eli laajemmin yhteiskuntaa koskettavissa häiriötilanteissa. Jatkuvuudenhallintaa varten tulisi selvittää, onko Tipakkeella tärkeitä yhteiskunnallisia tehtäviä esimerkiksi sosiaali- ja terveystoimen tietoliikennelaitteiden hallinnoijana ja tuen tarjoajana. Mahdolliset poikkeusolojen aikaiset tehtävät tai niiden puuttuminen tulisi kirjata valmiussuunnitelmaan.

Tipake arvioi riskit vähintään vuosittain ja aina suurissa toimintaympäristöön tai toimintaan kohdistuvissa muutoksissa. Arviointi toteutetaan johtoryhmän tekemänä tai heidän valtuuttamallaan taholla. Riskianalyysiä tehtäessä on varmistettava, että sen tekemiseen osallistuu IT-henkilöstöä ja liiketoimintaa ymmärtäviä henkilöitä. Mukana on oltava myös Tipakkeen toimintaa ymmärtäviä tahoja, jotta organisaation prosesseihin ja tietojärjestelmiin kohdistuvat uhat arvioidaan oikein.

Tällä hetkellä suurin osa Tipakkeen arvioimista riskeistä on teknisiä, operatiivisia riskejä. Osaamisen ja riittävän kapasiteetin puute on arvioitu riskinä merkittävimäksi kaikissa palveluissa. Sellaisia prosesseja, joissa tämän riskin vaikutus on arvioitu toteutuessaan merkittäväksi tai kriittiseksi ja todennäköisyys kohtalaiseksi tai suureksi on vähintään kaksi kertaa enemmän kuin muita arvioituja riskejä. Muita tunnistettuja merkittäviä riskejä ovat ilkeä ja häiriöt, tietoturvan ongelmatilanteet, ohjelmistojen ongelmatilanteet sekä puutteet ohjeistuksessa ja dokumentaatiossa.

Jatkuvuussuunnitelman mukaan jatkuvuudenhallintatoimenpiteiden tarvittava kouluttaminen on määritelty Tipakkeen johtajan määräämälle henkilölle. Kouluttamissuunnitelmaa ei ole kuitenkaan vielä laadittu.

Tipakkeen palvelut on asetettu toipumisjärjestykseen useiden samanaikaisten häiriötilanteiden varalta. Palveluille ei ole tällä hetkellä kuitenkaan määritelty häiriöiden sietokyvyn enimmäisaikaa tai minimipalvelutasoa. Tipakkeessa ollaan ottamassa käyttöön laadittu ”*palvelutasomääritykset*” -dokumentti vuoden 2016 alussa, jossa määritellään reagointiajat häiriöihin eri palveluissa ja häiriötilanteiden ratkaisuaikavoitteet. Sietokyvyn enimmäisajan määrittelyllä häiriön aiheuttamat haitalliset vaikutukset voidaan esimerkiksi todeta niin suuriksi, että ulkopuolisten lisäresurssien tai työjärjestelyiden tarve on helpommin perusteltavissa ja arvioitavissa. Minimipalvelutasot määrittelemällä voidaan kohdentaa rajallisia resursseja samanaikaisten häiriöiden välillä, kun yksi palvelu on saatu toimintaan hyväksyttävällä tasolla. Vaikka Tipakkeen ei ainoana toimijana tarvitse saavuttaa kilpailuetua muihin toimijoihin verrattuna, pitkään kestävät häiriöt aiheuttavat asiakasyksiköille taloudellisia tappioita tekemättömän työn muodossa sekä huonontavat Tipakkeen uskottavuutta selvittää häiriötilanteita.

Jatkuvuussuunnitelmassa kuvataan häiriönhallinnan olevan ITIL:n mukaista, häiriöt laajoihin ja yksittäisiin erottelevaa. Laajoihin häiriöihin on kuvattu toteutettavaksi monivaiheinen selvitysprosessi. Häiriönhallinnassa käytetään laajoissa häiriöissä koordinaattoria, joka toimii selvitysprosessin johtajana. Tipakkeen käyttämässä toimintamallissa määritetään häiriön laatu ja laajuus, otetaan tilanne hallintaan, käsitellään häiriö sekä kommunikoidaan sidosryhmien kanssa ISO/IEC 27031 -standardia vastaavalla tavalla. Tällä hetkellä laajan häiriönhallinnan koordinaattori nimetään Tipakkeen palvelupisteestä kaikissa laajoissa häiriötilanteissa, yksittäisiä henkilöitä ei ole kuitenkaan listattu jatkuvuussuunnitelmassa. Häiriötilanteiden varalta on huomioitava henkilöresurssien saatavuus palvelupisteessä, koordinaattorin osaamisvaatimukset ja mahdolliset varahenkilöjärjestelyt, jotta koordinaattori on nimettävissä myös poissaolojen aikana. ISO/IEC 27031 -standardissa suositetaan, että häiriöitä voidaan käsitellä myös jaoteltuna esimerkiksi teknisiin ja palvelullisiin häiriöihin. Tällaisella jaottelulla voidaan tarvittaessa jakaa häiriönhallinnan koordinaattorin tehtäviä ja osaamisvaatimuksia useammalle henkilölle.

Tipake on määritellyt häiriötilanteiden aikaisen viestinnän erilliselle tiedotusvastaavalle ja tiedotus toteutetaan ennalta määrätyllä tavalla. Häiriön alaisia tahoja tiedotetaan havaittaessa häiriö sekä häiriötilanteen selvityksen aikana ja sen jälkeen. Tiedottaminen on nykytilassa keskitettyä ja koordinoitua. Tiedottamisessa tulee varmistaa, että se on totuudenmukaista eli häiriötilanteen tulee olla oikein tunnistettu, jotta huonoon tiedottamiseen liittyvät maineriskit minimoidaan ja luottamus Tipakkeen kykyyn hoitaa häiriötilanteet asianmukaisesti säilyy edelleen. Erityisesti häiriötilanteiden aikainen, tilanteen edistymisestä kertova tiedotus on altis vääärälle informaatiolle, kun käsillä olevaa ongelmaa ei vielä välttämättä tunneta tarkoin ja paine tilanteen ratkaisun edistymisestä tiedottamiselle on suuri.

Tipake pyrkii toteuttamaan jatkuvuudenhallintaa ja pienentämään havaittuja riskejä normaaliolosuhteissa suoritettavilla ennakoivilla toimenpiteillä. Ennakoivat toimenpiteet kohdistuvat teknisiin ja operatiivisiin sekä henkilöllisiin uhkiin. Erityisesti henkilöstöön kohdistuviin, kaikkiin palveluihin vaikuttaviin uhkiin, kuten koulutuksen, dokumentoinnin ja varahenkilöjärjestelyjen puutteellisuuteen on esitetty runsaasti kehittämiskohteita.

Jatkuvuussuunnitelman mukaan kaikille palveluille laaditaan palvelukohtaiset jatkuvuudenhallintatoimenpiteet ja toipumissuunnitelmat. Tällä hetkellä tunnistetuista uhkista ei ole laadittu liiketoiminnan keskeytysvaikutusanalyysiä. Sen toteuttamiseksi tulisi koota työryhmä, johon kuuluu liiketoiminnasta tietävä liiketoimintajohto ja keskeytysten vaikutuksista tietävät prosessien omistajat sekä toipumistehtävissä työskennelleet tahot kokemusperäisen tiedon saamiseksi. Liiketoiminnan keskeytysvaikutusanalyysi tuo tietoa palveluiden kriittisyydestä ja keskinäisistä riippuvuuksista sekä resursseista, joista tärkeimmät toiminnot ovat riippuvaisia. Tällöin rajallisia resursseja voidaan kohdentaa paremmin keskeisimpien toimintojen

turvaamiseen. Tipakkeen suorittamassa riskianalyyssissä on selvitetty riskit eli keskeytysten syyt, liiketoiminnan keskeytysvaikutusanalyyssillä pyritään selvittämään keskeytysten erityisesti taloudelliset vaikutukset toimintaan. Analyysin tavoitteena on myös vaadittavan palautumisajan ja vaadittavien resurssien selvittäminen.

Jatkuvuussuunnitelman ylläpitoa, katselmointia, päivittämistä ja säilyttämistä ei ole tällä hetkellä vastuutettu nimetyille taholle. Vastuuhenkilön nimeämisen lisäksi tulee varmistaa, että jatkuvuussuunnitelma sekä sen liitteet ovat saatavilla myös paperisessa muodossa ja useissa erillisissä fyysisissä sijainneissa. Useiden erillisten dokumenttien ylläpidossa ja päivittämisessä on otettava huomioon myös versionhallinta, jotta kaikki olemassa olevat dokumentit ovat ajantasaisia ja käyttökelpoisia.

Jatkuvuussuunnitelman testaaminen ja harjoittelu on määritelty suoritettavaksi erillisen testaussuunnitelman mukaisesti. Tällä hetkellä testaussuunnitelmaa ei ole laadittu.

Tipakkeen jatkuvuussuunnitelmassa käsitellään riskejä siten, että yksittäiset riskit on pisteytetty kvalitatiivisella asteikolla todennäköisyyden ja vaikutuksen mukaan. Käyttämällä määrällistä riskianalyyssiä riskeistä saataisiin syvällisempi kuva ja riskin realisoitumisen seurauksia voitaisiin tarkastella esimerkiksi euromääräisesti. Tunnistettujen riskien taloudellisia vaikutuksia voitaisiin arvioida rahallisen arvon analyysillä. Tällöin riskien keskinäinen merkitys ja siten turvattavien kohteiden tärkeys saattaisivat muuttua vastaamaan paremmin todellisia taloudellisia menetyksiä.

Riskien arvioinnissa voitaisiin hyödyntää riskien suuruuden pisteyttävää riski-indeksi -mallia, jossa riskit pisteytetään kohteen arvon, uhan toteutumisen todennäköisyyden ja toteutumisen helppouden perusteella. Nykyisen arviointimallin ongelmana on, ettei siinä huomioida kohteelle ominaisia uhkatekijöitä tai rappeutumisriskejä. Rappeutumisriskit syntyvät varsinaisen välittömän vahingon lisäksi aiheutuvista toipumisen keston vahingoista. Toipumisen kestäessä pitkään menetetään tekemättömän työn lisäksi mainetta.

6.4 Kyselytutkimuksen tulokset ja analyysi

Kysely lähetettiin sähköpostitse ryhmälle, johon kuului yhteensä 31 henkilöä. Näistä kaksi henkilöä oli kyselyn ajan työvapaalla. Kohderyhmässä oli siis yhteensä 29 henkilöä. Kysely tuotti 23 vastausta eli kyselyyn vastasi 79 % kohderyhmästä. Avoimia kommentteja kertyi kolme kappaletta. Avoimet kommentit olivat:

- Tietoturvallisuus ja riskienhallinta -aihepiiri: ”*Haen toimintaohjeita ensisijaisesti omasta intranetistä.*”
- Koulutus ja harjoittelu -aihepiiri: ”*Koulutukseen liittyen: Tässä ei ihan käynyt ilmi tarkoitetaanko vain jatkuvuussuunnittelun koulutusta vai koulutusta yleensä. Vastasin nyt koulutukseen yleensä.*”

- Viestintä ja tiedottaminen -aihepiiri: ”*Asiantuntijoilta Service Deskin suuntaan tiedotuksen parannus.*”

Avoimista kommentteista kaksi koski kysymysten asettelua ja yksi kommentti liittyi tiedotuksen toteutukseen. Kysymysten asettelua koskevissa kommentteissa kysymykset on tulkittu oikein, sillä ”oma intranet” sisältyy kysymyksessä mainittuun ”Tipakkeen omaan dokumentaatioon” ja koulutukseen liittyvässä kysymyksessä tarkoitettiin koulutusta yleensä. Tiedotuksen toteutumiseen liittyvä kommentti on ymmärrettävissä joko siten, että asiantuntijat tiedottavat Service Deskiä aikaisempaa paremmin eli toiminnassa on tapahtunut parannusta tai siten, että asiantuntijoiden tulisi pyrkiä tiedottamaan Service Deskiä paremmin.

