Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Maija Penttinen

Julkisen asiantuntijalaitoksen riskien- ja jatkuvuudenhallinnan kehittäminen

Metropolia Ammattikorkeakoulu

Tekniikan ja liikenteen ylempi AMK-tutkinto

Hankintatoimi

Opinnäytetyö

27.11.2019

Tekijä(t) Otsikko Sivumäärä Aika	Maija Penttinen Julkisen asiantuntijalaitoksen riskien- ja jatkuvuushallinnan kehittäminen 57 sivua + 6 liitettä 27.11.2019
Tutkinto	Insinööri (ylempi AMK)
Tutkinto-ohjelma	Hankintatoimi
Suuntautumisvaihtoehto	
Ohjaaja(t)	Lehtori Erkki Sairanen Kehittämisjohtaja Markku Leino

Tutkimuksen kohdeorganisaationa toimii Celia, joka on saavutettavan kirjallisuuden ja julkaisemisen asiantuntijakeskus ja jonka tehtävänä on tukea yhdenvertaisuutta lukemisessa ja oppimisessa. Celia on osa opetus- ja kulttuuriministeriön hallinnonalaa ja tuottaa sekä välittää kirjallisuutta saavutettavassa muodossa pääosin verkkopalveluna.

Valtiohallinnossa vaatimukset palveluiden tarjoamiseksi digitaalisina ovat johtaneet uusiin lakeihin varmistamaan palveluiden digitaalista turvallisuutta. Vaikka tietoturvallisuus ei ole velvoitteena uusi, sen merkitys on korostunut digitalisaation myötä vastaamaan tekniikan kehityksen tuomiin tietoturvariskeihin. Teknisten laitteiden ja palveluiden käytön lisääntyminen on tuonut tietohallinnolle uusia haasteita digitaalisen turvallisuuden hallintaan. Turvallisuusosaamista ei voi enää asettaa pelkästään asiantuntijoiden vastuulle, vaan osaamista tulee myös jalkauttaa laitteita ja palveluita käyttäville loppukäyttäjille. Tehtävänä oli parantaa Celian palveluiden laatua ja luotettavuutta kehittämällä riskien- ja jatkuvuudenhallintaa täyttäen näin lain määräämiä velvoitteita.

Kehittämistyö toteutettiin toimintatutkimusmenetelmällä. Tiedonkeruumenetelminä käytettiin havainnointia, haastatteluja ja kirjallisia lähteitä. Tutkimuksen aikana suunniteltiin ja laadittiin riskienhallintapolitiikka sekä Celian palveluiden kannalta kriittisten järjestelmien jatkuvuussuunnitelmat toimintaohjekuvauksineen häiriötilanteiden varalta. Riskienhallintapolitiikan toteutuksessa ja jatkuvuussuunnitelmissa hyödynnettiin muun muassa Valtiovarainministeriön julkaisemia ohjemateriaaleja. Häiriötilanteiden toimintaohjeita testattiin valtiohallinnon yhteisessä digitaalisen turvallisuuden harjoituspäivässä, TAISTO:ssa.

Tutkimuksen johtopäätöksenä todettiin, että riskien- ja jatkuvuudenhallinta ovat aiheiltaan laajoja kokonaisuuksia ja näiden sovittaminen sekä sopivan, hyväksyttävän tason löytäminen on haastavaa pienessä organisaatiossa, jossa resurssit ovat rajalliset. Olennaista tulosten jalkauttamisessa sekä jatkokehityksen varmistamisessa on organisaation ymmärryksen syventäminen digitaalisesta turvallisuudesta.

Avainsanat	Riskienhallinta, jatkuvuudenhallinta, varautuminen, digitaalinen turvallisuus

Author(s) Title	Maija Penttinen Developing Risk and Continuity Management in Public Sector Organization.
Number of Pages Date	57 pages + 6 appendices 27 Nov 2019
Degree	Master of Engineering
Degree Programme	Master's Degree Programme in Supply Chain Management
Specialisation option	
Instructor(s)	Erkki Sairanen, Senior Lecturer, Metropolia Markku Leino, Chief of Development, Celia

The objective of the current thesis was to improve the quality and reliability of the target organisation's services by developing risk and continuity management. The target organization, Celia, is a center of excellence in accessible literature and publishing whose mission is to promote equality in reading and learning. Celia is part of the administration of the Ministry of Education and Culture. Celia produces and distributes literature in accessible formats, mainly as an online service. In Finnish government, requirements to provide digital services have led to new laws to ensure digital security of services. Although information security is not a new obligation, its importance has increased with digitalization to meet the security risks brought by technological advances. Increased use of technical equipment and services has brought new challenges for information management in managing digital security. Security expertise can no longer be placed solely on the responsibility of specialists but must also be imparted to end users of equipment and services.

The development work was carried out using action research. The data collection methods used were observation, interviews and written sources. During the study, a risk management policy and contingency plans for the systems critical to Celia's services were designed and developed, including plans of action for disruptions. The guidance materials published by the Ministry of Finance were used, among other things, in implementing the risk management policy and in the continuity plans. The plans of action for disruptions were tested at the Government's Common Digital Security Exercise Day, TAISTO.

The study concluded that risk and continuity management are broad topics and that adapting them and finding an appropriate, acceptable level is challenging in a small organization with limited resources. Deepening the organization's understanding of digital security is key to delivering results and ensuring future development.

Keywords	Risk management, contingency plan, plan of action, digital security

Sisällys

1 Johdanto

Euroopan Unionissa ja sen myötä Suomen valtiohallinnossa on viime vuosina pyritty nykyaikaistamaan julkisia palveluita digitalisoimalla ja hyödyntämällä nykyteknologian tarjoamia ratkaisuja palveluiden kehittämiseksi. Yksityisellä puolella nykyteknologiaa ollaan hyödynnetty jo pitkään ja osittain tämän vuoksi paine julkisten palveluiden kehittämiselle on kasvanut. Palveluiden digitalisoimisen ehtona on niiden turvallisuuden ja laadun varmistaminen, joka korostuu varsinkin julkisella puolella, sillä palvelut koskevat kansalaisten oikeuksia. Lukuun ottamatta valtion turvallisuuspalveluita, julkisen hallinnon digiturvallisuudessa on monin tavoin kehitettävää. Varsinkin pienemmissä julkisissa organisaatioissa digitaalisen turvallisuuden kehittäminen on jäänyt toteuttamatta tai sitä ei ole kyetty ylläpitämään tarvittavalla tasolla. Mahdolliset syyt tähän on olleet resurssien vähyys tai ymmärryksen ja osaamisen puute.

Teknisten laitteiden ja palveluiden hyödyntämisen laajentuessa loppukäyttäjille on tuonut osaltaan haasteita digitaalisen turvallisuuden hallinnassa. Digitaalisen turvallisuuden osaamista ei voida enää keskittää pelkästään sitä ohjaavalle tietohallinnolle, vaan osaamista tulee jalkauttaa laitteita ja palveluita käyttäville loppukäyttäjille. Tässä tutkimuksessa keskitytään digitaalisen turvallisuuden kehittämiseen riskien- ja jatkuvuudenhallinnan avulla, jotka tullaan jalkauttamaan koko organisaatiotasoisesti.

2 Uudet lait ja hankkeet

Valtiohallinnossa vaatimukset palveluiden tarjoamiseksi digitaalisina ovat tuoneet myös uusia lakeja ja velvoitteita varmistamaan palveluiden digitaalista turvallisuutta. Vaikka digitaalisen turvallisuuden varmistaminen ei ole uusi velvoite, sen merkitys on korostunut digitalisaation myötä vastaamaan tekniikan kehitystä. Seuraavissa alaluvuissa esittelen viime aikoina säädettyjä uusia lakeja, jotka ohjaavat digitaalisen turvallisuuden toteutumista niin julkishallinnossa kuin myös yksityisellä sektorilla.

2.1 Tiedonhallintalaki

Tarve uudelle tiedonhallintalaille syntyi Sipilän hallituksen kahdesta kärkihankkeesta, Digitalisoidaan julkiset palvelut - ja Sujuvoitetaan säädöksiä -kärkihankkeet, joiden tavoitteena on edistää julkisen hallinnon digitaalisten palveluiden tarjontaa sekä tehostaa ja

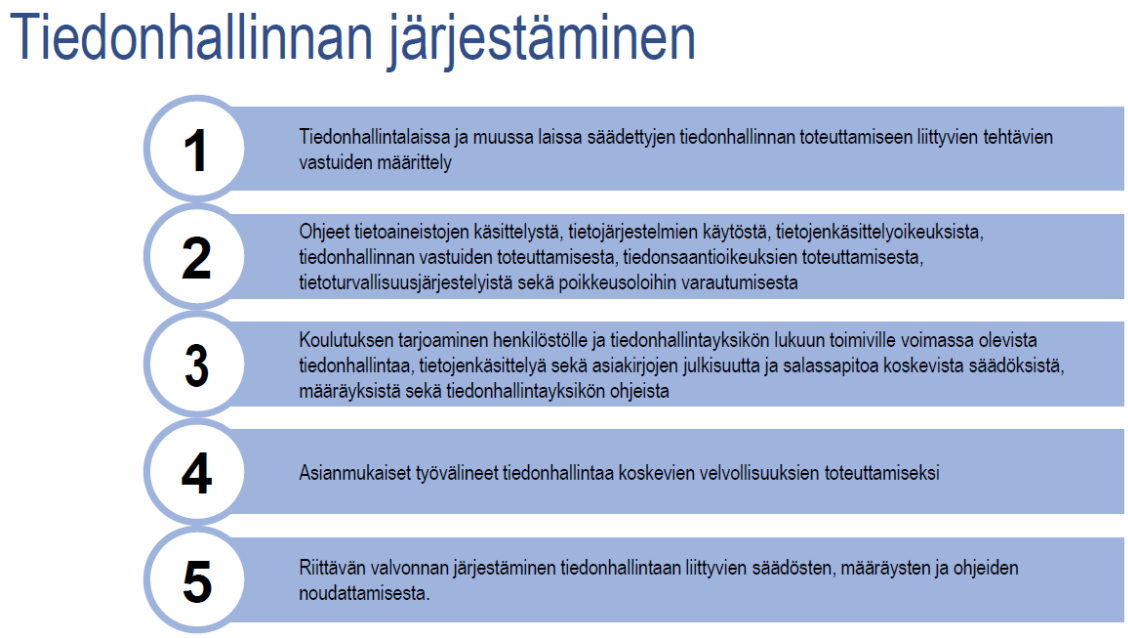
parantaa palveluiden laatua. Uusi tiedonhallintalaki tulee voimaan tammikuussa 2020 ja sitä koskevilla julkishallinnon toimijoilla on neljän vuoden siirtymäaika velvoitteiden toimeenpanemiseksi. Tiedonhallintalain tavoitteena on muun muassa vahvistaa tietoturvallisuutta viranomaispalveluissa sekä tehostaa palveluita yhdenmukaistamalla järjestelmärajapinnat, jotta tiedon hyödyntäminen ja välittäminen eri toimijoiden kesken on tehokasta, eikä esimerkiksi asiakkaiden tarvitse antaa samoja tietoja eri viranomaisille useampaa kertaa. (HE 284/2018 vp 2018, 8)

Tällä hetkellä tiedonhallintaan liittyvät määräykset ovat hajautuneet useampiin eri lakeihin, jotka ovat jo osaltaan vanhentuneita teknologian kehittymisen sekä muuttuneiden tiedonhallintatapojen vuoksi. Uusi tiedonhallintalaki tulee kumoamaan seuraavat lait ja säännökset:

1. Tietohallintolain (634/2011) kokonaisuudessaan,
2. Julkisuuslaista (621/1999) säännökset hyvästä tiedonhallintatavasta, asetus tietoturvallisuudesta valtiohallinnossa sekä osan asetuksesta viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta,
3. Asiointilaista (13/2003) säännökset rekisteröinneistä (HE 284/2018 vp 2019, 8)

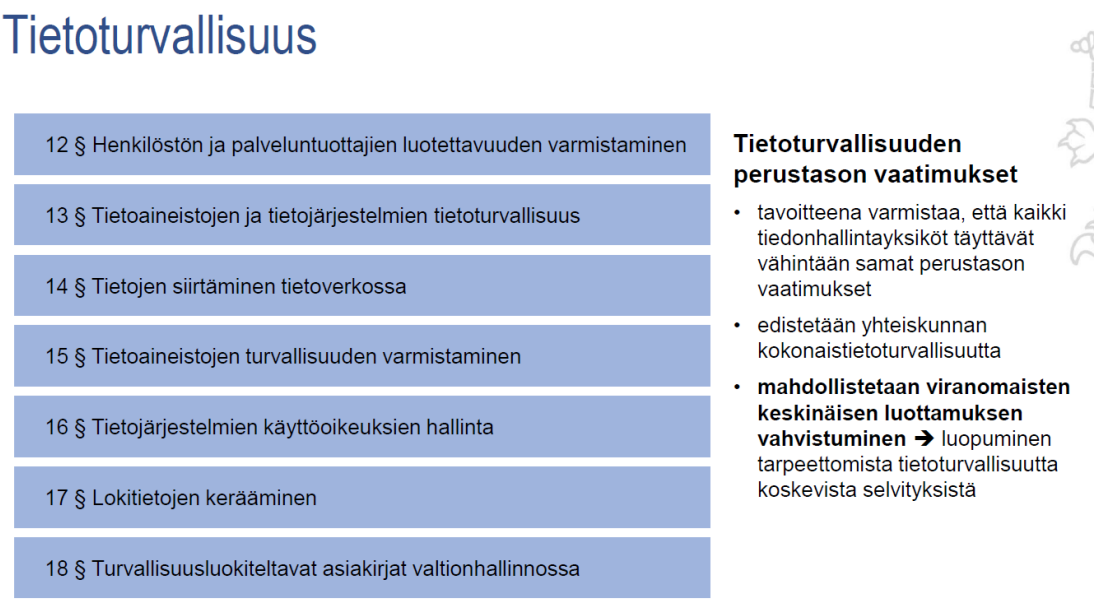
Tiedonhallintalain tavoitteena voidaan nähdä myös tiedonhallinnan laajentaminen kokonaisvaltaisemmaksi kokonaisuudeksi, jossa nostetaan vahvemmin esiin tiedolla johtaminen aikaisempien, lähinnä teknisten velvoitteiden, kuten kokonaisarkkitehtuurikuvauksen lisäksi. Kumoutuvassa tietohallintolaissa kokonaisarkkitehtuuria ohjasi JHS-179 -suositus, joka poistuu tai oikeastaan muuttuu uuden lain myötä. (HE 284/2018 vp 2019, 76)

14.5.2019 pidetyssä Valtiovarainministeriön järjestämässä virastojen tietohallintojohtajien kokouksessa käsiteltiin tiedonhallintalakia. Seuraava kuvio 1 on esitysmateriaalista, joka esittää ylätasolla tiedonhallintalain tehtävien järjestämisestä perustettavissa tiedonhallintayksiköissä. Tiedonhallintayksiköt ovat käytännössä valtiohallinnon virastot ja laitokset itsessään.



Kuvio 1. Tiedonhallintalain mukaiset tehtävät tiedonhallintayksikölle. (Tiedonhallintalaki - täytäntöönpano 2019, 4)

Tiedonhallinnan kuvausten, tiedon käsittelyohjeistuksien sekä yhteen toimivien järjestelmärajapintojen lisäksi tietoturvallisuus, riskienhallinta ja varautuminen esiintyvät suuressa roolissa lain velvoitteissa. Kuviossa 1 esitetyssä toisessa tehtäväosassa mainitaan juurikin tietoturvallisuusjärjestelyiden ja poikkeusoloihin varautumisen tehtävävaatimukset, jotka sisältyvät Tiedonhallintalain neljänteen lukuun. Kuviossa 2 esitetään tarkemmin Tiedonhallintalain 4. luvun lainpykälät, jotka koskevat tietoturvaa.



Kuvio 2. Tiedonhallintalain 4. luvun pykälät tietoturvasta. (Tiedonhallintalaki - täytäntöönpano 2019, 7)

Tässä tutkimustyössä pyrittiin ennakoimaan niitä toimenpiteitä ja tehtäviä, joita tiedonhallintalain koskettamat organisaatiot tulee toteuttaa lain voimaanastuessa tammikuusta 2020 lähtien.

2.2 Laki digitaalisten palvelujen tarjoamisesta

12.2.2019 eduskunnassa hyväksytty ja 1.4.2019 voimaan tullut laki digitaalisten palvelujen tarjoamisesta (306/2019) tehtävänä on varmistaa saavutettavuus digitaalisissa palveluissa, muun muassa verkkosivustoissa. Lain luvussa 2, 4 § velvoitetaan viranomaisia suunnittelemaan ja toteuttamaan digitaaliset palvelut tietoturvallisesti sekä varmistaen palveluiden tietosuojan, löydettävyyden ja helppokäyttöisyyden. 14.5.2019 pidetyssä Valtiovarainministeriön järjestämässä virastojen tietohallintojohtajien kokouksessa käsiteltiin tiedonhallintalain lisäksi myös lakia digitaalisten palveluiden tarjoamisesta. Esitysmateriaalissa kuvattiin lain tuomien velvoitteiden pääkohdat, jotka on esitetty kuviossa 3.

Kuvio 3. Laki digitaalisten palveluiden tarjoamisesta luku 2. (Digipalvelulaki pähkinänkuoressa 2019, 5)

Kuten kuviossa 3 esitetään, digitaalinen turvallisuus on myös tässä laissa vahvasti esillä. Digitaalisten palveluiden suunnitteluvaatimus -osio käsittelee tietosuojan ja -turvallisuuden velvoitteita ja digitaalisten palveluiden saatavuuden varmistaminen -osio tarkoittaa käytännössä jatkuvuudenhallinnan tehtäviä ja riskienhallintaa. (Digipalvelulaki pähkinänkuoressa 2019, 5)

2.3 Tietosuoja-asetus ja kansallinen tietosuojalaki

25.5.2018 voimaan tullut Euroopan Unionin yleinen tietosuoja-asetus uudisti henkilötiedon käsittelyn määräykset suojaamaan henkilöiden yksityisyyttä vastaamaan tekniikan kehittymisen myötä tulleisiin henkilötiedon hallinnan haasteisiin ja väärinkäytöksiin. Tekniikan kehittymisen vaikutuksena henkilötietoa on hyödynnetty uusien palveluiden kehittämiseen useinkin henkilön tietämättään tai ilman suostumusta.

Tietosuoja-asetus tarjoaa Euroopan unionille yhdenmukaisen tietosuojakehyksen, joka rajaa mitä henkilötietoa saa käsitellä, miten ja missä yhteyksissä. Asetus parantaa yksityisen henkilön oikeuksia sekä asettaa rajoituksia ja velvollisuuksia henkilötietoa käsitteleville elimille.

Kansallinen tietosuojalaki astui voimaan 1.1.2019, jonka seurauksena vanha Henkilötietolaki kumoutui. Tietosuojalailla täydennetään ja täsmennetään tietosuoja-asetusta ja sitä sovelletaan rinnakkain asetuksen kanssa.

2.4 Julkisen hallinnon digiturvallisuuden kehittämisohjelma JUDO

Toimintaympäristön digitalisoituminen ja sen mukana tulleet haasteet ja uhat ovat vaatineet lakien uudistamista ja päivittämistä vastaamaan nykypäivää. Näitä uudistettuja lakeja olen esitellyt edellä (ks. luvut 2.1 – 2.3). Varmistaakseen uusien lakien käyttöönoton Valtiovarainministeriö perusti kehittämisohjelman julkisen hallinnon digitaalisesta turvallisuudesta. Ohjelman tavoitteena on saavuttaa toimivat ja luotettavat digitaaliset palvelut. Kehittämisohjelmalla on kolme painoaluetta:

1. digiturvallinen johtaminen ja riskienhallinta
2. henkilöstön osaaminen
3. uuden teknologian hyödyntäminen palveluissa (Rousku 2019a, s. 6)

Näiden painoalueiden kehittämisestä ja toteuttamisesta operatiivinen vastuu on Väestörekisterikeskuksella, joka puolestaan asetti kehittämisohjelman toteuttamiseksi JUDO-hankkeen vuosille 2018-2021. Hankkeeseen osallistuu julkisen hallinnon organisaatioiden lisäksi myös kuntia ja yksityisen sektorin organisaatioita.
JUDO-hankkeessa on viisi projektia, joiden avulla kootaan digitaalisen turvallisuuden ohjepaketti. Projektien tehtävät ovat:

1. Projekti 1: Digiturvan yhteishanke digitaalisen turvallisuuden johtamisesta ja riskienhallinnan kehittämisestä, jonka avulla organisaatiot saavat nykyaikaisia työkaluja, malleja ja ohjeita. Projektin osana luodaan digitaalisen turvallisuuden johtamisen käsikirja sekä projektissa järjestettävien työpajojen aikana saatuja oppeja viedään käytäntöön muun muassa projektiin kuuluvassa TAISTO-harjoituksessa (ks. luku 2.5). Tässä yhteishankeprojektissa keskeisimpänä tehtävänä on riskienhallinnan kehittäminen.
2. Projekti 2: Digitaalisen turvallisuuden vaatimus- ja arviointikehikon toteuttaminen. Hankkeen aikana luodaan verkkopalvelu, jossa projektin aikana luodut soveltamis- ja arviointikehikon (VAHTI 100) materiaalit julkaistaan kaikkien käyttöön.

