LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Kohti tietoaineistojen luokittelua ammattikorkeakoulussa

Laakso, Matti

2016 Laurea

Laurea-ammattikorkeakoulu

Kohti tietoaineistojen luokittelua ammattikorkeakoulussa

Matti Laakso
Tietojärjestelmäosaaminen
Opinnäytetyö
Marraskuu, 2016

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojärjestelmäosaaminen
Ylempi ammattikorkeakoulututkinto

Matti Laakso

Kohti tietoaineistojen luokittelua ammattikorkeakoulussa

Vuosi 2016 Sivumäärä 77

Turun ammattikorkeakoulussa oli tarve selvittää miten työntekijöitä voidaan ohjeistaa erottelemaan julkiset ja salaiset tiedot toisistaan sekä käsittelemään tietoja organisaation omat tietojen käsittelyperiaatteet ja muiden osapuolten vaatimukset huomioiden. Ratkaisuksi arvioitiin tietojen luokittelua tiedon julkisuuden perusteella. Selvitystä varten otettiin käyttöön erillinen termi, tiedon julkisuusluokittelu. Opinnäytetyön tarkoituksena on muodostaa yleistietoa, ymmärrystä ja osaamista tietojen julkisuusluokittelusta.

Toimintaympäristöksi rajattiin organisaation IT-palveluita tuottava yksikkö ja sen käsittelemät sähköiset dokumentit. Kokonaisuutta lähestyttiin kolmen osatutkimuksen kautta. Osatutkimuksissa selvitettiin, miten sähköisten dokumenttien julkisuusluokittelua voidaan ymmärtää, toteuttaa ja hyödyntää IT-yksikössä. Ensimmäinen osatutkimus toteutettiin tapaustutkimuksena. Aineistona käytettiin IT-yksikön työntekijöiden haastatteluita ja organisaation toimintaa ohjaavia periaatedokumentteja. Toisessa osatutkimuksessa toteutettiin suunnittelututkimus, jonka avulla kehitettiin menetelmä julkisuusluokittelun aloittamiseksi. Menetelmän runko muodostettiin kirjallisuuskatsausta hyödyntäen. Menetelmää testattiin käytännössä ja parannettiin palautteiden perusteella. Kolmas osatutkimus toteutettiin tapaustutkimuksena ja siinä hyödynnettiin aikaisempia haastatteluaineistoja sekä menetelmän testauksen aikana tehtyjä havaintoja.

Tuloksista johdettiin vastaukset tutkimuskysymyksiin. Ensimmäisessä osatutkimuksessa löydettiin tapa ymmärryksen muodostamiseksi ja tunnistettiin aiheeseen liittyviä kehittämiskohteita IT-yksikössä. Toisessa osatutkimuksessa rakennettu ja testattu menetelmä todettiin toimivaksi ratkaisuksi julkisuusluokittelun aloittamiseksi. Kolmannessa osatutkimuksessa tunnistettiin monia potentiaalisia julkisuusluokittelun hyödyntämiskohteita. Osatutkimuksista muodostettiin myös jatkotutkimusaiheita.

Julkisuusluokittelu havaittiin monipuoliseksi kokonaisuudeksi, joka muodostuu useasta teemasta. Tulosten perusteella arvioitiin, että siirtyäkseen kohti laajamittaisempaa tietoaineistojen luokittelua, on organisaation ymmärrettävä yksittäiset teemat ja niiden muodostama kokonaisuus, edettävä systemaattisesti ja suunnitelmallisesti sekä viestittävä ja ohjeistettava aiheesta ymmärrettävästi. IT-yksikön lisäksi tuloksista hyötyvät myös muut organisaatiot, jotka pohtivat tietoaineistojensa luokittelua. Opinnäytetyön teoriatietoa ja tuloksia voidaan hyödyntää luokittelutoiminnan johtamisen, suunnittelun ja toteuttamisen tukena.

Asiasanat: tietoaineistojen luokittelu, tietojen luokittelu, turvallisuusluokittelu, julkisuusluokittelu

Laurea University of Applied Sciences
Degree Programme in Information Systems
Master's Thesis

Abstract

Matti Laakso

Towards information asset classification in a University of Applied Sciences

Year 2016 Pages 77

There was a need in Turku University of Applied Sciences to explore how employees can be instructed to separate public and secret information and to manage information by taking into account the organization's own information handling requirements and compliance requirements. Classification of information according to its publicity was appraised as a solution. The term publicity classification was coined to be used in this thesis. The primary objective of the thesis was to form common understanding and general and practical knowledge about publicity classification.

The context of the thesis was limited to the organization's IT unit and the electronic documents handled by the IT unit. The thesis was approached via three studies. The research questions were how the publicity classification of electronic documents can be understood, implemented and utilized in the organization's IT unit. In the first study a case study was conducted. Research data was collected from IT unit employee interviews and documents. In the second study a method for starting publicity classification of documents was developed using design science research methodology. The basis of the method was formed using literature review. The method was tested in a real work environment and improved according to the feedback. In the third study another case study was conducted. Research data was formed from the earlier interviews and observations made during the testing of the method.

Answers to the research questions were derived from the results of the studies. In the first study a way of gaining understanding was found. Suggestions of improvements for the organization's IT unit were recognized. A method for starting publicity classification in the organization was built in the second study. The method was proven to work by testing it in the real work environment. In the third study, many potential ways of benefitting from the classified information were recognized. New research targets were also revealed from the studies.

Publicity classification was proven to be a diverse scheme which builds up from different themes. The results indicate that should the organization move towards information asset classification, the organization must understand the different themes which build up the classification scheme, proceed systematically with a plan and communicate and give instructions about the classification in an understandable way. The IT unit will benefit from the results in their daily work. The theory and the results can also be beneficial for leading, planning and implementing the classification of information assets in other organizations.

Keywords: Information classification, asset classification, security classification, publicity classification

Sisällys

1 Johdanto 8
2 Tietojen luokittelu 10
2.1 Julkisuusluokittelun kokonaiskuva 11
2.1.1 Luokittelutarpeen tunnistaminen 12
2.1.2 Tiedon omistajuus 12
2.1.3 Tiedon luokitteluperiaatteet, merkintä ja käsittely 12
2.1.4 Koulutus ja ohjeistaminen 13
2.2 Luokittelumallit ja -menetelmät 13
2.3 Julkisuusluokittelun hyödyntäminen osana organisaation toimintaa 15
2.3.1 Riskienhallinta 15
2.3.2 Tiedon käsittelysäännöt 16
2.3.3 Tietoturvamekanismit 16
2.3.4 Dokumenttien hallinta 17
2.3.5 Tietojärjestelmät ja pääsynhallinta 18
2.3.6 Henkilöstön toiminta ja osaaminen 19
2.3.7 Toiminnan suunnittelu ja hallintajärjestelmät 19
2.3.8 Organisaatioiden välinen yhteistyö ja ulkoistaminen 20
3 Opinnäytetyön tutkimusmetodologia 21
3.1 Osatutkimusten rajaus, tutkimuskysymykset ja tavoitteet 22
3.2 Tutkimusmenetelmät ja osatutkimusten etenemisen kuvaus 23
3.2.1 Ensimmäinen ja kolmas osatutkimus 23
3.2.2 Toinen osatutkimus 24
3.3 Tutkimusaineiston kerääminen 25
3.3.1 Organisaation ja IT-yksikön dokumentit 26
3.3.2 IT-yksikön henkilöhaastattelut 26
3.3.3 Kirjallisuuskatsaus 27
3.3.4 Käytännön testaus ja havainnointi 28
3.3.5 Ulkopuoliset asiantuntijat 29
3.4 Tutkimusaineiston analysointi 29
3.4.1 Ensimmäinen osatutkimus 30
3.4.2 Toinen osatutkimus 31
3.4.3 Kolmas osatutkimus 31
4 Tulokset 32
4.1 IT-yksikön ymmärrys sähköisten dokumenttien julkisuusluokittelusta 33
4.1.1 Dokumenttien julkisuusluokittelun tarve 33
4.1.2 Luokitteluun liittyvät omistajuus- ja vastuukysymykset 34
4.1.3 Luokiteltavat tiedot ja luokitteluperiaatteet 34

4.1.4 Luokitellun tiedon merkintätavat 35
4.1.5 Luokitellun tiedon käsittely ja luokittelun ohjeistaminen 35
4.2 Menetelmä julkisuusluokittelun aloittamiseksi 36
4.2.1 Tunnista tarve 37
4.2.2 Osoita yritysjohdon tuki 37
4.2.3 Määritä vastuut ja velvollisuudet 38
4.2.4 Viestitä tarkoitus, tavoitteet ja hyödyt 38
4.2.5 Osallista työntekijät 39
4.2.6 Dokumentoi ja inventoi 39
4.2.7 Tunnista tietoaineistot 40
4.2.8 Toteuta vaikutusarviointi 40
4.2.9 Määrittele luokittelukategoriat ja luokittele tietoaineistot 41
4.3 Julkisuusluokittelun aloitusmenetelmän testaus ja kehitys 42
4.3.1 Testiympäristö 42
4.3.2 Menetelmän soveltaminen IT-yksikössä 43
4.3.3 Menetelmän kehitysprosessi 45
4.4 Julkisuusluokittelun hyödyntäminen IT-yksikössä 46
4.4.1 Tärkeiden tietojen tunnistaminen ja hallinta 47
4.4.2 Tietojärjestelmien ja palveluiden suunnittelu ja käyttöönotto 47
4.4.3 Pääsynhallinta ja tietoturvamekanismien toteuttaminen 48
4.4.4 Vastuiden ja velvollisuuksien selkeyttäminen 48
4.4.5 Riskienhallinta ja jatkuvuuden suunnittelu 48
4.4.6 Muut hyödyntämiskohteet 48
5 Pohdinta 49
5.1 Tulosten arviointi 49
5.1.1 Ensimmäinen osatutkimus 50
5.1.2 Toinen osatutkimus 51
5.1.3 Kolmas osatutkimus 53
5.1.4 Opinnäytetyö kokonaisuutena 54
5.2 Laadun arviointi 56
5.2.1 Käytetyt tutkimusmenetelmät 56
5.2.2 Aineiston keräys ja analysointi 57
5.2.3 Tutkimusprosessi 59
5.2.4 Tulosten oikeellisuus ja yleistettävyys 60
5.2.5 Roolini osatutkimuksissa 61
5.3 Jatkotutkimusaiheet 62
6 Lopuksi 63
Lähteet 64
Kuviot 70

Taulukot 71
Liitteet.. 72

1 Johdanto

Turun ammattikorkeakoulussa tuotetaan päivittäin paljon tietoa, esimerkiksi sähköisinä dokumentteina. Dokumentteja käsitellään eri paikoissa, kuten verkkolevyillä, intranetissä ja ulkoisissa tiedostojen tallennuspalveluissa. Tallennuspalveluiden käyttöönoton yhteydessä on kuitenkin havaittu ongelma. Työntekijöitä pitäisi pystyä helpommin ohjeistamaan, miten julkiset ja salaiset tiedot erotellaan toisistaan, ja miten tietoja saa käsitellä eri palveluissa lainsäädäntö, ulkopuolisten yhteistyökumppanien vaatimukset sekä organisaation omat tietojen käsittelyperiaatteet huomioiden.

Organisaatiossa arvioitiin, että tietojen luokittelu auttaisi ongelman ratkaisemisessa. Tietojen luokittelu on kokonaisuus, joka auttaa tunnistamaan organisaatiolle tärkeät tiedot ja suojaamaan ne asianmukaisilla tavoilla eri käyttötilanteissa. Suojaamisen lisäksi luokittelulla pyritään mahdollistamaan tiedon vapaa, mutta turvallinen liikkuvuus (SFS-ISO/IEC 2013a, 2013b).

Tietojen luokittelu ei ole organisaatiolle aiheena täysin uusi. Esimerkiksi organisaation toimintaa ohjaavissa periaatepäätöksissä todetaan, että tietojen luokittelu ja käsittely tullaan toteuttamaan valtionhallinnon suositusten mukaisesti. Lisäksi luokittelusta on arvioitu olevan hyötyä myös pilvipalveluiden käytön ohjeistamisessa. Pilvipalveluilla tarkoitetaan tässä opinnäytetyössä organisaation ulkopuolisen tahon tuottamia ja ylläpitämiä resurssipalveluita, joita työntekijät hyödyntävät päivittäisissä työtehtävissään verkkoyhteyden avulla. Tiedon tallennuspalveluiden lisäksi pilvipalveluna tuotettavia resursseja ovat esimerkiksi erilaiset sovelluspalvelut. (NIST 2011.)