6.4.1 Yleiset käsitykset

Kyselyyn vastanneista 35 % oli perehtynyt jatkuvuussuunnitteluun ja jatkuvuudenhallintaan huonosti tai hyvin huonosti. Toisaalta 48 % vastaajista oli perehtynyt jatkuvuussuunnitteluun ja jatkuvuudenhallintaan hyvin tai erinomaisesti. Toiminnan jatkuvuutta uhkaavat riskit tiedosti hyvin tai erinomaisesti 57 % vastaajista. Omaan työhön liittyvät riskit tiedosti hyvin tai erinomaisesti 78 % vastaajista. Jatkuvuudenhallintaa piti tärkeänä ja oli siihen motivoitunut hyvin tai erinomaisesti 70 % vastaajista.

Kyselytutkimuksen mukaan noin kolmasosa henkilöstöstä ei ole perehtynyt jatkuvuussuunnitteluun ja jatkuvuudenhallintaan. On huomioitava, että jatkuvuudenhallinta kuuluu epäsuorasti jokaiselle Tipakkeen työntekijälle työtehtävistä riippumatta ja suorasti jatkuvuussuunnittelua ja jatkuvuudenhallintatoimenpiteitä suorittaville henkilöille. Jatkuvuussuunnittelusta on hyötyä vain silloin, kun henkilöstö on riittävästi tietoista laadittujen jatkuvuussuunnitelmien sisällöstä. Suositus on, että henkilöstö perehdytetään jatkuvuudenhallintaan ensin yleisellä tasolla tietoisuutta lisäten. Tämän perehdytyksen tulisi käsitellä jatkuvuudenhallinnan vastuuta ja tehtäviä ja yleistä häiriötilanteiden aikaista toimintaa. Tämän jälkeen jatkuvuudenhallintaa suorasti suorittavat henkilöt voivat harjoitella häiriöskenaarioita tehtäviensä mukaisesti toimintavarmuuden ja oikeiden toimintatapojen oppimiseksi.

Toiminnan jatkuvuutta uhkaavat riskit tiedostetaan hyvin. On kuitenkin tärkeää tiedostaa, että ainoastaan havaittujen riskien hallinta on mahdollista. Toiminnassa tapahtuvat muutokset voivat myös aiheuttaa uusia riskejä. Riskien arvioinnissa on käytettävä riittävän monimuotoista ryhmää, jolla on sekä kohteen tai toiminnon substanssiosaamista että riskienhallinnan menetelmien hallintaosaamista. Tarvitaan eri asiantuntijoiden ryhmätyötä, jotta riskien syy-seuraussuhteet ovat havaittavissa tehokkaasti. Henkilöstön kouluttamisella voidaan lisätä tietoisuutta Tipakkeen kannalta tärkeistä prosesseista, laitteista ja palveluista.

Omaan työhön liittyvät riskit tiedostetaan myös erinomaisella tasolla. Ihmisillä on kuitenkin taipumusta tottua riskeihin eli henkilö ei aina ole oman työnsä riskien paras havaitsija.

Tipakkeen henkilöstö pitää jatkuvuudenhallintaa tärkeänä ja on hyvin motivoitunutta siihen. Sitoutumista jatkuvuudenhallintaan voidaan tarvittaessa lisätä varoittavilla esimerkeillä aikaisemmista katastrofeista tai ryhmätyöskentelyllä sekä aiheeseen liittyvillä luennoilla, tarvittaessa hyödyntäen Tipakkeen ulkopuolisia asiantuntijoita.

Yleiset käsitykset -aihepiirin vastausjakauma on esitetty taulukossa 10.

Taulukko 10. Yleiset käsitykset -aihepiirin vastausjakauma.

	1	2	3	4	5	Yhteensä	Keskiarvo
Olen perehtynyt jatkuvuussuunnitteluun ja jatkuvuudenhallintaan	3	5	4	7	4	23	3,17
Tiedän millaiset riskit muodostavat uhan toiminnan jatkuvuudelle	0	4	6	10	3	23	3,52
Tiedän omaan työhöni liittyvät riskit	0	2	3	12	6	23	3,96
Jatkuvuudenhallinta on tärkeää ja olen motivoitunut siihen	0	1	6	8	8	23	4
Yhteensä	3	12	19	37	21	92	3,66

6.4.2 Tietoturvallisuus ja riskienhallinta

Tipakkeen tietoturvaohjeisiin ja määräyksiin oli perehtynyt hyvin tai erinomaisesti 61 % vastaajista, kuitenkin huonosti tai hyvin huonosti perehtyneitä vastaajia oli 26 %. Annettuja tietoturvaohjeita ja määräyksiä noudatti hyvin tai erinomaisesti 74 % kyselyyn vastanneista. Etätyöhön liittyvät tietoturvariskit tiedosti hyvin tai erinomaisesti 91 % kyselyyn vastanneista. Fyysisen turvallisuuden riittävyys koettiin hyväksi tai erinomaiseksi 52 % vastauksista, kuitenkin fyysistä turvallisuutta piti huonona tai erittäin huonona 30 % vastaajista.

Tärkeät yhteystiedot koettiin huonosti tai erittäin huonosti saataviksi sähkökatkon aikana 39 % vastauksista. Toimintaohjeita haettiin ensisijaisesti sekä internetistä 43 % että Tipakkeen omasta dokumentaatiosta 30 %, internetin ollessa kuitenkin pääasiallinen tietolähde hieman useammalle.

Suurin osa vastaajista on perehtynyt Tipakkeen tietoturvaohjeisiin ja määräyksiin, tosin neljännes ilmoitti perehtymisen olleen vähäistä. Tipakkeen johdon ja esimiesten merkitys motivoivana tahona on suuri. On tunnustettu tosiasia, että tietoturvallisuuden merkitys tunnustetaan organisaatiossa vasta sitten, kun organisaation johto antaa siihen tukensa ja sitoumuksensa.

Annettuja tietoturvaohjeita ja määräyksiä noudatetaan Tipakkeessa hyvin. On kuitenkin huomioitava, että tietoturvapoikkeamiin johtavat tilanteet voivat olla tahattomia, kuten

näppäilyvirheitä. Tahattomia virheitä voidaan pyrkiä vähentämään esimerkiksi pitämällä käyttöoikeudet niin vähäisellä tasolla kuin on välttämätöntä. Käytössä olevat henkilöstöresurssit eli työhön käytössä oleva aika, työtyytyväisyys ja motivaatio vaikuttavat myös tietoturvallisuuden toteutumiseen käytännössä.

Etätyöhön liittyvät tietoturvariskit tiedostetaan erinomaisella tasolla. Mahdollisen tietoturvaongelman muodostavat henkilökohtaiset laitteet, jos niitä voidaan käyttää BYOD -tyyppisesti työskennellessä kotoa käsin. Tipakkeella on vähän tai ei ollenkaan hallintaa henkilöstön henkilökohtaisiin laitteisiin, jolloin esimerkiksi Tipakkeen sisäisistä suojaustoimenpiteistä ei ole hyötyä. Toinen etätyöhön liittyvä tietoturvauhka on etätyöpisteen fyysisen valvonnan puute, josta voi aiheutua esimerkiksi Tipakkeen omistamien laitteiden ja siirrettävien tallennusmedioiden katoaminen tai varkaudet. Tällöin arkaluontoista tietoa voi päätyä väärin käsiin, jos tietoa ei säilytetä tietoturvallisesti Tipakkeen verkkolevyillä.

Fyysisen turvallisuuden koetaan olevan pääsääntöisesti riittävää, kuitenkin osa vastaajista havaitsi siinä parantamisen tarvetta. Fyysistä turvallisuutta voidaan parantaa erilaisilla kulunvalvontaratkaisulla, kameravalvonnalla, hälytysjärjestelmillä ja henkilökunnan valppaudella. Rakennuksen omistaja tai sitä hallitseva taho on vastuussa tilojen hallinnasta ja turvallisuusjärjestelyjen toteutuksesta. Tipake tuntee tiloja käyttävänä tahona käytetyn tietotekniikan turvallisuustarpeet. Fyysisen turvallisuuden pettäminen voi aiheuttaa tietoriskejä. Tällaisia riskejä ovat esimerkiksi huolimattomasti säilytetyt asiakirjat ja selkokiekiset salasanat sekä tietovälineiden katoaminen. Henkilöstön tulee tunnistaa arvokas tieto, mikä vaatii henkilöstöltä kykyä tiedon tunnistamiseen, luokitteluun ja käsittelyyn. Tiedon käsittelyssä voidaan hyödyntää tiedon elinkaaren hallintaa, jonka avulla tietoon liittyviä riskejä voidaan vähentää. Henkilöstön perehdyttäminen tietoaikaineiston käsittelyyn on Tipakkeen johdon vastuulla.

Tärkeitä yhteystietoja pitää huonosti saatavilla sähkökatkon aikana yli kolmannes vastaajista. On suositeltavaa, että jatkuvuussuunnitelmat säilytetään useissa erillisissä fyysisissä sijainneissa sekä sähköisessä että paperisessa muodossa. Tärkeät yhteystiedot on oltava saatavilla silloinkin, kun tietoliikenneyhteydet eivät toimi tai sähköä ei ole käytettävissä vikatilanteen korjaamiseksi.

Tipakkeen henkilöstö hakee työssä tarvittavia toimintaohjeita tasaisesti sekä internetistä että Tipakkeen omista lähteistä. Tiedon elinkaaren hallintaperiaatteiden mukaan laaditun dokumentaation on oltava helposti saatavilla. Dokumentaation tulee olla myös ajantasaista. Tipakkeen ulkopuolisten tietolähteiden käyttö voi aiheuttaa ohjelmistoturvallisuuden riskejä, jos sovelluksia haetaan ja asennetaan internetistä omien lähteiden, kuten verkkolevyjen sijaan. Tästä saattaa aiheutua myös versioristiriitoja. Jos oman dokumentaation halutaan olevan ensisijainen ja ajantasainen tietolähde, tulee dokumentaatioon varata riittävästi resursseja. Dokumentaation yhtenäistämiseksi voidaan sopia yhtenäisistä muotoseikoista.

Tietoturvallisuus ja riskienhallinta -aihepiirin vastausjakauma on esitetty taulukossa 11.

Taulukko 11. Tietoturvallisuus ja riskienhallinta -aihepiirin vastausjakauma.

	1	2	3	4	5	Yhteensä	Keskiarvo
Olen perehtynyt Tipakkeen tietoturvaohjeisiin ja määräyksiin	3	3	3	11	3	23	3,35
Noudatan annettuja tietoturvaohjeita ja määräyksiä	0	1	5	11	6	23	3,96
Tiedostan etättyöhön liittyvät tietoturvariskit	0	2	0	12	9	23	4,22
Fyysinen turvallisuus (kuten kulkuoikeudet, vierailijoiden valvonta) on riittävää	1	6	4	9	3	23	3,3
Tärkeät yhteystiedot ovat helposti saatavilla sähkökatkon aikana	4	5	8	5	1	23	2,74
Haen toimintaohjeita ensisijaisesti Internetistä	1	3	9	9	1	23	3,26
Tipakkeen oma dokumentaatio on ensisijainen lähteeni etsiessäni toimintaohjeita	1	7	8	4	3	23	3,04
Yhteensä	10	27	37	61	26	161	3,41

6.4.3 Koulutus ja harjoittelu

Osaamis- ja koulutustarpeet koki selvitettyksi huonosti tai erittäin huonosti 26 % vastaajista, kuitenkin 39 % vastaajista koki selvityksen olleen hyvää. Tarvittavaa koulutusta koki saavansa tarvittaessa hyvin tai erinomaisesti 48 % vastaajista, toisaalta 35 % vastaajista koki tarvitsemansa koulutuksen saamisen huonoksi tai hyvin huonoksi.