3. Projekti 3: Julkisen hallinnon digitaalisen turvallisuuden koulutusjärjestelmä sekä digiturvasovellus. Projektin aikana toteutetaan digitaalisen turvallisuuden oppimisympäristö yhteistyössä HAUS Kehittämiskeskus Oy:n kanssa sekä pelillistävä digiturvan koulutussovellus yksityisten peliyritysten kanssa.
4. Projekti 4: Julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan raportoinnin kehittäminen. Tämän projektin osana toteutetaan seurantajärjestelmä, jonka avulla organisaatio voi seurata ja toteuttaa raportteja oman digitaalisen turvallisuuden kehittymisestä.
5. Projekti 5: Digitaalisen turvallisuuden harjoitussuunnitelma vuosille 2019-2021. Projektin aikana toteutetaan harjoitusmalli erilaisten digitaaliseen turvallisuuteen liittyvien harjoitusten toteuttamiseksi. (Rousku 2019a, s. 8-9).

Työnantajani Celia on osallisena projekti 1:sen yhteishankkeessa osallistuen hankkeen työpajoihin sekä TAISTO-harjoitukseen. Yhteishanke koostuu viidestä digitaalisen turvallisuuden osa-alueesta:

1. Riskienhallinta
2. Toiminnan jatkuvuus ja varautuminen
3. Tietoturvallisuus
4. Kyberturvallisuus
5. Tietosuoja

Vuoden 2019 järjestettävien työpajojen painopiste kohdistuu riskienhallintaan sekä toiminnan jatkuvuuteen ja varautumiseen. Näin ollen hyödynnän työpajoista saamaani osaamista tässä tutkimuksessa ja samalla Celia ennakoi tulevan tiedonhallintalain vaatimusten toteutumista.

2.5 TAISTO-harjoitus

Väestörekisterikeskus toteutti vuonna 2018 ensisijaisesti julkishallinnolle tarkoitetun, digitaalisen turvallisuuden yhteisen harjoituspäivän, jonka pääpaino oli tietoturva- ja tietosuojaloukkaustilanteiden hallinnan harjoituksessa. Harjoitukseen osallistui 234 julkisen hallinnon organisaatiota. (Rousku 2018, 24)

TAISTO-harjoituksessa on tarkoituksena harjoitella digitaaliseen turvallisuuteen liittyviä prosesseja sekä saada harjoituksen avulla selvitys organisaation digiturvallisuuden ny-

kytilanteesta. Harjoitukseen osallistuminen ei vaadi organisaatiolta sen digitaalisen turvallisuuden tason täydellisyyttä, jossa tulisi olla jo valmiit toimivat toiminta- ja valmiussuunnitelmat, vaan harjoitus on myös keino tuoda esiin kehittämiskohteet ja puutteet. Osana JUDO-hankkeen 1. projektia, Väestörekisterikeskus toteuttaa TAISTO-harjoitukset vuosille 2019-2021, joiden avulla JUDO-hankkeeseen osallistuneet organisaatiot voivat arvioida ja testata hankkeen aikana tekemiään digitaalisen turvallisuuden kehitystoimenpiteitä. (Rousku 2019b, s. 4)

Vuoden 2019 TAISTO-harjoituksen pääpaino on riskienhallinnassa, toiminnan jatkuvuudessa ja varautumisessa sekä tietosuojassa. Harjoituksen suunnittelussa ja toteuttamisessa on Väestörekisterikeskuksen lisäksi mukana Huoltovarmuuskeskus, Liikenne- ja viestintäviraston Kyberturvallisuuskeskus, Poliisi, Tietosuojavaltuutetun toimisto, Turvallisuuskomitea sekä Valtion tieto- ja viestintätekniikkakeskus Valtori. (Rousku 2019b, s. 4)

Harjoitus toteutetaan yhtenä, osallistuvan organisaation itse valitsemana päivänä. Organisaatio tulee saamaan ennen valitsemaansa varsinaista harjoituspäivää kaksi harjoittelusyötettä, jotka valmistavat itse harjoitukseen. Varsinainen harjoituspäivä on koko päivän kestävä tapahtuma, jolloin organisaatio tulee saamaan erilaisia tehtäväsyötteitä. Näihin syötteisiin organisaatio reagoi ennalta luotujen prosessien ja varautumiskuvausten mukaisesti sekä tuottaa päivän aikana harjoitusraportin.

Celia osallistuu vuoden 2019 TAISTO-harjoitukseen ensimmäistä kertaa. Harjoituksen tarkoituksena on luonnollisesti harjoitella Celian digitaalisen turvallisuuden tasoa ja varautumisprosesseja, mutta myös mitata tässä opinnäytetyössä kehitettyjen ja kuvattujen mallien onnistumista.

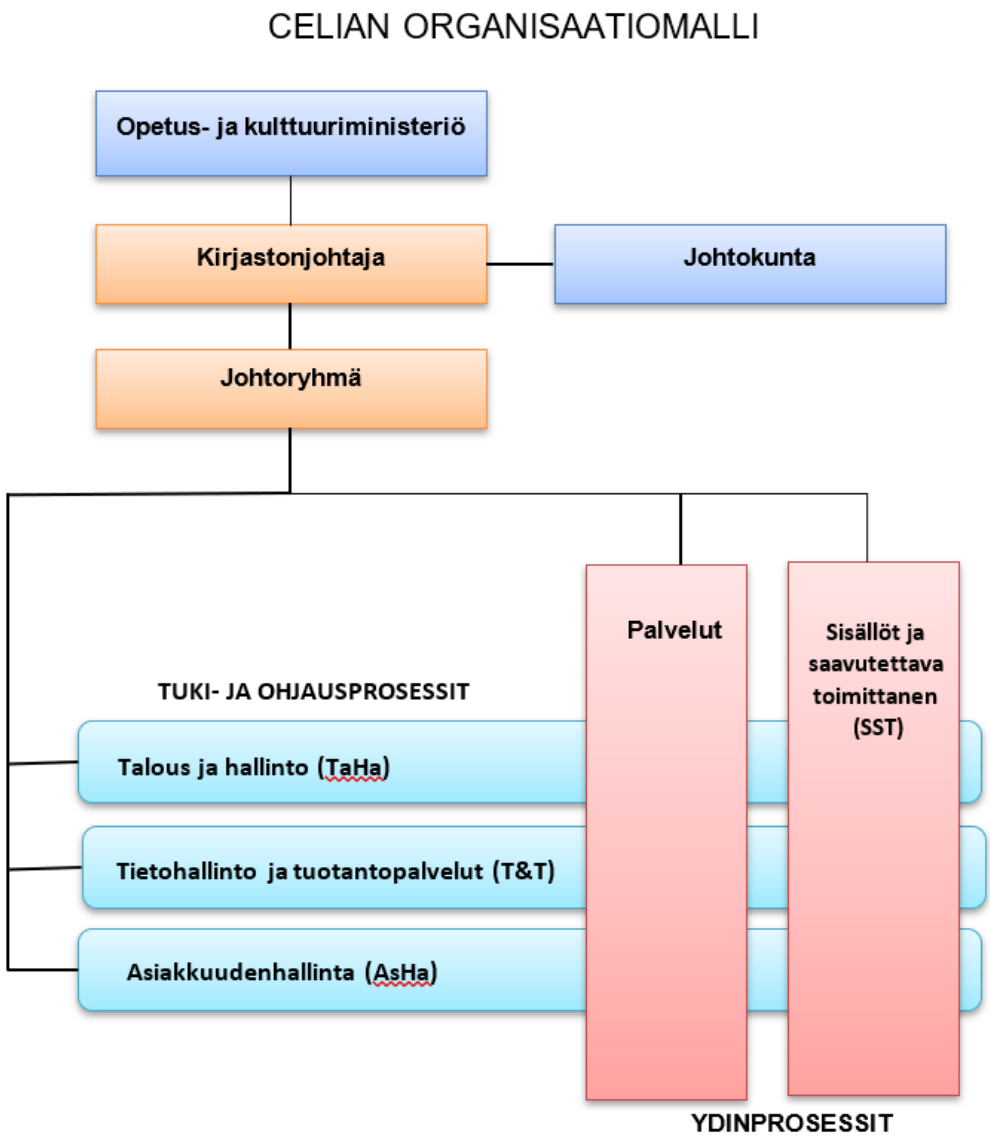
3 Kohdeorganisaation esittely

Tämä tutkimustyö tehtiin työnantajani Celian toimintaympäristössä. Celia on saavutettavan kirjallisuuden ja julkaisemisen asiantuntijakeskus, joka tukee yhdenvertaisuutta lukemisessa ja oppimisessa. Celia on osa opetus- ja kulttuuriministeriön hallinnonalaa ja tuottaa sekä välittää kirjallisuutta saavutettavassa muodossa, muun muassa äänikirjoina ja pistekirjoina, yhteistyössä kirjastojen ja kustantajien kanssa. Celian toimittamia erilaisia saavutettavia kirjatuotteita ovat kauno- ja tietokirjallisuus (piste- ja äänikirjamuodossa), korkeakoulukirjat (yhdistetty teksti- ja äänikirja) sekä oppikirjoja peruskouluun,

lukioon ja ammatillisiin opintoihin (piste-, luetus- ja yhdistetyt ääni- ja tekstikirjat). Näiden lisäksi Celia lainaa käsintyönä tehtyjä taktiilikirjoja (koskettelukirjat) lapsille sekä suunnittelee ja tuottaa erilaisia oppimateriaaliratkaisuja kouluille.

3.1 Celian organisaatiomalli

Celian organisaatiomalli on kuvattu alla olevassa kuviossa 4.



Kuvio 4. Celian organisaatiomalli.

Toimin itse tietohallintovastaavana Tietohallinto ja tuotantopalvelut -prosessissa (myöhemmin T&T). T&T-prosessi on kokenut viime vuosina suuria muutoksia, lähtien TORI-

lain voimaantulosta. TORI-laki, viralliselta nimeltä Laki valtion yhteisten tieto- ja viestintäteknisten palveluiden järjestämisestä (1226/2013), muutti T&T-prosessin toimintaa merkittävästi. Aiemmin Celia oli itse hoitanut ja ylläpitänyt ICT-ympäristöään, mutta TORI-lain tullessa kaikki toimialariippumattomat järjestelmät, ohjelmat, laitteet, sopimukset ja lisenssit sekä tehtävät mukaan lukien osan työntekijöistä tuli siirtää uuteen palvelukeskukseen, Valtion tieto- ja viestintäkeskus Valtoriin. Näiden muutosten myötä Celian tietohallinto vaati uudistamista ja roolin vahvistamista ohjaavana ja hallinnollisena yksikkönä.

3.2 Tutkimuskohteen taustaa

Teknologian kehittyminen on muuttanut merkittävästi yritysten tekniikan johtamista. Alussa organisaatioihin perustettiin tietotekniikan osastoja sitä mukaa, kun tietotekniikkaa alettiin hyödyntää liiketoiminnassa. IT-osastot olivat erillisiä toiminnallisia osastoja omine hallinnollisine vastuualueineen ja ne nähtiin lähinnä vain tukitoimintoina ja muusta liiketoiminnasta erillisinä osina. Tietohallinnon pyrkimyksenä on ollut kontrolloida tietotekniikan käyttöä ja hallinnoida sitä tiukoin säännöin. Teknologian hyödyntämisen yleistyminen ja digiajan kehittyessä kuilu tietohallinnon ja muun liiketoiminnan välillä on kaventunut. Perinteinen tietohallinto ei pysty kontrolloimaan nopeasti kehittyvää ja laajenevaa digitalisoitumista samalla tavalla kuin aikaisemmin ja näin myös sen hallinnointia tulee laajentaa kaikkiin liiketoiminnan osa-alueisiin ja koko liiketoimintaa koskevaksi. (The Business Technology Forum 2019, 3)

Celian tietohallinto on muodostunut organisaation kehittymisen ja digitalisoitumisen myötä. Celian tietotekniikan hyödyntäminen alkoi muutamasta IBM-36 -sarjan palvelimesta 1980-luvun lopulla ja on siitä lähtien laajentunut palveluita digitalisoitaessa. Pieneksi valtiohallinnon organisaatioksi Celialla on kokoonsa nähden suhteellisen mittavat ICT-järjestelmät. Celian palveluiden digitalisointi aloitettiin digitaalisen kirjaston suunnittelmilla 2000-luvun vaihteessa, jonka tuloksena vuonna 2005 digitoitiin aiemmin käytössä olleet äänikirjanauhat ja vuonna 2009 toteutettu digitaalisten äänikirjojen jakelujärjestelmä. Nykyään Celian palveluita voidaan käyttää selaimen kautta suoratoistona, tiedostolatauksilla tai mobiilisovelluksella. On-demand palveluna voidaan lainata CD:itä ja pistemateriaaleja, joita asiakkaan ei tarvitse palauttaa takaisin Celiaan tai perinteisellä lainauksella koskettelukirjoja lapsille. Voidaan sanoa, että Celia on ollut edelläkävijä palveluiden digitalisoinnissa suhteessa muuhun julkishallintoon.

Kuten varmasti monissa muissakin pienissä organisaatiossa, tietohallinnon johtaminen on ollut ja on edelleen reaktiivista. Järjestelmämäärien kasvu ja palveluiden digitalisoituminen vaativat enenevässä määrin myös ennakoivaa, proaktiivista hallintaa palveluiden toiminnan ja laadun varmistamiseksi. Celiassa resurssipuutteen ja mahdollisesti myös tiedon puutteen vuoksi hallinnollinen puoli on jäänyt toteuttamatta siinä määrin, mikä olisi tarpeen. Kun digitalisaation myötä ympäristö on monimutkaistunut ja digitaalisten laitteiden käyttö laajentunut yli tietohallinnon rajojen, sitä hankalammaksi on myös käynyt kokonaisuuden hallinta. Tämän vuoksi hallinnan osaaminen ei ole enää riittävää keskittää pelkästään tietohallinnon vastuulle vaan osa vastuusta on siirrettävä myös niille henkilöille, jotka hyödyntävät ja tekevät kehittämispäätöksiä. Tällä tavoin tietohallinnon rooli tulee muuttumaan enemmän ohjaavaksi yksiköksi.

Celian tietohallinnon yhtenä tehtävänä on varmistaa, että organisaation vaatimat tietoturvan ja tietosuojan tehtävät ja ohjaus toteutuvat. Ikävä kyllä, kuten useissa muissakin julkishallinnon organisaatiossa, riskienhallinta ja varautuminen eivät ole olleet hyväksyttävällä tasolla. Tämän tutkimuksen tuloksena on tarkoitus parantaa tilannetta molempien osalta. Riskienhallinta ja varautuminen ovat kumpikin lähtökohtaisesti kokonaisuuksiltaan suuria, joten työn suunnittelussa haasteena oli näiden suhteuttaminen riittävälle tasolle organisaation kokoon ja resursseihin nähden.

4 Tutkimuskohteen asetelma

4.1 Tutkimuksen tavoite

Tutkimuksen tavoitteena oli parantaa Celian digitaalista turvallisuutta riskienhallintaa kehittämällä sekä toteuttamalla jatkuvuudenhallintaa aluksi rajoitetusti. Toteutin molemmista aiheista nykytila-analyysin haastattelemalla johtoryhmän jäseniä. Nykytila-analyysin pohjalta suunnittelin tämän tutkimuksen rajoissa tehtävät kehitystoimet. Riskien- ja jatkuvuudenhallinta ovat molemmat laajoja kokonaisuuksia toteutettavaksi. Celian pienen organisaation koon ja vähäisten resurssien vuoksi tietohallinto ei pysty toteuttamaan näiden hallintaa siinä määrin, mitä riskien- ja jatkuvuudenhallinnan osalta olisi mallikasta tehdä.

Tutkimuksen tavoitteena oli toteuttaa:

- riskienhallinnan malli ja politiikka
- jatkuvuussuunnitelmat

- toimintaohjeet
- määriteltyä kriittiset järjestelmät

4.2 Tutkimuksen rajaus

Tutkimuksessa analysoin riskienhallinnan nykytilaa ja suunnittelin sen pohjalta kehitystoimenpiteet. Rajasin riskienhallinnan kehittämisen riskienhallintapolitiikan toteuttamiseen ja hallintamallin kuvaamiseen, ja jätin tämän tutkimuksen ulkopuolelle varsinaisen riskienhallinnan toteuttamisen.

Jatkuvuudenhallinnan osalta selvitin nykytilan, määrittelin kriittiset järjestelmät sekä toteutin jatkuvuussuunnitelmat toimintaohjeineen. Rajasin tutkimuksen ulkopuolelle jatkuvuudenhallintaan liittyvän valmiussuunnitelman, joka toteutetaan myöhemmin jatkokehityksenä.

4.3 Tutkimuskysymykset

Määritellyistä tutkimuskohteen ongelmista muodostetaan tutkimuskysymykset, jotka ovat kehittämisprojektin ohjaamisessa tärkeät elementit. Toimintatutkimus kehittämistutkimuksen muotona -teoksessa Jyväskylän ammattikorkeakoulun tutkimuksen ja kehittämisen yliopettaja Jorma Kananen toteaa, että ilman tutkimuskysymysten määrittelyä koko tutkimusta ei voida tehdä. Toimintatutkimuksen tutkimuskysymyksiä määritellessä tulee ilmetä toiminta, johon tutkija itse osallistuu. Kysymykset tarkentuvat tai voivat jopa muuttua kehittämisprosessin aikana, varsinkin kvalitatiivisessa tutkimuksessa, jossa myös tutkimuskohteen ongelmat voivat muuttua. (Kananen 2014, 44)

Tässä tutkimuksessa olin määritellyt kehittämiskohteiksi (tai ongelmiksi, jos näin halutaan tulkita) Celian digitaalisen turvallisuuden kehittämisen keskittyen riskien- ja jatkuvuudenhallintaan.

Tutkimus pyrki vastaamaan seuraaviin tutkimuskysymyksiin:

- Miten Celian digitaalista turvallisuutta voidaan kehittää?
- Miten saattaa digitaalinen turvallisuus uuden tiedonhallintalain vaatimusten mukaiseksi?

Tutkimuskysymyksiä tukevat seuraavat alakysymykset:

- Mikä on nykytaso?
- Mitä on tavoitetaso?
- Mitä toimenpiteitä vaaditaan tavoitetason saavuttamiseksi?
- Miten nämä toteutetaan käytännössä?

Kuviossa 5 esitän varsinaisten tutkimuskysymysten lisäksi laaditut, tehtävää tukevat kysymykset, jotka otettiin tutkimuksessa huomioon.

MITÄ? / MITKÄ?	**KUKA? / KETKÄ?**
Mitä muutoksia tarvitaan?	Ketkä ovat vastuussa digitaalisesta turvallisuudesta?
Mitkä ovat Celian kriittisen prosessit ja palvelut?	Keiden tulee osallistua tutkimuksen tehtäviin?
Mitä toimintoja pitää kehittää?	Keitä haastatellaan?
Mitä resursseja on käytettävissä?	Kuka tekee päätökset?
Mitä työkaluja käytetään?	
MILLOIN?	**KUINKA?**
Milloin suunnitelmaa testataan?	Miten haastattelut järjestetään?
	Miten testaus järjestetään?

Kuvio 5. Tutkimuskysymykset. (Kananen 2014, 39).

4.4 Tutkimuksessa käytetyt mittarit

Mittarit ovat tärkeä osa kehittämistyössä, sillä niiden kautta pystytään todentamaan tapahtunut muutos. Ilman mittareita muutoksia ei voida todentaa ja ne jäävät helposti subjektiivisiksi oletuksiksi. Hyödynsin tutkimuksen mittaamisessa KUJA-hankkeen pikatestiä sekä Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) laatimaa digitaalisen turvallisuuden barometria.

Tässä tutkimuksessa todesin muutokset seuraavilla mittareilla:

- Saimmeko paremmat tulokset digitaalisen turvallisuuden barometristä ja KUJA-pikatestistä? (Kyllä / Ei).
- Onko riskienhallinta otettu osaksi kehittämistoimia? (Kyllä / Ei).
- Onko jatkuvuudenhallinnan jatkuvuussuunnitelmat laadittu ja vastuuhenkilöt koulutettu? (Kyllä / Ei).

4.5 Tutkimuksen aikataulu

Työ aloitettiin jo keväällä osallistumalla JUDO-hankkeeseen ja tutkimalla Celian digitaalisen turvallisuuden nykytilaa. Alla esitetyssä kuviossa 6 on kuvattu tehtäväsuunnittelua aikatauluineen sekä vastuuhenkilöt. Tietohallintovastaava vastuuhenkilönä kuvaa omaa työtäni.

Tehtävä	**Aika**	**Vastuuhenkilö(-t)**	**Osallistujat**
JUDO-hankkeeseen osallistuminen	Toukokuu 2019	Tietohallintovastaava	Tietohallintovastaava
Nykytilan selvitys	Toukokuu 2019	Tietohallintovastaava	Tietohallintovastaava
TAISTO-harjoittelun esittely JORY:lle ja hyväksyntä.	Elokuu 2019	Tietohallintovastaava	Tietohallintovastaava
Riskienhallintatyökalun valinta, riskienhallintapolitiikan laatiminen ja esittäminen JORY:lle	Lokakuu 2019	Tietohallintovastaava	Tietohallinon työntekijät, JORY, yhteistyöryhmät
Kriittisten prosessien ja palveluiden tunnistaminen	Lokakuu 2019	Tietohallintovastaava	Yhteistyöryhmät
Jatkuvuushallinnan suunnittelu, kuvaaminen ja käyttöönotto	Lokakuu 2019	Tietohallintovastaava	Tietohallintovastaava, tietohallinnon suunnittelija, viestintäasiantuntija
TAISTO-harjoitukseen osallistuminen	Lokakuu – marraskuu 2019	Tietohallintovastaava	Yhteistyöryhmä
Analyysi tutkimuksen onnistumisesta	Marraskuu 2019	Tietohallintovastaava	Tietohallintovastaava ja kehittämisjohtaja

Kuvio 6. Toteutussuunnitelma ja aikataulutus.