Kohdeorganisaation lisäksi luokittelu on ajankohtainen aihe myös muualla. Tiedon määrän kasvu on johtanut haasteisiin, suurta tietomäärää on vaikeampi hallinnoida ja suojata. Organisaatioiden tietopääomat ovat olleet, ja tulevat jatkossakin olemaan rikollisten kiinnostuksen kohteina. (Mitchell, Marcella & Baxter 1999, 214–216; PwC 2015; Reed 2007, 177–178.)

Kaikki tieto ei ole samanarvoista. Oppenheimin ym. (2003) tutkimuksessa haastateltujen yritysjohtajien mukaan tärkeäksi tietopääomaksi pitäisi luetella vain liiketoimintatarpeet täyttävät tiedot. Organisaation on tunnettava tietopääomansa, sekä sen arvo, jotta tiedon säilyttäminen, hallinta ja turvaaminen onnistuisivat tehokkaasti (Raman, Beets & Kabay 2014, 67.6.1). Tämä on mahdollista tietojen luokittelun avulla (Cazemier, Overbeek & Peters 2010, 65; Peltier & Tompkins 2014, 298). PwC (2013, 10) kuitenkin raportoi, että iso osa yrityksistä ei ole asianmukaisesti tunnistanut tai turvannut heille tärkeitä tietoja.

Tiedon luokittelu on laaja ja monipuolinen kokonaisuus. Tietoa voidaan luokitella esimerkiksi tiedon luottamuksellisuuden, eheyden ja saatavuuden perusteella (NIST 2008, 10–11). Luottamuksellisuudella tarkoitetaan, että tietoa käsittelevät vain ne tahot, joilla on siihen oikeus. Eheydellä ja saatavuudella tarkoitetaan puolestaan sitä, että tieto on pysynyt muuttumattomana ja se on käytettävissä tarvittaessa. (Raggad 2010, 20.) Luottamuksellisuutta voi lähestyä myös arvioimalla, kuinka julkista tieto on. Tästä johtuen otettiin käyttöön erillinen termi, tiedon julkisuusluokittelu.

Tietojen luokittelun kokonaisuuden hahmottamiseksi organisaatiossa tarvittiin yleistietoa, ymmärrystä ja osaamista aiheeseen liittyen. Kokonaisuutta lähestyttiin kolmen osatutkimuksen kautta, joiden aiheet rajattiin käsittelemään luokittelua tiedon julkisuuden näkökulmasta. Osatutkimusten eteneminen ja tulokset on raportoitu tässä YAMK-opinnäytetyössä. Organisaatiolle ei ole aikaisemmin tehty tutkimuksia, kehittämistehtäviä tai opinnäytetöitä aiheeseen liittyen.

Osatutkimusten toimintaympäristöä rajattiin kaksivaiheisesti. Turun ammattikorkeakoulussa toimintaympäristöksi rajattiin korkeakoulun turvallisuus-, tila-, tietohallinto- ja IT-palveluita tuottava Oppimisympäristöpalvelut-yksikkö. Sen sisällä osatutkimukset kohdistettiin IT-palveluita tuottavaan toimintoon. Selkeyden vuoksi toiminnosta puhutaan tässä opinnäytetyössä nimellä IT-yksikkö. IT-yksikkö vastaa organisaation ydintoiminnan kannalta keskeisten tietojärjestelmien suunnittelusta, käyttöönotosta, ylläpidosta ja kehittämisestä sekä muista tehtäväkokonaisuuksista. IT-yksikössä on noin 30 työntekijää. Koko organisaatiossa työntekijöitä on noin 650.

Osatutkimuksissa selvitetään, miten sähköisten dokumenttien julkisuusluokittelua voidaan ymmärtää, toteuttaa ja hyödyntää IT-yksikössä. Ensimmäinen osatutkimus toteutettiin nykytilan selvittämiseksi. Peruste toiselle osatutkimukselle saatiin ensimmäisessä osatutkimuksessa tunnistettujen kehittämiskohteiden kautta. Kolmas osatutkimus toteutettiin, jotta voitaisiin tunnistaa muita potentiaalisia hyödyntämiskohteita pilvipalveluiden käytön ohjeistamisen lisäksi.

Tuloksina saadaan kuvaus julkisuusluokittelun nykytilasta IT-yksikössä, kehittämiskohteita, menetelmä luokittelun aloittamiseksi sekä potentiaalisia julkisuusluokittelun hyödyntämiskohteita. Tuloksista, opinnäytetyön teoreettisesta viitekehyksestä ja aiheeseen liittyvistä käsitekuvauksista on hyötyä kaikille, jotka suunnittelevat tietojen luokittelua omassa toimintaympäristössään. Opinnäytetyötä voidaan hyödyntää luokittelutoiminnan johtamisen, suunnittelun ja toteuttamisen tukena.

Seuraavassa luvussa kerrotaan tietojen luokittelun teoriaa ja aiheeseen liittyviä keskeisiä käsitteitä. Metodologialuvussa on kuvattu käytetyt tutkimusmenetelmät ja osatutkimusten eteneminen. Tulosluvussa esitellään yksittäisten osatutkimusten tulokset. Pohdintaluvussa arvioidaan osatutkimusten toteuttamista ja tuloksia. Lisäksi pohditaan yksittäisten osatutkimusten merkitystä koko aihekokonaisuuden näkökulmasta.

2 Tietojen luokittelu

Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI (2008, 101) määrittelee tietojen luokittelun toiminnaksi, jossa suoritetaan ”tietojen jakaminen luokkiin tietojen omistajan asettamien perusteiden mukaisesti”. Peltier ja Tompkins (2014, 300) laajentavat näkemystä ja kiteyttävät koko toiminnan seuraavasti: kyseessä on riskilähtöinen liiketoimintaprosessi, jossa otetaan huomioon lainsäädännön ja kolmansien osapuolien vaatimukset. Luokittelu on siis osa tiedon elinkaaren kokonaisvaltaista hallintaa (Raman ym. 2014, 67.2).

Luokittelulla on suuri merkitys tiedon elinkaaren turvallisuudelle (Reed 2007, 178). Tietoja voidaan luokitella eri kategorioihin arvioimalla mahdollisia haittavaikutuksia tiedon eheyden, saatavuuden ja luottamuksellisuuden näkökulmasta. Kategorioista muodostettavat turvallisuusluokat ovat ensiaskel tehokkaalle riskienhallinnalle (NIST 2004; NIST 2008, 6).

Ulkomaisissa lähteissä (esim. NIST 2008) tiedon eheyden, saatavuuden ja luottamuksellisuuden perusteella tehtävää luokittelua kutsutaan esimerkiksi termillä ”security categorization”. Vapaasti suomennettuna se tarkoittaa turvaluokitusta tai turvallisuusluokittelua. VAHTI (2008, 119) on määritellyt käsitteen ”turvaluokitus” seuraavasti: ”luottamuksellisten asiakirjain ja tietojen jakaminen luokkiin salassapidettävyyden perusteella”. Turvallisuusluokittelu on puolestaan paljon käytetty termi suomalaisten ja kansainvälisten viranomaisten asiakirjojen käsittelyssä (VAHTI 2010, 57). Turvallisuusluokat perustuvat niin sanottuihin suojaustasoihin, joilla määritellään vaatimukset tietojenkäsittely-ympäristölle sekä tietojen käsittelylle (VAHTI 2010, 20–21).

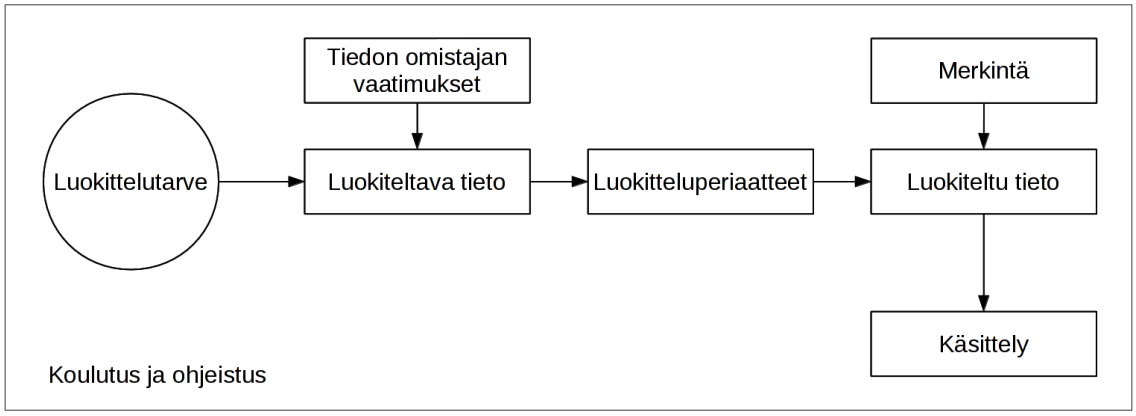
Tässä opinnäytetyössä otetaan käyttöön oma erillinen käsite, julkisuusluokittelu. Käyttämällä julkisuus-etuliitettä halutaan ilmaista, että termi käsittelee tietoa vain sen luottamuksellisuuden näkökulmasta. Toisin sanoen arvioidaan, kuinka julkista tieto on. Lisäksi pyritään siihen, että opinnäytetyössä ei käytettäisi turva- tai turvallisuusluokittelu -termejä mahdollisesti ristiriitaisessa merkityksessä muiden tahojen määritysten kanssa. ”Tietojen luokittelu” on puolestaan opinnäytetyön näkökulmasta liian yleinen käsite, koska termin voidaan ymmärtää sisältävän myös tiedon eheyden ja saatavuuden perusteella tehtävän luokittelun (VAHTI 2010, 61).

2.1 Julkisuusluokittelun kokonaiskuva

Tietojen julkisuusluokittelu on monipuolinen kokonaisuus, joka rakentuu useista toisiinsa linkittyneistä teemoista. Kokonaisuudelle on olemassa monta erilaista termiä. Lähteestä riippuen termi on luokittelumalli, -skeema (Raman ym. 2014, 67.1), -metodologia (Boyer 2003, 3) tai -järjestelmä (Fowler 2003, 1), joka voi sisältää vielä erillisen luokittelukehikon (Furness 2005, 3).

Osa termeistä voi tarkoittaa myös täysin samantyyppistä kokonaisuutta vaikka käsite viittaisikin laajempaan tai suppeampaan kokonaisuuteen. Tässä opinnäytetyössä kaikkiin edellisiin kokonaisuuksiin viitataan tästä eteenpäin sanalla luokittelumalli.

Kuviossa 1 on esitetty yksi tulkinta julkisuusluokittelun kokonaisuudesta. Se on muodostettu kansainvälisesti tunnustettujen ISO27001 ja ISO27002 (SFS-ISO/IEC 2013a, 2013b) -tietoturvastandardien sekä muiden lähteiden (Raman ym. 2014, 67.1–67.6; Raggad 2010, 69–71; Tudor 2001, 45) perusteella. Kuviossa 1 esitettyä kokonaiskuvaa voidaan pitää myös yhtenä luokittelumallina.



Kuvio 1: Hahmotelma julkisuusluokittelun kokonaiskuvasta

Kuvion 1 mukaisesti julkisuusluokittelulle on oltava tarve, jotta luokitteluun liittyvä toiminta olisi perusteltua. Tiedon omistaja puolestaan määrittelee tietoaineiston tietoturvavaatimukset organisaatiokohtaiset vaatimukset huomioiden. Luokitteluperiaatteet kertovat, miten tietoa luokitellaan eri luokkiin. Luokiteltu tieto merkitään, jonka jälkeen tietoa käsitellään sovittujen käytäntöjen mukaisesti. Kokonaisuus koulutetaan ja ohjeistetaan työntekijöille. Kuviossa 1 mainitut osakokonaisuudet on kuvattu tarkemmin seuraavissa alaluvuissa.

2.1.1 Luokittelutarpeen tunnistaminen

Organisaatioilla on eri tarpeita dokumenttien ja tietojen julkisuusluokittelun toteuttamiseksi. Tarpeet voivat muodostua esimerkiksi vaatimustenmukaisuusvelvoitteiden kautta, toisin sanoen lain, toimialan, standardien tai kolmannen osapuolen vaatimuksista. Asianmukainen dokumenttien hallinta nähdään myös osana tietoturvallisuustyötä (VAHTI 2006).

Dokumenttien julkisuusluokittelu ei ole kaikille organisaatioille pakollista. Tudor (2001, 45) kehottaa ensin päättämään, miksi luokittelua halutaan tehdä. Usein syy luokittelun aloittamiselle on nimenomaan organisaatiolle tärkeiden tietojen hahmottamisen ja suojaamisen tarve. Euroopan neuvoston (Council of the European union 2013, 21) tietojen luokitteluohje kiteyttää asian seuraavasti: jos tietojen luottamuksellisuus on turvattava, niin tiedot luokitellaan.