Tipakkeen jatkuvuussuunnitelmiin perehdyttäminen koettiin huonoksi tai erittäin huonoksi 52 % vastauksista. Jatkuvuudenhallinnan teoriakoulutusta haluaisi paljon tai erittäin paljon 30 % vastaajista, mutta 61 % vastaajista ei osannut kommentoida teoriakoulutuksen tarvettaan. Häiriötilanteiden harjoittelemista käytännössä haluaisi paljon tai erittäin paljon 52 % vastaajista.

Uuden henkilön perehdyttämistä häiriötilanteisiin piti huonona tai erittäin huonona 70 % vastaajista. Nykyistä häiriötilanteiden dokumentointia ja niistä oppimista piti hyvänä tai erinomaisena 48 % vastaajista. Tapahtuneiden häiriötilanteiden läpikäymistä jälkikäteen piti tarpeellisena tai erittäin tarpeellisena 78 % vastaajista. Koulutuksen järjestämistä Tipakkeen sisäisenä koulutuksena piti hyvänä tai erinomaisena 30 % vastaajista, kuitenkin 39 % vastaajista piti ulkoista koulutusta parempana vaihtoehtona.

Kyselyyn vastanneiden osaamis- ja koulutustarpeet oli selvitetty yli kolmanneksen mielestä hyvin, neljäsosa vastaajista piti kuitenkin selvitystä riittämättömänä. Työssä tarvitsemaansa koulutusta koki saavansa hyvin yli kolmanneksen vastaajista, mutta toisaalta yli kolmanneksen vastaajista ei kokenut saavansa tarvittavaa koulutusta. Tipake toimii hyvin tietointensiivisellä IT-alalla, jossa jatkuva kouluttautuminen ja kehittyminen on yleisesti tunnustettu kriittinen menestystekijä. Osaamiseen ja koulutukseen liittyy riskejä, oli näiden määrä sitten liian vähäinen tai liiallinen.

TTL:n vuonna 2012 tekemän tutkimuksen mukaan IT-alalla kolme viidestä merkittävimmästä kuilutekijästä (asian tärkeys suhteessa nykytilanteeseen) työssä olivat osaamiseen liittyviä: osaamisen kehittämismahdollisuudet, urakehitysmahdollisuudet sekä kykyjen ja osaamisen huomioiminen (Tietotekniikan liitto ry, 2012). Jos henkilöstöllä on käyttämätöntä tieto- ja osaamispotentiaalia, sen käyttämättä jättäminen voi aiheuttaa ”tyhjäkäyntiä”. Tällöin organisaation toiminta ei kehity ja henkilöstön työmoraaali laskee liian yksinkertaisten tai osaamista vastaamattomien työtehtävien takia. Riskinä on myös psyykinen kyllästyminen eli tila, jossa yksilö ei pääse hyödyntämään osaamistaan työssään ja suuntaa voimavaransa varsinaisen työn ulkopuolelle. (Ranki, 1999). Yksilön kyllästyminen liian yksinkertaisiin tai toistaviin työtehtäviin ei huononna ainoastaan yksilön työtehoa, vaan se voi vaikuttaa koko organisaatiotasolla negatiivisesti. Henkilö, joka kokee olevansa ylikoulutettu työtehtäviinsä, on useammin tyytymätön työhönsä kuin henkilö, joka ei koe olevansa ylikoulutettu. (Vuorinen & Valkonen, 2007).

Tipakkeen jatkuvuussuunnitelmiin perehdyttäminen koettiin riittämättömäksi yli puolessa vastauksia ja korkeintaan keskinkertaiseksi lähes kaikissa vastauksissa. Jatkuvuussuunnitelmiin tulee perehtyä ennen häiriöiden tapahtumista ja tämän lisäksi tarvitaan myös harjoittelua oikeiden toimintatapojen oppimiseksi. Henkilöstön on oltava tietoinen jatkuvuussuunnitelmissa mainituista asioista, jotta jatkuvuussuunnitelmia voidaan hyödyntää käytännössä.

Kyselyyn vastanneet kokivat jatkuvuudenhallinnan teoriakoulutuksen ja häiriötilanteiden harjoittelun käytännössä pääosin tärkeänä, tosin puolet vastaajista ei osannut kommentoida teoriakoulutuksen tarvetta. Koulutus ja harjoittelu auttavat varmistamaan ja kasvattamaan henkilöstön osaamista tarvittavissa taidoissa. Harjoittelu suositellaan toteutettavaksi siten, että harjoiteltuja asioita testattaisiin käytännössä häiriöskenaarioiden avulla harjoittelun jälkeen. Tällä pyritään varmistamaan, että harjoitellut asiat vastaavat oikeissa tilanteissa tarvittavaa osaamista. Harjoittelun avulla voidaan myös havaita jatkuvuussuunnitelmissä olevia puutteita sekä kasvattaa henkilöstön itseluottamusta ja vähentää hätäntymistä tositilanteissa. Tipakkeen on myös varmistettava, että jatkuvuudenhallintaan vaadittava osaaminen on saavutettu testaamalla henkilöstöä säännöllisesti. Testaaminen varmistaa jatkuvuussuunnitelmien kyvyn vastata riskeihin. Testaamisella kasvatetaan samalla henkilöstön luottamusta jatkuvuussuunnittelun tarpeeseen.

Yli kaksi kolmesta vastaajasta koki uuden henkilön perehdyttämisen häiriötilanteiden aikaisiin toimintatapoihin olevan riittämätöntä. Organisaatioon uusina henkilöinä rekrytoituille ja lisäksi organisaation sisällä tehtäviään vaihtaneille tulee järjestää koulutusta jatkuvuudenhallinnasta. Perehdyttämisen tulee vastata kohderyhmän häiriöiden aikaisten tehtävien tasoa työtehtävien edellyttämällä tavalla. Uusille henkilöille tarkoitettu perehdyttämisohjelma voidaan järjestää esimerkiksi neljännesvuosittain.

Nykyinen häiriötilanteiden dokumentointi ja niistä oppiminen koettiin hyväksi noin puolessa vastauksista. Kaikki vastaajat pitivät häiriötilanteiden läpikäymistä jälkikäteen vähintään kohtalaisena toimintatapana ja neljä viidestä vastaajasta piti sitä hyvänä tai erinomaisena toimintatapana. Häiriötilanteiden dokumentointi ja läpikäynti voidaan ajatella koulutuksena, jossa käydään lävitse häiriötilanteiden syitä, seurauksia ja ratkaisuja. Aikaisemmin tapahtuneet selvitetty häiriötilanteet toimivat jatkuvuudenhallinnan motivaation lisääjänä ja häiriötilanteiden aikaisia toimintatapoja voidaan kehittää edelleen laaditun dokumentaation perusteella. ISO/IEC 27031 -standardi suosittelee häiriötilanteiden dokumentointia, analysointia ja katselmointia, jotta vastaavissa tilanteissa osataan toimia aikaisempaa paremmin ja aikaisemmin tehdyt virheet voidaan jättää toistamatta.

Kyselyyn vastanneet jakoutuivat mielipiteissään kahteen osaan siitä, tulisiko jatkuvuudenhallinnan koulutusta järjestää Tipakkeen sisäisenä vai ulkoisena koulutuksena. Tipake voi hyödyntää tarvittaessa koulutuksessa ulkopuolista osaamista, jos tarvittavaa osaamista tai resursseja ei ole saatavilla. Tipakkeen sisäisen koulutuksen vahvuutena on organisaatiokohtaisen informaation määrä.

Koulutus ja harjoittelu -aihepiirin vastausjakauma on esitetty taulukossa 12.

Taulukko 12. Koulutus ja harjoittelu -aihepiirin vastausjakauma.

	1	2	3	4	5	Yhteensä	Keskiarvo
Osaamis- ja koulutustarpeeni on selvitetty	3	3	8	9	0	23	3
Saan halutessani työssä tarvitsemaani koulutusta	5	3	4	9	2	23	3
Tipakkeen henkilöstö on perehdytetty riittävän hyvin Tipakkeen ja sen eri palvelujen jatkuvuussuunnitelmiin	4	8	10	1	0	23	2,35
Haluaisin saada teoriakoulutusta jatkuvuudenhallinnasta	0	2	14	4	3	23	3,35
Haluaisin harjoitella häiriötilanteita käytännössä	1	2	7	9	3	22	3,5
Uuden henkilön perehdytyksessä huomioidaan myös häiriötilanteiden aikaiset toimintatavat	5	11	4	2	1	23	2,26
Tapahtuneet häiriötilanteet dokumentoidaan ja niistä pyritään oppimaan	1	3	8	8	3	23	3,39
Tapahtuneet häiriötilanteet on syytä käydä yhdessä läpi jälkikäteen	0	0	5	8	10	23	4,22
Jos koulutusta järjestetään, Tipakkeen sisäinen koulutus on parempi vaihtoehto kuin ulkoinen koulutus (Sovelton kurssi tms.)	1	8	7	5	2	23	2,96
Yhteensä	20	40	67	55	24	206	3,11

6.4.4 Viestintä ja tiedottaminen

78 % vastaajista tiesi hyvin tai erinomaisesti millaisissa häiriötilanteissa on tiedotettava esimiestä tai Service Deskiä. Alkaneiden häiriötilanteiden tiedotusta piti riittävän nopeana 52 % vastaajista, mutta 30 % vastaajista ei pitänyt tiedotusta riittävän nopeana. Sisäistä viestintää häiriötilanteissa piti riittävänä ja selkeänä 39 % vastaajista, kuitenkin 30 % vastaajista piti sisäistä viestintää häiriötilanteissa riittämättömänä ja epäselvänä.

Häiriötilanteissa tarvittavat henkilöt tavoitti mielestään helposti 43 % vastaajista. Mahdollisesti häiriötä aiheuttavien toimenpiteiden tiedottamista riittävästi etukäteen piti hyvänä tai erinomaisena 35 % vastaajista, toisaalta 30 % vastaajista piti etukäteen tiedottamista huonona tai hyvin huonona. Tapahtuneiden häiriötilanteiden syistä, vaikutuksista ja ratkaisuista tiedotettiin hyvin tai erinomaisesti 39 % vastaajista, mutta huonosti tai hyvin huonosti 35 % vastaajista.

Neljä viidestä vastaajasta ilmoitti tietävänsä, millaisissa häiriötilanteissa esimiestä tai Service Deskiä on tiedotettava. Tipakkeen jatkuvuussuunnitelmassa tällaisiksi tilanteiksi on määritelty laajat häiriötilanteet. Tipakkeen tiedottamiskäytännöt voidaan tarvittaessa käydä lävitse esimerkiksi henkilöstökokouksen yhteydessä yhteisymmärryksen saavuttamiseksi.

Häiriötilanteiden alkamisesta ilmoittavaa tiedotusta piti riittävän nopeana puolet vastanneista, kolmannes ei kokenut saavansa tietoa alkaneesta häiriötilanteesta riittävän nopeasti. Tipakkeen sisäisen viestinnän häiriötilanteissa koki riittäväksi ja tarpeeksi selkeäksi noin samat vastaajamäärät. Jatkuvuussuunnittelun tarkoituksena on, että häiriötilanteissa tiedetään, kuka tekee, mitä tekee, milloin tekee, missä tekee ja miksi tekee. Jatkuvuudenhallintatoimenpiteitä ei voida käynnistää, jos alkaneesta häiriötilanteesta ei olla tietoisia. Häiriötilanteissa on oleellista, että rajalliset resurssit saadaan kohdennettua keskeisimpien toimintojen turvaamiseen. ISO/IEC 27031 -standardi suosittaa, että häiriöistä vastuullisilla tahoilla on suunnitelmat häiriötä vastaavan reaktion aktivoimiseen, toimenpiteisiin, koordinointiin ja viestintään. Viestinnän on oltava siis ennalta määritetyn toimintamallin mukaista. Tipakkeen tapauksessa voitaisiin hyödyntää esimerkiksi tekstiviestityyppistä tiedotusratkaisua häiriötilanneviestinnässä, sillä matkapuhelinverkko ja -laitteet ovat riippumattomia toimipisteen tietoliikenneyhteyksien ja sähköverkon toiminnasta. Tällainen ratkaisumalli ottaa myös huomioon henkilöstön liikkumisen Tipakkeen toiminta-alueella.