5 Tutkimusmenetelmä

5.1 Toimintatutkimus

Toimintatutkimuksella tarkoitetaan tapaa lähestyä tutkimuskohdetta, niin sosiaalisena prosessina, osallistujan tietoisuutta laajentavana kuten myös kriittistä tarkastelua kehittävänä. Toimintatutkimuksella etsitään ratkaisuja organisaatioiden konkreettisiin toiminnallisiin ongelmiin, jossa edetään ongelmien tunnistamisesta toiminnan suunnitteluun, itse toimintaan sekä toiminnan tulosten arviointiin. Varsinkin kriittisessä toimintatutkimuksessa on oleellista vapauttaa osallistuja vanhoista käytänteistä ja toimintatavoista. (Suojanen 2014)

Toimintatutkimuksen avulla on tarkoituksena saada muutettua osallistujien ajattelu- sekä toimintatapoja. Tämä osallistava ongelmien ratkaisutapa antaa paremmat edellytykset muutoksen onnistumiselle kuin se, että organisaation ulkopuolelta esimerkiksi konsultin avulla tarjotaan valmista ratkaisua. Toimintatutkimuksen tuoma koulutus on usein tarpeellinen ohjaamaan ja rikkomaan totuttua arkiajattelua. Sen avulla osallistuja oppii näkemään asiat laaja-alaisemmin ja ymmärtää ongelman kokonaisuuden. Jos organisaatiolle tarjotaan valmista ratkaisua, osallistuja ei välttämättä opi ymmärtämään sitä kokonaisuudessaan ja joka puolestaan voi vaikuttaa heikompaan sitoutumiseen muutostilanteessa. Kun osallistuja on itse osallisena ratkaisun löytämisessä, sitouttaa se hänet paremmin muutokseen. Toimintatutkimukseen sisältyvä osallistuva tutkimus, tiedonhankinta, tiedon analysointi sekä näiden pohjalta tapahtuva toiminta voivat lisätä ihmisen tietoisuutta omasta toiminnastaan ja aktivoida häntä muutos- ja kehittämistyöhön. (Suojanen 2014)

Toimintatutkimuksessa on kaksi pääsuuntausta, koulutus- sekä hankepainotteinen toimintatutkimus. Koulutuspainotteisessa toimintatutkimuksessa keskeisenä tekijänä on osallistujien kouluttautuminen itseään ja työskentelyään kriittisesti arvioiviksi. Hankepainotteinen toimintatutkimus keskittyy puolestaan tutkimuskohteen kehittämiseen paremmaksi ja toimivammaksi ratkaisuksi tilanteessa, jossa toiminnan tuotoksessa on parannettavaa. (Suojanen 2014) Tämä tutkimus suuntautui hankepainotteiseen toimintatutkimukseen, mutta sillä on myös koulutuspainotteisia vaikutuksia.

Toimintatutkimuksen toteuttamisen pääperiaatteena käytetään kiinteästi Lean-menetelmästäkin tuttua, alun perin W. E. Demingin luomaa kehittämisen toimintasykliä, joka on esitetty kuviossa 7.

Kuvio 7. Demingin ympyrä. (Sixsigma, 2019).

Lean-menetelmässä kehittämisen sykliä kutsutaan Demingin ympyräksi (PDCA), jota käytetään syklimäisesti prosessien ongelmakohtien kehittämisessä. PDCA muodostuu sanoista Plan (suunnittele), D = Do (toteuta), C = Check (tarkista) ja A = Act (toimi). Jokainen käsitelty ongelma ja sille suunniteltu ratkaisu toteutetaan PDCA-syklin mukaisesti. Plan-kohdassa on tunnistettu ongelma, miten sen ratkaiseminen tulisi toteuttaa ja mikä on haluttu lopputulos. Do-vaiheessa ratkaisua testataan, Check-vaiheessa tarkistetaan ja analysoidaan, toiko muutos halutun lopputuloksen. Jos lopputulos on haluttu ratkaisu, se standardoidaan ja otetaan käyttöön. Jos ratkaisu ei tuottanut haluttua lopputulosta, sitä analysoidaan selvittämällä miksi tavoite ei toteutunut, tehdään korjaavat toimenpiteet ja aloitetaan koko sykli uudelleen niin kauan, että haluttu lopputulos saavutetaan. (Sixsigma, 2019)

5.2 Tiedonkeruumenetelmät

Tiedonkeruumenetelmät jaetaan kvalitatiivisiin eli laadullisiin ja kvantitatiivisiin eli määrällisiin menetelmiin. Toimintatutkimuksissa käytetään yleisemmin kvalitatiivista menetelmää, mutta oikean menetelmän valinta tehdään lopulta tutkittavan ongelman perusteella. Ongelma tulee olla selvitetty tarpeellisella tarkkuudella, jotta sen ratkaisemiseksi

tehtävään kehittämistyöhön voidaan valita oikeat tiedonkeruumenetelmät. Tässä tutkimuksessa käytin kvalitatiivista eli laadullista tiedonkeruumenetelmää. Kvalitatiivisia tiedonkeruumenetelmiä ovat havainnointi, haastattelut, kirjalliset lähteet ja kyselyt. (Kananen 2014, 77-78)

Havainnointia käytetään usein toimintatutkimuksen alkuvaiheessa ongelman määrittämiseen. Kananen jakaa havainnoinnin seuraaviin toteutustapoihin:

- piilohavainnointi, jossa havainnointitilanteessa havainnoitavat eivät tiedosta havaitsijaa,
- suora havainnointi, jossa havainnoitsija on esillä havainnointitilanteessa,
- osallistuva havainnointi, jossa havainnoitsija osallistuu toimintaan ja
- osallistavalla havainnoinnilla, jossa havainnoitsija pyrkii samalla kehittämään kohdetta,
- strukturoitu havainnointi, jossa havainnoitsija tietää mitä tapahtumaa hän haluaa seurata ja
- strukturoimatonta haastattelua, jossa havainnoitsija kirjaa ylös kaikki havainnot ilman selvää viitekehystä. (Kananen 2014, 80)

Kananen toteaa haastattelujen olevan tarpeen tutkimusongelman selvittämisessä, alkukartoituksessa ja kehittämistyössä tehtyjen muutosten vaikutusten arvioinnissa. Hän jakaa haastattelumenetelmät kolmeen eri muotoon: syvähaastatteluun, yksilöhaastatteluun ja ryhmähaastatteluun. (Kananen 2014, 87) Kananen esittää myös haastattelujen jakautuvan seuraaviin luokkiin, joissa kysymysten sekä vastausten ennakkoon määrittelyn määrä toimii muuttuvana tekijänä:

- strukturoidut haastattelut eli lomakekyselyt, jossa vastausvaihtoehdot on asetettu ennakkoon,
- puolistrukturoidut haastattelut eli avoimet lomakekyselyt, joissa ei ole ennalta asetettuja vastausvaihtoehtoja,
- teemahaastattelut, jossa haastattelija jakaa käsiteltävät aiheet teemoittain ja
- avoimet haastattelut, jossa ei olla määritelty käsiteltävien aiheiden teemoja (Kananen 2014, 91)

Tässä tutkimuksessa käytin kvalitatiivisina tiedonkeruumenetelminä haastatteluja, havainnointia, kirjallisia lähteitä ja kyselyitä. Havainnointimenetelminä käytin suoraa, strukturoitua ja osallistuvaa havainnointimenetelmää. Haastattelut toteutin niin joukko- kuin yksilöhaastatteluna. Haastatteluissa käytin strukturoitua sekä avointa haastattelumuotoa. (Kananen 2014, 78 - 80).

6 Tietoperustat

6.1 Riskienhallinta

6.1.1 Uhka, haavoittuvuus ja riski

Kyberturvallisuus-nimisessä teoksessa Limnéll, Majewski ja Salminen erottelevat uhkan, riskin ja haavoittuvuuden käsitteet. Nämä mielletään helposti samaa tarkoittavaksi, ja usein nämä ovatkin päällekkäisiä tapahtumia ja vaikuttavat toisiinsa. Uhkalla, riskillä ja haavoittuvuudella on kuitenkin eronsa. (Limnéll & Majewski & Salminen 2014, 105)

Uhka määritellään yleensä pakottavana toimintana, jossa uhattu pakotetaan toimimaan oman etunsa vastaisesti. Uhkan voi aiheuttaa uhkan tekijä, mutta se voi olla myös muodoltaan abstraktimpi, jolloin uhka nähdään mahdollisena vahingollisena asiana kohteelle. (Limnéll ym. 2014, 105-106)

Turvallisuuskomitea määrittelee Suomen uhkamallit osana kansallista riskiarviota kolmen vuoden välein. Turvallisuuskomitean verkkosivuilla esitetystä uhkamallista poimin seuraavat, jotka ovat todennäköisimpiä uhkia Celialle, vaikka sivuilla esitettyjä muita uhkia ei voi rajata poiskaan:

- voimahuollon vakavat häiriöt, esimerkiksi sähkön saanti
- tietoliikenteen ja tietojärjestelmien häiriöt
- suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhkat. (Turvallisuuskomitea 2019)

Haavoittuvuudella tarkoitetaan joko teknistä toteutusta tai tekijöitä. Teknisessä toteutuksessa esimerkiksi tietojärjestelmissä voi olla haavoittuvuutta, jos niihin on korostunut mahdollisuus vikaan tai heikkouteen, joka heikentää toimintavarmuutta. Haavoittuvuus

voi myös ilmetä henkilötekijöinä, joilla on esimerkiksi naiivi luottamus teknisiin ratkaisuihin. Haavoittuvuutta voidaan pitää myös uhkan mahdollistajana, mitä suurempi haavoittuvuus, sitä suurempi mahdollisuus uhkaan. (Limnéll ym. 2014, 110)

Riski voidaan määritellä kuvaavan mahdollisuutta, että jokin negatiivinen tapahtuma toteutuu tulevaisuudessa. Toisin sanoen se on epävarmuutta suhteessa tavoitteisiin tai mahdollista poikkeamaa odotetusta. Kaikkeen toimintaan liittyy aina kiinteästi riskejä. Jos pyrittäisiin poistamaan kaikki riskit, ei olisi myöskään toimintaa. (Limnéll ym. 2014, 108)

Riskejä ei voida torjua samalla tavalla kuin uhkia, mutta niitä voidaan pienentää lieventämällä tai hallita rajaamalla ja omaksumalla niitä. Ymmärrys riskeistä ja niiden tunnistaminen auttaa organisaatiota toimimaan vakaammin, sillä riskienhallinnalla pystytään ennalta ehkäisemään mahdollisia toimintaa halvauttamia tapahtumia. Luonnollisesti kaikkia riskejä ei aina pystytä tunnistamaan ja hallitsemaan, sitä varten organisaatiolla tulisi olla varautumis- ja toipumissuunnitelmat.

Johda riskejä -käytännön opas yrityksen riskienhallintaan -nimisessä teoksessa Ilmonen, Kallio, Koskinen ja Rajamäki kuvaavat yleistä ymmärrystä riskienhallinnasta, jonka avulla pyritään suojautumaan ei-toivotuilta tapahtumilta, kuten riskeiltä ja niiden seurauksilta. Riskienhallinta voidaan nähdä kuitenkin myös mahdollisuutena. Jos organisaation riskienhallinta on kunnossa, voidaan myös ottaa turvallisimmin mielin riskejä, jotka puolestaan voivat edistää liiketoimintaa positiivisesti. (Ilmonen & Kallio & Koskinen & Rajamäki 2010, 17)

Hyvällä riskienhallinnalla on useita positiivisia vaikutuksia. Jos riskienhallinta on kunnossa, se tuo läpinäkyvyyttä organisaatiossa toiminnastaan ja päätöksistä, joka puolestaan avoimuudellaan lisää työtyytyväisyyttä työyhteisössä. Hyvä riskienhallinta heijastuu myös organisaation asiakkaisiin, mieltymyksinä palveluiden luotettavuudesta. Kuten Ilmonen, Kallio, Koskinen ja Rajamäki toteavat, useimmin riskienhallinnan tilan näkyvyys tapahtuu kuitenkin negatiivisen tapahtuman kautta, kun huomataan, ettei organisaation riskienhallinta ollutkaan kunnossa. Tämä puolestaan voi vaikuttaa liiketoimintaan jopa tuhoisasti. Asiakkaan kerran menetettyä luottamusta palveluista on vaikea saada takaisin. (Ilmonen ym. 2010, 19)

Riskienhallintaa voidaan toteuttaa eri lähtökohdista. Organisaation johdolle se on työkalu strategisten, liiketoimintaa koskevien päätösten tueksi. Henkilöstöhallinto voi puolestaan hallita riskienhallinnalla organisaation resurssikyvykkyyttä.

Leinon, Steinerin ja Wahlroosin kirjoittamassa artikkelissa kuvataan Corporate Governancen merkitystä ja miten riskienhallinta liittyy siihen. Vaikka suomenkielessä Corporate Governancelle ei ole yksiselitteistä käännöstä, merkitystä voidaan kuvata muun muassa yrityksen hallinnalla ja hallinnoinnilla, toisin sanoen, miten yrityksen hallinto toimii. (Leino & Steiner & Wahlroos 2005, 124)

Yrityksen sisäinen valvonta kuuluu yrityksen johtamistehtäviin ja on Corporate Governancen keskeinen elementti. Sisäinen valvonta velvoitetaan toteuttamaan myös Talousarviolain (423/1988) 24 b §:n mukaan, jossa viraston tai laitoksen on huolehdittava sisäisen valvonnan järjestämisestä sen omassa vastuussa olevassa toiminnassa. Sisäisellä valvonnalla tarkoitetaan yrityksen kykyä johtaa asetettujen tavoitteiden saavuttamista, resurssien tehokasta käytettävyyttä sekä riittävää riskienhallintaa. Riskienhallinta on näin ollen osa sisäistä valvontaa. (Leino ym. 2005, 124-125)

Leino, Steiner ja Wahlroos määrittelevät artikkelissaan kokonaisvaltaisen riskienhallinnan prosessiksi, jossa tekijöinä ovat organisaation hallitus, johto ja työntekijät. Näin ollen riskien tunnistamiseen ja hallinnan suunnittelemiseen otetaan mukaan koko organisaatio (Leino ym. 2005, 126)

Kuten Leino, Steiner ja Wahlroos toteavat, riskienhallinnan projekti ei tulisi olla vain kertaluonteinen tehtävä, vaan riskienhallintaa, riskien tunnistamista ja raportointia tulisi toteuttaa säännöllisesti. Tämä määrittelee riskienhallinnan onnistumisen, jos organisaatio on motivoimalla saanut vakiinnutetuksi riskienhallinnan jatkuvaan käyttöön. (Leino ym. 2005, 138)

6.1.2 Politiikat

Jotta henkilöstö saisi tarkemman ohjeistuksen toiminta-alueittensa tueksi, organisaatio voi laatia erillisiä toimintapolitiikkoja, kuten riskienhallinta-, tietoturva- ja tietosuojapolitiikat. Toimintapolitiikat ohjaavat toimintaa tarkemmalla tasolla kertoen henkilöstölle organisaation määrittelemät toimintamallit. (Leino ym. 2005, 129)

Organisaation hyväksymä riskienhallintapolitiikka ohjaa organisaation riskienhallinnan toteutusta. Riskienhallintapolitiikka kuvaa organisaatiokohtaisesti riskienhallinnan periaatteita, tavoitteita sekä kattavuutta, mutta siinä voidaan kuvata myös, miten se linkitetään strategisiin tavoitteisiin, kuinka riskienhallinta organisoidaan vastuuroolituksilla ja miten riskienhallintatehtävät dokumentoidaan. (Leino ym. 2005, 128)

Riskienhallintapolitiikka määrittelee myös organisaation riskienhallinnan tason eli millä tasolla organisaatio haluaa investoida riskienhallintaan. Organisaation tulisi löytää tasapaino tavoitetilan ja niihin vaikuttavien riskien välillä. Tämän seurauksena muodostuu organisaation riskinhallinnan taso. Kuviossa 9 on esitetty riskienhallinnan tason vaikutukset kustannuksiin ja riskien näkyvyyteen. (Rousku 2017, 15)

Kuvio 8. Riskienhallinnan taso. (Rousku 2017, 15)

Riskienhallintapolitiikan lisäksi organisaatio voi toteuttaa riskienhallinnan periaatteet -dokumentaation, jossa esitetään riskienhallintapolitiikkaa tarkemmin riskienhallinnan toteuttaminen:

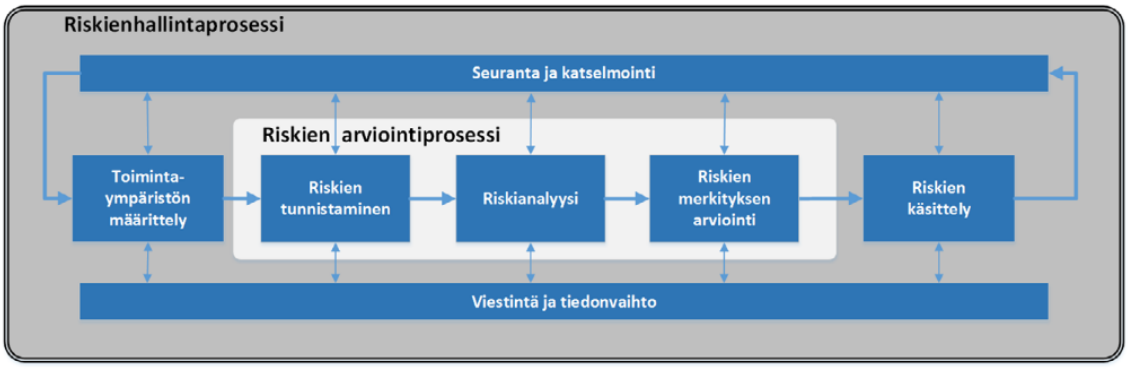
1. riskienhallinnan strategia ja tavoitteet
2. kriittisimpien riskialueiden tunnistaminen
3. vastuut riskien omistajista, seurannasta ja raportoinnista
4. riskienhallinnan mittarit
5. johdon varmistaminen riskienhallinnan tasosta. (Leino ym. 2005, 128)

6.1.3 Riskienhallinnan prosessi

Kokonaisvaltaisessa riskienhallinnan toteutuksessa on tarkoituksena saavuttaa yhtenäinen käytäntö organisaation eri yksiköiden välillä sopimalla tehokkaimmat prosessit ja

toiminnot. Sen sitominen organisaation strategiaan sekä liiketoiminnan eri prosesseihin varmistaa riskienhallinnan perimmäisen lähtökohdan, jossa on tunnistettava ne riskit, mitä tarvitaan organisaation päätösten teon tueksi. (Leino ym. 2005, 135)

Riskienhallinnan prosessi on systemaattinen ja ennalta sovittu tapa, jolla riskejä tunnistetaan, arvioidaan ja käsitellään. Valtiovarainministeriön VAHTI julkaisussa 22/2017 riskienhallinnan ohjeessa prosessi on kuvattu alla olevassa kuviossa 9.