2.1.2 Tiedon omistajuus

Tiedon kriittisyys ja liiketoiminta-arvo määrittelevät sen, kuinka hyvin tietoa tulisi suojata. Arvon, kriittisyyden ja suojaustarpeet tunnistavat parhaiten tiedon omistaja (Raggad 2010, 71). Tiedon omistajalla on tärkeitä tehtäviä. Hän vastaa tiedon luokittelusta ja määrittelee tiedon turvallisuusvaatimukset (SFS-ISO/IEC 2013b), tiedon käyttötavat (Raggad 2010, 71) sekä tahot, joilla on oikeus käsitellä kyseistä tietoa (Peltier & Tompkins 2014, 309).

Kuka tiedon omistaa? Tudorin (2001, 41) mukaan tiedon luoja on tiedon omistaja. Kansainvälinen tietoturvastandardi ISO27002 (2013b) määrittelee omistajaksi sen henkilön tai tahon, joka on vastuutettu huolehtimaan kyseisen tietoaineiston elinkaaresta. Viime kädessä tiedon omistajuus on kuitenkin organisaation ylimmällä johdolla. He vastaavat organisaation tietoaineiston tietoturvallisuudesta (VAHTI 2006, 9). Vaikka tiedon omistajan määritys voi vaihdella, niin tiedolla on kuitenkin oltava omistaja.

2.1.3 Tiedon luokitteluperiaatteet, merkintä ja käsittely

Kansainvälisten tietoturvastandardien ISO27001 ja 27002 (SFS-ISO/IEC 2013a, 2013b) ja kansallisten suositusten (VAHTI 2010, 51) mukaan organisaatiolla tulisi olla dokumentoidut periaatteet tietojen luokittelusta eri julkisuusluokkiin, luokiteltujen tietojen merkinnästä ja käsittelystä. Periaatteet otetaan käyttöön koko organisaatiossa.

Tietoturvastandardit (SFS-ISO/IEC 2013a, 2013b) ja yhdysvaltalainen National Institute of Standards and Technology (NIST 2008) ohjeistavat luokittelemaan tietoaineistot lakisääteisten vaatimusten sekä liiketoiminnan tarpeiden perusteella eri kategorioihin. Samoja suojatoimenpiteitä vaativat tietoaineistot kootaan yhteen ja näille määritellään yksi luokitteluluokka. Luokalle määritellään tarvittavat suojaustoimenpiteet. (SFS-ISO/IEC 2013b.)

Luokka voidaan nimetä siten, että se kuvaa siinä olevan tietoaineiston sisältöä. Esimerkkejä luokkien nimistä ovat julkinen, sisäinen ja salainen. Salaiset tiedot vaativat eri suojaustasoa kuin julkiset tiedot. Näin ollen julkisuusluokkien lisäksi voidaan puhua myös suojausluokista.

Eri julkisuusluokkiin kuuluvat tietoaineistot tulee merkitä siten, että tiedon käsittelijä tietää selkeästi, mihin luokkaan tieto kuuluu. Merkintä voidaan tehdä dokumenttiin esimerkiksi erillisenä tekstimerkintänä tai teknisenä metatietona. (SFS-ISO/IEC 2013b.)

Organisaation tulee toteuttaa luokitellun tiedon käsittelyä varten toimintamallit ja -ohjeet. Niiden tarkoituksena on kertoa miten luokiteltua tietoa saa esimerkiksi käsitellä, siirtää, tallentaa ja kertoa eteenpäin. (SFS-ISO/IEC 2013b.) Ohjeilla pyritään varmistamaan, että kaikki työntekijät luokittelevat tietoa samalla tavalla (Furness 2005, 8).

2.1.4 Koulutus ja ohjeistaminen

Työntekijöiden kouluttaminen ja ohjeistaminen ovat olennaisessa osassa julkisuusluokitteluun liittyvissä asioissa. Jos organisaatiossa ei ole luokittelumallia ja siihen liittyviä toimintaohjeita, niin työntekijät eivät voi luotettavasti tietää, miten tietoa käsitellään (Raman ym. 2014, 67.2). Lisäksi käyttäjille on kerrottava, miksi luokittelua tehdään (Council of the European union 2013, 28–29), mikä tieto on organisaatiolle arvokasta, mitä julkisuusluokkia on olemassa ja mitkä tiedot kuuluvat mihinkin luokkaan (Laaksonen, Nevasalo & Tomula 2006, 161).

Kouluttamaton käyttäjä saattaa käyttää luokittelua väärin ja se voi puolestaan johtaa aliluokitteluun sekä väärään turvallisuuden tunteeseen. Myös tiedon yliluokittelu on uhkana. Tällöin tietoa suojataan liikaa ja liiketoiminta voi kärsiä, koska tarvittavaan tietoon ei päästy käsiksi ajallaan. (SFS-ISO/IEC 2013b; Tudor 2001, 46.)

2.2 Luokittelumallit ja -menetelmät

Kuviossa 1 esitetty peruskokonaisuus hahmottaa tilannetta, jossa luokittelumalli on jo käytössä. Päästäkseen kyseiseen tilanteeseen, on luokittelumalli ensin rakennettava.
Tietojen luokittelumallin rakentamiseksi on olemassa erilaisia vaihtoehtoja. Kokonaisuudet eroavat toisistaan sisällön, laajuuden, yksityiskohtaisuuden ja painopistealueiden perusteella. Tämä voi aiheuttaa haastetta kokonaisuuden hahmottamiselle. Esimerkiksi Furness (2005) vaiheistaa luokittelumallinsa tekemisen selkeisiin kokonaisuuksiin ja kertoo vaiheiden sisällöstä yksitellen. Raman ym. (2014, 67.5) puolestaan kertovat luokittelumallin rakennusvaiheet lyhyessä listassa ja vaiheisiin pitää osata etsiä lisätietoja omatoimisesti.

Useista tietojen luokittelumallin tekemiseen kehitetyistä menetelmävaihtoehdoista on tunnistettavissa selkeästi kolme eri perusvaihetta. Vaiheet ovat tietoaineistojen tunnistaminen, aineistojen tärkeyden arviointi sekä aineistojen tärkeyteen perustuva luokittelukategorioiden rakentaminen (Furness 2005; Greene 2006, 118–128; Peltier & Tompkins 2014, 298–316; Smallwood 2012, 187–193; Whitman & Mattord 2014, 282–290). Menetelmästä riippuen vaiheiden järjestys voi vaihdella.

Kolmen perusvaiheen lisäksi eri menetelmistä on tunnistettavissa useita muita kohtia. Niitä ovat esimerkiksi luokittelutoiminnan ja liiketoiminnan välisen hyödyn tunnistaminen (Smallwood 2012, 187–188), yritysjohdon tuen hankkiminen esimerkiksi erillisellä tietojen luokittelupolitiikalla (Boyer 2003, 3; Furness 2005, 6), tunnistettujen tietoaineistojen omistajuuden määrittely (Boyer 2003, 3; Greene 2006, 119–121) sekä luokittelutoiminnan hyötyjen kuvaaminen työntekijöille (Raman ym. 2014, 67.5). Luokittelutoiminta on laaja käsite, jolla tarkoitetaan kaikkia luokittelumallin rakentamiseen ja luokittelun tekemiseen liittyviä asioita.

Mallien ja menetelmien painopistealueissa on selkeitä eroja. Ramanin ym. (2014, 67.5) lähestymistapa painottuu suojeltavan tiedon löytämiseen ja tiedon käsittelytoimenpiteiden ymmärtämiseen. Greene (2006, 120–121) puolestaan painottaa vastuiden määrittelyä ja tiedon omistajan roolia. Whitman ja Mattord (2014, 282) sekä Peltier ja Tompkins (2014, 300) sen sijaan liittävät koko luokittelutoiminnan vahvasti organisaation riskienhallintaprosessiin.

Tiedon luokitteluun liittyvissä tieteellisissä artikkeleissa on tarjottu erityisesti tiedon tunnistamiseen ja kategorisoimiseen liittyviä menetelmiä, ohjelmistologiikoita sekä matemaattisia malleja. Niitä voidaan hyödyntää esimerkiksi tunnistamaan tietyssä dokumentissa olevaa suojattavan tiedon määrää (Eloff, Holbein & Teufel 1996), luokittelemaan dokumentin automaattisesti sen sisällön perusteella (Alparslan, Karahoca & Bahsi 2011; Booysen & Eloff 1995) tai muuttamaan jo luokitellun tiedoston luokittelua sen käyttötarpeen perusteella (DuraiPandian & Chellappan 2006). Tietokoneavusteisten mallien tarkoituksena on pyrkiä luokittelutoiminnan nopeuttamiseen, helpottamiseen ja ihmisen tekemien luokitteluvirheiden minimoimiseen.

Luokittelumalleista ja -menetelmistä puhuttaessa ei voi olla mainitsematta eri valtioiden toteuttamia, aiheeseen liittyviä ohjeistuksia. VAHTI (2010) tarjoaa erittäin kattavat ohjeet tietoaineistojen luokittelua varten. Ohjeita kannattaa hyödyntää varsinkin silloin, kun halutaan rakentaa viranomaistoiminnan kanssa yhteensopiva julkisuusluokittelumalli. Yhdysvaltalainen NIST (2008), on myös julkaissut paikalliseen viranomaiskäyttöön usean dokumentin kokonaisuuden tietojen ja tietojärjestelmien turvallisuusluokittelusta.

2.3 Julkisuusluokittelun hyödyntäminen osana organisaation toimintaa

Luokitteluun liittyvän kokonaisuuden on tarkoitus tukea ja hyödyttää liiketoimintaa. Se tapahtuu hallitsemalla tietojen luottamuksellisuutta, eheyttä ja saatavuutta (VAHTI 2010, 51) sekä minimoimalla tiedon käsittelyyn liittyvät uhkatekijät (Krutz & Vines 2003, 6). Luokittelu tuo myös systemaattisesti ymmärrystä organisaation prosesseista, tietojärjestelmistä ja niiden sisällöstä sekä tietojen hallinnasta ja omistajuudesta (NIST 2008, 5).

Organisaatio voi saavuttaa kilpailuetua hoitamalla tietoturvansa paremmin (Krutz & Vines 2003, 6). Luokittelun hyödyntäminen voi vähentää tietoaineistojen menettämisestä johtuvia maineriskejä (Tankard 2015, 10–11) sekä yleisesti parantaa organisaation mainetta (mukaillen Boyer 2003, 11) ja näin ollen johtaa liiketoiminnan kasvamiseen (Fowler 2003, 3-4). Luokittelusta saavutettava parempi tietojen hallinta voi myös avata liiketoimintamahdollisuuksia muissa maissa (Tankard 2015, 11).

Julkisuusluokittelu on laaja kokonaisuus ja aiheen monipuolisuus on havaittavissa myös hyödyntämiskohteiden määrässä. Kirjallisuudesta on tunnistettavissa useita toisiinsa linkittyneitä ja osittain päällekkäisiä hyödyntämiskohteita, joita voidaan lähestyä esimerkiksi seuraavien aihealueiden kautta: 1) riskienhallinta, 2) tiedon käsittelysäännöt, 3) tietoturvamekanismit, 4) dokumenttien hallinta, 5) tietojärjestelmät ja pääsynhallinta, 6) henkilöstön toiminta ja osaaminen, 7) toiminnan suunnittelu ja hallintajärjestelmät, 8) organisaatioiden välinen yhteistyö ja ulkoistaminen. Aihealueita on kuvattu tarkemmin seuraavissa alaluvuissa.

2.3.1 Riskienhallinta

Luokiteltuja tietoaineistoja voidaan hyödyntää organisaation riskienhallintaprosessissa (Peltier & Tompkins 2014, 300). Riskienhallinta on prosessi, jossa liiketoiminnan tarpeet ja tiedon suojaamisen käytettävät resurssit pyritään saamaan kustannustehokkaaseen tasapainoon (Peltier 2010, 137). Tietoaineistojen tunnistaminen ja luokittelu ovat ensimmäiset sekä olennaisimmat vaiheet prosessin aloittamisessa (NIST 2008, 6; Whitman & Mattord 2014, 288).

Tietoaineistoon kohdistuva riskienhallinta voi olla haastavaa. Grimaila ja Fortson (2007, 207) havaitsivat, että organisaatiot suosivat ennemmin teknologialähtöistä riskienhallintaa, koska teknologiset resurssit ovat konkreettisempia asioita kuin tieto. Teknologiaan kohdistuva riskienhallinta vaatii vähemmän subjektiivista arviointia ja näin ollen vähemmän ajatustyötä.