Noin puolet vastaajista koki tavoittavansa tarvittavat henkilöt helposti häiriötilanteissa. Tässäkin tapauksessa puhelinyhteydet toimivat toimipisteen tietoliikenneyhteyksien tai sähköjaketun ollessa pois käytöstä. Tarvittavien henkilöiden tavoittamisen hankalaksi kokevat henkilöt viittaavat mahdollisesti Tipakkeen ulkopuolisiin tahoihin, kuten teleoperaattoreihin, huoltoyhtiöihin ja muihin ulkoisiin yhteistyökumppaneihin. Jatkuvuussuunnitelmissa tulee listata kaikki häiriötilanteissa tarvittavat yhteystiedot ja

nämä tiedot on oltava saatavilla myös paperisessa muodossa, jotta tarvittaviin tietoihin päästään käsiksi myös sähkö- ja tietoliikennekatkosten aikana.

Muutoksista, kuten uusien kytkimien asentamisesta tai konfiguraatiomuutoksista mahdollisesti aiheutuvista häiriöistä tiedottaminen etukäteen koettiin sekä hyväksi että huonoksi noin kolmasosassa vastauksia. Tietoliikennepalveluiden turvallisuuden kuuluu oleellisesti muutosten hallinta. Pieniäkin muutoksia tehtäessä voidaan tahtomatta lisätä uusia, merkittäviä vikoja. Teknologian, laitteiden tai verkkojen muutokset voivat aiheuttaa uhkia. Tipakkeen toipumissuunnitelmassa tulee huomioida tiedotusjärjestelyt jatkuvuuden ollessa uhattuna. On huomioitava, että organisaation ympäristön ollessa jatkuvassa muutoksessa myös tietoturvatarpeet muuttuvat jatkuvasti. Tietoturvatarpeita on arvioitava jatkuvana prosessina.

Myös tapahtuneiden häiriötilanteiden syyt, vaikutukset ja ratkaisut koettiin tiedotettavan sekä hyvin että huonosti noin kolmasosassa vastauksia. IT-riskien hallinnan tavoitteena on organisaatioon IT:n kautta vaikuttavien riskien tunnistaminen. Tipakkeen tulee varmistua siitä, että koko organisaatio tutustuu toimintaan liittyviin riskeihin oppien niistä hyviä toimintatapoja tulevia vastaavia tilanteita varten. IT-riskien hallinnan tulee kuulua ennalta määritettyjen henkilöiden työnkuvaan sen sijaan, että henkilöstön oletettaisiin suorittavan vaadittavia toimia omasta aloitteestaan.

Viestintä ja tiedottaminen -aihepiirin vastausjakauma on esitetty taulukossa 13.

Taulukko 13. *Viestintä ja tiedottaminen -aihepiirin vastausjakauma.*

	1	2	3	4	5	Yhteensä	Keskiarvo
Tiedän, millaisissa häiriötilanteissa minun on tiedotettava esimiestäni ja / tai Service Deskiä	1	1	3	11	7	23	3,96
Saan tiedon alkaneesta häiriötilanteesta riittävän nopeasti	1	6	3	8	4	22	3,36
Sisäinen viestintämme on häiriötilanteiden aikana riittävää ja selkeää ja pysyn tilanteen tasalla	2	5	7	8	1	23	3,04
Tavoitan häiriötilanteessa tarvittavat henkilöt helposti	0	5	8	9	1	23	3,26
Mahdollisesti häiriötä aiheuttavista toimenpiteistä (kuten uuden kytkimen asennus tai konfiguraatiomuutos) tiedotetaan riittävästi etukäteen	3	4	8	7	1	23	2,96
Saan riittävästi tietoa tapahtuneiden häiriötilanteiden syistä, vaikutuksista ja ratkaisuista	3	5	6	7	2	23	3
Yhteensä	10	26	35	50	16	137	3,26

6.4.5 Resurssit

43 % vastaajista koki omaavansa hyvin tai erinomaisesti aikaa työtehtävien tekemiseen huolellisesti, mutta 39 % vastaajista koki ajan olevan riittämätöntä työtehtävien huolelliseen tekemiseen. Huolelliseen työn dokumentointiin koki omaavansa hyvin tai erinomaisesti aikaa 26 % vastaajista, kuitenkin aikaa koettiin olevan huonosti tai hyvin huonosti 52 % vastauksista. Muiden tekemään dokumentaatioon ja ohjeiden lukemiseen koki olevan huonosti tai erittäin huonosti aikaa 61 % vastaajista.

Työssä tarvittavia ohjeita piti riittämättöminä, vanhentuneina ja epäselvinä 52 % vastaajista. Varahenkilöjärjestelyissä huomioitiin lomat ja poissaolot huonosti tai erittäin huonosti 48 % vastaajien mielestä. 26 % vastaajista koki, että työtehtävien määrä mahdollistaa lyhytaikaisen sijaistamisen, mutta 39 % vastaajista koki työtehtävien määrän vaikeuttavan lyhytaikaista sijaistamista.

Työtehtävien huolelliseen tekoon koki olevan riittävästi aikaa hieman yli kolmannes vastaajista, noin yhtä moni koki aikaa olevan liian vähän. Liian vähäiset resurssit aiheuttavat stressiä, uupumusta ja huolimattomuutta. Henkilöstön kokemaa stressiä vaikuttaa organisaation sairauspoissaoloihin niitä kasvattavasti (Joensuu et. al. 2008, s. 18). Tämä puolestaan laskee asiakastyytyväisyyttä. Jatkuvuudenhallinnan kannalta on huomioitava, että henkilöt saattavat tehdä katastrofaalisia päätöksiä IT-riskien aiheuttamien, selkeästi virheellisten tietojen perusteella resurssien puutteesta johtuen. Tipakkeen johdon tulee tunnistaa jatkuvuuden turvaamisen vaatimukset ja osoittaa tarvittavat resurssit jatkuvuuden turvaamisen edellyttämiin toimiin. Johdon tehtäviin kuuluu myös henkilöllisten resurssien jatkuva varmistaminen. Jatkuvuussuunnitelmien testaamisella voidaan arvioida, ovatko asetetut palvelutasot realistiset ja saavutettavissa olemassa olevilla resursseilla.

Tehdyn työn huolelliseen dokumentointiin koki olevan liian vähän aikaa yli puolet vastaajista. Suurin osa vastaajista koki myös, että aikaa ei ole riittävästi perehtyä muiden tekemään dokumentaatioon ja ohjeisiin. Dokumentointi on yksi normaalitoiminnan jatkuvuutta edistävästä toimenpiteistä. Häiriötilanteissa toiminnan palauttaminen ennalleen tehostuu, jos dokumentaatio on hyvin tehtyä. Dokumentoinnilla vähennetään myös avainhenkilöihin liittyviä riskejä. Puutteellinen dokumentaatio voi aiheuttaa operatiivisia normaalitilaan vaikuttavia riskejä vahinkojen, virheiden, epäonnistumisten ja laatupoikkeamien muodossa, jos toimintatavat eivät ole yhtenäisiä dokumentaation mukaisesti.

Työssä tarvittavia ohjeita piti riittämättöminä, vanhentuneina ja epäselvinä yli puolet vastaajista. Käyttöturvallisuuden hyvien käytäntöjen mukaisesti tietojärjestelmien käytön tulee olla selkeästi ohjeistettua. Järjestelmien ja niihin liittyvien menettelytapojen tulee olla ajantasaisesti dokumentoituja. Tietoriskien hallinnan perusvaatimusten mukaisesti tiedolle tulee määritellä oikeellisuus-, käytettävyyden- ja luottamuksellisuusvaatimukset.

Näiden vaatimusten mukaisesti luodaan menettelyt ja keinot, joilla varmistetaan tiedon ja järjestelmien ajantasaisuus. Tiedon elinkaaren hallinnan parhaiden käytäntöjen mukaisesti dokumentaatio on katselmoitava ja päivitettävä vähintään vuosittain.

Varahenkilöjärjestelyjä piti riittämättöminä puolet vastaajista. Myös sijaistaminen koettiin hankalaksi työtehtävien määrän takia yli neljännessä vastauksia. Varahenkilöjärjestelyt ovat yksi riskienhallinnan keinoista, jonka avulla voidaan pyrkiä torjumaan riskin toteutumisesta aiheutuvaa haittaa. ISO/IEC 27031 -standardi määrittelee henkilöstön eli asiantuntijat ja varahenkilöt, joilla on riittävä osaaminen yhdeksi seitsemästä ICT-valmiuden pääelementistä. Jatkuvuussuunnitelmassa tulee olla jatkuvuuden turvaamisiosio, jossa esitetään muun muassa IT-järjestelmien varmistuksiin liittyvät asiat ja varahenkilöjärjestelyt. Häiriötilanteiden varalta on huomioitava tarvittavat varahenkilöjärjestelyt ja toiminnassa on huomioitava henkilöstön lomat, poissaolot, työnkierto ja väliaikaisjärjestelyt sekä henkilöstön valmentaminen henkilöstöturvallisuuden eli henkilöstöstä aiheutuvien riskien hallitsemiseksi.

Resurssit -aihepiirin vastausjakauma on esitetty taulukossa 14.

Taulukko 14. Resurssit -aihepiirin vastausjakauma.

	1	2	3	4	5	Yhteensä	Keskiarvo
Minulla on aikaa tehdä työtehtäväni huolellisesti	3	6	4	9	1	23	2,96
Minulla on aikaa dokumentoida työni huolellisesti	5	7	5	5	1	23	2,57
Minulla on aikaa perehtyä muiden tekemään dokumentaatioon ja lukea ohjeita	4	10	4	5	0	23	2,43
Työssä tarvitsemiani ohjeita on riittävästi ja ne ovat ajantasaisia ja selkeitä	3	9	8	3	0	23	2,48
Lomat ja poissaolot on huomioitu riittävästi varahenkilöjärjestelyissä	8	3	8	4	0	23	2,35
Työtehtävieni määrä mahdollistaa lyhytaikaisen sijaistamisen	5	4	8	6	0	23	2,65
Yhteensä	28	39	37	32	2	138	2,57

6.4.6 Vastuut

74 % vastaajista tiesi hyvin tai erinomaisesti, kuinka toimia häiriötilanteissa. Eri henkilöiden ja tiimien tehtävät ja vastuut häiriötilanteissa tunsivat hyvin tai erinomaisesti 52 % vastaajista, toisaalta 17 % tunsivat tehtävät ja vastuut huonosti tai hyvin huonosti. 74 % vastaajista koki hallitsevansa vastualueensa hyvin tai erinomaisesti. Määritettyjä vastualueita piti hyvin tai erittäin selkeinä 35 % vastaajista, kuitenkin 35 % vastaajista piti määritettyjä vastualueita epäselvinä tai hyvin epäselvinä.

Vastaajista 35 % luotti, että muut pystyvät hoitamaan hänen vastualueensa tehtävät poissaolon aikana. Toisaalta 22 % vastaajista ei luottanut, että muut pystyvät hoitamaan vastualueet poissaolon aikana. Vastuualueisiin koettiin olevan saatavilla ainakin yksi

asian hallitseva varahenkilö 48 % vastauksista. Riittäviä Tipakkeen henkilöstön osaamisalueiden ja koulutuksen tietoja piti huonosti tai hyvin huonosti saatavilla 52 % vastaajista. 78 % vastaajista koki pystyvänsä vaikuttamaan hyvin tai erinomaisesti häiriötilanteista palautumiseen työtehtäviensä ja osaamisensa puolesta.