Kuvio 9. Riskienhallintaprosessi. Kuvio perustuu standardiin SFS-ISO 31000. (Rousku 2017, 18)

Toimintaympäristön tunteminen ja määrittely on riskienhallintaprosessin lähtökohta. Prosessin alussa on tunnistettava organisaation kriittiset toiminnot ja palvelut, jotka ovat yleensä organisaation tai yhteiskunnan toiminnan kannalta merkityksellisiä. JUDO-hankkeen työpajassa 3 esitettiin ensisijaisina suojattavina kohteina liiketoiminnan prosessit ja tieto. Näitä tukevia kohteita ovat puolestaan ohjelmistot ja palvelut, tietoliikenne, henkilöstö ja toimipaikka. (Kirves & Ahokas 2019, 38)

6.1.4 Riskien tunnistaminen

Riskien tunnistaminen edellyttää työntekijöiden asiantuntijuuden hyödyntämistä, jotta riskien tunnistaminen olisi mahdollisimman laaja-alaista. Tavoitteena on tunnistaa kaikki merkittävät riskit ja mahdollisuudet, riskien lähteet, vaikutusalueet, tapahtumat, mukaan lukien olosuhteiden muutokset ja niiden syyt sekä mahdolliset seuraukset. (Rousku 2017, 21)

Riskien luokittelu on keskeinen tehtävä riskien tunnistamisessa. Luokittelu mahdollistaa yhdenmukaisemman hallinnan ja niitä voidaan vertailla helpommin. Usein myös tietty luokitus kuuluu niitä hallinnoiville henkilöille, kuten esimerkiksi strategisia riskejä käsitte-

levät usein organisaation johto. Yleisimmät käytössä olevat luokitukset ovat edellä mainittu strateginen riski, operatiivinen riski, taloudellinen riski ja vahinkoriski. Riskien luokittelu voidaan toteuttaa joko riskin lähteen tai tyypin mukaan. (Ilmonen ym. 2010, 70)

Riskien tunnistaminen kannattaa aloittaa alustavalla riskikartoituksella, jossa riskit ovat arvioitu karkealla tasolla. Kartoituksessa esiin nousseet korkean vaikutuksen ja todennäköisimmät riskit tulee ottaa tarkempaan analysointiin ja välittää tieto ylimmälle johdolle ja hallinnolle, jolloin he voivat arvioida toimintasuunnitelmien toteutusta. (Leino ym. 2005, 139)

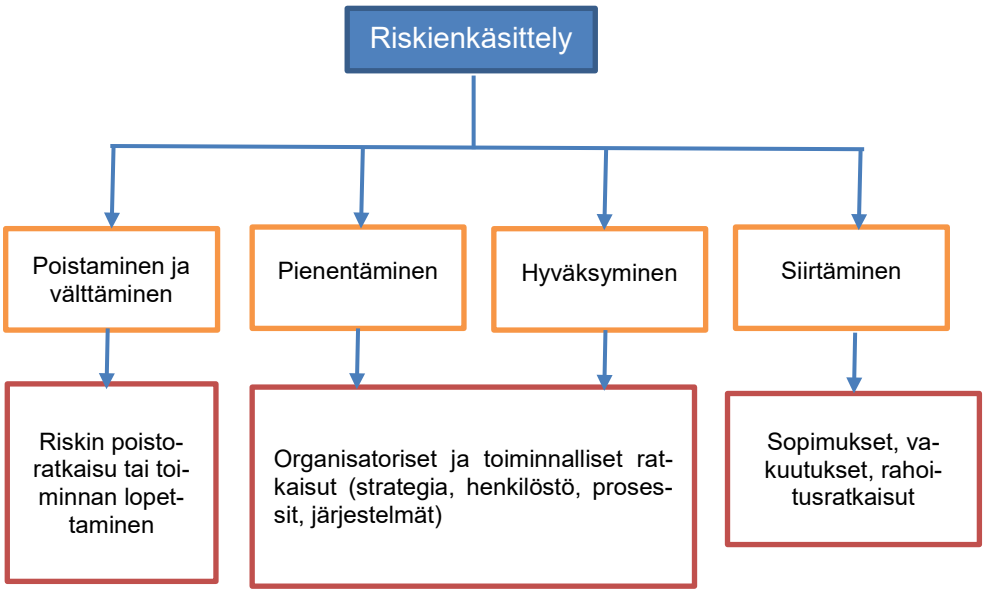
6.1.5 Riskien arviointi riskianalyysillä

Kuten edellä on mainittu, riskienhallinnan prosessin aloittaminen kannattaa aloittaa alustavasti karkealla tasolla. Riskit kannattaa arvioida ensin kapeammalla arviointiasteikolla, kuten esimerkiksi ”vähäinen vaikutus”, ”keskitasoinen vaikutus” ja ”suuri vaikutus”. Kun alustava karkea kartoitus on arvioitu kapeammalla arviointiasteikolla, voi tulla tarve laajentaa arviointiasteikkoa esiin tulleiden riskien perusteella. On myös tärkeää, että eri liiketoiminnan osa-alueilla arvioidaan riskit samalla tasolla yhtenäisesti. (Leino ym. 2005, 137)

Vaikutusarvioinnin lisäksi riskien toteutumisen todennäköisyys tulee arvioida. todennäköisyyttä voidaan arvioida esimerkiksi ”alhainen todennäköisyys”, ”keskitasoinen todennäköisyys” ja ”suuri todennäköisyys” -asteikolla. Vaikutuksen ja todennäköisyyden arvioinnilla saadaan riskin arvo. (Leino ym. 2005, 137)

6.1.6 Tunnistettujen riskien käsittely

Riskien arviointityön jälkeen määritellään tunnistetuille riskeille käsittelytoimenpiteet. Jokaiselle tunnistetulle riskille tulee tehdä suunnitelma, miten riskiä käsitellään. Riski voidaan pienentää tai poistaa kokonaan suunnitelluilla toimenpiteillä, siirtää esimerkiksi sopimuksin alihankkijoille tai hyväksyä riskin olemassaolo ja jättää se sellaisenaan jäännösriskiksi. Seuraava kuvio 10 mukailee Ilmosen, Kallion, Koskisen ja Rajamäen esittämää riskienhallinnan käsittelyn vaihtoehtoja.



Kuvio 10. Riskienkäsittelyn vaihtoehdot. (Ilmonen ym. 2010, 124)

Riskienkäsittelysuunnitelman lisäksi käsittelyyn tulee nimetä käsittelyn vastuuhenkilö sekä käsittelytoimenpiteiden tavoiteaika. Vastuuhenkilöpäätöksiin voidaan hyödyntää vastuujakotaulukkoa eli RACI-matriisia (RACI = Responsible, Accountable, Consulted, Informed) tai nimetä suoraan vastuullinen henkilö. RACI-mallia suositellaan hyödynnettävän, jos riskin käsittely on työläämpi ja organisaation koko isompi. Pienemmissä organisaatioissa riittää usein vastuuhenkilön kirjaaminen suoraan riskien arviointi- ja käsittelydokumenttiin.

Hyvään riskienhallintaan kuuluu riskienkäsittelysuunnitelmat, jotka käsittävät usein tunnistetut riskit ja niiden käsittelytavat, vastuuhenkilö riskin käsittelyyn, hyväksyjätahot, toimenpidesuunnitelmat, tavoiteaikataulut sekä raportointi ja seuranta. Riskienkäsittelysuunnitelmista koostuu organisaation riskisalkku, johon kerätään merkittävimmät riskit riskiarvojen suuruusjärjestyksessä. (Ilmonen ym. 2010, 182)

6.1.7 Seuranta ja raportointi

Valtiovarainministeriön riskienhallinnan ohjeessa mainitaan hyvänä huomiona se, että riskien käsittelyprosessi voi myös itsessään aiheuttaa uusia riskejä, jos se on tehotonta tai siinä epäonnistutaan. Muun muassa tämän vuoksi riskienhallinnan seuranta on tärkeä osa riskienhallintaprosessia. Seurannan avulla varmistetaan riskienkäsittelyn toteutu-

mista ja tavoitteiden onnistuminen. Seurantaan liittyy myös havainnointi riskiin kohdistuvista mahdollisista muutoksista, jotka voivat johtua sekä sisäisistä että ulkoisista tekijöistä. Seurantaa tulee toteuttaa säännöllisesti ja sille tulee asettaa vastuuhenkilö tai -taho. (Rousku 2017, 28)

Raportointi riskeistä ja näiden käsittelystä kuuluu olennaisena osana riskienhallintaa ja sen johtamista. Raportointitapa ja ajankohta tulee sopia etukäteen ja se usein liitetään organisaation strategiaprosessiin tai johtamisen vuosikelloon. Organisaation koosta ja liiketoimintavastuista riippuen raportointi voi olla eri tasoista. Ilmonen, Kallio, Koskinen ja Rajamäki kuvaavat raportoinnin eri tasoja vertaamalla organisaation hallintotason raportointia yksikkökohtaiseen raportointiin. Hallintotason raportointi esitetään usein koosteena riskien kokonaiskuvasta ja kriittisimpien riskien kehitystrendeistä, kun taas yksikkötason raportointi voi olla kattavampi tarkemman tason raportointia riskienkäsittelyn suunnitelmista ja käsittelytoteutusten kehittymisestä. (Ilmonen ym. 2010, 17)

6.2 Toiminnan valmius ja jatkuvuudenhallinta

Kuten edellä olen kuvannut riskienhallintaosiossa, organisaation liiketoimintaa voi uhata erilaisia uhkia ja riskejä. Organisaation on varmistettava, että toimintakyky säilytetään suunnitellusti uhkien realisoituessa häiriö- ja poikkeustilanteiksi. Häiriötilanteet tapahtuvat yleensä yllättäen. Tämän kaltaisissa tilanteissa organisaation toiminta voi pahimmassa tapauksessa lamaantua ja liiketoiminnan kriittiset palvelut voivat olla pitkääkin toimimatta ja näin ollen aiheuttaa niin talouteen, tietoturvallisuuteen kuin myös maineeseen liittyvää haittaa. Julkisella puolella varautumisen tärkeys korostuu, sillä palvelut koskevat yleensä kansalaisten oikeuksia.

Huoltovarmuuskeskuksen verkkosivuilla esitetään jatkuvuudenhallinnan elementit, joita organisaation tulisi toteuttaa:

- Tunnistaa uhkat, riskit, häiriötilanteet ja riippuvuudet
- Arvioida uhkien vaikutukset
- Suunnitella ja organisoida toimintasuunnitelmat häiriötilanteiden varalle
- Tunnistaa ja varmistaa kriittisten kumppanien ja toimittajien toimintakyvyn häiriötilanteissa
- Suojata liiketoiminnan ydinprosessit ja -palvelut. (Huoltovarmuuskeskus 2019).

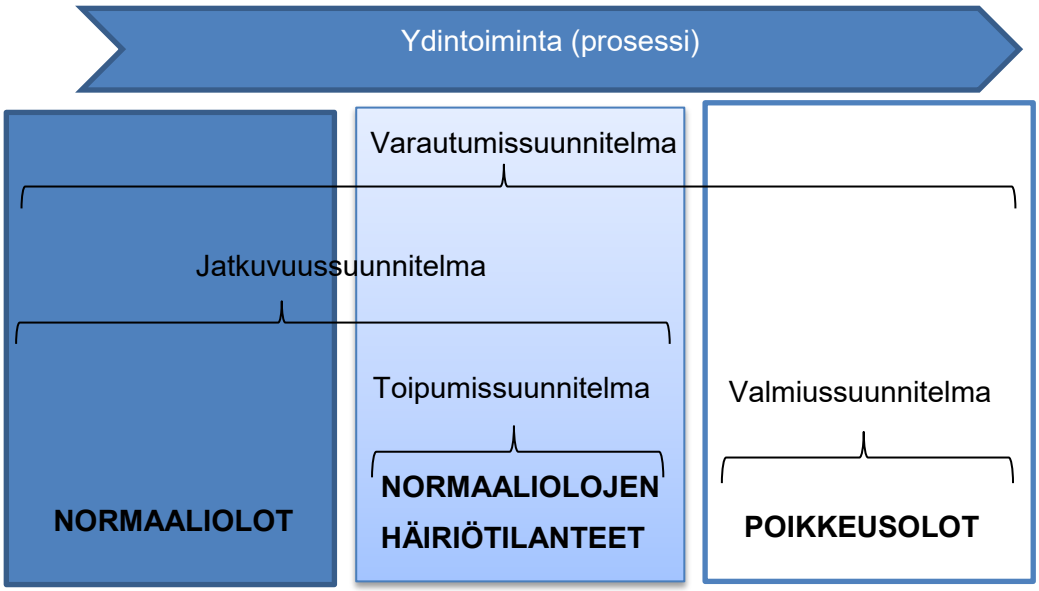
Nämä elementit ovat osin päällekkäisiä riskienhallinnan kanssa, ja riskienhallintaa ja jatkuvuudenhallintaa voidaankin pitää toisiaan vahvistavina tehtävinä.

Jatkuvuudenhallinnalla on siis perimmäisenä tarkoituksena luoda ja dokumentoida suunnitelma, miten organisaatio reagoi ja toimii erilaisissa häiriötilanteissa. Jatkuvuudenhallinta ei ole, kuten ei riskienhallintakaan, kertaluonteinen tehtävä, vaan sen kehittäminen tulisi olla jatkuvaa toimintaa ja sen toimivuutta tulisi myös testata säännöllisesti.

6.2.1 Jatkuvuudenhallinnan käsitteet

Jatkuvuudenhallinnan käsitteisiin kuuluu keskeisesti varautumissuunnitelma, jatkuvuussuunnitelmat, toipumissuunnitelmat ja valmiussuunnitelma. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen -teoksessa Iivari ja Laaksonen esittävät, että käsitteiden eroja on helpompi ymmärtää, jos ymmärretään ensin häiriöiden laajuuksien ja vaikutuksien erot.

Kuviossa 11 esitetyt normaaliolot ja normaaliolojen häiriötilanteet eroavat siinä, että normaaliolossa organisaatioon voi kohdistua merkitykseltään pieniä lyhytkestoisia häiriöitä, jotka vaikuttavat vain organisaation sisällä ja ne voidaan korjata perustyötehtävien ohessa. Normaaliolojen häiriötilanteet ovat edelleen organisaation sisäisiä häiriöitä, mutta ovat merkitykseltään suurempia, kuten esimerkiksi organisaatioon kohdistunut vakava onnettomuus. Normaaliolojen häiriötilanteita voidaan kutsua myös poikkeustilanteiksi. Poikkeusoloilla puolestaan tarkoitetaan laajempaa, yhteiskunnallista erityistilannetta, joita voivat olla muun muassa sähköinfrastruktuurin häiriöt, suuronnettomuudet, luonnonkatastrofit ja taloudellisen tilanteen vakavat häiriöt. (Iivari & Laaksonen 2009, 18)



Kuvio 11. Jatkuvuudenhallinnan käsitteet. (Iivari & Laaksonen 2009, 19)

Iivari ja Laaksonen esittävät, että termit varautumissuunnitelma ja valmiussuunnitelma eivät ole täysin vakiintuneet. Heidän väitteensä mukaan näiden käytössä on eroja varsinkin julkisella ja yksityisellä puolella. Näitä voidaan pitää toistensa synonyymeinä tai valmiussuunnitelma osana varautumissuunnitelmaa. (Iivari & Laaksonen 2009, 19)

Varautumissuunnitelma on laaja dokumentti, joka käsittää kuvaukset toimintaohjeista, tehtävistä ja rooleista aina normaalioloista poikkeusoloihin. Jatkuvuussuunnitelmissa toiminnan ohjeistus kattaa kapeamman osan häiriötilanteiden laajuudesta ja ne keskittyvät lähinnä normaalioloista merkittävämpiin häiriötilanteisiin eli normaaliolojen häiriötilanteisiin. Toipumissuunnitelmat kuuluvat osana jatkuvuussuunnitelmaa ja näiden tehtävänä on esittää ohjeet ja tiedot häiriötilanteesta toipumiseen, kuten varajärjestelmien vaatimukset, vastuuroolit ja toimintaohjeet. Toipumissuunnitelmat ovat yleensä järjestelmä- ja prosessikohtaisia, lyhyen aikajänteen suunnitelmia. Valmiussuunnitelmat kattavat yleensä vain harvinaisempien poikkeusolojen aikaisen toiminnan ohjeistuksen ja suunnitelmat. (Iivari & Laaksonen 2009, 19-21)

Julkisen ja yksityisen puolen organisaatioiden jatkuvuudenhallinnat eroavat myös siinä, että julkisen hallinnon toimielimiä velvoitetaan valmiuslailla (1552/2011), jolla varmistetaan yhteiskunnan toimivuus poikkeusoloissa. Näin ollen julkisella puolella on tehtävä suunnitelmat poikkeusolojen varalta ja varsinkin niiden viranomaisten, jotka tarjoavat yhteiskunnalle elintärkeät toiminnot. Vaikka Celia on velvoitettu toteuttamaan valmiuslain

perusteella suunnitelmat häiriö- ja poikkeustilanteiden varalta, Celialla ei ole vastuuta yhteiskunnan välttämättömimmistä toiminnoista.

6.2.2 Jatkuvuussuunnitelman laatiminen

Jatkuvuussuunnitelman laatimiselle ei ole yhtä ainoaa oikeaa vaihtoehtoa. Olen mukaillut kuviossa 12 Iivarin ja Laaksosen kuvausta jatkuvuussuunnittelutyön eri vaiheista.

Kuvio 12. Jatkuvuussuunnitelman laatimisen vaiheet. (Iivari & Laaksonen 2009, 93)

Kuviossa 12 esitetään Jatkuvuussuunnittelun toteuttamiseksi eri vaiheet alkaen suunnittelemalla vastuuroolit ja ohjeistus. Koordinoinnin, ohjeistuksen ja vastuiden nimeämisen jälkeen tehtävänä on tunnistaa organisaation kriittisimmät prosessit ja palvelut sekä luokitella ne kriittisyyden mukaan. Kriittisimpien prosesseja vastaan tunnistetaan ja analysoidaan riskit, jonka jälkeen toteutetaan vaikutusanalyysi. Vaikutusanalyysi voidaan toteuttaa toiminnan vaikutusanalyysi BIA-työkalulla (Business Impact Analysis), joka on

saatavilla Valtionvarainministeriön verkkosivuilta VAHTI-ohjeesta. Kuten Iivari ja Laaksonen toteavat, liiketoiminnan vaikutusanalyysia ja riskianalyysia ei voi helposti erottaa toisistaan. Liiketoiminnan vaikutusanalyysi täydentää riskianalyysia syventyen tarkemmin tarkasteltavan kohteen vaikutuksiin häiriö- tai tiedon menetystilanteissa. (Iivari & Laaksonen 2009, 138). BIA-työkalun avulla organisaatio voi siis kartoittaa erilaisten riskien toteutumisen toiminnalliset vaikutukset. Kun riskit ja niiden vaikutukset on tunnistettu, toteutetaan riskienhallintastrategiat ja prosessien kehittäminen riskien torjumiseksi. Lopuksi kuvataan toimintasuunnitelmat, suunnitelmat testataan ja koulutetaan asianosaiset henkilöt.

Prosessikuvaukset ovat tärkeä osa organisaation johtamis- ja hallintamenetelmää. Kuvausten avulla pystytään varmistamaan kokonaiskuvan hallinta organisaation liiketoiminnassa. Kuvauksilla on sekä informatiivinen tehtävä kuin myös kehittämis- ja muutostilanteiden suunnittelussa tarvittavana työkaluna, jota hyödynnetään muun muassa vaikutusten arvioinnissa. Prosessien kuvaus on myös edellytys onnistuneelle jatkuvuussuunnittelulle. Jatkuvuussuunnittelussa tarvitaan niin ikään organisaation strategisten prosessien kuvauksia kriittisten prosessien arviointia varten kuin myös operatiivisen tason toimintaohjeiden kuvaamiseen häiriötilanteissa.

Jatkuvuussuunnittelussa yhtenä tärkeänä osana on myös kuvata viestinnän toteutus häiriötilanteissa. Kuvauksissa tulisi ilmetä ohjeet sekä sisäiseen että ulkoiseen tiedottamiseen, roolit ja vastuut, sidosryhmät sekä kontaktipisteet yhteystietoineen. Kuviossa 13 on esitetty JUDO-hankkeen kolmannen työpajan materiaalissa kuvattu prosessimalli viestinnän tehtävistä häiriötilanteessa, jossa esitetään viestinnän tehtävät häiriötilanteen ilmaantumisesta aina sen päättymiseen saakka.

Kuvio 13. Sisäinen ja ulkoinen viestintä häiriötilanteissa. (JUDO-hanke 3# 2019, 79)

7 Tutkimuksen kehittämiskohteiden toteutus

7.1 Nykytilan selvittäminen

Nykytilan selvittämiseksi toteutin haastatteluja ja kaksi eri arviointikyselyä. Ensimmäisenä laajempana kyselynä käytin Kuntaliiton kehittämää varautumisen ja jatkuvuudenhallinnan kehittämistoimenpiteiden tarpeellisuuden arviointi KUJA-pikatestiä. Toisena kyselynä käytin julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) sihteeristön laatimalla digiturvakyselyä. Nykytilan arvioinnin lisäksi hyödynnän näitä testejä tämän tutkimuksen mittareina. Toteutin testit tutkimuksen alussa sekä lopussa, joiden tulosten eroista voin todistaa kehittymisen.

7.1.1 Haastattelu

Haastateltuani kirjaston johtajaa, selvisi, että Celiassa on olemassa johtokunnan vuonna 2007 hyväksymä Celian sisäisen valvonnan ohjesääntö. Ohjesäännössä kuvataan Celian velvollisuudet sisäiseen valvontaan ja ohjeistus riskienhallintaan. Vaikka ohjesäännössä esitetään riskienhallinnan toteuttamisen velvoite ja ylätason ohjeistus, olimme samaa mieltä kirjastonjohtajan kanssa siitä, että on tarpeellista päivittää riskienhallinnan

ohjeistusta uudella riskienhallintapolitiikalla, jossa yhdistyy aikaisemmin kuvattu (kt. luku 6.2.1) riskienhallintapolitiikka ja riskienhallinnan periaatteet -dokumenttien tehtävät.

Haastateltaessa kirjastonjohtajaa, sovimme myös sen, että tulen toteuttamaan jatkuvuudenhallintaa priorisoiden tehtävät tarvelähtöisesti. Aloitan Celian jatkuvuudenhallinnan kehittämistyön rakentamalla ensin toimintaohjeet jatkuvuussuunnitelmineen ja siitä eteenpäin aina koko organisaatiotasoiseen valmiussuunnitelmaan.

7.1.2 KUJA-pikatesti

KUJA-pikatestissä arvioidaan karkealla tasolla organisaation jatkuvuudenhallinnan tasoa ja sen tulokset ohjaavat organisaation kehittämistarpeita. Testissä on kymmenen väittämää, joista arvioijan tulee valita, onko väittämä kunnossa (0 pistettä), osittain kunnossa / selvitettävä (2 pistettä) tai ei kunnossa (4 pistettä). Arvioitujen väittämien yhteen laskettu pistemäärä antaa tuloksen organisaation jatkuvuudenhallinnan tasosta ja ohjeistuksen kehitystoimenpiteisiin. Tulokset on jaettu kolmeen osaan, jossa alle 8 pistettä saaneilla riski on pieni ja varautumisen sekä jatkuvuudenhallinnan taso on hyvä. 8-14 pistettä saaneilla riski on jonkin verran lisääntynyt ja pieniä korjaavia kehitystoimenpiteitä tulisi toteuttaa. 15-25 pistettä tarkoittaa jo kohtalaista riskitasoa, jossa varautumisessa ja jatkuvuudenhallinnassa on selkeitä puutteita. 26-40 pistettä saaneilla riski on suuri ja organisaatiossa on selkeitä ja vakavia puutteita jatkuvuudenhallinnassa. (Kuntaliitto 2018)

KUJA-PIKATESTI VARAUTUMISEN JA JATKUVUUDENHALLINNAN KEHITTÄMISTOIMENPITEIDEN TARPEELLISUUDEN ARVIOINTI

Tällä pikatestillä voitte kartoittaa varautumisen ja jatkuvuudenhallinnan tasoa sekä kehittämistoimenpiteiden tarpeellisuutta organisaatiossanne.