Luokittelu tekee tietoaineistosta konkreettisemman asian ja auttaa hahmottamaan siihen liittyviä riskejä omina kokonaisuuksinaan. Niin sanotun laadullisen riskianalyysin näkökulmasta on olennaista, että kriittinen tieto pystytään erottelemaan muusta tiedosta (Landoll 2011,

444). Se onnistuu julkisuusluokittelun avulla. Myös riskien priorisointi helpottuu, kun tärkeimmät suojattavat kohteet on tunnistettu. Esimerkiksi salaisten tietojen paljastumisella on eritasoiset vaikutukset kuin julkisten tietojen paljastumisella. Tiedon julkisuusluokka vaikuttaa siis olennaisesti riskianalyysin lopputulokseen.

Riskienhallintaprosessin aikana kerätyistä tiedoista on hyötyä tietojen luokittelutoiminnalle sekä koko organisaatiolle. Tuloksista voidaan arvioida, mihin sijoittaa aikaa, rahaa, työtä ja muita tarvittavia resursseja (Greene 2006, 137–139; Pavlov & Karakaneva 2011, 23). Resurssitarpeet on helpompi viestiä muille työntekijöille ja yritysjohdolle, koska tarpeille on olemassa selkeät perusteet. Resursseja kohdentamalla voidaan saada kustannussäästöjä aikaiseksi.

2.3.2 Tiedon käsittelysäännöt

Luokittelua voidaan hyödyntää tiedon käsittelyn turvaamisessa luomalla luokitellun tiedon käsittelysäännöt (Laaksonen ym. 2006, 157). Sääntöjen tarkoituksena on ohjata toimintaa siten, että käsittely tukee tietoaineistolle asetettuja tietoturvavaatimuksia (Bayuk 2009, 59). Käsittelysäännöillä ohjataan kaikkia tiedon elinkaaren aikana tapahtuvia toimia, kuten esimerkiksi tiedon luomista, tallettamista, muokkaamista, siirtämistä, luovuttamista ja tuhoamista.

Tyypillisiä käsittelysääntöjen ohjaamia tilanteita ovat esimerkiksi luottamuksellisen tiedon lähettäminen sähköpostilla tai tiedon tallettaminen ulkoisiin pilvipalveluihin. Salaisen tietoaineiston luottamuksellisuuden varmistamiseksi voidaan sopia, että tietoa ei lähetetä laisinkaan sähköpostilla, joka liikkuu vapaasti avoimessa tietoverkossa. Vastaavasti voidaan päättää, että salaisiksi luokiteltuja tiedostoja ei tallenneta ulkoisiin pilvipalveluihin salaamattomana. Julkista tietoa saa puolestaan käsitellä huolettomammin eri viestintävälineissä.

Julkisuusluokiteltua tietoa voidaan hyödyntää myös eri laitekokonaisuuksien käytön suunnittelussa. Organisaatio voi esimerkiksi päättää, että luottamuksellisia dokumentteja ei saa käsitellä mobiililaitteissa salaamattomana. Tietoaineistojen ja niihin liittyvien riskien tunnistaminen ovat myös yksi olennainen osa organisaation mobiililaitteista aiheutuvien riskien hallintaa (Brand, Kruger-Van Renen & Rudman 2015, 209).

2.3.3 Tietoturvamekanismit

Tiedon suojaaminen käytännössä tapahtuu kohdistamalla tiedon käsittelytapahtumiin erilaisia tietoturvallisuutta parantavia toimenpiteitä. Voidaan puhua myös tietoturvamekanismeista. Tietoturvamekanismien kohdistaminen on yksi julkisuusluokittelun merkittävimmistä hyödyntämiskohteista (Tudor 2001, 45).

Mekanismit voivat olla esimerkiksi tietoturvallisuutta parantavia teknisiä suojauksia tai hallinnollisia toimenpiteitä. Organisaatiossa on voitu päättää, että salaisia tietoja sisältävien järjestelmien etäkäyttö ei ole sallittua. Tekniset ratkaisut, mekanismit, estävät käytön organisaation verkon ulkopuolelta. Myös käyttäjätunnuksen ja salasanan kysyminen on yksi tyypillinen esimerkki tietoturvamekanismista, jolla suojellaan organisaation tietoja.

Kun tiedetään, mitä pitää suojata ja millä tavalla, voidaan tietoturvamekanismit kohdistaa jo etukäteen. Raggadin (2010, 70) mukaan proaktiivinen lähestymistapa tekee toiminnasta vähemmän riskialtista ja laskee kustannuksia.

2.3.4 Dokumenttien hallinta

Luokittelutoiminnan sisäistäminen päivittäisessä työssä auttaa rakentamaan turvallisempia dokumentteja. Kun tiedetään, mikä tieto on julkista ja mikä salaista, niin dokumentit voidaan rakentaa paremmin tiettyä tarkoitusta palvelevaksi (VAHTI 2010, 55). Esimerkiksi turhaan luottamuksellista tietoa sisältävä dokumentti rajoittaa sen julkista jakelua. Dokumentin rakentaminen sen käyttötarkoituksen ja kohderyhmän mukaan helpottaa tiedon jakamista ja hallintaa.

Hyödyntämällä tietojen luokittelua, dokumenttien hallintajärjestelmiä ja rakenteisia dokumentteja, voidaan saavuttaa lisähyötyjä. Rakenteiset dokumentit ovat tietokokonaisuuksia, jotka muodostuvat aina tietyistä elementeistä (Kaario & Peltola 2008, 39). Näistä yksi esimerkki on julkisuusluokitusmerkintä. Dokumenttien hallintajärjestelmä on puolestaan tietojärjestelmä, johon tallennetaan dokumentteja, ja joka pitää kirjaa esimerkiksi tiedoston luojasta, muokkaajasta, tiedoston versioista sekä julkisuusluokasta.

Rakenteisiin dokumentteihin voidaan liittää käyttöoikeuksiin liittyviä sääntöjä (Kaario & Peltola 2008, 39). Lisäksi dokumentista voidaan automaattisesti tunnistaa suojattavan tiedon määrä (Eloff ym. 1996) ja dokumentti voidaan luokitella automaattisesti sen sisällön perusteella (Alparslan ym. 2011; Booysen & Eloff 1995). Pitkälle kehitetty dokumenttien hallinta mahdollistaa myös jo luokitellun tiedoston luokituksen muuttamisen sen käyttötarpeen perusteella (DuraiPandian & Chellappan 2006).

Liittämällä luokituksen sähköisen dokumentin metadataan, saadaan dokumentti merkittyä siten, että sitä on helpompi seurata tietoverkoissa. Seurantaan tarkoitetut työkalut havaitsevat dokumentin liikkeet tietoverkossa ja esimerkiksi estävät sen lähettämisen organisaation ulkopuolelle. (Tankard 2015, 9-11.)

Jos organisaatio pystyy tunnistamaan vanhaksi ja tarpeettomaksi jääneet tiedot ja dokumentit, niin ne voidaan poistaa käytöstä. Tätä kautta saadaan resursseja säästettyä, kun ei tarvitse tallentaa tai varmuuskopioida turhia tietoaineistoja (Raman ym. 2014, 67.2).

Tiedon vanhentuessa voi muuttua myös tiedon suojaustarpeet. Esimerkiksi yrityksen tilinpäätöstiedot ovat salaisia ennen niiden virallista julkaisua. Sen jälkeen tiedot muuttuvat julkisiksi (Laaksonen ym. 2006, 158). Julkisen tiedon luottamuksellisuuden varmistamiseksi ei tarvita enää niin paljoa resursseja. Luokittelu auttaa arvioimaan, miten tietoa pitäisi suojata tiedon elinkaaren eri vaiheissa (VAHTI 2010, 53).

2.3.5 Tietojärjestelmät ja pääsynhallinta

Tietojen luokittelulla on paljon vaikutuksia tietojärjestelmiin. Luokittelua voidaan hyödyntää järjestelmien suunnittelussa (VAHTI 2010, 53), kehityksessä (NIST 2008, 5) tai olemassa olevien järjestelmien suojaustarpeiden arvioinnissa. Kun tiedetään millaisia tietoja järjestelmä sisältää, tai tulee sisältämään, voidaan järjestelmälle asettaa asianmukaisia tietoturvavaatimuksia (Fowler 2003, 4; Smallwood 2012, 193). Tämä mahdollistaa järjestelmän suunnittelun alusta alkaen tietoturvalliseksi ja organisaation ydintoimintaa tukevaksi.

Hyvin suunniteltu ja toteutettu tekninen infrastruktuuri luo perustan järjestelmien turvalliselle käytölle (Boyer 2003, 10–11). Esimerkiksi tietojärjestelmiin liittyvien palvelinten sijainnin ja hallinnan määrittely voivat olla riippuvaisia järjestelmässä olevien tietojen luokittelusta (Andreasson, Koivisto & Ylipartanen 2015, 98). Salaisia tietoja sisältävät palvelimet voidaan päättää sijoittaa Suomeen ja omaan ylläpitoon, kun taas julkiset tiedot voidaan sijoittaa tarkoituksella ulkomaisiin pilvipalveluihin.

Luokittelusta on hyötyä myös laitteiden ja järjestelmien elinkaaren hallinnassa. Jos tiedetään, että järjestelmään yhdistetyllä laitteella on käsitelty luottamuksellisia tai salaisia tietoja, niin laite voidaan poistaa käytöstä erikseen määritetyn prosessin avulla. Laitteen kiintolevy esimerkiksi ylikirjoitetaan tai poistetaan kokonaan.

Luokituksella voidaan säädellä, kenellä on oikeus päästä käsittelemään tietoa (Calder & Watkins 2012, 118). Esimerkiksi luottamuksellisia tietoja sisältävät tietojärjestelmän osiot voidaan rajata vain tietylle käyttäjäryhmälle, kun taas kaikille avoimeen osioon pääsee muutkin organisaation työntekijät (Pfleeger & Pfleeger 2006, 246–249). Tietojärjestelmien lisäksi vastaavia luokitteluun liittyviä käyttöoikeusperusteita voidaan hyödyntää myös laajemmissa tietoaineistoissa tai yksittäisissä dokumenteissa.

2.3.6 Henkilöstön toiminta ja osaaminen

Luokittelu auttaa työntekijöitä ymmärtämään, millaisia tietoja organisaatiossa käsitellään (Andreasson ym. 2015, 98) ja millaista merkitystä tiedolla on organisaatiolle (Laaksonen ym. 2006, 161). Luokittelu kuvaa työntekijöille tiedon arvoa (Raman ym. 2014, 67.3) ja tärkeyttä (Furness 2005, 3), tiedon suojaustarvetta (Boyer 2003, 3-4) sekä tiedon luottamuksellisuuden menettämisestä aiheutuvan haitan määrää (VAHTI 2010, 55).

Luokittelu auttaa ymmärtämään sekä määrittämään tietojen käsittelyyn liittyviä vastuita ja velvollisuuksia (Peltier & Tompkins 2014, 298; Tankard 2015, 9). Organisaatiossa voidaan esimerkiksi sopia, että omistajat määrittelevät vaatimukset ja IT-asiantuntijat toteuttavat tekniset suojamekanismit. Kaikki työntekijät ovat puolestaan velvollisia käsittelemään tietoa sovitulla tavalla.

Kun työntekijä käsittelee luokittelua dokumenttia, hän joutuu pohtimaan tietoaineiston sisältöä. Salaiseksi merkitty dokumentti kertoo, että tietoa tulee käsitellä erityisen huolellisesti (Tudor 2001, 45). Tankardin (2015, 9) mukaan tämä kasvattaa työntekijän tietoturvatietoisuutta.

Tietoturvatietoisuutta on mahdollista kasvattaa myös ottamalla luokitteluun liittyvä kokonaisuus olennaiseksi osaksi perehdyttämistä ja tietoturvakampanjoita (Tudor 2001, 45). Työntekijät saavat selkeämmän kuvan, millaista toimintaa kohti pitäisi edetä (Fowler 2003, 4).

Ramanin ym. (2014, 67.2) mukaan luokittelu lisää työntekijöiden tuottavuutta. Luokittelu tehostaa tiedon käsittelyä ja tukee sillä tavalla tiedon vapaata, mutta turvallista liikkumista. Myös Fowler (2003, 4) on tuottavuuden lisääntymisen kannalla. Hänen mukaansa luokittelu vapauttaa resursseja, kun henkilöiden ei tarvitse kysyä enää toisiltaan, saako tietoa jakaa vai ei. Sen sijaan luokittelumerkintä kertoo, miten tietoa saa käsitellä.