Lähes kaikki kyselyyn vastanneet tietävät, kuinka heidän tulee toimia häiriötilanteissa, lisäksi Tipakkeen työntekijät kokevat myös hallitsevansa vastuualueensa hyvin tai erinomaisesti. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilöstö. ISO/IEC 27031 -standardin suositusten mukaan Tipakkeen tulee varmistaa, että jatkuvuudenhallinnasta vastuulliset henkilöt ovat riittävän osaavia tehtäviinsä.

Eri henkilöiden tehtävät ja vastuut tiedettiin pääsääntöisesti hyvin. Hieman yli kolmannes piti määriteltyjä vastuualueita selkeinä ja yhtä suuri joukko piti vastuita epäselvinä. IT-riskien hallitsemiseksi on määriteltävä henkilöstön roolit ja niihin oikeat vastuuhenkilöt. IT-riskien hallintaroolit on sovitettava olemassa oleviin rakenteisiin, jos se on mahdollista toteuttaa luontevasti. Uusia rooleja on tarvittaessa luotava esimerkiksi osastojen välille. On myös varmistettava siitä, että jokainen osa-alue on varmasti jonkun vastuulla. Toipumissuunnitelmassa on määriteltävä toimintaohjeet häiriöistä toipumiseen siten, että se sisältää vastuut ja toimintaohjeet normaaliolojen häiriötilanteissa. On tärkeää lisäksi tiedostaa henkilöstön moninaiset roolit ja vastuut häiriötilanteissa. Erityisesti häiriötilanteisiin koulutetut henkilöt alkavat toimimaan, ottamaan vastuuta ja hallitsemaan tapahtumia häiriötilanteissa joidenkin jäädessä toimintakyvyttömiksi. Häiriötilanteiden aiheuttama stressi voi heikentää toimintakykyä myös koulutetussa henkilöstössä.

Kolmannes vastaajista pystyi luottamaan tehtäviensä hoitoon poissa ollessaan. Viidennes vastaajista ei luottanut tehtäviensä hoitoon poissaolojen aikana. Tyypilliset vahinkoriskit liittyvät henkilöstöön, kuten henkilöstön poissaoloihin ja kompetenssin riittämättömyyteen. Riittämätön henkilöstö voi johtaa myös operatiivisiin riskeihin. Näihin riskeihin voidaan varautua laatimalla toimintasuunnitelmien erilaisten tilanteiden varalle.

Noin puolet kyselyyn vastanneista koki, että heidän vastuualueisiinsa on saatavilla ainakin yksi asian hallitseva varahenkilö. Jos vastuualueeseen ei ole saatavilla asian hallitsevia varahenkilöitä, on kyseessä avainhenkilöriski, joka on operatiivinen riski. Avainhenkilöihin liittyviä riskejä voidaan pyrkiä pienentämään parantamalla dokumentointia ja kouluttamalla henkilöstöä. Avainhenkilöt on tunnistettava ja heidän käytettävyytensä on varmistettava avainhenkilöriskien hallitsemiseksi. Jatkuvuussuunnitelmia testattaessa tunnistetut avainhenkilöt voidaan jättää testitilanteen ulkopuolelle, jotta saadaan selville organisaation toimintakyky ilman avainhenkilöä.

Eri henkilöiden osaamisalueet ja koulutuksen riittävät tiedot olivat huonosti saatavilla useimpien mielestä. ISO/IEC 27031 -standardi suosittaa, että koulutuksesta, osaamisesta,

taidoista, kokemuksesta ja pätevyyksistä ylläpidetään tarvittavat tiedot. Eräs keino osaamisen selvittämiseen on osaamiskartoitus.

Osaamisen tunnistamisella saadaan tietää, kuka tietää ja osaa mitäkin ja kuka osaa parhaiten tietyn työn. Osaamiskartoituksella voidaan selvittää organisaation osaaminen ja kehittämiskohteet. Eri tapoja suorittaa osaamiskartoitus ovat kehityskeskustelut, itsearviointi, kyselyt ja haastattelut. Osaamisen arviointiin voidaan käyttää erityistä pätevyyshenkilöä tai ulkopuolisia konsultteja. Kartoitusten avulla voidaan myös laatia suunnitelmia tiedolliseen tavoitetilään pääsemiseksi. (Viitala, 2003). Osaamisen hyödyntämisessä organisaatiotasolla on keskeistä saada henkilöstön osaaminen integroitua organisaation osaamispäähän. Tämän toteuttamiseen tarvitaan tietojohtamista. (Stähle & Grönroos, 1999).

Jos osaamista ei johdeta, se on hajanaista eikä se palvele organisaation toimintaa tehokkaasti. Osaamisen kehittyminen organisaation toiminnan mukana eli osaamispääoman muodostuminen vaatii johtamista. Tällä johtamisella tulee olla oma näkyvä prosessi, jolla on tavoitteet ja mittarit, joilla tavoitteiden saavuttamista voidaan mitata. Osaamisen johtamisen pitää olla samaan tapaan vastuutettua ja aikataulutettua kuin mikä muu tahansa johtamisen osa-alue. Prosessin lopullisena tavoitteena on organisaation arvon kasvattaminen ja toiminnassa menestyminen. Johtajatasolla osaamisen johtamisen prosessi kuvataan ja siihen sisältyy selkeät toiminnalliset tavoitteet. Oppimistarpeiden selvittäminen, kommunikointi osaamistarpeista ja olemassa olevan osaamisen selvittäminen osaamiskartoitusten avulla ovat tärkeitä. On laadittava osaamisstrategia, jossa määritellään tärkeimmät ja kriittisimmät osaamisalueet ja niissä olevat puutteet. Osaamisen kehittämissstrategiassa asetetaan tavoitteet kehittämistoimenpiteistä. Strategioita toteutetaan sekä rekrytoinnin eli uuden osaamisen että kehittämissohjelmien eli olemassa olevan osaamisen avulla. (Ojala, 2008).

Lähes kaikki kokivat voivansa vaikuttaa häiriötilanteista palautumiseen työtehtäviensä ja osaamisensa puolesta. Mahdollisimman nopea palautuminen häiriötilanteista on kriittistä organisaation toimintakyvyn kannalta. Tipakkeen palvelupisteen ollessa tavallinen yhteydenottokanava häiriötilanteiden aikana on varmistuttava, että asiakaspalvelussa työskentelevät henkilöt kykenevät kommunikoimaan asiakkaille häiriötilanteista tavalla, joka ei vaikuta asiakaskokemukseen negatiivisesti. Hyvin hoidetut kriisitilanteet saattavat kasvattaa organisaation mainetta jopa korkeammalle kuin se oli ennen kriisitilannetta. On hyvin tärkeää, että henkilöstö ymmärtää jatkuvuussuunnittelun käytön ja siihen osallistumisen tärkeyden. ISO/IEC 27031 -standardi suosittelee, että jatkuvuudenhallintaan allokoitun henkilöstön riittävä kyvykkyys suoritua vaadittavista tehtävistä varmistetaan selvittämällä koulutustarpeet ja tarjoamalla tarvittavaa koulutusta.

Vastuut -aihepiirin vastausjakauma on esitetty taulukossa 15.

Taulukko 15. Vastuut -aihepiirin vastausjakauma.

	1	2	3	4	5	Yhteensä	Keskiarvo
Tiedän, kuinka minun tulee toimia häiriötilanteissa	0	2	4	14	3	23	3,78
Tiedän Tipakkeen eri henkilöiden ja tiimien tehtävät ja vastuut häiriötilanteissa	2	2	7	10	2	23	3,35
Koen hallitsevani vastuualueeni riittävän hyvin	0	0	6	11	6	23	4
Määritetyt vastuualueet ovat selkeät	2	6	7	5	3	23	3,04
Voin luottaa, että poissaollessani muut pystyvät hoitamaan vastuualueeni	0	5	10	6	2	23	3,22
Vastuualueisiini on saatavilla ainakin yksi asian hallitseva varahenkilö	3	1	8	8	3	23	3,3
Tipakkeen eri henkilöiden osaamisalueista ja koulutuksesta on saatavilla riittävät tiedot	3	9	6	5	0	23	2,57
Pystyn vaikuttamaan häiriötilanteista palautumiseen työtehtävieni ja osaamiseni puolesta	0	1	4	16	2	23	3,83
Yhteensä	10	26	52	75	21	184	3,39

6.5 Jatkuvuudenhallinnan kehittämisen ratkaisumalli

Tipakkeen jatkuvuussuunnitteluprosessi on tällä hetkellä henkilöstön kouluttamista ja jatkuvuussuunnitelman testaamista vaille valmis. Ivarin & Laaksosen (2009, s. 22-23), Kliemin & Richien (2015, s. 95) ja Craigin (2001) mukaan jatkuvuussuunnittelun tulee kuitenkin olla jatkuva prosessi, joten Tipakkeen jatkuvuussuunnitteluprosessin ensimmäisen syklin eli iteraation voidaan ajatella olevan lähes valmis. Jatkuvuussuunnitteluprosessi ei itsessään PDCA-ideologian mukaisena jatkuvana prosessina pääty kaikkien vaiheiden suorittamisen jälkeen.

NIST:n määrittelemän jatkuvuussuunnitteluprosessin vaiheiden mukaisesti jatkuvuudenhallintatoimenpiteet tulisi kouluttaa Tipakkeen henkilöstölle koulutussuunnitelman mukaisesti. Tämän jälkeen jatkuvuussuunnitelman kyky vastata tositilanteisiin tulisi testata testaussuunnitelmassa määritetyllä tavalla. Testauksessa havaitut kehittämiskohteet tai puutteet johtavat uusiin kehittämistarpeisiin ja jatkuvuussuunnitteluprosessin uusi iteraatio käynnistyy. Tämä voi tapahtua myös muista syistä, kuten organisaatiossa tapahtuvista suurista muutoksista, uuden teknologian käyttöönotosta tai ajan kulumisesta eli katselmoinnin tullessa ajankohtaiseksi.