Nro.	Arviointikysymys	Arvio nykytilasta			Lisäselvitys tarvittaessa
		Kunnossa	Osittain kunnossa / selvitettävä	Ei kunnossa	
1.	Varautumisen ja jatkuvuudenhallinnan perusteet ja vaatimukset on tunnistettu (esim. lainsäädäntö, sidosryhmävaatimukset). Varautumisen ja jatkuvuudenhallinnan toimintamalli on kuvattu sekä ohjeistettu. Varautumiseen liittyvät vastuut ja roolit on määritelty kirjallisesti.				
2.	Varautumisen ohjaamiseen ja kehittämiseen on varattu riittävästi resursseja. Minimissään organisaatiotason varautumisen koordinaattori (vast.) on nimetty, koulutettu sekä työaikaa on osoitettu koordinoimisen toteuttamiseksi.				
3.	Varautumisen ja jatkuvuudenhallinnan kaikki keskeiset suunnitelmat ja toimintakortit on laadittu/päivitetty kolmen vuoden sisällä ja organisaation ylin johto on ne hyväksynyt.				
4.	Käytettävissä on selkeä toimintamalli vakavissa häiriötilanteissa avainhenkilöiden hälyttämiseksi, toiminnan johtamiseksi sekä kriisiviestintään.				
5.	Toimintamallit ja suunnitelmat ovat helposti saatavilla ja henkilöstö on perehtynyt niihin. Toiminnan kannalta keskeiset henkilöt kaikilla tasoilla on perehdytetty toimintamallien ja suunnitelmien keskeisiin kohtiin.				
6.	Kaikissa tilanteissa ylläpidettävät kriittiset toiminnot ja tehtävät on tunnistettu. Myös näiden ylläpitämiseen liittyvät kriittiset järjestelmät, toiminnot ja tehtävät on tunnistettu ja määritetty riittävät hallintakeinot.				
7.	Koulutus ja harjoittelu on suunnitelmallista sekä säännöllistä. Koulutuksia ja harjoituksia järjestetään organisaation kaikilla tasoilla huomioiden henkilöiden roolit sekä tehtävät osana organisaation varautumista. Koulutuksien ja harjoituksien toteutumista seurataan.				
8.	Riskienhallinnan perusteet on määritelty ja riskienhallinnassa on läpi organisaation ohjeistettu menettelytapa. Riskien arvioinneissa otetaan huomioon toiminnan häiriöttömyyteen vaikuttavat toiminnalliset ja vahinkoriskit. Merkittävimpiä riskejä seurataan ja niiden hallinnasta raportoidaan säännöllisesti.				
9.	Organisaatio on tunnistanut dokumentoidusti keskeiset sidosryhmät ja ulkoiset palveluntuottajat. Varautumisvastuut, yhteistoimintajärjestelyt sekä varajärjestelyt häiriötilanteissa on sovittu ja kuvattu, tarvittaessa sopimuksin.				

Kuvio 14. KUJA-pikatesti. (Kuntaliitto 2018)

Nykytila-analyysia varten pyysin Celian johtoryhmän jäseniä sekä tietohallinnon ICT-asiantuntijoita täyttämään KUJA-pikatestin. Yhteensä kymmenestä arviosta saaduista pistemääristä laskin keskiarvon, jota käytän Celian varautumisen ja jatkuvuudenhallinnan tason laskemiseen. Tulosten keskiarvona saimme 30 pistettä, joten lähtötasona riskimme on suuri ja kehittämistyötä on tehtävä. Tämän tutkimuksen yhtenä tavoitteena oli saada lopputestissä vähintään yhden tason parempi tulos. Havaitsin testitilanteessa useamman henkilön myöntävän, etteivät täysin ymmärtäneet kaikkia kysymyksiä. Heillä ei ollut myöskään näiden osalta tietoa, millä tasolla väittämät on toteutettu Celiassa. Tämä havainto vahvisti hypoteesia Celian heikosta tietämyksen tasosta riskienhallinnassa ja varautumisessa.

7.1.3 Digiturvakysely

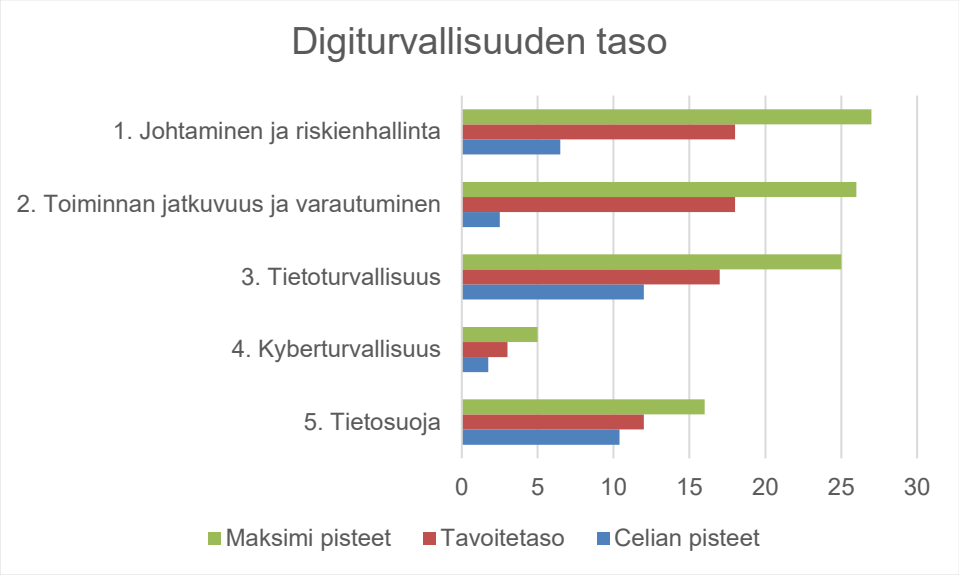
Väestörekisterin toteuttama ja VAHTI -sihteeristön laatima digiturvakysely lähetettiin täytettäväksi vuoden 2019 alussa kaikille julkishallinnon organisaatioille, ja sen tarkoituksena oli mitata kansallista tietoturvan tasoa. Celiassa kysely arvioitiin tietohallinnon toimesta. Hyödynsin tässä työssä alkuvuotena arvioitujen digiturvakyselyn tuloksia kuvaamaan Celian nykytilaa. Digiturvallisuuden mittaamisessa käytettiin viittä eri osatekijää, joille jokaiselle oli asetettu väittämiä arvioitavaksi.

Alla olevasta taulukossa 1 näkyy kyselystä saadut Celian tulokset sekä maksimipisteet. Näiden lisäksi olen lisännyt oman sarakkeen tavoitetasosta, jota tämän tutkimuksen avulla pyrittiin saavuttamaan.

Taulukko 1. Digiturvakyselyn tulokset lähtötilan arvioimiseksi.

Digiturvan osa- alueet	Celian pisteet	Tavoitetaso	Maksimi-pisteet
5. Tietosuoja	10,4	12	16
4. Kyberturvallisuus	1,75	3	5
3. Tietoturvallisuus	12	17	25
2. Toiminnan jatkuvuus ja varautuminen	2,5	18	26
1. Johtaminen ja riskienhallinta	6,5	18	27

Jotta pistetaulukkoa on helpompi havainnoida, olen kuvannut tulokset myös kuviossa 15 esitetyllä kaaviolla.



Kuvio 15. Digiturvallisuuden taso.

Kuviossa 15 esitetyistä tuloksista näkee, että jokaisessa osa-alueessa on kehitettävää. Varsinkin toiminnan jatkuvuudessa ja varautumisessa sekä johtamisessa ja riskienhallinnassa on eniten puutteita. Tavoitetasot esittävät sitä tasoa, mitä tämän tutkimuksen avulla pyritään saavuttamaan. Tavoitetasot ovat tarkoituksella maksimitason alapuolella, sillä digitaalista turvallisuustasoa on lähes mahdoton saavuttaa sataprosenttisesti siihen

vaikuttavan ympäristön jatkuvan muutostilan vuoksi. Tärkeintä on saavuttaa sellainen taso, joka turvaa organisaation kriittisimmät toiminnot ja joka vastaa lain velvoittamia vähimmäisvaatimuksia.

7.2 Tutkimuksen riskianalyysi

Koska tutkimukseni käsittelee riskienhallintaa, olen testannut valitsemaani riskianalyysimallia myös tämän tutkimuksen analysoimisessa. Alla olevassa kuviossa 16 esitetyssä riskianalyysissä olen esittänyt tässä tutkimuksessa tunnistamiani mahdollisia riskitilanteita. Jokaiselle riskille olen antanut sen toteutumisen todennäköisyyden arvon asteikolla 1-4, riskin vaikutuksen arvon asteikolla 1-4 ja näiden edellisten arvioitujen pisteiden tuloksen (todennäköisyys x vaikutus), joka esittää riskin suuruutta. Riskienhallintatyökalu mittaa automaattisesti toimenpidetarpeet ja -ehdotukset riskin suuruuden perusteella. Olen kuvannut niille riskille toimenpidekuvauksen, jossa toimenpide-ehdotus vaatii suunnitelman laatimista.

Riskien tunnistaminen					Riskianalyysi		Riskin merkityksen arviointi		Riskin käsittely			
Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys	Vaikutus	Riskin suuruus (T x V)	Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyk	Toimenpide-ehdotukset riskin käsittelylle	Toimenpiteiden vapaamuotoinen (sanallinen) kuvaus	Vastuuhenkilö	Tavoiteaikataulu (mihin mennessä
OPNT01	2 Operatiivinen	Johdon tuki	Kehittämistyölle ei saada riittävästi aikaa ja tukea johdolta	2 Mahdollinen	3 Merkittävä	6 Merkittävä riski	3 Huomioitava riski	3 Luotava suunnitelma pienentämiseksi	Riskiä voi pienentää viittaamalla kirjalliseen sopimukseen kehittämistyön teosta	Kehittämistyön tekijä	Riskin realisoituessa
OPNT02	2 Operatiivinen	Resurssiriski	Kehittämistyö viivästyy avainhenkilöiden estymisen vuoksi	2 Mahdollinen	4 Kriittinen	8 Merkittävä riski	3 Huomioitava riski	3 Luotava suunnitelma pienentämiseksi	Riskiin ei voi vaikuttaa		
OPNT03	2 Operatiivinen	Nykytila-analyysin puutteet	Nykytila-analyysi ei ole tarpeeksi kattava	1 Epätodennäköinen	2 Kohtalainen	2 Ei riskiä	1 Ei riskiä	1 Ei vaadi akuutteja toimenpiteitä			
OPNT04	2 Operatiivinen	Mittarit	Kehitystyössä käytetyt mittarit eivät mittaa tarkoitusta	1 Epätodennäköinen	2 Kohtalainen	2 Ei riskiä	1 Ei riskiä	1 Ei vaadi akuutteja toimenpiteitä			

Kuvio 16. Tutkimustyön riskianalyysi.

Tunnistin tutkimustyöhön kohdistuviksi mahdollisiksi riskeiksi seuraavat:

1. johdon tuki: kehittämistyölle ei saada riittävästi aikaa ja tukea johdolta,
2. resurssiriskit: tutkimustyö viivästyy avainhenkilöiden estymisen vuoksi,
3. nykytila-analyysin puutteet: nykytila-analyysi ei ole tarpeeksi kattava ja
4. mittarit: tutkimustyössä käytetyt mittarit eivät mittaa tarkoitusta.

Näistä tunnistetuista riskeistä suurimmat arvot saivat johdon tuen puute ja resurssiriskit, joille kirjasin molemmille käsittelysuunnitelmat riskien pienentämiseksi. Johdon tuki -riskiä voidaan pienentää Celian ja oppilaitoksen välisellä kolmikantasopimuksella tutkimustyön toteuttamisesta. Resurssiriskiin ei tämän tutkimuksen osalta voida vaikuttaa, joten se jäi jäännösriskiksi.

7.3 Celian riskienhallintapolitiikan luominen

Riskienhallintapolitiikka ohjaa Celian riskienhallinnan toteutusta ja mahdollistaa niiden riskien tunnistamista, joita tarvitaan päätöstenteon tueksi. Tarkoituksena on saavuttaa Celian eri yksiköiden välillä yhtenäinen käytäntö, joka pohjautuu sovittuun riskienhallintaprosessiin. Riskienhallinnan prosessi on systemaattinen, riskienhallintapolitiikassa sovittu tapa, jolla riskejä tunnistetaan, arvioidaan ja käsitellään.

Celian riskienhallintapolitiikan laatimiseen käytin pohjamateriaalina Valtiovarainministeriön julkaisemaa riskienhallintapolitiikkamallia. Malli varmistaa, että sitä hyödyntävä virasto tai laitos toteuttaa riskienhallintapolitiikassa suositellut vähimmäisvaatimukset ja että organisaation käsitys riskeistään on ajantasainen ja riittävän kattava sekä tarvittavat vastuut on määritelty. Riskienhallintapolitiikkamallissa on hyödynnetty riskienhallinnan tunnettuja standardeja, kuten ISO 31000, COSO-ERM ja PESTLE:ä. (Valtionvarainministeriö 2019)

Haastattelemalla kehittämisjohtajaa sekä kirjastonjohtajaa sain tarvittavat tiedot mallin muokkaamiseen Celian toimintaan sopivaksi ja varmistettua riskienhallintaan nimettävät vastuuhenkilöt. Celian riskienhallintapolitiikka koostuu mallin mukaisesti seuraavista osista:

1. Riskienhallinnan soveltamisalan esittely, jossa esitetään yleisellä tasolla riskienhallinnan soveltaminen Celiassa ja kenelle dokumentti on tarkoitettu käytettäväksi.

2. Säädöspohja sekä muut määräykset ja ohjeet -kohdassa kuvataan riskienhallintaa ohjaavat lait ja asetukset, kuten valtion talousarviolaki (423/1988), EU:n yleinen tietosuoja-asetus sekä vuoden 2020 alussa voimaan tuleva Tiedonhallintalaki.

3. Keskeiset käsitteet -kohdassa esitetään riskienhallinnan käsitteet ja niiden merkitykset. Varsinaisessa politiikkadokumentissa esitettyjen käsitteiden lisäksi politiikkaan kuuluvassa liite 1:ssä on laajempi kuvaus riskienhallintaa koskevista käsitteistä ja niiden merkityksistä.

4. Riskienhallinnan tavoitteet -kohdassa esitellään kaikki ne tavoitteet, mitä riskienhallinnalla tulisi saavuttaa. Näitä ovat esimerkiksi ennakoivan ja hyvän johtamis- ja hallintotavan vahvistaminen, talouden ja toiminnan laillisuuden varmistaminen sekä se, että riskinottohalukkuus on tietoista eikä hallitsemattomat riskit pääse vaikuttamaan Celian toimintaan.

5. Riskienhallinnan periaatteet -kohdassa on lueteltu Celialle keskeisimmät periaatteet, jotka ohjaavat riskienhallinnan toteutusta. Näitä ovat muun muassa riskienhallinnan avulla saavutettu lisäarvo tavoitteiden onnistumiselle, riskienhallinnan oleellisuus ja tärkeys johtamisessa ja päätöksenteossa, riskienhallinnan toteuttamisen järjestelmällisyys, avoimuus ja sen kehittäminen.

6. Riskienhallinnan vastuut -kohdassa on esitetty riskienhallintaa koskevat roolit ja nimetyt vastuuhenkilöt sekä heille kuuluvat tehtävät. Roolit on jaettu Celian johtokunnasta aina työntekijöihin asti:
    - Johtokunta on hyväksynyt Celian sisäisen valvonnan ohjesäännön, joka luo perustan Celian riksienhallintapolitiikalle.
    - Kirjastonjohtaja hyväksyy riksienhallintapolitiikan ja talous- ja hallintojohtaja vastaa sisäisestä valvonnasta sekä riskienhallinnan toteuttamisesta Celiassa. Johto varmistaa myös riskienhallinnan toteuttamisen strategisissa prosesseissa ja tulosohjauksessa.
    - Johtajat ja päälliköt vastaavat oman yksikkönsä vastuualueen riskienhallinnasta. Johtoryhmä käsittelee organisaatiotasoiset riskit ja niiden käsittelytoimenpiteet vuosikellon mukaisesti.
    - Hankkeet, projektit tai työryhmät vastaavat vastuualueittensa riskienhallinnasta suhteessa tehtävään ja sen tavoitteiden saavuttamiseen.
    - Henkilöstö arvio ja tunnistaa omaan työhön liittyviä riskejä ja välittää tiedon niistä päällikölle.
    - Edellä kuvattujen roolien lisäksi riskienhallinnan koordinoinnista ja toteutumisen seurannasta vastaavaksi nimettiin erillinen riskienhallinnan asiantuntija.

7. Riskienhallintaprosessi ja siihen kuuluvat tehtävät ohjeineen on kuvattu dokumentin erillisessä liitteessä. Liitteessä esitetään riskienhallintaprosessin kuvaus, mitä riskiluokituksia ja arvoasteikkoja Celian riskienarvioinnissa tulee käyttää sekä kerrotaan millä tavoin riskejä voidaan tunnistaa, arvioida ja käsitellä. Nämä

luokitukset, arvoasteikot ja tehtävät esittelen tarkemmin riskianalyysityökalu-kohdassa.

8. Riskienhallinnan arviointi ja kehittäminen -kohdassa määritellään rikienhallinnan asiantuntijan tehtävät Celian riskienhallinnan arvioinnissa ja sen kehittämisessä. Asiantuntijan tulee esittää arviointi ja kehittämisehdotukset vuosittain johtoryhmässä ja ne kirjataan Celian toimintakertomukseen. (Valtionvarainministeriö 2019)

Riskienhallintapolitiikan liitteinä olevien käsite- ja riskienhallintaprosessin kuvausten lisäksi lisäsin politiikan liitteeksi valitsemani Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) -ohjesivuilta saatavan riskienhallintatyökalun (liite 1) Celian riskienarviointityön tueksi. (VAHTI 2017)

Kuvasin myös Celian riskienhallinnan vuosikellon ja siihen liittyvien tehtävien ja roolien prosessikuvauksen (liite 2). Riskienhallintapolitiikan mukaisesti riskien arviointi ja käsittely tullaan liittämään koko organisaation tasolla yksiköiden omiin toimintasuunnitelmiin sekä Celian yhteiseen strategiseen toimintasuunnitelmaan ja tulossopimukseen. Riskienhallintaa tullaan toteuttamaan lisäksi kaikissa kehitystyöryhmissä, hankkeissa ja projekteissa sekä riskiarvioinnit tulee laatia strategisten palveluiden mahdollistaville järjestelmille.

Riskienhallintapolitiikka hyväksyttiin johtoryhmässä kirjastonjohtajan allekirjoituksella ja sen soveltaminen aloitetaan ensi vuoden alusta. Henkilöstön koulutus riskienhallintapolitiikkaan toteutetaan myöhemmin vuoden lopulla järjestettävässä henkilökuntatilaisuudessa.

7.4 Riskienhallintatyökalu

Kuten edellä mainitsin, valitsin riskianalyysin työkaluksi VAHTI -ohjesivuilta löytyvän valmiin riskienhallintatyökalun, jonka lisäsin Celian riskienhallintapolitiikan liitteeksi. Työkalu jakautuu neljään osa-alueeseen, jotka ovat riskien tunnistaminen, riskien analysoiminen, riskien merkityksen arviointi ja riskin käsittely. Riskienhallintatyökalu toteuttaa yhteenvetoraportin analysoiduista riskeistä, joista saadaan helposti tulkittava kuvaus arvioidun kohteen riskitasosta.