2.3.7 Toiminnan suunnittelu ja hallintajärjestelmät

Luokittelua voidaan hyödyntää organisaation toiminnan suunnittelussa, esimerkiksi arkistonmuodostussuunnitelman rakentamisessa (VAHTI 2010, 51) sekä liiketoimintaan liittyvien jatkuvuus- ja toipumissuunnitelmien toteutuksessa (Greene 2006, 139; Tudor 2001, 46). Peltier ja Tompkins (2014, 298) toteavat, että varautumissuunnitelmien ja tietojen luokittelun yhdistäminen on kasvattanut usean eri organisaation johdon ymmärrystä tietojen luokittelun roolista ja tärkeydestä.

Liiketoiminnan kannalta tärkeitä tietoaineistoja sisältävät tietojärjestelmät tulee saada käyttöön mahdollisimman nopeasti. Luokittelu auttaa määrittämään tärkeimmät järjestelmät.

Laaksosen ym. (2006, 156) mukaan luottamuksellisuuden näkökulmasta tärkeän järjestelmän ei kuitenkaan tarvitse olla toipumisjärjestyksessä ensimmäisenä. Saatavuuden kannalta kriittisimmän järjestelmän palauttaminen on olennaisempaa.

Luokittelusta on olennaista hyötyä, jos organisaatiossa halutaan rakentaa kunnollinen tietoturvallisuuden hallintajärjestelmä (Calder & Watkins 2012, 118; Grimaila & Fortson 2007, 211–212). Vaikka luokittelu on vain yksi elementti organisaation tietojen hallinnassa, on tietojen ja niiden tärkeyden tunnistaminen avain onnistuneeseen tietoturvaan koko organisaatiossa (Peltier & Tompkins 2014, 298).

Luokittelun toteuttaminen voi olla myös vaatimuksena tietoturvaan liittyvissä sertifiointiprosesseissa (Peltier & Tompkins 2014, 298). Jos organisaatio haluaa noudattaa esimerkiksi kansainvälisesti tunnustettua ISO27001-tietoturvastandardia, on luokittelu oltava käytössä (SFS-ISO/IEC 2013a). Luokittelu auttaa myös tiedon hallintapolitiikkojen luomisessa (Smallwood 2012, 188), auditointien toteuttamisessa (Fowler 2003, 4), tietojen asianmukaisen käytön valvomisessa (Peltier & Tompkins 2014, 300) ja tietoturvapoikkeamien selvittämisessä (Grimaila & Fortson 2007, 212).

2.3.8 Organisaatioiden välinen yhteistyö ja ulkoistaminen

Luokittelun pitäisi helpottaa (Andreasson ym. 2015, 100) ja yksinkertaistaa (Calder & Watkins 2012, 118) tietojen vaihtoa eri organisaatioiden välillä. Luokittelu kuvaa tietoaineistojen tärkeyttä yhteistyökumppaneille samalla tavalla, kuin organisaation omille työntekijöillekin (Greene 2006, 129).

Luokittelu auttaa huolehtimaan tietoturvasta, kun toimintoja ollaan ulkoistamassa. Siepmannin (2014, 131) mukaan luokittelu on kriittinen asia, joka tulee huomioida hyvissä ajoin. Toinen osapuoli ei voi tietää, mitkä organisaation tiedoista ovat tärkeitä ilman asianmukaista luokittelua. Organisaatio voi kuitenkin velvoittaa, esimerkiksi sopimuksin, toista osapuolta toimimaan määritettyjen periaatteiden mukaisesti.

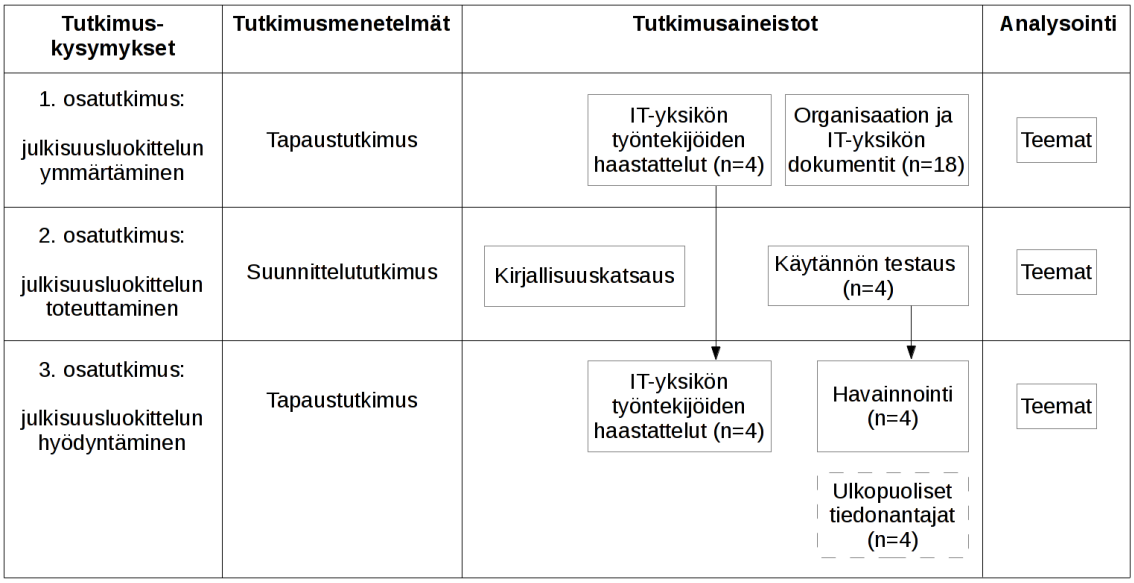
Luokittelusta, ja sen mukaan toimimisesta, on vastaavasti hyötyä myös tilanteessa, jossa organisaatio käsittelee jonkin toisen osapuolen tietoaineistoja. Luokittelutoiminta auttaa pienentämään sitä riskiä, että organisaatiosta vuotaisi toisen osapuolen tietoja maailmalle (Calder & Watkins 2012, 118). Pienentynyt riski puolestaan parantaa organisaation mainetta ja luottamusta sekä mahdollistaa uusien yhteistyökumppanien hankkimisen (Pavlov & Karakaneva 2011, 25).

Kokonaisten IT-palveluiden tuottaminen voidaan myös sitoa tietojen luokitteluun. Esimerkiksi tietojärjestelmiin liittyvät palvelutasotasosopimukset (Andreasson ym. 2015, 98) sekä varajärjestelyt (Laaksonen ym. 2006, 156–157) voidaan sopia tietojen luokituksesta johdettujen vaatimusten perusteella.

3 Opinnäytetyön tutkimusmetodologia

Opinnäytetyön tarkoituksena on tuottaa yleistietoa, ymmärrystä ja osaamista tietojen julkisuusluokittelusta kohdeorganisaation IT-yksikölle. Opinnäytetyö muodostuu kolmesta erillisestä osatutkimuksesta, joiden tutkimusmetodologiaa on esitelty kuviossa 2. Osatutkimukset toteutettiin kvalitatiivisina, laadullisina tutkimuksina.

Laadullinen tutkimus on prosessi, jossa tutkimusaihe, käytetyt tutkimusmenetelmät sekä aineiston analysointi yhdistyvät tiiviisti toisiinsa. Tutkittavaa aihetta lähestytään tutkimuskysymysten määrittelyllä. Kysymyksiin pyritään löytämään vastauksia keräämällä tutkimusaineistoa eri menetelmiä hyödyntäen. (Denzin & Lincoln 2011, 11.) Aineisto voi muodostua esimerkiksi tutkittavan ilmiön toimintaympäristöstä kerätystä haastattelu- tai havainnointimateriaalista sekä dokumenteista (Miles, Huberman & Saldaña 2014, 10–11). Lopulta aineisto analysoidaan ja siitä tehdään johtopäätöksiä. Tulokset dokumentoidaan muiden hyödynnettäväksi. (Denzin & Lincoln 2011, 11.)



Kuvio 2: Kuvaus opinnäytetyön kokonaisuudesta

Kuviossa 2 on esitetty tiiviisti opinnäytetyön eteneminen, tutkimusaiheet, käytetyt tutkimusmenetelmät sekä tutkimusaineistot. Kuvion eri osia on avattu tarkemmin seuraavissa alaluvuissa. Liitteessä 1 on kuvattu tutkimuksen attribuutit, muuttujat. Attribuuteilla pyritään tiiviisti kuvaamaan tutkimusmetodologian tieteellistä luotettavuutta (Dubé & Paré 2003).

3.1 Osatutkimusten rajaus, tutkimuskysymykset ja tavoitteet

Osatutkimuksia rajattiin seuraavasti. Kaikissa osatutkimuksissa tutkittavaksi ilmiöksi ja kohteeksi, analysointiyksiköksi, valittiin julkisuusluokittelu. Osatutkimusten toteutushetkellä julkisuusluokittelu ilmenee IT-yksikön päivittäisessä toiminnassa vähäisessä määrin. Julkisuusluokittelusta on mainintoja organisaation dokumenteissa, käsite tunnetaan yleisellä tasolla ja satunnaisia dokumentteja on myös luokiteltu. Toimintaympäristöksi rajattiin organisaation noin 30 henkinen IT-yksikkö ja sen käytössä oleviin tietojärjestelmiin tallennetut sähköiset dokumentit. Ensimmäinen osatutkimus sai alkunsa keväällä 2015. Jälkimmäiset osatutkimukset toteutettiin, osittain yhtä aikaa, keväällä 2016.

Jokaisella osatutkimuksella oli oma tutkimuskysymyksensä, joka oli johdettu osatutkimuksen tarkoituksesta, rajauksista ja tutkittavasta kohteesta. Ensimmäisen osatutkimuksen tutkimuskysymykseksi muodostui ”miten sähköisten dokumenttien julkisuusluokittelua voidaan ymmärtää organisaation IT-yksikössä?”. Lisäksi tavoitteena on selvittää julkisuusluokittelun nykytilaa ja kehittämiskohteita IT-yksikön näkökulmasta.

Toisen osatutkimuksen tarkoituksena oli selvittää, miten organisaation IT-yksikössä voitaisiin suunnitelmallisesti ja hallitusti aloittaa tietojen julkisuusluokittelu. Tutkimuskysymykseksi muodostui ”miten sähköisten dokumenttien julkisuusluokittelua voidaan toteuttaa organisaation IT-yksikössä?”. Tavoitteena oli suunnitella ja toteuttaa alan asiantuntijoiden suosituksiin perustuva ohjeistus, jonka toimivuus on käytännössä testattu. Näin ohjeistus sisältäisi ainakin ne asiat, joita alan asiantuntijat suosittelevat huomioimaan julkisuusluokittelua toteuttaessa.

Toisen osatutkimuksen tutkimuskysymystä on mahdollista tulkita kahdesta eri näkökulmasta. Toteuttaminen ensimmäistä kertaa, toisin sanoen julkisuusluokittelun aloittaminen. Tai toteuttaminen, kun julkisuusluokitteluun liittyvät toimintamallit ovat jo käytössä. Tässä osatutkimuksessa toteutuksella tarkoitetaan julkisuusluokitteluun liittyvän toiminnan aloittamista.

Kolmannen osatutkimuksen tarkoituksena oli hahmottaa julkisuusluokiteltujen tietojen hyödyntämiskohteita. Tutkimuskysymykseksi muodostui ”miten sähköisten dokumenttien julkisuusluokittelua voidaan hyödyntää organisaation IT-yksikössä?”. Tavoitteena on löytää useita IT-yksikön arjen kannalta olennaisia hyödyntämiskohteita.

Kolmas osatutkimus toteutettiin osittain yhtä aikaa toisen osatutkimuksen kanssa. Koska luokittelutoiminta on vasta alkuvaiheessa, ei käytännössä todennettuja hyödyntämiskohteita ole vielä laajamittaisesti mahdollista tunnistaa. Tästä johtuen kolmatta osatutkimusta lähestytään teoreettisemmin ja osatutkimuksessa etsitään potentiaalisia hyödyntämiskohteita.

3.2 Tutkimusmenetelmät ja osatutkimusten etenemisen kuvaus

Tutkimusmenetelmien valinta tehtiin tutkittavana olleen ilmiön, sen ajankohtaisuuden sekä osatutkimusten tutkimuskysymysten, tarkoitusten ja tavoitteiden perusteella. Ensimmäisen ja kolmannen osatutkimuksen tutkimusmenetelmäksi valittiin tapaustutkimus. Toinen osatutkimus toteutettiin suunnittelututkimuksena.