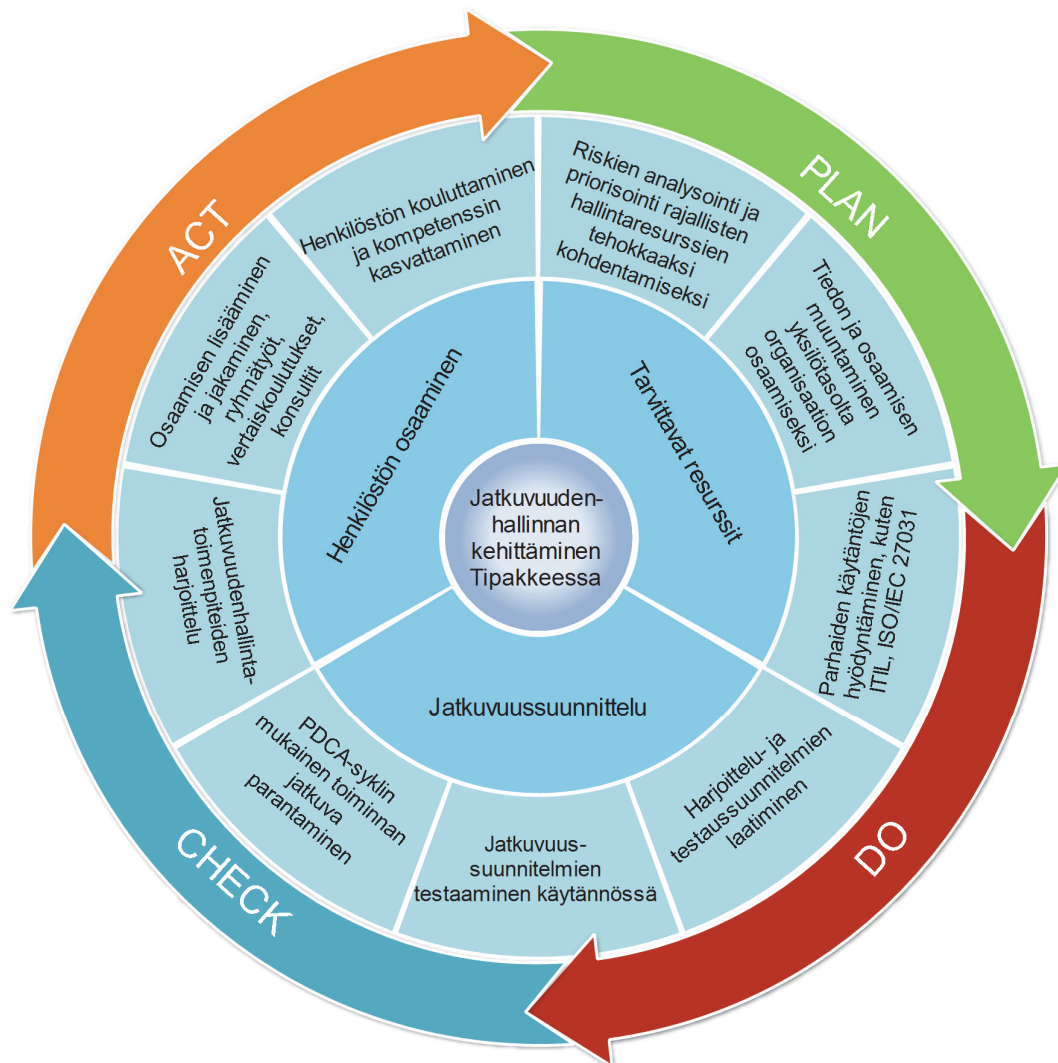
Nykytilan analyysin ja kyselytutkimuksen tulosten perusteella Tipakkeen jatkuvuudenhallinnassa havaittiin useita kehittämiskohteita. Keskeisimmät kehittämiskohteet olivat nykytilan analyysissä havaittu harjoittelu- ja testaussuunnitelmien puute ja kyselytutkimuksessa havaittu henkilöstön osaamiseen ja resurssien riittävyyteen liittyviin riskeihin varautuminen.

Keskeisimpien kehittämiskohteiden pohjalta laadittiin ratkaisumalli Tipakkeen jatkuvuudenhallinnan kehittämisen työkaluksi. Laadittu ratkaisumalli sijoittuu NIST:n

määrittelemässä jatkuvuussuunnitteluprosessissa pääosin ”suunnitelman dokumentointi, testaus ja ylläpito” -vaiheeseen. Ratkaisumalliin sisältyy kuitenkin elementtejä jatkuvuussuunnitteluprosessin jokaisesta vaiheesta, sillä jokaisessa kehittämissyklissä jatkuvuussuunnitteluprosessi etenee vaihe vaiheelta koordinoinnista, ohjeistuksesta ja vastuutuksesta aina testausvaiheeseen asti.

Laadittu ratkaisumalli noudattaa PDCA-syklin mukaista jatkuvan parantamisen ideologiaa. Kun ratkaisumallin kehittämistoimenpiteet on suoritettu, toiminnan taso arvioidaan uudelleen. Tässä tutkimuksessa suoritettun kyselytutkimuksen tuloksia voidaan käyttää lähtöarvoina toiminnan kehittymistä arvioitaessa. Kehittämistoimenpiteiden onnistuneisuutta voidaan mitata ja arvioida suorittamalla uusi kyselytutkimus ja vertaamalla siinä saatuja tuloksia lähtöarvoihin.

Tipakkeen keskeisimpien kehittämiskohteiden ratkaisumalli on esitetty kuvassa 17.



Kuva 17. Tipakkeen keskeisimpien kehittämiskohteiden ratkaisumalli.

Laaditun ratkaisumallin keskiössä on sen perimmäinen tavoite eli Tipakkeen jatkuvuudenhallinnan kehittäminen. Seuraavat kolme sektoria ovat tavoitteen saavuttamiseksi tarvittavat havaitut kehityskohteet. Viimeiset yhdeksän sektoria kuvaavat havaittujen kehittämiskohteiden toteuttamiseksi tarvittavia toimenpiteitä yleisellä tasolla. Sektoritason jaottelua voidaan hyödyntää esimerkiksi työnjaossa jakamalla tavoitteen saavuttamiseksi tarvittavat kehityskohdesektorit tiimitasolle ja kehittämiskohteiden toteuttamiseksi tarvittavat toimenpiteet henkilö- tai pienryhmätasolle. Sektoritasoinen jaottelu helpottaa myös kehittämistoimenpiteiden edistymisen seurantaa, koska kehittämistoimenpiteet on jaoteltu pienempiin kokonaisuuksiin.

Jatkuvuussuunnittelu -sektori käsittää harjoittelu- ja testaussuunnitelmien laatimisen, jatkuvuussuunnitelmien testaamisen käytännössä sekä PDCA-syklin mukaisen jatkuvan parantamisen.

Harjoittelu- ja testaussuunnitelmat laaditaan Cerullon & Cerullon (2004, s. 71) mukaan luomalla jatkuvuudenhallintatoimenpiteiden testaus- ja arviointimenetelmät sekä arviointikriteerit eli tavoitteet. ISO/IEC 27031 -standardin (2011, s. 22-23) mukaisessa harjoittelu- ja testausohjelmassa määritellään harjoitusten tiheys, laajuus ja muoto. Harjoittelu ja testaaminen eroavat toisistaan ainoastaan tavoitteiden osalta. Jatkuvuussuunnitelman kykyä vastata häiriöihin ei voida selvittää ilman testaamista.

Tipakkeessa on mahdollista rakentaa suljettuja verkkoympäristöjä häiriötilanteiden simuloimiseksi harjoittelua varten. Tipakkeessa tulisi myös harkita tunnistettujen avainhenkilöiden sulkemista harjoitusten ulkopuolelle operatiivisten riskien vaikutusten selvittämiseksi sekä avainhenkilöriskejä vähentävien toimien, kuten dokumentoinnin riittävyden arvioimiseksi. Valtiovarainministeriön (2012, s. 35) mukaan selkeä dokumentaatio ja harjoittelu ovat edellytyksenä toimia häiriötilanteissa.

Tipakkeen jatkuvuudenhallinnan jatkuva parantaminen PDCA-syklin mukaisesti toteutetaan harjoittelun ja testaamisen avulla. Uusien toimintatapojen soveltuvuus toimintaan selvitetään testaamalla ja hyväksi havaitut toimintatavat harjoitellaan.

Henkilöstön osaaminen -sektori käsittää jatkuvuudenhallintatoimenpiteiden harjoittelun, osaamisen lisäämisen ja jakamisen sekä henkilöstön kouluttamisen ja kompetenssin kasvattamisen.

Morwoodin (1998, s. 30-31) mukaan jatkuvuudenhallintatoimenpiteiden harjoittelulla varmistetaan henkilöstön osaaminen häiriötilanteissa. Harjoittelu voi myös paljastaa jatkuvuussuunnitelmissa piileviä puutteita ja täten tuoda esiin uusia kehittämiskohteita. ISO/IEC 27031 -standardin mukaisessa harjoittelussa käydään lävitse kaikki palvelun toimittamiseen vaadittavat osuudet. ISO/IEC 27031 (2011, s. 23) -standardin mukaan harjoittelulla koulutetaan myös henkilöstöä ja varmistetaan osaamisen riittävydestä jatkuvuudenhallinnan toteuttamiseksi.

Ilmonen et. al. (2010, s. 72-73) määrittelevät osaamisen kehittämisen ja johtamisen ongelmat IT-riskeiksi. Iivari & Laaksonen (2009, s. 148-149) puolestaan korostavat osaamisen merkitystä jatkuvuudenhallinnassa, jotta henkilöstö on harjaantunutta ja kykenevää suorittamaan jatkuvuudenhallintatoimenpiteitä. Virtainlahden (2009) mukaan henkilöstön välinen yhteistyö tiedon ja osaamisen levittämisessä soveltuu erittäin hyvin tiimipohjaisissa organisaatioissa toteutettavaksi, millainen Tipake on. Tiimityöskentely synnyttää vuorovaikutusta yksilöiden välille, jossa tiimin jäsenet käyttävät henkilökohtaista osaamistaan yhteisen päämäärän saavuttamiseksi levittäen samalla osaamistaan muihin.

Viitala (2003) mainitsee, että henkilöstön kehittämisessä voidaan hyödyntää henkilökohtaisia kehittämissuunnitelmia. Näiden tarkoituksena on havaita henkilön kehittämistarpeet, tuoda ne esimiestason tietoon toteuttamisen mahdollistamiseksi ja saada täysi käsitys olemassa olevasta osaamisesta. Tipake voi käyttää henkilökohtaisia kehittämissuunnitelmia henkilöstön osaamisen kehittämisen suuntaamiseksi Tipakkeen kannalta hyödylliseen suuntaan, kuten uusiin teknologioihin tai tuleviin johto- ja esimiestehtäviin. Tipakkeen olemassa olevan osaamisen tunnistaminen ja dokumentointi on tunnistettu kehittämiskohteeksi myös toteutetussa kyselytutkimuksessa. Ilmonen et. al. (2010, s. 71-72) korostavat, että organisaation riittämätön kompetenssi strategisesti tärkeimmillä osa-alueilla tai kompetenssivajeen tunnistamisessa epäonnistuminen ovat strategisia eli pidemmän aikavälin tavoitteiden saavuttamista vaikeuttavia riskejä. ISO/IEC 27031 -standardi (2011, s. 11-12) suosittelee tietojohtamista, dokumentointia ja osaamisen hajauttamista useille henkilöille keinoina jatkuvuudenhallinnassa tarvittavan tiedon ja osaamisen ylläpitämiseen.

Tarvittavat resurssit -sektori käsittää riskien analysoinnin ja priorisoinnin, tiedon ja osaamisen muuntamisen organisaation osaamiseksi sekä parhaiden käytäntöjen hyödyntämisen.

Aven (2010, s. 177) korostaa organisaation johdon merkitystä riskienhallinnan onnistumisessa. Tipakkeessa voitaisiin hyötyä riskienhallintakulttuurin viestinnästä ja koulutuksesta, jolloin henkilöstön kompetenssi, ymmärrys ja motivaatio riskienhallintaan kasvavat. Iivari & Laaksonen (2009, s. 123-124) lisäävät, että riskianalyyssissä tulee huomioida kaikki oleelliset liiketoimintaprosessit, ei ainoastaan IT-asioihin liittyviä riskejä. Tästä syystä Tipakkeen riskianalyyssissä voidaan tarvittaessa hyödyntää Tipakkeen ulkopuolisia asiantuntijoita esimerkiksi riskien realisoidumisen taloudellisten vaikutusten arvioimisessa.

Tipakkeessa ei ole toteutettu vielä riskien kustannusvaikutusanalyyssiä, jota voidaan hyödyntää riskejä priorisoitaessa. Kustannusvaikutusanalyyssillä voitaisiin selvittää esimerkiksi Tipakkeelle optimaaliset vasteajat ulkoisten palveluntarjoajien tuki- ja huoltosopimuksiin. Snedaker (2007) korostaa, että aina toimiva palvelu on erittäin kallis toteuttaa ja tästä syystä suojauksen tasoa valittaessa on huomioitava organisaation kyky

toimia ilman suojattavaa kohdetta ja suojaukseen käytettävissä olevat resurssit. Doughtyn (2001) mukaan kustannusvaikutusanalyysillä pystytään saavuttamaan tasapaino riskien ja niiden ehkäisemisestä aiheutuvien kustannusten välillä. Oikean tasoiset suojaukset vaikuttavat positiivisesti Tipakkeeseen alentuneina kustannuksina sekä kriittisten palveluiden parempana toimintavarmuutena.