Riskienarviointia aloittaessa, arvioijien tulee määritellä ja kirjata arvioinnin lähtötiedot, kuten riskiarvioinnin kohde, arviointiin osallistuvat henkilöt, käytettävät riskiluokat ja riskiarvioinnissa käytettävät arvot. Riskiluokiksi valitsimme työkalun oletusluokat, jotka ovat myös samat, mitä Celian riskienhallintapolitiikassa on sovittu:

1. strateginen riski (vaikutus organisaation tavoitteisiin)
2. taloudellinen riski (vaikutus talouteen ja varojen käyttöön)
3. operatiivinen riski (vaikutus toimintaan ja palveluun)
4. vahinkoriski (vaikutus ihmisiin, toimitiloihin ja laitteisiin) (Kangas 2017, 8)

Riskien tunnistamisosiossa arvioijat kirjaavat ylös tunnistetut riskit, määrittelevät riskeille luokan, yksilöivän tunnisteen ja riskin nimen. Riskien analysointiosassa määritellään riskeille todennäköisyyden ja vaikutuksen arvot. Näiden arvoiksi valitsimme niin ikään työkalun oletusarvot. Käyttämämme riskien todennäköisyysarvot olivat:

1. Epätodennäköinen, kun riskin realisoitumisen mahdollisuus on vain teoreettisella tasolla tai riskin realisoituminen voi tapahtua vain harvinaisissa poikkeustilanteissa.
2. Mahdollinen, kun riski voi realisoitua joissain tietyissä tilanteissa.
3. Todennäköinen, kun riski on melkein tai kokonaan realisoitunut vähintään kerran.
4. Lähes varma, jolloin riskin realisoitumisen todennäköisyys on suuri ja se on tapahtunut usein. (Kangas 2017, 9)

Vaikutuksen arvioinnissa tulisi arvioida, miten riskin realisoituminen tulee vaikuttamaan organisaation strategiaan. Vaikutuksen arvioinnissa käytettävät arvot ovat:

1. Vähäinen tai ei lainkaan, kun riskin realisoitumisesta aiheutuu vain vähäinen haitta strategisen tavoitteen saavuttamiselle.
2. Kohtalainen, kun riskin realisoituminen ei estä, mutta viivästyttää tai heikentää strategisten tavoitteiden saavuttamista.
3. Merkittävä, kun strategisten tavoitteiden saavuttaminen on vaarantunut merkittävästi. Vaikutus on niin suuri, että se aiheuttaa mahdollisesti kustannusten nousua, omaisuuden tai terveyden vaarantumista tai mainehaittaa.
4. Kriittinen, kun riskin realisoituminen estää tai keskeyttää kokonaan strategisen tavoitteen saavuttamisen. (Kangas 2017, 9)

Riskien merkityksen arviointiosioissa työkalu laskee riskien suuruuden automaattisesti todennäköisyyden ja vaikutuksen arvojen tulona. Riskien suuruutta kuvaavat tulot jakautuvat neljään arvoon, joiden perusteella työkalu laskee myös toimenpidetarpeet riskien käsittelylle. Riskien suuruuden ja toimintatarpeet käsittelylle -arvot ovat samat, vaikka laskennallisesti näillä on eri numeroarvot:

1. Ei riskiä
2. Huomioitava riski
3. Merkittävä riski
4. Sietämätön riski (Kangas 2017, 10)

Riskien käsittely -osiossa työkalu laskee automaattisesi toimenpide-ehdotuksien arvot riskien käsittelylle:

1. Ei vaadi akuutteja toimenpiteitä
2. Seurattava riskin kehittymistä
3. Luotava suunnitelma pienentämiseksi
4. Vaatii välittömiä toimenpiteitä (Kangas 2017, 12)

Niille riskeille, jotka ovat saaneet toimenpide-ehdotuksen tuloksena listan kaksi viimeistä vaihtoehtoa, laaditaan suunnitelma riskien käsittelyyn. Riskien käsittelylle kirjataan riskinkäsittelyn toimenpiteiden kuvaus, vastuuhenkilö ja tavoiteaikataulu.

7.5 Kriittiset prosessit ja palvelut

Niin riskienhallinta kuin myös varautumissuunnitelman toteuttamisen lähtökohtana on tunnistaa organisaation kriittiset prosessit ja palvelut. Kriittisten prosessien ja palveluiden tunnistaminen on hyvä aloittaa määrittelemällä ylätasolla organisaation ydintehtävää tukevat prosessit ja niihin liittyvät tiedot. Näiden tunnistamisen jälkeen voidaan jatkaa tarkemmalle tasolle, jossa tunnistetaan edellä mainittuihin liittyvät tukevat kohteet, kuten ohjelmistot ja palvelut, tietoliikenneverkot, henkilöstö, toimipaikka sekä organisaation rakenne. (Kirves & Ahokas 2019, 38)

Tässä tutkimuksessa sovelsin kriittisten järjestelmien määrittelemiseksi Väestörekisterikeskuksen laatimaa Excel-pohjaista Palveluiden kriittisyysluokittelutyökalua Palkoa (ks. liite 1), jonka tarkoituksena on määritellä organisaation kriittisiä prosesseja ja palveluita.

Kriittisten palveluiden ja prosessien sijaan kohdensin arvioinnin näitä tukevien järjestelmien määrittelemiseen ja tunnistamiseen. Palko-työkalussa kirjataan ylös määritelty kriittinen palvelu, prosessi tai järjestelmä omalle rivilleen ja tälle analysoitavalle kriittiselle kohteelle määritellään numeeriset arvot suhteessa seuraaviin tekijöihin:

- palvelun toiminnallisuus/saatavuus
- julkisuuskuva
- lakisääteiset tehtävät (lait, määräykset, ohjeet)
- taloudelliset vaikutukset (vaikutus resurssin käyttöön, sanktiot, korkeakoulut jne)
- tiedon eheys.

Määrittelyn jälkeen työkalu laskee arvioitavan kriittisen kohteen kokonaisvaikutuksen sekä kriittisyystason. Työkalun toiselle sivulle päivittyy raportti määritellyistä kohteista, jotka on jaettu kolmiasteiseen kriittisyysluokkaan käytettävyysvaateen mukaan. 1-tason kriittisyysluokkaan kuuluvat ne prosessit, palvelut tai järjestelmät, joiden turvaaminen tulee varmistaa kaikissa olosuhteissa. 2-tason kriittisyysluokkaan kuuluvat ne kohteet, jotka voidaan harkinnan ja tilanteen mukaan keskeyttää. 3-taso puolestaan kuvaan niitä palveluita, prosesseja tai järjestelmiä, jotka eivät ole niin kriittisiä ja jotka voidaan palauttaa häiriötilanteissa viimeisenä.

Arvioimme Celian järjestelmiä Palko-työkalun avulla ensin järjestelmäasiantuntijan ja kehittämisjohtajan kanssa, jonka jälkeen käsittelin tulokset vielä asiakkuushallinnan yhteistyöryhmän kanssa, jotta arviointeihin saatiin laajempi näkökanta. Arviointi oli osin haastavaa, sillä se mikä on kriittistä Celialle ei ole välttämättä niin kriittistä koko valtiohallinnon tasolla. Sen vuoksi arvioinnissa tuli ymmärtää, millä tasolla haluamme arvioida kriittisyyttä ja miten se vastaa eniten Celian tavoitteita.

Tuloksena saimme yhden 1-tason ja 4 kappaletta 2-tason kriittisyysluokan järjestelmää. Loput arvioidut järjestelmät ja palveluratkaisut asettuivat 3-tason kriittisyysluokkaan. 1- ja 2-tason kriittisille järjestelmille tulisi laatia jatkuvuussuunnitelmat häiriötilanteiden varalle.

7.6 Jatkuvuussuunnitelman toteuttaminen

Tässä tutkimuksessa soveltamani Palko-työkalun käyttö on yksinkertainen tapa määritellä ne kriittiset palvelut ja prosessit tai järjestelmät, joita vasten on myös suunniteltava

riskienhallinta sekä varautuminen. Tämän tutkimuksen aikana oli tarkoitus toteuttaa jatkuvuussuunnitelmat 1- ja 2-tason kriittisille järjestelmille, mutta aikataulun sekä avainhenkilöiden estymisen vuoksi jatkuvuussuunnitelma toteutettiin ainoastaan arvioidulle 1-tason kriittisyysluokan järjestelmälle. Tietoturvasyistä esittelen tästä eteenpäin valitsemaani järjestelmää X-nimellä. 2-tason kriittisyysluokitelluille järjestelmille toteutan jatkuvuussuunnitelmat jatkokehityksenä tämän tutkimushankkeen jälkeen.

Kriittisen järjestelmämme X jatkuvuussuunnitelma-dokumentin laadintaan hyödynsin soveltaen VAHTI 2/2016 – ohjeen liite 3:ssa esitetyn palvelun jatkuvuussuunnitelman sisällysluettelorunkoesimerkkiä. Liitteessä esitetty sisällysluettelorunkoesimerkki ohjaa myös tässä työssä aiemmin esitettyä jatkuvuussuunnitteluprosessin tehtäviä. (Pietikäinen 2016)

Järjestelmämme X jatkuvuussuunnitelma sisältää seuraavat kohdat ja kuvaukset:

1. Johdanto, jossa esitetään jatkuvuussuunnitelman tarkoitus organisaation toimintakyvyn säilyttämiseksi ja häiriötilanteiden aiheuttamien negatiivisten vaikutusten minimoimiseksi sekä sitä ohjaavan Valmiuslain (1552/2011) esittely ja kuvaus dokumentin sisällöstä.

2. Palvelun yleiskuvaus, jossa esitetään kohdejärjestelmä ja sen mahdollistamat toiminnot ja palvelut.

3. Roolit ja vastuut, jossa on nimetty järjestelmän kaikki vastuuhenkilöt ja toimijat, kuten palvelutoimittajat, järjestelmän omistaja, pääkäyttäjät ja testaajat.

4. Riskianalyysi, jossa esitetään tarvittavat tehtävät riskien arviointiin. Varsinainen riskianalyysi käsittelysuunnitelmineen on dokumentin liitteenä. Riskianalyysin toteuttamisen ja kuvaksen olen esittänyt tarkemmin tämän työn kriittisen järjestelmän riskianalyysi -kohdassa.

5. Vaikutuksen arviointi BIA, jossa on kuvattu vaikutusarvioinnin tarkoitus ja BIA-arvioinnin yhteenveto. Varsinainen BIA- arviointi on dokumentin liitteenä. Vaikutuksen arviointi BIA:n toteuttamisen ja kuvaksen osalta olen esittänyt tarkemmin tämän työn BIA -vaikutusanalyysi -kohdassa.

6. Järjestelmän riippuvuudet ja kriittisyydet -kohdassa on esitetty kohteen keskeiset riippuvuudet ja niille arvioidut kriittisyysarvot. Riippuvuuksia on esitetty hyödyntäen BIA-analyysiä, jossa tunnistetaan ja arvioidaan niitä asioita ja toimintoja, joista järjestelmän toiminta on riippuvainen sekä vastavuoroisesti tunnistetaan ne kohteet ja toiminnot, jotka ovat järjestelmästä riippuvaisia. Edellä mainitun lisäksi on esitetty tarkempi tekninen kuvaus järjestelmän rajapintojen ja tietoliikenteen riippuvuuksista.

7. Varautuminen toiminnan häiriöihin ja keskeytyksiin – kohdassa on esitetty järjestelmän osalta ne tehtävät ja ratkaisut, millä varaudutaan ennakoivasti häiriöihin. Kohdassa on esitetty muun muassa palvelimen ja tietokannan varmuuskopiointien toteutus (täys- ja differentiaalisten varmuuskopiontien ajastukset, säilytysrotaatio ja eheystarkastukset), kuvataan päivystyksen toteuttama seuranta ja palvelutoimittajien kanssa sovitut palvelutasot.

8. Häiriötilanteen aikainen toiminta -kohdassa on kuvattu toimintaohjedokumentit sekä häiriötilanteen ja tietosuojaloukkaustilanteiden varalle. Varsinaiset toimintaohjeet ovat jatkuvuussuunnitelman liitteinä, jotka säilytetään myös tulostettuina kappaleina häiriötilanteiden varalle. Toimintaohjeet on kuvattu sekä prosessikuvauksena että kirjallisena ohjeena, jossa esitetään tarvittavat yhteystiedot, vastuuroolit ja tehtävät. Toimintaohjeiden lisäksi suunnitelman liitteeksi toteutetaan viestintäasiantuntijoiden kanssa erillinen viestintäsuunnitelma häiriötilanteiden ja tietosuojaloukkaustilanteiden varalle. Tämä viestintäsuunnitelma ei ole vielä valmis ja se liitetään jatkuvuussuunnitelmaan myöhemmin. Toimintaohjeiden toteuttamisen ja kuvaksen olen esittänyt tarkemmin tämän työn toimintaohjeet häiriötilanteen tai tietosuojaloukkauksen varalle -kohdassa.

9. Paluu normaalitilaan -kohdassa esitetään häiriötilanteiden jälkeisen jälkipalaverin toteuttamisen ohje ja siinä käsiteltävät aiheet. Jokaisen mittavamman häiriötilanteen jälkeen järjestetään jälkipalaveri häiriöön kohdistuneen järjestelmän tai järjestelmien pääkäyttäjien sekä järjestelmäasiantuntijoiden kesken, jossa dokumentoidaan ja käsitellään seuraavat asiat:

    a. miten häiriö huomattiin?

    b. häiriön syyt ja vaikutus

c. tehdyt korjaustoimenpiteet

d. ketkä osallistui

e. esiin nousseet kehitysehdotukset ja päätökset näiden kehittämisestä

f. päivitetään riskianalyysi

g. päivitetään tarvittaessa BIA

10. Suunnitelman koulutus, ylläpito ja viestintä -kohdassa on kuvattu miten ja milloin jatkuvuussuunnitelmaa ylläpidetään sekä kenelle ja milloin tehdyistä muutoksista viestitään ja koulutetaan. Suunnitelman mukaisesti järjestelmäpääkäyttäjät koulutetaan jatkuvuussuunnitelmien ylläpitämiseen. Jatkuvuussuunnitelmaa tulisi ylläpitää vähintään seuraavissa tilanteissa:

    a. kirjastojärjestelmään tai siihen kohdistuvaan muuhun palveluun tehdyn muutoksen jälkeen

    b. häiriö- tai harjoittelutilanteista esiin nousseiden kehitysehdotusten toteuttamisen jälkeen

    c. henkilöstövaihdoksen tai vastuuhenkilöiden työroolimuutosten jälkeen.

    Jatkuvuussuunnitelmaan liittyvää riskianalyysia seurataan ja päivitetään riskienhallintapolitiikan mukaisesti. Suunnitelmaan tehdyistä muutoksista viestitään järjestelmän omistajalle ja pääkäyttäjille. Riippuen muutosten laajuudesta, voidaan siitä tiedottaa kohdassa 3. esitetyille henkilöille tai tilanteen mukaan koko henkilökunnalle.

11. Suunnitelman harjoittelu ja testaus -kohdassa esitetään suunnitelman harjoittelun ja testauksen toteuttaminen tulevien TAISTO-harjoituspäivien yhteydessä. Lisäksi varsinaisia häiriötilanteita voidaan pitää jatkuvuussuunnitelman ja toimintaohjeiden testaamisena.

12. Suunnitelman katselmointi ja raportointi -kohdassa kuvataan, milloin suunnitelma esitetään Celian johtoryhmälle ja miten suunnitelmaa katselmoidaan vuosittain testauksen yhteydessä. (Pietikäinen 2016)

Jatkuvuussuunnitelman riskianalyysi ja vaikutuksen arviointi BIA toteutettiin järjestelmäasiantuntijamme kanssa. Tämän jälkeen katselmoimme järjestelmän pääkäyttäjien kanssa koko dokumentin ja varmistimme, ettei riskianalyysissä tai BIA:ssa jäänyt mitään huomioimatta.

Jatkuvuussuunnitelma esiteltiin kirjastonjohtajalle, talous- ja hallintojohtajalle sekä kehittämisjohtajalle. Sovimme, että tulen esittelemään kaikkien kriittisten järjestelmiemme jatkuvuussuunnitelmat ja toimintaohjeet henkilökuntatilaisuudessa, kun ne on saatu valmiiksi.

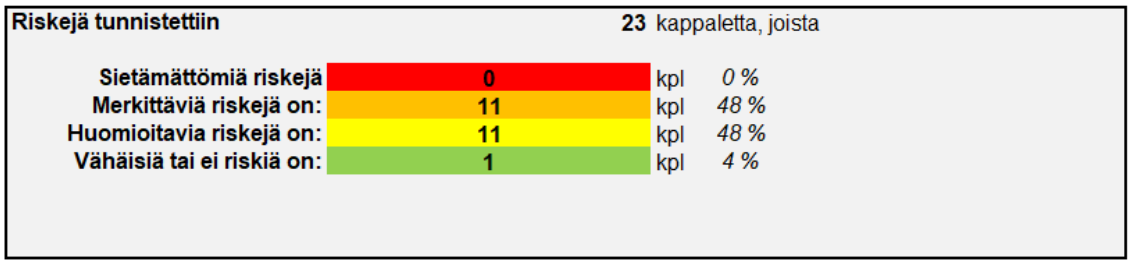
7.6.1 Kriittisen järjestelmän riskianalyysi

Jatkuvuussuunnitelman liitteeksi tehtävän järjestelmä X:n riskianalyysin tein aluksi järjestelmäasiantuntijamme kanssa. Analyysin tuloksista ja tulkinnasta keskusteltiin tämän jälkeen järjestelmän pääkäyttäjien kanssa, jotta riskejä ei jäisi huomioimatta ja analyysi olisi tarpeeksi kattava. Olimme kuitenkin saaneet tunnistettua riskejä jo niin laajasti, ettei uusia tunnistettu pääkäyttäjien toimesta.

Käytimme riskien arviointiin Celian riskienhallintapolitiikan mukaista arviointityökalua ja ohjeistusta. Totesimme, että kaikki järjestelmää koskevat riskit ovat luokitukseltaan operatiivisia, vaikka tunnistamillamme riskeillä voi olla vaikutuksia myös talouteen ja strategiaan. Haastavinta arvioinnissa oli ylläpitää ajatusta, mitä kohdetta arvioidaan ja mihin arviointi suhteutetaan. Tämän vuoksi politiikan ohjeistus ja sen tuoma rajaus oli erittäin tarpeellinen.

Tunnistimme 23 erilaista riskiä, mitkä voivat vaikuttaa järjestelmän toimintaan tai sen tuottaman palveluun. Tämän tutkimuksen liitteenä (ks. liite 3) on esitetty kuvakaappauksena riskienhallintatyökalusta tunnistamistamme riskit ja niille suunnitellut käsittelytoimet. Riskit ja käsittelysuunnitelmat on peitetty tietoturvasyistä.

Kuviossa 17 on esitetty yhteenveto tunnistetuista riskien arvoista, jonka arviointityökalu tuottaa automaattisesti raporttivälilehdelle.



Kuvio 17. Yhteenveto järjestelmä X:n riskien arvoista.

Arvoltaan sietämättömiä riskejä ei ollut lainkaan. Merkittäviä riskejä tunnistimme 11 kappaletta ja näille kaikille suunnittelimme käsittelytoimet riskin pienentämiseksi tai poistamiseksi. Suunnitelmaan nimesimme käsittelystä vastaavat henkilöt ja tavoiteaikataulun, jolloin toimenpiteet tulisi aloittaa. Näistä käsittelysuunnitelmista raportoimme kehittämisjohtajalle, joka voi tarvittaessa välittää toimenpiteistä tiedon johtoryhmälle.

Tunnistamistamme riskeistä useat pienenevät tai poistuvat kevään 2020 aikana toteutettavan palvelinsalitransformaatio-projektin jälkeen, jolloin Celian palvelimet on siirretty Celian tiloista Valtorin tuotteistamaan konesalipalveluun. Osa riskeistä pienenee sopimuksin palvelutoimittajien kanssa tai muuttamalla omaa toimintaa. Näiden lisäksi jäi vielä sellaisia merkittäviä riskejä, joille ei voida tehdä mitään ja nämä jäävät seurattaviksi jäännösriskeiksi. Arvoltaan huomioitavia riskejä oli myös 11 kappaletta ja osalle näistä suunnittelimme käsittelytoimet. Loput näistä riskeistä jää seurantaan.

Jatkuvuussuunnitelman mukaisesti tätä riskiarviointia tullaan seuraamaan ja päivittämään järjestelmäasiantuntijan tai pääkäyttäjien toimesta jokaisen järjestelmään kohdistuvan muutoksen jälkeen tai muussa tapauksessa vähintään kerran vuodessa.

7.6.2 BIA-vaikutusanalyysi

Kuten järjestelmä X:n riskianalyysia tehtäessä, toteutimme BIA-vaikutusanalyysin aluksi järjestelmäasiantuntijan kanssa, jonka jälkeen kävimme sen läpi pääkäyttäjien kanssa. Käytimme vaikutusten analysoimiseen VAHTI -ohjesivuilta löytyvää valmista vaikutusanalyysityökalua. Työkalu on excel-pohjainen lomake, jossa on kuusi eri määritys- ja arviointiosiota. Työkalun toiselle taulukkosivulle tulostui arviointimme yhteenveto sekä vaikutusanalyysin raportti, jotka ovat esitetty tämän tutkimuksen liitteenä (ks. liite 4). (VAHTI 2016)

Vaikutusanalyysityökalun ensimmäiseen osioon kirjasimme tiedon arvioitavasta kohteesta, kohteen omistajan, arvioinnin tekijät ja arvioinnin aloitus- ja päättymisajat. Ensimmäisessä osiossa on myös versionhallintaa koskeva kohta, johon arvioija voi kirjata tiedon siitä, mitä dokumentissa on muokattu, tekijän ja päivämäärän.

Toinen osio käsittelee kohteen ja siinä käsiteltävien tietojen tietoturva- ja ICT-varautumisen luokitukset. Osiossa arvioimme ensin työkalussa esitettyjen valmiiden luokitusesimerkkien avulla järjestelmän sisältämistä tiedoista korkeimmat tietojen suojaus- ja turvallisuustasoluokitukset, joiden perusteella työkalu laski automaattisesti tietoturvatason. Tämän lisäksi arvioimme erillisen asteikon mukaan ICT-varautumistason.

Kolmannessa osiossa arvioimme kohteen tietoturvallisuuden tärkeyden sekä palvelutasotavoitteet. Arvioinnissa tuli täyttää omat arvot järjestelmässä olevan tiedon luottamuksellisuudelle, eheydelle ja saatavuudelle. Näiden lisäksi täytimme järjestelmään liittyvän sopimuksen tämän hetken palvelutason. Arviointien avuksi työkalu tarjosi vastaavasti esimerkit käytettävistä vaihtoehdoista.