Tapaustutkimus sopii tutkimuksiin, joissa tutkitaan ajankohtaista ilmiötä sen omassa toimintaympäristössä ja tutkijalla on vähän, tai ei ollenkaan, kontrollia tutkittavaan ilmiöön (Benbasat, Goldstein & Mead 1987, 370–371; Runeson & Höst 2009, 134; Yin 2014, 2). Tapaustutkimus menetelmänä todetaan hyväksi myös silloin, kun halutaan tutkia jotain ilmiötä laajasti ja syvällisesti (Dubé & Paré 2003, 598; Patton 2002, 447; Yin 2014, 4). Pattonin (2002, 447) mukaan tapaustutkimusta voidaan pitää myös analysointiprosessina, joka määrittelee, miten tutkimusaineisto kerätään, organisoidaan ja analysoidaan tutkittavan ilmiön kuvaamiseksi.

Toisen osatutkimuksen tutkimusongelman ratkaisuksi hahmoteltiin yksityiskohtaista ohjeistusta julkisuusluokittelun aloittamiseksi. Ohjeistusta voidaan pitää myös menetelmänä, eli metodina, ja metodit puolestaan kertovat kuinka ongelmat ratkaistaan (Hevner, March, Park & Ram 2004, 79). Marchin ja Smithin (1995, 255–258) mukaan metodit ovat yksi lopputulos, joita suunnittelututkimus (eng. Design Science Research) tuottaa. Käsitettä metodi käytetään myös silloin, kun kuvataan, miten jokin tutkimus on tehty. Tässä opinnäytetyössä metodilla tarkoitetaan suunnittelututkimuksen lopputulosta.

Toisessa osatutkimuksessa päätettiin soveltaa suunnittelututkimuksen tutkimusmenetelmiä. Suunnittelututkimuksen tarkoituksena on suunnitella, toteuttaa, arvioida ja kehittää artefakteja (eng. artifact). Ne ovat keinotekoisia ihmisen tuottamia ilmiöitä (Simon 1996), jotka ratkaisevat tosielämän ongelmia niiden todellisessa toimintaympäristössä. (Hevner & Chatterjee 2010, 2; Hevner ym. 2004, 76; Simon 1996.) Suunnittelututkimus hyödyntää insinööritieteistä tuttua ideaa, jossa jokin asia todetaan toimivaksi rakentamalla se oikeasti (Nunamaker & Briggs 2011, 4).

3.2.1 Ensimmäinen ja kolmas osatutkimus

Tapaustutkimus päätettiin toteuttaa soveltamalla Yinin (2002, 2014) suosittelemaa lineaarista, mutta iteratiivista toteutusmallia hyödyntäen. Mallin sijasta voidaan puhua myös tutkimusstrategiasta (Eisenhardt 1989, 534; Runeson & Höst 2009, 138). Tutkimusstrategian toteuttamisen olennaisia vaiheita ovat tutkimusmallin valinta, tutkimuksen suunnittelu, tutkimusaineiston keräys ja analysointi sekä tulosten raportointi (Runeson & Höst 2009; Yin 2014).

Tapaustutkimus voidaan tehdä neljällä erilaisella tutkimusmallilla, riippuen siitä, millaista ilmiötä tutkitaan ja missä ympäristössä. Molempien osatutkimusten kohteena oli vain yksi ilmiö yhdessä organisaatiossa, joten ilmiötä tutkittiin kokonaisuutena. (Yin 2014, 50–51.)

Osatutkimusten kulku ja tutkimusaineiston keräyssuunnitelma kirjattiin erilliseen tutkimussuunnitelmaan. Suunnitelma tuo selkeämmän kokonaiskuvan tutkimuksesta, sen tarkoituksesta ja tutkimuksen kulusta (Dubé & Paré 2003 615–616; Runeson & Höst 2009, 141; Yin 2002, 67–69).

Tutkimusaineiston keräys ja analysointi on kuvattu myöhemmin tässä luvussa. Tulosten raportointi toteutetaan tällä opinnäytetyöllä.

3.2.2 Toinen osatutkimus

Toisen osatutkimuksen tutkimusmenetelmänä sovellettiin Peffersin, Tuunasen, Rothenbergerin ja Chatterjeen (2008) esittelemää DSRM-mallia (Design Science Research Methodology). Malli on kehitetty nimenomaan suunnittelututkimuksen tekemistä varten, rakennettu aikaisemmin julkaistujen sekä hyväksi havaittujen mallien (Peffers ym. 2008, 51–52) pohjalta ja käytännössä testattu toimivaksi (Gregor & Hevner 2013, 342), joten malli on tutkimusongelman ratkaisuun sopiva tutkimusmenetelmä.

DSRM-malli jakautuu kuuteen eri aktiviteettiin: 1) tutkimusongelman ja sen ratkaisun tärkeyden tunnistaminen, 2) tavoitteiden määrittely, 3) suunnittelu ja kehitys, 4) toteutuksen testaaminen käytännössä, 5) arviointi ja 6) tutkimustulosten viestintä (Peffers ym. 2008, 52–56). DSRM-mallia sovellettiin toisessa osatutkimuksessa seuraavasti.

Ensimmäisessä osatutkimuksessa oli havaittu, että tietojen luokittelumallia ei ole viety systemaattisesti IT-yksikön työntekijöiden tietouteen. Tästä johdettiin tutkimusongelma, jota lähdettiin ratkaisemaan toisessa osatutkimuksessa. Tavoitteena oli löytää ratkaisu, joka tukisi luokittelun systemaattista toteuttamista.

Tutkimusongelman ratkaisemiseksi kehitettiin menetelmä, artefakti, jota seuraamalla organisaatio voisi aloittaa tietojen julkisuusluokittelun. Artefaktin toteuttaminen vaatii kattavaa teoriatietoa (Peffers ym. 2008, 55) sekä luovuutta (Hevner & Chatterjee 2010, 31; Hevner ym. 2004, 81; Vaishnavi & Kuechler 2008, 21). Menetelmä rakennettiin alan kirjallisuudessa esitettyjen mallien pohjalta, jotta ratkaisu tukisi paremmin tehtävän tavoitteita.

Vaishnavin ja Kuechlerin (2008, 21) mukaan suunnittelututkimus katsotaan loppuneen onnistuneesti vasta, kun saadaan tarpeeksi hyvä ja toimiva ratkaisu aikaiseksi. Ratkaisun toiminnan varmistamiseksi menetelmää testattiin käytännössä organisaation IT-yksikössä.

Arviointivaiheessa selvitettiin, miten hyvin artefakti suoriutuu ongelman ratkaisemisesta (mukaillen Nunamaker, Chen & Purdin 1991, 100; Peffers ym. 2008, 56). Iteratiivinen testiprosessi mahdollistaa artefaktin jatkokehittämisen kehitystyön aikana (Hevner ym. 2004, 88–89).

Viimeisen vaiheen tarkoituksena on viestittää tutkimusprosessi ja sen lopputulokset sellaisessa laajuudessa, että muutkin voivat hyödyntää kerättyä tietoa (Peffers ym. 2008, 56). Tämä opinnäytetyö edustaa osatutkimuksesta tehtyä dokumentaatiota.

3.3 Tutkimusaineiston kerääminen

Aineistoa kerättiin eri menetelmillä, useista lähteistä, aina tutkimuskysymys huomioiden. Useamman tietolähteen ja menetelmän hyödyntämistä kutsutaan triangulaatioksi. Sen tarkoituksena on mahdollistaa monipuolinen aineiston keräys, aineiston keskinäinen vertailu sekä aineistosta johdettujen tulosten varmistaminen eri lähteistä. Usean tietolähteen käyttö parantaa myös tutkimustulosten uskottavuutta (Dubé & Paré 2003 615; Patton 1999, 1195; Yin 2002, 85). Triangulaatiota, pidetään olennaisena osana esimerkiksi tapaustutkimuksen toteuttamista (Yin 2002, 97–101).

Tutkimusaineistoa pyrittiin keräämään ja analysoimaan iteratiivisesti. Kyseinen etenemismalli mahdollistaa uusien näkökulmien ja löydösten huomioimisen tutkimusaineistoa kerättäessä (Eisenhardt 1989, 538–539; Miles ym. 2014, 70; Runeson & Höst 2009, 151).

Ensimmäisessä osatutkimuksessa tutkimusaineistoa kerättiin haastatteluiden avulla sekä organisaation ja IT-yksikön tietoaineistoja tutkimalla. Keräys toteutettiin julkisuusluokittelun kokonaisuuteen liittyvien teemojen perusteella. Keräyksessä etsittiin aineistoa, jossa käsitellään julkisuusluokittelun tarvetta, tiedon omistajuutta, luokitteluperiaatteita, tiedon merkintää ja käsittelyä sekä työntekijöiden ohjeistamista.

Toisessa osatutkimuksessa kehitetty menetelmä rakennettiin laajemman kirjallisuuskatsauksen ja käytännön testien avulla. Käytännön testin tulosten avulla lopullista menetelmää kehitettiin edelleen.

Kuten kuviosta 2 huomaa, kolmannessa osatutkimuksessa hyödynnettiin aikaisemmin kerättyjä haastattelumateriaaleja, toisen osatutkimuksen käytännön testauksesta saatuja havaintoja ja ulkopuolisten asiantuntijoiden tietoja. Haastattelukysymyksissä oli huomioitu myös julkisuusluokittelun hyödyntäminen, joten kolmatta osatutkimusta varten ei toteutettu erillisiä haastatteluita.

Ulkopuolisilta asiantuntijoilta saadut tiedot eivät sellaisenaan auta tutkimuskysymykseen vastaamisessa, koska kyselyn kohteena oli IT-yksikön ulkopuolisia tahoja. Aineisto kuitenkin kerättiin, jotta osatutkimuksen tulosten pohdinta olisi monipuolisempaa. Tästä johtuen ulkopuoliset tiedonantajat on merkitty kuviossa 2 katkoviivalla.

3.3.1 Organisaation ja IT-yksikön dokumentit

Julkisuusluokitteluun liittyviä tietoja etsittiin organisaation ja IT-yksikön dokumentoiduista toimintaperiaatteista ja -ohjeista. Organisaation yleiset toimintaohjeet ohjaavat koko organisaatiota, myös IT-yksikköä. IT-yksikön omat ohjeet taas tarkentavat toimintaa yksikön osalta. Periaatepäätökset puolestaan kertovat, millaista toimintaa organisaatio ja IT-yksikkö odottavat itseltään ja millaista toimintaa kohti ollaan etenemässä.

Organisaatiotasoista tietoa haettiin intranetin rakenteita tutkimalla sekä intranetin hakutoimintoa käyttäen. IT-yksikön osalta tietoa etsittiin IT-yksikön digitaalisesta työtilasta sekä verkkolevyiltä. Työtilassa ja verkkolevyillä on satoja dokumentteja. Kaikkia ei tutkittu, vaan keskityttiin mahdollisesti luokittelutietoa sisältäviin dokumentteihin. Osatutkimuksen kannalta olennaisiksi tutkittaviksi dokumenteiksi valittiin organisaation periaatepäätökset (n=4) sekä tietoturvadokumentaatio ja -ohjeet (n=14).

3.3.2 IT-yksikön henkilöhaastattelut

Haastatteluihin osallistui neljä eri tahon edustajaa IT-yksiköstä. Eri haastateltavien vastaukset on eroteltu tässä dokumentissa seuraavilla merkinnöillä: H1, H2, H3, H4. Haastateltavien kanssa sovittiin, että yksityisyyden suojaamiseksi heidän nimiään, titteleitään tai työtehtäviään ei kerrota.

Haastatteluiden avulla voidaan selvittää haastateltavan kokemuksia ja käsityksiä tutkittavasta asiasta (Peräkylä & Ruusuvuori 2011, 529; Tong, Sainsbury & Craig 2007, 351). Haastattelut olivat yksilöhaastatteluita, mutta haastattelukysymykset (liite 2) muotoiltiin siten, että ne kartoittivat aihetta koko IT-yksikön näkökulmasta. Haastattelukysymyksiin sai vastata vapaasti ja niin laajasti kuin halusi. Kysymykset olivat luonteeltaan puoli-strukturoituja. Toisin sanoen kysymykset ja niiden järjestys on ennalta määritelty, mutta haastattelun kuluessa järjestys saattaa muuttua haastateltavien vastausten perusteella (Eriksson & Kovalainen 2008, 82).

Haastatteluaineisto voi muodostua muistiinpanoista, ääni- ja videotallenteista (Eriksson & Kovalainen 2008, 85). Haastateltavat kokivat haastatteluiden nauhoittamisen epämiellyttävänä, joten vastaukset dokumentoitiin kirjallisesti haastattelun aikana. Kirjallisen aineiston käyttäminen vaikuttaa aineiston analysointitapaan ja -mahdollisuuksiin, mutta aineisto voi silti olla täysin riittävä tutkimuskysymykseen vastaamiseksi (Huttunen 2010, 41).