Tipakkeen tulee pyrkiä levittämään henkilöstöön sitoutunutta yksilötason osaamista henkilöstön sisällä toiminnan kehittämiseksi. Stähle & Grönroos (1999) korostavat, että organisaatio ilman osaamis pääomaa ei ole kilpailukykyinen, eikä tätä resurssia pystytä korvaamaan muilla resursseilla, kuten rahalla. Otalan (2008) mukaan organisaation rakenteet, teknologia, tietojärjestelmät, toimintatavat ja organisaatiokulttuuri ovat tekijät, jotka mahdollistavat henkilöstön osaamisen kehittämisen organisaation tarpeiden mukaiseksi ja organisaation yhteiseksi osaamiseksi. Tipake voi edistää osaamisen levittämistä tukemalla tiimi- ja ryhmätyötä sekä kehittämällä johtamiskulttuuria ja ilmapiiriä yhteistyötä ja osaamisen levittämistä tukevaksi. Käytännössä tämä voi tarkoittaa esimerkiksi tiimi- tai ryhmäkohtaisia kannustepalkkioita henkilökohtaisen suoriutumisen perusteella maksettavien kannustepalkkioiden sijaan sekä koulutuksen arvostamista ja siihen tukemista. Tipakkeen esimiehet ovat keskeisessä asemassa tiedon levittämisen puitteiden luomisessa.

ISO/IEC 27031 -standardin (2011, s. 28) suosituksen mukaan jatkuvuudenhallintatoimenpiteiden tason ja laadun seuraaminen on oleellista jatkuvuudenhallinnan kehittämisessä. Tipakkeen tulisi määritellä seurattavat tehokkuuskriteerit, joiden toteutumista valvotaan. Tipakkeen tapauksessa voidaan hyödyntää sekä määrällisiä että laadullisia kriteereitä jatkuvuudenhallinnan tehokkuuden mittaamisessa. Tipakkeen toimintaan hyvin soveltuvia, ISO/IEC 27031 -standardin mukaisia määrällisiä tehokkuuskriteereitä ovat esimerkiksi havaittuihin häiriöihin kulunut havaitsemis- ja korjausaika sekä sellaisten häiriöiden lukumäärä, joita ei voida tehokkaasti hallita vaikutusten vähentämiseksi. Nämä tiedot ovat saatavilla Tipakkeen toiminnanohjausjärjestelmästä. Vastaavia laadullisia tehokkuuskriteereitä ovat esimerkiksi asiakaspalautteet ja suoritettavien kyselyiden tulokset.

Tipake suorittaa tällä hetkellä säännöllisesti vuosittain asiakaskyselyn, jossa pyydetään arvioimaan myös jatkuvuudenhallintaan liittyviä asioita, kuten tietoliikenneyhteyksien ja käytössä olevien laitteiden ja sovellusten toimintavarmuutta. Kyselystä saadaan tietoa koetusta tasosta pitkällä ajanjaksolla eli siitä saatava tieto soveltuu hyödynnettäväksi pitkän tähtäimen strategisen tason suunnittelussa. On hyvä tiedostaa, että erilaisia hyviä ja testattuja käytäntöjä, kuten ISO/IEC 27031 -standardia voidaan hyödyntää toiminnassa myös osittain. Tipakkeen ei tarvitse pyrkiä täysin standardin mukaiseen, auditoitavaan toiminnan tasoon. Hyvistä käytännöistä voidaan poimia Tipakkeeseen sopivia kokonaisuuksia toiminnan parantamiseksi.

7. YHTEENVETO

Suoritetun nykytilan analyysin ja kyselytutkimuksen perusteella Tipakkeen jatkuvuudenhallinnan kannalta tärkeimmäksi kehittämiskohteeksi nousi henkilöstön osaamiseen ja resursseihin liittyviin riskeihin varautuminen. Toinen havaittu oleellinen kehittämiskohde oli jatkuvuussuunnitelmien testaaminen ja niissä mainittujen toimenpiteiden harjoittelu.

Rajallisilla resursseilla toimiminen on haasteellista, erityisesti kun tuettavien ja ylläpidettävien laitteiden ja teknologioiden määrä kasvaa jatkuvasti. Lisäresursseja ei voida saada jatkuvasti, joten tilanteeseen on kyettävä sopeutumaan olemassa olevilla resursseilla mahdollisimman tehokkaasti. Olemassa olevan henkilöstön tieto- ja osaamispotentiaali on saatava hyödynnettyä mahdollisimman tehokkaasti.

Tipakkeen on analysoitava, arvoitettava ja priorisoitava sitä uhkaavat riskit rajallisten riskienhallintaresurssien tehokkaaksi kohdentamiseksi. Henkilöstön koulutuksella ja siihen tukemisella voidaan kasvattaa henkilöstön kompetenssia. Henkilöstön yleistä osaamistasoa voidaan kasvattaa erilaisilla ryhmätyömenettelyillä ja sisäisillä vertaiskoulutuksilla. Tipakkeen esimiehillä on keskeinen vastuu johtaa organisaation oppimisprosessia, jolla henkilöstöön sitoutunutta, yksilötason osaamista muunnetaan organisaation osaamispääomaksi. Tipakkeen kannalta tärkeimmät osaamispääomaa kasvattavat tekijät ovat henkilöstön määrä, koulutus, osaamistaso ja oppimishalu.

Tipakkeen jatkuvuussuunnitelmat ovat tällä hetkellä lähes valmiita. Nykytilan arviointia, jatkuvuussuunnitelman perustana olevien riskiskenaarioiden läpikäyntiä ja parhaiden käytäntöjen hyödyntämistä on tehty jatkuvuussuunnitelmia laadittaessa. Jatkuvuussuunnitelmien harjoittelua ja siitä seuraavaa oppimista ei ole vielä päästy toteuttamaan. Seuraavan vaiheen Tipakkeen jatkuvuussuunnitteluprosessissa tulisi olla jatkuvuutta edistävien toimenpiteiden koulutus, harjoittelu ja sitä kautta saavutettava toiminnan jatkuva parantaminen. Tämän jälkeen jatkuvuussuunnitelmia tulee testata käytännössä. Tätä varten Tipakkeen tulee luoda harjoittelu- ja testaussuunnitelmat.

Tipakkeen tulee kouluttaa henkilöstöään jatkuvuussuunnitelmiin sisältyvien asioiden osalta henkilöstön tehtävien ja vastuiden edellyttämällä tavalla jatkuvuussuunnitelmien valmistuttua. Jatkuvuudenhallintatoimenpiteiden koulutuksella ja harjoittelulla pystytään parantamaan henkilöstön reagoitinopeutta ja erilaisten häiriöskenaarioiden harjoittelu luo rutiinia toimia vastaavissa tilanteissa aikaisempaa paremmin. Lisäksi koulutuksella ja harjoittelulla varmistetaan henkilöstön oikeat toimintatavat, kasvatetaan kompetenssia ja vähennetään hätäntymistä häiriötilanteiden ollessa ennalta tuttuja. Jatkuvuudenhallintatoimenpiteiden kouluttaminen, harjoittelu ja testaaminen on välttämätöntä palautumisen varmistamiseksi tositilanteissa.

Jatkuvuudenhallinnan kehittämisen toteutumista ja jatkokehitystä ajatellen suoritettu kyselytutkimus voidaan toistaa esimerkiksi puolen vuoden kuluttua, kun kehittämistoimenpiteet on suoritettu. Havaittujen kehittämissuositusten vaikutukset voidaan selvittää vertaamalla tässä tutkimuksessa saatuja havaintoja uudelleen suoritettun kyselytutkimuksen tuloksiin. Vastaavasti henkilöstön tietoutta ja osaamista jatkuvuudenhallinnasta voidaan mitata koulutuksen ja harjoittelun jälkeen, jotta voidaan varmistua koulutuksen ja harjoittelun parantaneen suoriutumista aikaisemmin tunnistetuissa kehittämiskohteissa.

LÄHTEET

Aven, T. (2010). Risk Management. Teoksessa Grimvall, G., Holmgren, Å., Jacobsson, P. & Thedéen, T. (2010) Risks in Technological Systems. S. 174-198.

Basin, D., Schaller, P. & Schläpfer, M. (2011). Applied Information Security. A Hands-on Approach. Saksa, Springer-Verlag Berlin Heidelberg. 202 s.

Carr, H. & McManus, D. (2001). Risk and the Need for Business Continuity Planning. Teoksessa Doughty, K. (2001). Business Continuity Planning: Protecting Your Organization's Life.

Cerullo, V. & Cerullo, M. (2004). Business Continuity Planning: A Comprehensive Approach. Information Systems Management, Vol. 21, Issue 3, s. 70-78.

Craig, S. (2001). Business Continuity in the Distributed Environment. Teoksessa Doughty, K. (2001). Business Continuity Planning: Protecting Your Organization's Life.

Dederer, M. & Dmytrenko, A. (2015). 8 Steps to Effective Information Lifecycle Management. Information Management Journal, Jan/Feb 2015, Vol. 49 Issue 1, s. 32-35.

Dey, M. (2011). Business continuity planning (BCP) methodology - Essential for every business. GCC Conference and Exhibition (GCC), 2011 IEEE. Dubai, Yhdistyneet Arabiemiirikunnat. 19-22.2.2011. S. 229-232.

Doughty, K. (2001). Maintenance and Update of Business Continuity Plans. Teoksessa Doughty, K. (2001). Business Continuity Planning: Protecting Your Organization's Life.

Doughty, K. (2001). Selecting the Right Business Continuity Planning Strategies. Teoksessa Doughty, K. (2001). Business Continuity Planning: Protecting Your Organization's Life.

Ernst & Young LLP (2002). Security Survey Indicates Alarming Gaps in Information Security Planning. [Verkkosivusto]. [Viitattu 16.12.2015].
Saataavilla: <http://www.prnewswire.com/news-releases/ernst--young-2002-security-survey-indicates-alarming-gaps-in-information-security-planning-77334267.html>

Flink, A-L., Reiman, T. & Hiltunen, M. (2007). Heikoin lenkki? Riskienhallinnan inhimilliset tekijät. Helsinki, Edita Prima Oy. 306 s.

- Fåk, V. (2010). IT - Risks and Security. Teoksessa Grimvall, G., Holmgren, Å., Jacobsson, P. & Thedéen, T. (2010). Risks in Technological Systems. S. 143-160.
- Gordon, S. (2002). Watch your back. The mounting risks of unauthorized data access, theft and corruption in secondary storage. Computer Technology Review, Fourth Quarter 2002. S. 12-15.
- Humphreys, E. (2012). Are you ready? ICT readiness and business continuity. ISO Focus+, May 2012. S. 19-21.
- Iivari, M. & Laaksonen, M. (2009). Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Helsinki, Tietosanoma Oy. 273 s.
- Ilmonen, I., Kallio, J., Koskinen, J., & Rajamäki, M. (2010). Johda riskejä - käytännön opas yrityksen riskienhallintaan. Helsinki, Kustannusosakeyhtiö Tammi. 213 s.
- ISACA (2009). The Risk IT Framework. Saatavilla:
http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework-Excerpt_fm_k_Eng_0109.pdf
- ISO 22301 (2012). Societal security - Business continuity management systems - Requirements. Sveitsi, ISO. 24 s.
- ISO/IEC 27031 (2011). Information technology - Security technologies - Guidelines for information and communication technology readiness for business continuity. Sveitsi, ISO/IEC. 36 s.
- Jackson, C. (2001). The Business Impact Assessment Process. Teoksessa Doughty, K. (2001). Business Continuity Planning: Protecting Your Organization's Life.
- Joensuu, M., Kivistö, S., Malmelin, J. & Lindström, K. (2008). Pitkä sairausloma ja työhönpaluu. Työ ja ihminen. Tutkimusraportti 34. Saatavilla:
http://www.ttl.fi/fi/tyo_ja_ihminen/Documents/Tutkimusraportti_34.pdf
- Jordan, E. & Silcock, L. (2006). Strateginen IT-riskien hallinta. Helsinki, Edita Prima Oy. 339 s.
- Järveläinen, J. (2013). IT incidents and business impacts: Validating a framework for continuity management in information systems. International Journal of Information Management, Jun 2013, Vol. 33, Issue 3, s. 583-590.
- Järvinen, P. (2012). Arjen tietoturva. Jyväskylä, Docendo. 323 s.