Neljännessä osiossa arvioimme järjestelmässä tapahtuvan odottamattoman käyttökatkoksen, tietojen menetyksen ja vanhenemisen vaikutuksia organisaatiolle. Osiossa määrittelimme erikseen häiriöiden ja tietojen menetysten kestot, joilla on sekä pienin että suurin vaikutus toimintaan. Kestoille annoimme aika-arviot tunneissa ja vaikutuksen suuruuden merkitykset valmiin 6-tasoisen arvoasteikon mukaisesti. Arvioinnit toteutettiin kolmesta eri lähtökohdasta, jotka olivat palveluaika, virka-aika ja muu aika. Lisäksi arvioimme erillisen kriittisen ajan, joka pohjautui tietyn Celian kriittisen palvelun toteuttamisen ajankohtaan. Suurimman vaikutuksen kestoa voidaan pitää kohteen toipumisaikana (Recovery Time Objective, RTO), joka määrittelee aikarajan, jolloin kohde tulee saada toimintaan ennen kuin häiriön tai tiedon menetyksen vaikutus on sietämätön.

Viidennessä osiossa määrittelimme kohteen riippuvuudet. Siinä tunnistimme ja arvioimme niitä asioita ja toimintoja, joista järjestelmän toiminta on riippuvainen. Vastavuoroisesti tunnistimme ne kohteet ja toiminnot, jotka ovat järjestelmästä riippuvaisia. Jokaiselle tunnistetulle riippuvuudelle asetettiin 6-tasoinen tärkeysarvo työkalussa annetun ohjeen mukaisesti.

Kuudennessa osiossa arvioimme yhteiskunnan turvallisuusstrategian (YTS 2010) uhkakuvien vaikutusta järjestelmään. Osion alussa vastasimme esitettyihin alkumäärityksiin,

jossa piti vastata, aiheuttaako valmiuslaki tai muu säädös velvoitteita järjestelmäämme kohtaan tai liittyykö järjestelmämme toiminta yhteiskunnan turvallisuusstrategian mukaisiin tehtäviin. Koska järjestelmämme toiminta ei liity tai siihen ei vaikuta mikään näistä velvoitteista, meidän ei tarvinnut toteuttaa arviointia kohteen merkityksestä yhteiskunnan elintärkeille tehtäville. Osion lopussa arvioimme yhteiskunnan turvallisuusstrategiassa kuvattujen uhkamallien vaikutusta järjestelmään ja annoimme jokaiselle uhkamallille arvon 6-asteisen merkitysasteikon mukaisesti. Niille uhkamalleille, joille merkityksen arvoksi tuli joko sietämätön, kohtuuton tai merkittävä, arvioimme vaikutusanalyysin kolmannen osion mukaisesti vaikutusten pienimmät ja suurimmat arvot sekä kestot.

BIA vaikutusanalyysin toteutus oli suhteellisen aikaa vievä, mutta tarpeellinen monin tavoin. Aikaisemmin olemme tehneet järjestelmään kohdistuvia päätöksiä sen hetken parhaimman tietämyksen mukaan, mutta vaikutusanalyysin toteutuksen jälkeen voimme verrata tulevia järjestelmään kohdistuvia kehittämissuunnitelmia vaikutusanalyysiin, jossa on jo valmiiksi pohdittu eri tekijöiden vaikutuksia järjestelmään. Analyysia tulee päivittää tietohallinnon toimesta aina, kun järjestelmään toteutetaan merkittäviä muutoksia.

7.6.3 Toimintaohjeet häiriötilanteen tai tietosuojaloukkauksen varalle

Suunnittelin tietohallinnon suunnittelijan kanssa toimintaohjeet häiriötilanteen ja tietosuojaloukkaustilanteiden varalle. Laadimme toimintaohjeista useita versioita ennen kuin lopullinen malli löysi muotonsa. Toimintaohjeen laatimisessa tuli ottaa huomioon kaikki mahdolliset häiriötilanneprosessin vaiheet sekä miten ja kuka toimii näiden mukaisesti. Toimintaohje tuli olla myös mahdollisimman selkeä lukijalleen, sillä sen mukaisesti toimitaan häiriötilanteiden sattuessa. Kuvasimme toimintaohjeen sekä uimaratamallisena prosessikaaviona (liite 5) sekä kirjallisena ohjeena, jossa on kuvattu myös järjestelmän osalta tarvittavat toimijat ja niiden yhteystiedot. Tarkoituksena oli, että tämä toimintaohje tulostetaan yhden sivun paperiversioksi, jossa toisella puolella on prosessikuvaus ja toisella puolella kirjallinen selitys. Häiriötilanteessa toimintaohjeiden tulisi tukea ja ohjata häiriön aikaista toimintaa sekä varmistaa tarvittavien toimenpiteiden toteutumisen.

Häiriötilanteen prosessin tehtävät kuvattiin toimintajärjestyksessä alkaen häiriön havaitsemisesta häiriötilanteen päätöspalaveriin:

1. Ilmoitus häiriöstä vastaanotetaan / häiriö huomataan

2. Häiriön esiselvitys: onko henkilötiedot uhattuna?

    a. Jos henkilötiedot ovat vaarantuneet, siirrytään tietosuojaloukkaustilanteen toimintaohjeeseen.

3. Häiriön jatkoselvitys: kuinka laajasta häiriöstä on kyse? Ketä toimijoita tarvitaan lisäselvitys- ja korjaustoimenpiteisiin?

    a. Jos häiriö tai sen uhka on merkittävä, kutsutaan koolle kriisiryhmä, jonka tehtävänä on johtaa häiriötilannetta, tehdä korkeamman tason päätökset, toteuttaa viranomaisilmoitukset ja vastata mahdollisiin median yhteydenottoon.

4. Korjaustoimenpiteet ja mahdollisesta käyttökatkosta sopiminen

5. Korjaustoimenpiteiden jälkeinen testaus

6. Palautuminen normaalitilaan

7. Häiriötilanteen jälkeinen päätöspalaveri

Toimintaohjeessa kuvataan edellä mainittujen päätehtävien lisäksi tarkemmat tehtävät ja niille määritellyt vastuuroolit. Ohjeissa kuvataan myös viestintä, mitä ja milloin kussakin päätehtävässä tulee viestiä niin Celian sisäisesti kuin myös ulkoisesti palveluiden loppukäyttäjille ja yhteistyötahoille.

Tietosuojaloukkaustilanteiden toimintaohje (liite 6) on vastaavanlainen kuin häiriötilanteiden toimintaohje, mutta siinä on ohjeistettu toiminta tietosuojaloukkaustilanteiden kannalta. Ero näiden välillä on kriisiryhmän koolle kutsuminen aikaisemmassa vaiheessa, viranomaisilmoitusten tekeminen sekä selvitys kuinka laajasta tietosuojaloukkaustilanteesta on kyse, millaiset vaikutukset sillä on kohteille sekä milloin ja kuinka laajasti siitä viestitään.

Toimintaohjeissa olevat viestinnän tehtävät kuvataan tarkemmin erillisessä häiriö- ja tietosuojaloukkaustilanteiden viestintäsuunnitelmassa. Kyseinen suunnitelma on tärkeä osa ja tuki häiriötilanteiden johtamisessa. Siinä kuvataan vastuuroolit, Celian käyttämät

eri viestintäkanavat ja ohjeet, missä tapauksissa viestitään ja missä tilanteissa päätös viestimisestä tulee sopia kriisiryhmän kanssa. Suunnitelmassa on myös valmiit, tilanteen mukaan muokattavat häiriötiedotepohjat sekä poikkeustilanteita varten ohjeistus median yhteydenottoa varten. Celialla on ollut tämän kaltainen suunnitelma, mutta se on jäänyt päivittämättä ja sen tiedot ovat jo vanhentuneet. Aloitimme suunnitelman päivittämisen viestinnän asiantuntijoiden toimesta, jotta se saadaan yhteneväksi uusien toimintaohjeiden ja niiden mukana sovittujen roolien kanssa. Viestintäsuunnitelmaa ei saatu valmiiksi tämän tutkimuksen luovutukseen mennessä, mutta se liitetään osaksi jatkuvuussuunnitelmaa sen valmistuttua.

7.6.4 Testaus

Kuten tutkimuksen alussa kerrottiin (ks. luku 2.5), Celia osallistui ensimmäistä kertaa Väestörekisterikeskuksen toteuttamaan julkishallinnolle tarkoitettuun TAISTO-harjoituspäivään, jonka tarkoituksena on harjoitella organisaation toimintaa kyberhyökkäystilanteiden varalta. Ennen varsinaista harjoittelupäivää saimme kahtena aikaisempana ennalta ilmoitettuna ajankohtana syötteet, joissa esitettiin keksityn Tietovuoto321-nimisen hakkeriryhmän kyberhyökkäyksen ensimmäiset uhkavaatimukset lunnasvaatimuksineen. Näiden perusteella Celian tuli päättää, mihin kriittiseen palveluun tai järjestelmään hyökkäyksen uhkaus kohdistuu ja varmistaa, että olemme varautuneet suunnitelmin, jos uhkavaatimukset käyvät toteen. Varsinainen harjoituspäivä pidettiin 7.11., jonka aikana saimme sarjasyötteinä tiedot aikaisempien uhkavaatimusten toteutumisesta ja hyökkäysten etenemisestä. Pahimmassa tilanteessa Celiaan kohdistui kaksi isoa hyökkäystä samanaikaisesti. Harjoituksen aikana testasimme lisäksi tämän tutkimuksen osana valitulle kriittiselle järjestelmälle suunnittelemaamme toimintaohjetta.

Harjoitus onnistui osaltamme hyvin ja sen tuloksena tunnistimme tärkeitä kehityskohteita, jotka Celian tulisi toteuttaa parantaakseen varautumista. Verratessa toimintaohjettamme harjoitustilanteessa, löysimme korjattavaksi muutaman kohdan, jotta ohje tukisi paremmin häiriötilanteen aikaista toimintaa. Näitä oli muun muassa häiriön selvitystilanteen aikainen toiminta häiriön osoittautuessa merkittäväksi, päätös kriisiryhmän koollekutsumisesta aikaisemmassa vaiheessa. Lisäksi totesimme, että toimintaohjeet toimivat paremmin pienemmissä häiriötilanteissa, jossa häiriön vaikutus kohdistuu vain osaan Celian tuottamiin palveluihin tai toimintaan. Laajempia ja Celian kannalta äärimmäisiä poikkeustilanteita varten tulisi toteuttaa vielä erillinen valmiussuunnitelma, jossa sovitaan

esimerkiksi resurssien varallaolot ja miten valtuuttaa päätösten teot sijaisille, jos päätöksiin oikeutetut henkilöt ovat estyneet.

Testauksena voidaan pitää myös aidon häiriötilanteen toteutuminen. Sattumalta Celian toimintaan on viime aikoina kohdistunut normaalia enemmän erilaisia häiriötilanteita, jotka ovat osaltaan vahvistaneet ymmärrystä varautumisen tärkeydestä. Esimerkiksi erääseen järjestelmään ilmaantui toimintahäiriö, joka onneksemme osoittautui vaikutukseltaan pieneksi ja tilanne saatiin nopeasti korjatuksi. Tässä tilanteessa seurasin ja ohjeistin häiriötilanteen aikaista toimintaa toimintaohjeemme mukaisesti.

8 Tulokset ja arviointi

Tutkimuksen alussa määriteltiin tutkimuksen toteuttamista ohjaavat tutkimuskysymykset, joihin tutkimuksen aikana ja tuloksena pyrittiin löytämään vastaukset. Tutkimuskysymykset olivat:

1. Miten Celian digitaalista turvallisuutta voidaan kehittää?
2. Miten saattaa digitaalinen turvallisuus uuden tiedonhallintalain vaatimusten mukaiseksi?

Koska tutkimuskysymykset asetettiin varsin ylätasolle, vastauksena voidaan pitää jo itsessään koko tutkimuksen aihetta riskien- ja jatkuvuudenhallinnasta. Tutkimuksen aikana toteutettu riskienhallintapolitiikka ja jatkuvuussuunnitelma toimintaohjeineen vahvistavat Celian digitaalisen turvallisuuden tasoa sekä ennakointikykyä. Ne toimivat myös ensimmäisinä askeleina kohti tiedonhallintalain velvoitteiden toteuttamista. Ilman toimivaa riskienhallintaa ja varautumista, Celia ei pysty saavuttamaan tarvittavaa tietoturvatasoa tietoaineistoille ja järjestelmille. Tarvittava tietoturvataso tulee puolestaan varmistaa, kun viranomaispalveluita tullaan lain mukaisesti yhdenmukaistamaan.

Tutkimuksessa käyttämäni mittarit, jotka todentavat tehdyt muutokset, olivat seuraavat:

1. Saimmeko paremmat tulokset digitaalisen turvallisuuden barometristä ja KUJA-pikatestistä? (Kyllä / Ei).

2. Onko riskienhallinta otettu osaksi kehittämistoimia? (Kyllä / Ei).

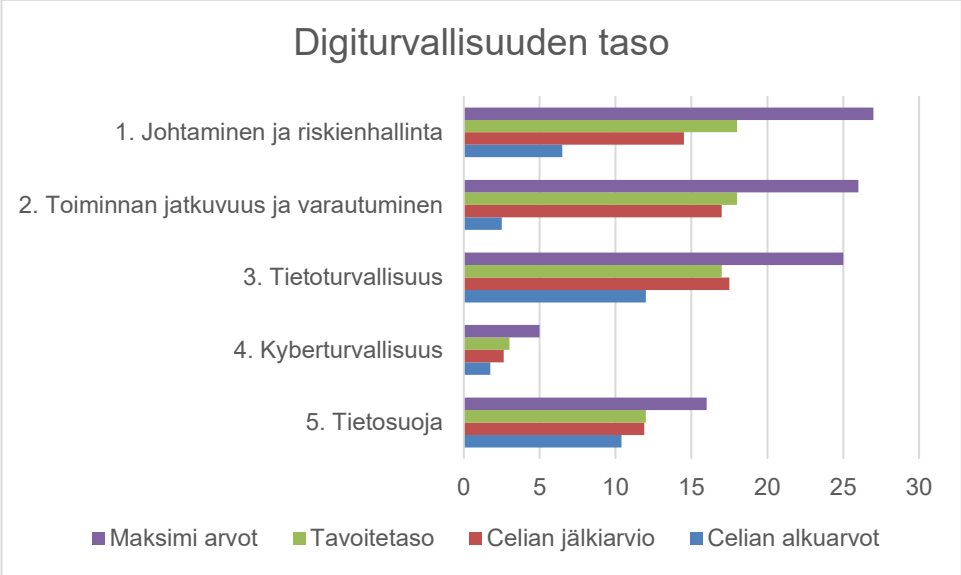
3. Onko jatkuvuudenhallinnan jatkuvuussuunnitelmat laadittu ja vastuuhenkilöt koulutettu? (Kyllä / Ei).

Nykytilan selvittämiseen hyödynsin vuoden 2019 alussa vastattua digiturvakyselyä ja sen tuloksia. Toteutin saman kyselyn uudelleen tämän hetken tilannetta arvioiden, kun tutkimuksessa esitetyt kehittämistehtävät oli toteutettu. Tuloksena saadut arvot ovat parantuneet suhteessa alkutilan arvoihin, kuten taulukosta 2 näkee.

Taulukko 2. Digiturvakyselyn arviot

Celian alkuarvot	Celian jälkiarvio	Tavoitetaso	Maksimi arvot
10,4	11,9	12	16
1,75	2,625	3	5
12	17,5	17	25
2,5	17	18	26
6,5	14,5	18	27

Jotta digiturvakyselyn pistetaulukkoa on helpompi havainnoida, olen kuvannut tulokset jälleen kuviossa 18 esitetyllä kaaviolla.

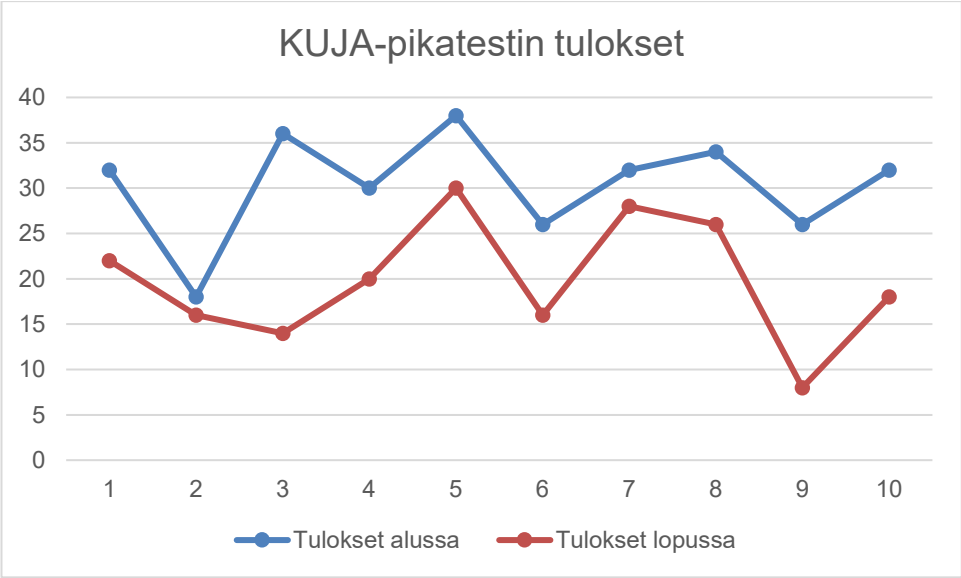


Kuvio 18. Digiturvallisuuden tason jälkiarviointi.

Taulukossa 2 ja kuviossa 18 on esitetty arvioinnin maksimipistemäärät, asettamani tavoitetaso, jonka Celian tulisi saavuttaa, Celian alkuarvot, jotka arvioitiin vuoden 2019 alussa sekä nyt tutkimuksen jälkeen toteutettu jälkiarvio. Kuviosta 18 näkee, että tutkimuksen aikana Celian digiturvallisuuden taso on parantunut selvästi, vaikka asettamaani

tavoitetasoa emme ole vielä saavuttaneet. Kyselyn osiossa johtamisesta ja riskienhallinnasta on vielä eniten kehitettävää. Tämä johtuu osin siitä, että toteuttamaani riskienhallintapolitiikkaa ei olla vielä tämän vuoden puolella otettu käyttöön. Vaikka tutkimuksen aikana keskityttiin ainoastaan riskien- ja jatkuvuudenhallintaan, työn tuloksena on myös parantuneet tietosuoja, kyberturvallisuus ja tietoturvallisuus -osiot.

Toisena, laajempana kyselynä käytin Kuntaliiton kehittämää varautumisen ja jatkuvuudenhallinnan kehittämistoimenpiteiden tarpeellisuuden arviointi KUJA-pikatestiä. Toteutin kyselyn uudelleen samoille kymmenelle henkilöille, jotka vastasivat kyselyyn myös tutkimuksen alussa. Alla olevassa kuviossa 19 näkyy KUJA-pikatestin tulokset ennen ja jälkeen tutkimuksen, jossa vasemmanpuoleisessa akselissa esitetään saadut pistearvot ja ala-akselilla esitetään kunkin vastaajan tulos.



Kuvio 19. KUJA-pikatestin tulokset tutkimuksen jälkeen.

Kuviosta 19 näkee, että jokaisella vastaajalla pistemäärä on alentunut alkuarvoista, joka tarkoittaa Celian riskitason pienentymistä varautumisen ja jatkuvuudenhallinnan toteutumisessa. Kuviosta näkyy myös suuria eroavuuksia vastaajien välillä. Tämä johtuu siitä, että vastaajilla on eri tasoinen tietämys tai ymmärrys aiheesta. Kyselyn alkuarvojen keskiarvo oli 30 pistettä ja jälkiarvioinnin keskiarvo laski 20 pisteeseen. Tuloksena saavutimme yhden tason paremman arvon, jolloin Celian jatkuvuuden ja varautumisen kehittämistarpeen riskitaso parani kohtalaiseen (pistearvot 15-25). Mittarina KUJA-testi ei välttämättä anna täysin todenmukaista tilannekuvaa, mutta siitä voidaan nähdä, että tut-

kimuksen aikana taso on parantunut. Tavoitteena oli saada lopputestin tuloksena vähintään yksi taso paremmaksi ja testin mukaan se saavutettiin. Näiden kahden testin perusteella voidaan todeta, että tutkimuksen mittarina käytetty ensimmäinen osa digitaalisen turvallisuuden parantamisesta saavutettiin.

Toisena mittarina oleva riskienhallinnan ottaminen osaksi kehittämistoimia saavutettiin mielestäni myös osin. Kuten aikaisemmin totesin, riskienhallintaa ei olla vielä otettu käytännössä kunnolla käyttöön, mutta sen ohjaava ja tukeva politiikka hyväksyttiin ja vastuuroolit on nimetty.

Kolmantena mittarina oli saada laadituksi jatkuvuudenhallinnan jatkuvuussuunnitelmat ja niiden vastuuhenkilöiden kouluttaminen. Myös tämä saatiin toteutettua osin. Tarkoituksena oli saada laadituksi kaikkien kriittisten järjestelmiemme jatkuvuussuunnitelmat, mutta aikataulusyistä ja avainhenkilön kiireellisyyden vuoksi ehdimme toteuttaa suunnitelman ainoastaan yhdelle kriittisimmälle järjestelmälle ja kouluttaa sille kuuluvat vastuuhenkilöt.

Tutkimuksen alussa kuvasin (ks. luku 4.5) aikataulun toteutukselle. Siinä kuvatut tehtävät tavoiteaikoineen pysyivät pääosin aikataulussa, mutta jatkuvuussuunnittelun toteuttaminen vei enemmän aikaa, mitä olin suunnitellut. Tämän tutkimuksen aikataulupaineiden ja järjestelmäasiantuntijamme kiireellisyyden vuoksi emme pystyneet toteuttamaan muiden järjestelmiemme jatkuvuussuunnitelmia, jotka alun perin olin suunnitellut olevan osa tutkimuksen tulosta. Näin ollen myös tutkimustyöhön tehdyssä riskianalyysissä (ks. luku 7.2) tunnistamani resurssiriski realisoitui, joka ei onneksi estänyt tutkimustyön tekoa, vaan muutti hieman suunniteltua tulosta.