3.3.3 Kirjallisuuskatsaus

Tiedon hakuprosessi aloitettiin käsitteiden selvittämisellä. Julkisuusluokitteluun ja turvallisuusluokitteluun liittyviä käsitteitä etsittiin kolmen eri valtion (Cabinet Office 2014; NIST 2008; VAHTI 2010) ja Euroopan Unionin (Council of the European union 2013) tietojen luokitteluohjeista sekä kansanvälisesti tunnustetuista tietoturvastandardeista ISO27001 ja ISO27002 (SFS-ISO/IEC 2013a, 2013b).

Tiedon haku aloitettiin tietoturva-alan ammattilaisten tuottamasta kirjallisuudesta. Aiheeseen liittyvää kirjallisuutta etsittiin kirjastoista ja eBrary-palvelusta (ProQuest Ebrary). Verkkopalvelussa hakusanoina käytettiin aikaisemmin muodostettua käsitteistöä. Fyysisistä kirjoista tutkittiin sisällysluetteloita ja niistä etsittiin julkisuusluokitteluun liittyviä kokonaisuuksia.

Kirjojen valinnan perusteena käytettiin sitä, että niissä käsiteltiin julkisuusluokittelumallin rakentamista, ei pelkästään sen hyödyntämistä. Selkeästi muihin tietoturvallisuuden aiheisiin liittyvät kirjat rajattiin suoraan pois. Näitä olivat esimerkiksi kryptologian kirjallisuus.

Seuraavaksi lisätietoa etsittiin tietoturva-alan julkaisuista. Tarkasteluun valitut julkaisut ovat listattuna taulukossa 1. Julkaisut valittiin tarkasteluun, koska niitä pidetään alan olennaisimpina julkaisuina, ne ovat olleet olemassa jo kauan ja ne ovat laadullisesti todettu hyviksi (Dlamini, Eloff & Eloff 2009, 193–194; Julkaisufoorumi 2015; Microsoft 2015; Silic & Back 2014; Stamp 2015).

Julkaisu	**Lyhenne**	**Tarkastelu-vuodet**	**Artikkeleita, n=**
Information Management & Computer Security	IMCS	1995–2014	100
Information and Computer Security	ICS	2015	5
IEEE Security and Privacy	-	2003–2015	79
Journal of Computer Security	JCS	1996–2015	95
Transactions on Information and System Security	TISSEC	1998–2015	67
Computers and Security	-	1995–2015	160

Taulukko 1: Tutkitut tietoturva-alan julkaisut

Taulukossa 1 mainittujen tieteellisten julkaisujen jokainen artikkeli käytiin otsikkotasolla läpi manuaalisesti. Mikäli artikkelin otsikko viittasi aihealueeseen, kyseinen artikkeli tutkittiin tarkemmin.

Kirjallisuuskatsauksen kolmannessa vaiheessa tietoa haettiin kahdesta artikkelitietokannasta (EBSCOhost; ProQuest). Tavoitteena oli löytää aiheeseen liittyviä, vertaisarvioituja artikkeleita, joita ei löydetty taulukossa 1 listattuja julkaisuja tutkimalla.

Viimeisessä vaiheessa tutkittiin löydettyjen artikkeleiden lähdeluetteloita. Tämän menetelmän avulla löydettiin vielä muutamia yksittäisiä artikkeleita tutkittavaksi.

Toissijaisina lähteinä käytettiin SANS-Instituutin (SANS) julkaisuja. SANS järjestää tietoturvallisuuteen liittyvää koulutusta ja tutkimusta. He julkaisevat tietokannoissaan koulutuksiin ja sertifiointikokeisiin osallistuneiden opiskelijoiden lopputöitä ja tutkimusartikkeleita. Lähteitä pidettiin toissijaisina, koska niiden laatua ja arviointiprosessia ei täysin voi varmistaa.

Menetelmän runko rakennettiin lopulta seuraavia lähteitä hyödyntäen: (Boyer 2003; Calder 2005; Fowler 2003; Furness 2005; Peltier & Tompkins 2014; Raman ym. 2014; Smallwood 2012; Whitman & Mattord 2014).

3.3.4 Käytännön testaus ja havainnointi

Toisen osatutkimuksen aikana tunnistettiin ja käsiteltiin IT-yksikön dokumentteja yhdessä IT-yksikön työntekijöiden kanssa. Työntekijät kertoivat ja näyttivät, missä he säilyttävät palveluidensa dokumentaatiota ja miten he niitä käsittelevät. Lisäksi aiheesta keskusteltiin vapaasti tilanteen aikana.

Tutkimusmenetelmällisestä näkökulmasta kyseessä oli osallistuva, ei-strukturoitu havainnointitilanne. Se tarkoittaa, että tutkija osallistuu osittain havainnoitavaan tapahtumaan (Ronkainen, Pehkonen, Lindblom-Ylänne & Paavilainen 2013, 115), mutta tapahtumaa varten ei ole määritetty erillisiä havainnointikohteita (Eriksson & Kovalainen 2008, 86).

Testaustilanteiden (n=4) havainnoinnista ja keskusteluista saadut tiedot yhdistettiin omaan ymmärrykseeni toimintaympäristöstä. Kokonaisuus dokumentoitiin kirjallisesti muistiinpanoiksi. Aineistoa hyödynnettiin toisessa ja kolmannessa osatutkimuksessa.

3.3.5 Ulkopuoliset asiantuntijat

Ulkopuolisilta asiantuntijoilta kerättiin aiheeseen liittyvää lisätietoa kevyellä sähköpostikyselyllä. Asiantuntijoilta kysyttiin kaksi vaihtoehtoista kysymystä: A) mitä hyötyä organisaatiossa on tietojen luokittelusta saatu, tai B) mitä hyötyä he uskovat saavansa, jos luokittelisivat tietonsa.

Kysymykset lähetettiin 27:n eri organisaation tietoturva-asiantuntijoille. Todellinen vastaanottajien määrä oli tuntematon, koska sähköposti saattoi mennä usealle vastaanottajalle samassa organisaatiossa. Vastauksia saatiin neljältä asiantuntijalta, jotka työskentelevät kolmessa eri organisaatiossa. Kaikilla vastanneilla organisaatioilla oli tietojen luokitteluun liittyvä toimintamalleja käytössä.

Vastaukset muodostuivat sähköpostiviesteistä sekä erillisestä luokitteluun liittyvästä tietoaineistosta. Aineisto sisälsi esimerkiksi luokitteluohjeita ja yleisiä kuvauksia luokittelusta kyseisessä organisaatiossa.

3.4 Tutkimusaineiston analysointi

Laadullisen tutkimusaineiston analysointi on prosessi, jossa aineisto jaetaan pienempiin kokonaisuuksiin siten, että aineistoa voidaan helpommin käsitellä ja tulkita tutkimuskysymyksen näkökulmasta (Ellingson 2011, 595). Milesin ym. (2014, 12) mukaan analysointiprosessi muodostuu kolmesta iteratiivisesta aktiviteetista, aineiston tiivistämisestä (eng. condensation), kuvaamisesta (eng. display) sekä johtopäätösten tekemisestä ja varmistamisesta (eng. conclusion drawing/verification).

Tiivistämisvaiheessa tutkimusaineistoa yksinkertaistetaan ja lajitellaan esimerkiksi koodauksen ja kategorisoinnin avulla (Miles ym. 2014, 12; Patton 2002, 463). Koodauksessa tietoaineistosta tunnistetaan yhteneväisyyksiä, jotka merkitään yhteisillä koodeilla. Kokoamalla samalla tavalla koodattuja kokonaisuuksia yhteen, voidaan tietoaineistosta muodostaa ja hahmottaa laajempia kategorioita tai teemoja. (Miles & Huberman 1994, 69; Miles ym. 2014, 86–87; Patton 2002, 463.) Miles ym. (2014, 72) mukaan koodaus vaatii aineistoon tutustumista syvällisesti, joten koodaus itsessään on jo aineiston analysointia.

Aikaisemmin Miles ja Huberman (1994, 10) käyttivät tiivistämiseen sijaan käsitettä pelkistäminen (eng. reduction). Tästä kuitenkin luovuttiin, koska se antaa väärän kuvan koodauksesta ja analysoinnista. Tarkoituksena ei ole karsia tutkimusaineistoa, vaan vahvistaa sitä tiivistämällä, kuitenkin alkuperäinen informaatioarvo säilyttäen. (Miles ym. 2014 12.)

Kuvaamisvaiheessa aineisto organisoidaan erilliseen näkymään. Aineisto voidaan kuvata esimerkiksi tekstinä, taulukkona tai käsitekarttana. Tarkoituksena on esittää yhdessä näkymässä mahdollisimman paljon informaatiota, joka mahdollistaa johtopäätösten tekemisen. Näkymien suunnittelu ja toteuttaminen ovat olennaisia analysointitoimenpiteitä, koska ne vaativat aineiston syvällistä tuntemista. (Miles ym. 2014, 12–13.)

Aineiston tiivistäminen ja kuvaaminen luovat pohjan aineiston tulkinnalle (Patton 2002, 465). Tutkija tulkitsee aineistoa ja yrittää ymmärtää, oma taustansa huomioiden, mitä aineisto kertoo tutkittavasta ilmiöstä (Patton 2002, 477–478). Lopulta tutkija muodostaa johtopäätöksiä, jotka hän pyrkii varmistamaan esimerkiksi peilaamalla päätelmiä tutkimusaineistoa vasten (Miles ym. 2014, 13–14). Pattonin (2002, 433) mukaan jokainen laadullinen tutkimus on uniikki, joten myös analyyttiset valinnat ovat uniikkeja. Ei ole olemassa yksiselitteistä etenemismallia, joka sopisi kaikkiin tilanteisiin (Ellingson 2011, 601).

Osatutkimusten analysointivaiheet toteutettiin soveltamalla Milesin ym. (2014, 12) analysointiprosessia. Jokaisessa osatutkimuksessa teoreettisesta viitekehyksestä valitut lähdeaineistot analysoitiin yksitellen tutkimuskysymyksen näkökulmasta. Kirjallisuudesta etsittiin julkisuusluokittelun ymmärtämiseen, toteuttamiseen ja hyödyntämiseen liittyviä tietoja. Tällainen ongelmalähtöinen tiedon keruu ja analyysi perustuu ajatukselle, että tutkija uskoo löytävänsä vastauksen tutkimusongelmaansa, systemaattisesti analysoimalla mahdollisesti ratkaisuja tarjoavaa kirjallisuutta (Krippendorff 2004, 342–343).

Kirjallisuudesta kerätyt tiedot tiivistettiin ja jaoteltiin aiheittain omiksi kokonaisuuksiksi, joille annettiin kokonaisuutta kuvaava otsikko. Näin saatiin induktiivisesti muodostettua tarvittavat teemat. Toisin sanoen isosta tietomassasta pyrittiin löytämään uusia, ennalta määrittämättömiä aihekokonaisuuksia. Deduktiivisessa lähestymistavassa aineistoa käsitellään puolestaan ennalta määritettyjen teemojen pohjalta. (Miles ym. 2014, 81.) Seuraavissa alaluvuissa on kuvattu eri osatutkimusten tutkimusaineistojen analysointi sekä niissä käytetyt teemat.

3.4.1 Ensimmäinen osatutkimus

Ensimmäisen osatutkimuksen tutkimusaineistoa olivat IT-yksikön dokumentit ja kirjalliset haastatteluvastaukset. Tekstipohjaisen materiaalin ja haastattelun analysointia varten on olemassa useita erilaisia menetelmiä (Ruusuvuori, Nikander & Hyvärinen 2010; Silverman 1993). Tässä osatutkimuksessa sovellettiin vapaamuotoisempaa lähestymistapaa, koska mikään yksittäinen aineisto ei ollut tutkimuksen pääasiallinen kohde ja lähestymistavalla saatiin tuloksia aikaiseksi (soveltaen Peräkylä & Ruusuvuori 2011, 530). Olennaisempaa on tunnistaa koko aineiston analysoinnin perusteella asioita, jotka eivät suoraan sellaisenaan aineistossa ilmene (soveltaen Ruusuvuori ym. 2010, 19).

Tutkimusaineiston analysointi toteutettiin deduktiivista lähestymistapaa soveltaen. Analyysissä käytetyt teemat olivat julkisuusluokittelun tarve, tiedon omistajuus, luokitteluperiaatteet, tiedon merkintä ja käsittely sekä ohjeistaminen. Kerätty aineisto, IT-yksikön kirjalliset dokumentit ja haastatteluvastaukset, jaettiin ja tiivistettiin teemojen mukaisesti omiin teemaryhmiinsä analysointiprosessin yhteydessä.