- Karvi, T. (2012). Tietoturvan perusteet. Helsingin yliopisto. Saatavilla: http://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf
- Kliem, R. & Richie, G. (2015). Business Continuity Planning: A Project Management Approach. USA, Auerbach Publications. 402 s.
- Kuronen, T. (1998). Tietovarantojen hyödyntäminen ja demokratia - Esimerkkejä tiedon prosesseista. Helsinki, Sitra. 124 s.
- Kyrölä, T. (2001). Esimies ja tietoriskien hallinta. Juva, WS Bookwell Oy. 307 s.
- Laihonen, H., Hannula, M., Helander, N., Ilvonen, I., Jussila, J., Kukko, M., Kärkkäinen, H., Lönnqvist, A., Myllärniemi, J., Pekkola, S., Virtanen, P., Vuori, V. & Yliniemi, T. (2013). Tietojohtaminen. Tampere, Juvenes Print. 84 s.
- Lam, W. (2002). Ensuring Business Continuity. IT Pro, May/Jun 2002, s. 19-25.
- Lehtinen, R., Russell, D. & Gangemi G. (2006). Computer Security Basics 2nd Edition. USA, O'Reilly Media, Inc. 296 s.
- Mawson, T. (2003). Crucial Business Impact Analysis. Security: Solutions for Enterprise Security Leaders, Sep 2003, Vol. 40, Issue 8, s. 44.
- Morwood, G. (1998). Business continuity: awareness and training programmes. Information Management & Computer Security, Vol. 6, Issue 1, s. 28-32.
- Otala, L. (2008). Osaamispääoman johtamisesta kilpailuetu. Helsinki, WSOYpro. 378 s.
- Ranki, A. (1999). Vastaako henkilöstön osaaminen yrityksen tarpeita? Helsinki, Kauppakaari OYJ. 174 s.
- Siponen, A. (2014). SFS-ISO/IEC 27002:2014 Tietoturvallisuuden hallintakeinojen menettelyohjeet - Yleisesittely. Microsoft Oy. Saatavilla: http://www.sfs.fi/files/5608/SFS-ISO-IEC_27002_esittely_Siponen.pdf
- Snedaker, S. (2007). Business Continuity & Disaster Recovery for IT Professionals. USA, Syngress. 456 s.
- Solms, B. (2001). Corporate Governance and Information Security. Computers & Security, May 2001, Vol. 20, Issue 3, s. 215-218.
- Stähle, P. & Grönroos, M. (1999). Knowledge Management - Tietopääoma yrityksen kilpailutekijänä. Porvoo, WSOY. 218 s.

Suomen standardoimisliitto SFS Ry. (2015). [Verkkosivusto]. [Viitattu 2.10.2015]. Saatavilla: http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta

The British Standards Institution (2012). Moving from BS 25999-2 to ISO 22301. Saatavilla: <http://www.bsigroup.com/documents/iso-22301/resources/bsi-bs25999-to-iso22301-transition-uk-en.pdf>

Tietotekniikan liitto ry (2012). IT-ura-tutkimus 2012. Saatavilla: http://www.tivia.fi/sites/d7.tivia.fi/files/tivia/pdf/Palkkaraportti_7%209%202012.pdf

Tipake jatkuvuudenhallinnan toimenpiteet ja toipumissuunnitelmat (2015). Julkaisematon.

Tipake jatkuvuussuunnitelma (2015). Julkaisematon.

Tipake riskiarviointi (2015). Julkaisematon.

Torabi, S., Soufi, H. & Sahabjamnia, N. (2014). A new framework for business impact analysis in business continuity management. Safety Science, Oct 2014, Vol. 68, s. 309-323.

Tucker, G. (2015). Business Continuity from Preparedness to Recovery. A Standards Based Approach. USA, Elsevier Inc. 324 s.

VAHTI-ohjeet. Jatkuvuussuunnittelu. (2015). [Verkkosivusto]. [Viitattu 3.10.2015]. Saatavilla: <https://www.vahtiohje.fi/web/guest/jatkuvuussuunnittelu>

Valtiokonttori (2012). Riskienhallinta: Lyhyt teoria. Saatavilla: <http://valtiokonttori.fi/download/noname/%7B17B3FC7E-2AC5-4FC2-8F93-FC6B84056923%7D/84881>

Valtiovarainministeriö (2007). Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Helsinki, Edita Prima Oy. 111 s.

Valtiovarainministeriö (2012). ICT-varautumisen vaatimukset. Helsinki, Edita Prima Oy. 88 s.

Viestintävirasto. Etätyön riskit osaksi organisaation tietoturvan hallintaa. (2015). [Verkkosivusto]. [Viitattu 30.10.2015]. Saatavilla: <https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/08/ttn201508040837.html>

Viitala, R. (2003). Henkilöstöjohtaminen. Helsinki, Edita Prima Oy.

Virtainlahti, S. (2009). Hiljaisen tietämyksen johtaminen. Helsinki, Talentum. 262 s.

Vuorinen, P. & Valkonen, S. (2007). Korkeakoulutuksesta työelämään - Työhön sijoittuminen ja työelämävalmiudet kaupan ja tekniikan alalla. Saatavilla: <https://jyx.jyu.fi/dspace/bitstream/handle/123456789/47498/978-951-39-2926-8.pdf>

Wilbanks, L., Kuhn, R. & Chou, W. (2014). IT Risks. IT Pro, Jan/Feb 2014, s. 20-21.

Wrobel, L. (2001). Testing Business Continuity Plans. Teoksessa Doughty, K. (2001). Business Continuity Planning: Protecting Your Organization's Life.

LIITE A: KYSELYLOMAKE

Kysely jatkuvuudenhallinnasta

07.12.2015

Teen diplomityötä Tipakkeessa ja olen laatinut siihen liittyen kyselyn Tipakkeen henkilöstölle.

Kyselyn tarkoituksena on selvittää Tipakkeen henkilöstön käsityksiä jatkuvuudenhallinnasta sekä Tipakkeen jatkuvuudenhallinnan nykytilaa. Kyselystä saatavilla tuloksilla pyritään parantamaan Tipakkeen jatkuvuudenhallintaa. Käsitellen kyselyn tulokset organisaatiossalla eikä vastauksista voida tunnistaa yksittäistä vastaajaa.

Jatkuvuudenhallinnalla tarkoitetaan toimenpiteitä, joilla pyritään parantamaan toiminnan jatkuvuutta

- ehkäisemällä häiriötilanteiden tapahtumista
- vähentämällä häiriötilanteiden vaikutuksia ja kestoja
- palautamalla häiriötilanteista mahdollisimman tehokkaasti ja nopeasti

Häiriötilanteella tarkoitetaan toiminnan harjoittamista vaikeuttavaa tilannetta, kuten laajaa ja pitkäkestoista tietoliikennekatkosta tai tietojärjestelmien toimimattomuutta.

Arvioi väittämiä sen mukaan, miten koet väittämän pitävän paikkansa. Arviointiasteikko 1-5 on määritelty seuraavasti:

1. Täysin eri mieltä
2. Jonkin verran eri mieltä
3. Ei samaa eikä eri mieltä
4. Jonkin verran samaa mieltä
5. Täysin samaa mieltä

Voit myös kirjoittaa avoimia kommentteja aihepiireittäin.

Kiitos vastauksestasi!

Jonas Kurtto

YLEISET KÄSITYKSET**1 2 3 4 5**

Olen perehtynyt jatkuvuussuunnitteluun ja jatkuvuudenhallintaan
 Tiedän millaiset riskit muodostavat uhan toiminnan jatkuvuudelle
 Tiedän omaan työhöni liittyvät riskit
 Jatkuvuudenhallinta on tärkeää ja olen motivoitunut siihen

TIETOTURVALLISUUS JA RISKIENHALLINTA**1 2 3 4 5**

Olen perehtynyt Tipakkeen tietoturvaohjeisiin ja määräyksiin
 Noudatan annettuja tietoturvaohjeita ja määräyksiä
 Tiedostan etättyöhön liittyvät tietoturvariskit
 Fyysinen turvallisuus (kuten kulkuoikeudet, vierailijoiden valvonta) on riittävää
 Tärkeät yhteystiedot ovat helposti saatavilla sähkökatkon aikana
 Haen toimintaohjeita ensisijaisesti Internetistä
 Tipakkeen oma dokumentaatio on ensisijainen lähteeni etsiessäni toimintaohjeita

KOULUTUS JA HARJOITTELU**1 2 3 4 5**

Osaamis- ja koulutustarpeeni on selvitetty
 Saan halutessani työssä tarvitsemani koulutusta
 Tipakkeen henkilöstö on perehdytetty riittävän hyvin Tipakkeen ja sen eri palvelujen jatkuvuussuunnitelmiin
 Haluaisin saada teoriakoulutusta jatkuvuudenhallinnasta
 Haluaisin harjoitella häiriötilanteita käytännössä
 Uuden henkilön perehdytyksessä huomioidaan myös häiriötilanteiden aikaiset toimintatavat
 Tapahtuneet häiriötilanteet dokumentoidaan ja niistä pyritään oppimaan
 Tapahtuneet häiriötilanteet on syytä käydä yhdessä läpi jälkikäteen
 Jos koulutusta järjestetään, Tipakkeen sisäinen koulutus on parempi vaihtoehto kuin ulkoinen koulutus (Sovelton kurssi tms.)

VIESTINTÄ JA TIEDOTTAMINEN**1 2 3 4 5**

Tiedän, millaisissa häiriötilanteissa minun on tiedotettava esimiestäni ja / tai Service Deskiä

Saan tiedon alkaneesta häiriötilanteesta riittävän nopeasti

Sisäinen viestintämme on häiriötilanteiden aikana riittävää ja selkeää ja pysyn tilanteen tasalla

Tavoitan häiriötilanteessa tarvittavat henkilöt helposti

Mahdollisesti häiriöitä aiheuttavista toimenpiteistä (kuten uuden kytkimen asennus tai konfiguraatiomuutos) tiedotetaan riittävästi etukäteen

Saan riittävästi tietoa tapahtuneiden häiriötilanteiden syistä, vaikutuksista ja ratkaisuista

RESURSSIT**1 2 3 4 5**

Minulla on aikaa tehdä työtehtäväni huolellisesti

Minulla on aikaa dokumentoida työni huolellisesti

Minulla on aikaa perehtyä muiden tekemään dokumentaatioon ja lukea ohjeita

Työssä tarvitsemiani ohjeita on riittävästi ja ne ovat ajantasaisia ja selkeitä

Lomat ja poissaolot on huomioitu riittävästi varahenkilöjärjestelyissä

Työtehtävieni määrä mahdollistaa lyhytaikaisen sijaistamisen

VASTUUT**1 2 3 4 5**

Tiedän, kuinka minun tulee toimia häiriötilanteissa

Tiedän Tipakkeen eri henkilöiden ja tiimien tehtävät ja vastuut häiriötilanteissa

Koen hallitsevani vastuualueeni riittävän hyvin

Määritetyt vastuualueet ovat selkeät

Voin luottaa, että poissaollessani muut pystyvät hoitamaan vastuualueeni

Vastuualueisiini on saatavilla ainakin yksi asian hallitseva varahenkilö

Tipakkeen eri henkilöiden osaamisalueista ja koulutuksesta on saatavilla riittävät tiedot

Pystyn vaikuttamaan häiriötilanteista palautumiseen työtehtävieni ja osaamiseni puolesta