9 Johtopäätökset ja jatkokehitys

Tutkimuksen aihe oli suhteellisen laaja ja tutkimuksen aluksi olikin haastavaa löytää sellainen taso, joka oli toteutettavissa ja järkevä suhteessa Celian organisaation kokoon. Pelkästään riskienhallintaa tai varautumista olisi voinut kehittää laajemmin, mutta silloin niistä ei olisi ollut välttämättä enää käytännöntasolla hyötyä Celialle. Organisaation pienuuden ja resurssien vähyyden vuoksi oli löydettävä sellainen taso, jota pystymme toteuttamaan ja ylläpitämään. Oli myös hyväksyttävä, ettei kaikkea ole mahdollista saada valmiiksi kerralla, sillä vasta ajan kanssa kehittämällä tutkimuksen aikana toteutettuja ratkaisuja voidaan saavuttaa toivottu taso digitaalisen turvallisuuden toteutumisessa.

Johdonmukaisen tarkastelun ja oikean suhteellisuustason ylläpitäminen arvioitaessa Celian kriittisiä järjestelemiä sekä toteuttaessa riskiarviointia ja vaikutusarviointia oli myös haastavaa. Arvioinneissa oli välillä pysäytettävä analysointi ja tarkistettava, että suhteutamme arvioinnin oikealle tasolle. Esimerkiksi tehtäessä riskianalyysia ja vaikutusarviointia oli varmistettava, mitä tarkoitetaan kriittisyydellä ja miten se ymmärretään. Se mikä Celialle voi olla äärimmäisen kriittistä, ei välttämättä ole kriittistä koko valtiohallinnon tasolla. Arvioinneissa oli löydettävä näiden kahden näkökannan väliltä sopiva taso.

Celian toimintaympäristöön kohdistuneet häiriötilanteet ovat vahvistaneet ymmärrystä varautumisen tärkeydestä ja miten häiriötilanteita tulisi ennalta ehkäistä toimivalla riskienhallinnalla. Lisäksi häiriötilanteiden toimintaohjeiden tärkeys korostuu Celian ulkoistaessa yhä enemmän palveluitaan. Celiassa on totuttu toimimaan itsenäisesti ja ketterästi erilaisissa häiriötilanteissa. Tämän kaltainen reaktiivinen toiminta on ollut mahdollista pääosin sen vuoksi, että olemme ylläpitäneet ympäristöä itse ja organisaation koko on pieni. Tämän tyyppinen ad hoc -toimintamalli ei enää riitä, sillä koordinointi useamman ulkopuolisen toimittajan kanssa on monimutkaistanut toimintaympäristöä ja sen hallitsemiseksi tarvitsemme sovitut roolit ja toimintaohjeet.

Tutkimuksen aikana saatu kehitys on vasta ensimmäinen askel kohti tietoturvallisempaa toimintaa. Työn aikana syventynyt ymmärrys tietoturvan, riskienhallinnan ja varautumisen tärkeydestä on ollut lähtökohtaisesti yksi tärkeimmistä saavutuksista. Ymmärryksen ja osaamisen kasvu tulee sekä helpottamaan että edesauttamaan tietoturvatyötä ja sen jatkokehitystä. Jatkokehityksenä tulen toteuttamaan jatkuvuussuunnitelmat järjestelmä X:n tavoin myös muille järjestelmillemme. Tulen myös toteuttamaan valmiussuunnitelman Celialle. Jatkokehitys ei suinkaan jää näihin, vaan digitaalisen turvallisuuden kehittäminen tulee olemaan jatkuvaa työtä toimintaympäristön jatkuvan muutoksen vuoksi.

Lähteet

Digipalvelulaki pähkinänkuoressa 2019. Virastojen tietohallintojohtajien kokous 14.5.2019 esitysmateriaali Digipalvelulain toimeenpano.pdf. Valtiovarainministeriö.

HE 284/2018 vp 2018. Hallituksen esitys eduskunnalle laiksi julkisen hallinnon tiedonhallinnasta sekä eräiksi siihen liittyviksi laeiksi. Eduskunta. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_284+2018.pdf. Luettu 11.6.2019.

Huoltovarmuuskeskus.fi. Jatkuvuudenhallinta. https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/ Luettu 29.9.2019.

Iivari, Mika & Laaksonen, Mika 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tietosanoma Oy.

Ilmonen, Ilkka & Kallio, Jani & Koskinen, Jani & Rajamäki, Markku 2010. Johda riskejä – käytännön opas yrityksen riskienhallintaan. PRO Tammi.

Kangas, Arto 2017. VM 22/2017 Ohje riskienhallintaan Riskiarviointityökalu -käyttö- ja täyttöohje. Valtiovarainministeriö. https://www.vahtiohje.fi/c/document_library/get_file?uuid=40bf6302-b7b8-4afc-88ce-106c40790d88&groupId=10128. Luettu 27.10.2019.

Kananen, Jorma 2014. Toimintatutkimus kehittämistutkimuksen muotona – Miten kirjoitan toimintatutkimuksen opinnäytetyönä? Suomen Yliopistopaino Oy

Kirves, Juha & Ahokas, Antti 2019. JUDO, projekti 1: Case riskienhallinta – toimintamallit ja Case-esimerkit sekä verkkokeskustelut. JUDO-työpaja #3 esitysmateriaali. https://vrk.fi/documents/2252790/13076333/Digiturvayhteishanke_ty%C3%B6paja_03_1206_2019_netti_VALMIS.pdf/22ef3429-8409-3882-cbda-e2fd91cad0c9/Digiturvayhteishanke_ty%C3%B6paja_03_1206_2019_netti_VALMIS.pdf . Luettu 26.9.2019.

Kuntaliitto 2018. Kuja-pikatesti – Jatkuvuuden ja varautumisenhallinnan kehittämistoimenpiteiden tarpeellisuuden arviointi. Päivitetty 22.5.2018. Kuntien jatkuvuudenhallintaprojektit KUJA 1 ja 2. > Uusi KUJA-pikatesti. Copy Right Jaakko Pekki 2015. https://www.kuntaliitto.fi/yhdyskunnat-ja-ymparisto/turvallisuus-ja-varautuminen/varautuminen-ja-jatkuvuudenhallinta/kuja-jatkuvuudenhallintaprojektit. Luettu 19.10.2019.

Leino, Mirel & Steiner, Maj-Lis & Wahlroos, Juha 2005. Corporate Governance ja riskienhallinta. Teoksessa Kuusela, Hannu & Ollikainen, Reijo (toim.) Riskit ja riskienhallinta. Tampereen Yliopistopaino – Juvenes Print. Tampere 2005.

Limnéll, Jarno & Majewski, Klaus & Salminen, Mirva 2014. Kyberturvallisuus. Docendo Oy.

Pietikäinen, Suvi 2016. VAHTI 2/2016 Toiminnan jatkuvuuden hallinta. Liite 3: Palvelun jatkuvuussuunnitelman sisällysluettelorunko (esimerkki). Päivitetty 22.6.2016. Valtionvarainministeriö. https://www.vahtiohje.fi/web/guest/776 Luettu 17.11.2019.

Rousku, Kimmo 2017. Ohje riskienhallintaan. Valtiovarainministeriön VAHTI julkaisu 22/2017. https://julkaisut.valtionevosto.fi/bitstream/hadle/10024/80013/VM_22_2017.pdf?sequence =1&isAllowed=y. Luettu 20.10.2019

Rousku, Kimmo 2018. Miten Suomen julkisen hallinnon organisaatiot pärjäsivät tietoturvan ja tietosuojan ollessa uhattuna? TAISTO18-harjoitus. 29.11.2018 esitysmateriaali. Väestörekisterikeskus. https://vrk.fi/documents/2252790/9592142/TAISTO+tiiviisti+-esitys/72eaedff-4498-d66f-fbc8-588c3973170e/TAISTO+tiiviisti+-esitys.pdf?version=1.1. Luettu 20.9.2019.

Rousku, Kimmo 2019a. Digiturvaopas – JUDO-hanke sekä digitaalinen turvallisuus toiminnan mahdollistajana. Versio 1.0. 12.6.2019. Väestörekisterikeskus. https://vrk.fi/documents/2252790/13076333/Digiturvaopas_1206_2019.pdf/f8d7e2ab-7395-2e4a-88e9-291cea4d0b41/Digiturvaopas_1206_2019.pdf. Luettu 20.9.2019.

Rousku, Kimmo 2019b. TAISTO19-harjoituskäsikirja. Väestörekisterikeskus. https://vrk.fi/taisto19. Luettu 20.9.2019.

Sixsigma 2019. Yleistä Leanista, Viisi kysymystä. Quality Knowhow Karjalainen Oy. http://www.sixsigma.fi/index.php/fi/lean/yleinen/viisi-kysymystae/. Luettu 11.9.2019

Suojanen, Ulla 2014. Toimintatutkimus ammatillisen kehittymisen välineenä. Internet-artikkeli, EKATUO. https://metodix.fi/2014/05/19/suojanen-toimintatutkimus/. Luettu 8.4.2018.

The Business Technology Forum 2019. Business Technology Standard Version 4.0.1.

Tiedonhallintalaki – Täytäntöönpano 2019. Virastojen tietohallintojohtajien kokous 14.5.2019 esitysmateriaali Tiedonhallintalaki_Tietohallintojohtajat_20190514.pdf. Valtiovarainministeriö.

Turvallisuuskomitea.fi. Uhkamallit. https://turvallisuuskomitea.fi/yhteiskunnan-turvallisuusstrategia/uhkat/. Luettu 29.9.2019.

VAHTI 2016. BIA-vaikutusarviointityökalu. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto. Valtionvarainministeriö 14.9.2016. https://www.vahtiohje.fi/web/guest/home;jsessionid=8C1C2A04C27E8DB9B41E6C4A576CDD777BB2CB6A83EA2B7289362BE9A40B1925BA8C8B60A96E161C9F13B5. Luettu 20.11.2019.

VAHTI 2017. Riskienhallintatyökalu – Excel – perusversio. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto. https://www.vahtiohje.fi/web/guest/home;jsessionid=8C1C2A04C27E8DB9B41E6C4A576CDD777BB2

CB6A83EA2B7289362BE9A40B1925BA8C8B60A96E161C9F13B5. Luettu 10.11.2019.

Valtiovarainministeriö 2019. Riskienhallintapolitiikka > Riskienhallintapolitiikkamalli > Asiakirjapohja viraston riskienhallintapolitiikan valmisteluun. https://vm.fi/riskienhallinta/riskienhallintapolitiikka. Luettu 10.11.2019.

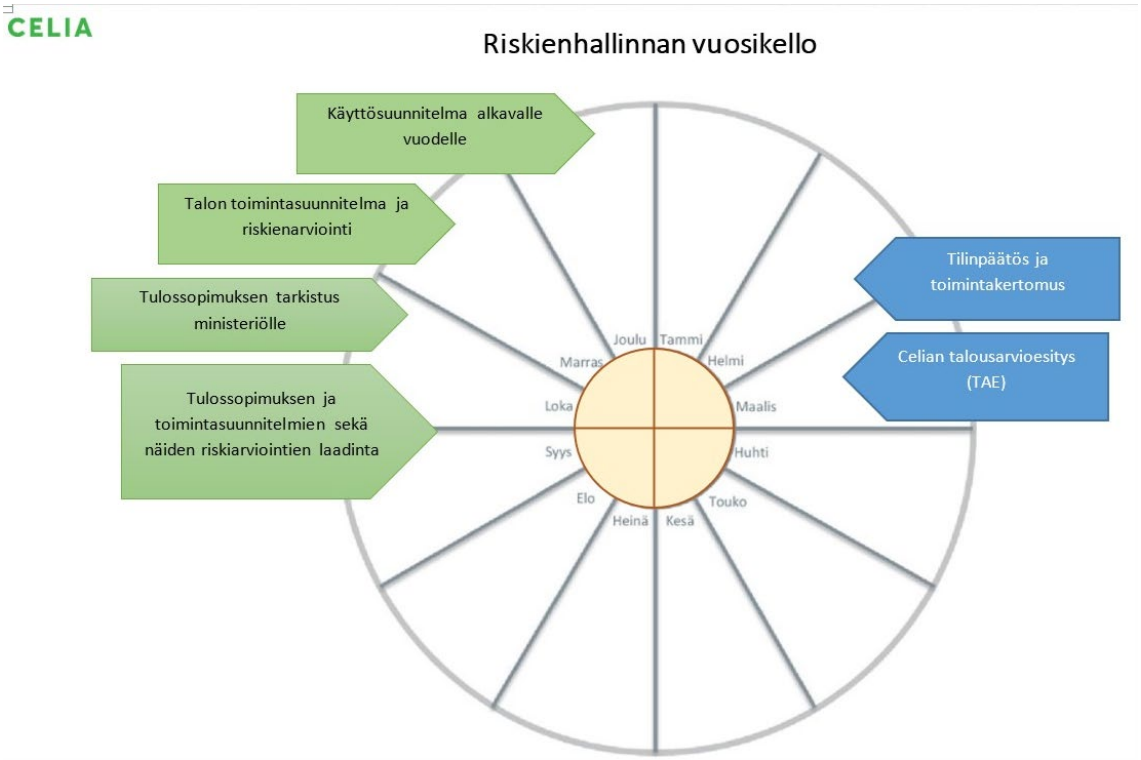
LIITE 1: Celian riskienhallintapolitiikan riskienhallintatyökalu.

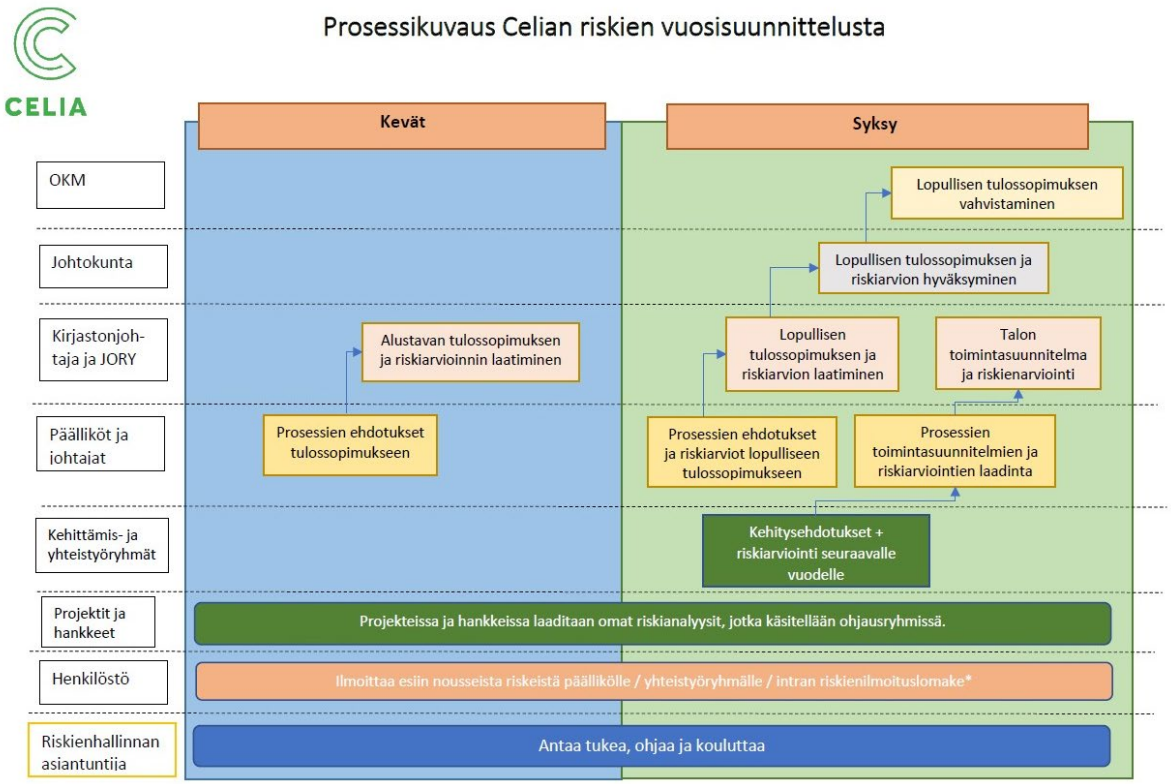
Kuvakaappaus Celian riskienhallintapolitiikkaan liitetystä VAHTI-ohjeen riskienhallintatyökalusta. (VAHTI 2017)

Riskien tunnistaminen				Riskianalyysi	
Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys	Vaikutus
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu

Riskin merkityksen arviointi				Riskin käsittely				Lisätietoja
Riskin suuruus (T x V)		Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyk		Toimenpide-ehdotukset riskin käsittelylle		Toimenpiteiden vapaamuotoinen (sanallinen) kuvaus	Vastuuhenkilö	Tavoiteaikataulu (mihin mennessä	
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				
0	Ei arvioitu	0	Ei arvioitu	0	Ei arvioitu				

LIITE 2: Celian riskienhallintapolitiikan vuosikello ja prosessikuvaus

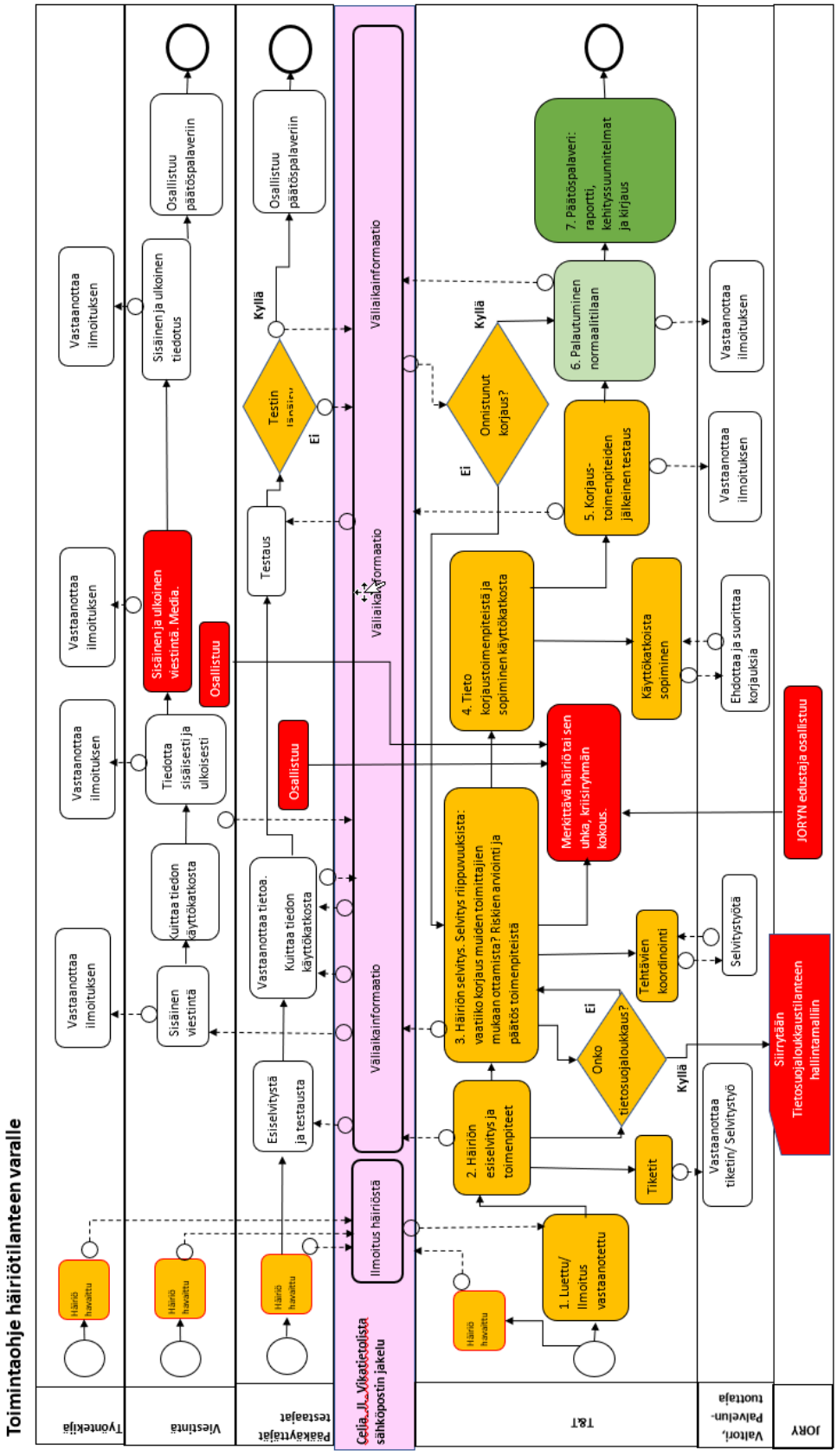




LIITE 3: Järjestelmän X riskiarviointi jatkuvuussuunnitelmaan. (SALATTU)

LIITE 4: Järjestelmän X BIA vaikutusanalyysin yhteenveto ja raportti jatkuvuus-suunnitelmaan (SALATTU)

LIITE 5: Toimintaohjeen prosessikuvaus häiriötilanteissa



LIITE 6: Toimintaohjeen prosessikuvaus tietosuojaloukkaustilanteissa