Teemoista muodostettiin tekstimuotoisia kuvauksia, jotka on esitelty tulosluvussa. Aineistoa ja kuvausta tulkitsemalla pyrittiin muodostamaan käsitys siitä, miten IT-yksikkö ymmärtää kyseiseen teemaan liittyvän aihealueen. Johtopäätökset varmistettiin aineiston perusteella.

3.4.2 Toinen osatutkimus

Toisessa osatutkimuksessa teoreettinen viitekehys oli ensisijainen tutkimusaineisto. Ensin teoriasta muodostetuille teemoille keksittiin aihetta kuvaava otsikko. Sitten teemojen otsikoista ja lähdeaineistosta muodostettiin erillinen matriisimuotoinen taulukko. Taulukkoa hyödyntämällä pyrittiin hahmottamaan, mitä teemoja alan asiantuntijat pitävät olennaisena luokittelumallin rakentamisessa.

Laajan aineiston uskottava ja luotettava analysointi vaatii, että tieto on tiivistetty yhteen näkymään ja järjestettynä systemaattisesti niin, että se vastaa tutkimuskysymykseen. Tiedon järjestäminen matriisimuotoiseen analyysitaulukkoon on yksi tapa toteuttaa näkymä. (Miles ym. 2014, 108–109.)

Lopuksi teemojen otsikot aseteltiin loogisesti etenevään järjestykseen. Tavoitteena oli hahmottaa, missä järjestyksessä luokittelumenetelmä etenee. Teemojen otsikoista muodostettiin menetelmän eri vaiheet, jotka on kerrottu tarkemmin toisen osatutkimuksen tuloksia käsittelevässä luvussa. Johtopäätökset muodostettiin ja varmistettiin tulosten ja luokittelumenetelmän käytännön testauksesta saatujen tietojen perusteella.

3.4.3 Kolmas osatutkimus

Kolmannessa osatutkimuksessa aineiston analysointia lähestyttiin deduktiivisesti. Analysoinnissa käytettiin teoreettisesta viitekehyksestä muodostettuja teemoja. (Miles ym. 2014, 81.) Teemoja tunnistettiin yhteensä 14 kappaletta. Ne olivat tärkeiden suojattavien kohteiden tunnistaminen sekä niihin liittyvien käsittelysääntöjen ja tietoturvamekanismien toteuttaminen. Henkilöstön näkökulmasta olennaisia teemoja olivat vastuut ja velvollisuudet, perehdyttäminen sekä tietoturvatietoisuus.

Lisäksi tunnistettiin myös laajoja, osittain muiden teemojen kanssa päällekkäisiä teemoja: riskienhallinta, dokumenttien hallinta, pääsynhallinta sekä elinkaaren hallinta esimerkiksi dokumenttien ja järjestelmien osalta. Muita tunnistettuja teemoja olivat vaatimustenmukaisuus, tietojärjestelmät, ulkoistaminen sekä toiminnan suunnittelu.

Toiminnan suunnittelu ja tietojärjestelmät ovat laajoja ylätason teemoja, jotka sisältävät niihin liittyviä yksityiskohtaisempia aiheita. Toiminnan suunnittelu kattaa esimerkiksi jatkuvuus- ja toipumissuunnitelman sekä arkistonmuodostussuunnitelman toteuttamisen. Tietojärjestelmät puolestaan esimerkiksi niiden suunnittelun ja kehittämisen.

Kolmatta osatutkimusta varten haastatteluaineistoa analysoitiin kaksivaiheisesti. Ensimmäiseksi tulkittiin suoraan haastattelukysymysten vastauksia. Haastatteluvastauksista voitiin havaita, millaisia hyödyntämiskohteita IT-yksikössä on jo tunnistettu. Toiseksi toteutettiin koko haastatteluaineiston teemoittelu tutkimuskysymyksen näkökulmasta. Tällä pyrittiin selvittämään myös ne hyödyntämiskohteet, joita haastateltavat eivät itse suoraan maininneet.

Myös käytännön testausvaiheen havainto- ja keskustelumuistiinpanoja analysoitiin teemalähtöisesti. Lisäksi arvioitiin, tapahtuiko hyödyntämisteemaa vastaava tilanne käytännössä. Teemalistauksesta on apua, kun pyritään hahmottamaan havainnointitilanteessa tapahtuvia asioita (soveltaen Silverman 1993, 39).

Teemakohtaiset tekstimuotoiset kuvaukset on esitelty tulosluvussa. Aineistosta ja kuvauksista johdettuja huomioita peilattiin ulkopuolisten asiantuntijoiden haastatteluvastauksiin sekä muuhun tutkimusaineistoon.

4 Tulokset

Koko opinnäytetyön tulokset muodostuvat seuraavasti. Ensimmäisen osatutkimuksen tuloksena saatiin kokonaiskuva siitä, miten IT-yksikössä ymmärretään julkisuusluokittelun kokonaisuutta. Toisen osatutkimuksen tuloksena luotiin menetelmä, jolla julkisuusluokittelu voidaan aloittaa. Kolmannen osatutkimuksen tulokset puolestaan kertovat, miten IT-yksikkö voi potentiaalisesti hyödyntää dokumenttien julkisuusluokittelua.

Seuraavissa alaluvuissa on kuvattu eri osatutkimusten tulokset yksityiskohtaisesti. Toisen osatutkimuksen tulosten jälkeen on myös kuvattu, miten kehitettyä menetelmää testattiin käytännössä IT-yksikössä.

4.1 IT-yksikön ymmärrys sähköisten dokumenttien julkisuusluokittelusta

Ensimmäisen osatutkimuksen tuloksia tarkastellaan kuviossa 1 esitettyjen julkisuusluokittelun kokonaisuuden teemojen näkökulmasta. Ymmärrystä oli helpompi selvittää, kun tiedettiin, mitä teoreettista mallia vasten IT-yksikön ymmärrystä reflektoidaan.

Seuraavissa alaluvuissa tuloksia on kuvattu teemoittain. Luokiteltavat tiedot ja luokitteluperiaatteet käsitellään samassa alaluvussa. Luokittelun kokonaisuuden ohjeistamiseen ja koulutukseen liittyvät tulokset on puolestaan esitetty tiedon käsittelyyn liittyvien tulosten yhteydessä.

4.1.1 Dokumenttien julkisuusluokittelun tarve

Tarpeita ja perusteita julkisuusluokittelun tekemiselle tunnistettiin useista eri dokumenteista. Olennaisimmat perusteet ja niiden lähteet organisaatiossa on listattuna taulukossa 2.

Peruste tai tarve luokittelutoiminnalle	**Perusteen lähde, esim. dokumentti**
Lakien ja säädösten noudattaminen	Suomen laki ja organisaation tietoturvapolitiikka
Valtionhallinnon ohjeiden ja suositusten hyödyntäminen	Tietoturvapolitiikka
Kolmansien osapuolien tietoturvavaatimukset	Tietoturvapolitiikka
Julkisuuslain hyvä tiedonhallintatapa	Tietoturvapolitiikka
Tiedon julkisuusperiaatteen noudattaminen	Organisaation toimintaa ohjaavat periaatepäätökset
Salassa pidettävyyden huomiointi tiedon elinkaaressa	Organisaation toimintaa ohjaavat periaatepäätökset
Valtiohallinnon tietoturvallisuuden perustason saavuttaminen	IT-yksikön toimintaa ohjaavat periaatepäätökset
Tietojen luokittelu ja käsittely valtionhallinnon suojaustasojen mukaisesti	IT-yksikön toimintaa ohjaavat periaatepäätökset
Tietoturvatoimien suhteuttaminen tietoaineiston kriittisyyteen	IT-yksikön toimintaa ohjaavat periaatepäätökset
Kriittisen tiedon huomioiminen jatkuvuus- ja toipumissuunnitelmissa	IT-yksikön toimintaa ohjaavat periaatepäätökset
Järjestelmien ja laitteiden kriittisyyden johtaminen niissä olevien tietojen perusteella	IT-yksikön toimintaa ohjaavat periaatepäätökset

Taulukko 2: IT-yksikön perusteet dokumenttien luokittelulle

Taulukosta 2 voidaan havaita, että julkisuusluokittelun perusteita on käsitelty organisaation eri tasoilla. Esimerkiksi tietoturvapolitiikassa otetaan kantaa perusteisiin yleisellä tasolla. Periaatepäätökset tuovat julkisuusluokittelun puolestaan lähemmäksi IT-yksikön arkea.

Haastateltavat olivat kaikki sitä mieltä, että julkisuusluokittelulle olisi tarvetta. Organisaation tietojen suojaaminen ja oman toiminnan kehittäminen olisi helpompaa luokittelun ansiosta.

”Esimerkiksi pilvipalveluiden käytön ohjeistaminen on helpompaa, kun tiedot on luokiteltu.”, H3.

Vaikka luokittelua halutaankin tehdä, niin pientä epäuskoa oli myös havaittavissa. H1 kuvailee asian näin:

”Toisaalta, koska asiaa ei vieläkään ole saatu aikaiseksi, niin odottaako tätä tosiaan joku?”, H1.

4.1.2 Luokitteluun liittyvät omistajuus- ja vastuukysymykset

Organisaation tietoturvapolitiikan ja haastatteluiden perusteella IT-yksikön dokumenttien luokittelusta vastaa tietoaineiston omistaja. Haastateltavien mielestä tämä tarkoittaa sitä, että dokumentin luoja tekee luokitteluehdotuksen, koska hän tuntee dokumentin sisällön parhaiten. Palvelun, tai muun vastaavan kokonaisuuden, omistaja tai esimies vastaa lopullisesta luokittelusta.

Tietoturvapolitiikan mukaan myös organisaation tietoturvaryhmällä on rooli tietojen luokittelussa. Ryhmä on mukana tietoaineistojen luokittelussa ja luokitteluperiaatteiden sekä tietoturvatoimenpiteiden toteuttamisessa.

4.1.3 Luokiteltavat tiedot ja luokitteluperiaatteet

Haastatteluiden perusteella IT-yksikkö tunnistaa paljon omia dokumenttejaan, jotka kannattaisi luokitella. Ensisijaisesti tulisi julkisuusluokitella teknisiä yksityiskohtia sisältävät asiakirjat, joita ei haluta hakkereiden tai muiden haitallisten toimijoiden tietouteen.

Luokiteltaviksi dokumenteiksi lueteltiin myös henkilötietoja, sopimustietoja sekä ohjelmistojen asennusavaimia sisältävät asiakirjat. Projektisuunnitelmien luokittelua pidettiin haastavana. Dokumentin luojasta riippuen projektisuunnitelma saattaa sisältää luokiteltavaa tietoa.

Julkisuusluokkia tunnistettiin useita. Esimerkiksi kolmessa haastattelussa, tietoturvapolitiikassa, organisaation ja yksikön periaatepäätöksissä sekä ohjeissa käytettiin seuraavia termejä: julkinen, ei-julkinen, luottamuksellinen, salainen, vain sisäiseen käyttöön, tärkeä ja kriittinen tieto. Kaikissa haastatteluvastauksissa painotettiin yksinkertaisuutta, mutta vain H4 konkretisoi asian:
”Tässä organisaatiossa lähtisin vain kahdella luokalla: luottamuksellinen ja salainen. Ei ole valtionhallinnon malli, mutta toimii hyvin.”

Yksikön toimintaperiaatteista löytyi maininta, että tietojen luokittelu hoidetaan valtionhallinnon suojaustasojen mukaisesti. Muita luokitteluperiaatteisiin liittyviä mainintoja ei tunnistettu.

4.1.4 Luokitellun tiedon merkintätavat

Haastatteluissa mainittiin, että luokitteluluokan voisi merkitä esimerkiksi dokumentin nimeen, tiedoston metatietoihin tai dokumentin sisältöön. Valmiit, luokittelua tukevat dokumenttipohjat tai dokumenttien hallintajärjestelmät helpottaisivat työtä.

Dokumentit tulisi olla yksinkertaisesti ja helposti luokiteltavissa: ”Aikaisemmin näkemässäni dokumentissa piti huomioida luottamuksellisuus, käytettävyys ja eheys, julkisuusluokittelun lisäksi. Sellainen on liian raskasta täyttää.”, H1.

Osatutkimusta tehdessä organisaatiosta löytyi myös muutamia merkittyjä dokumentteja. Niitä oli kuitenkin kokonaisuuteen verrattuna vähän.

4.1.5 Luokitellun tiedon käsittely ja luokittelun ohjeistaminen

Osatutkimuksessa etsittiin materiaalia, joka sisältäisi konkreettisia toimintaohjeita dokumenttien käsittelyn tueksi. Yksikön toimintaperiaatteista löytyi viitteitä valtionhallinnon ohjeistuksiin. Lisäksi tietoturvaohjeissa mainittiin, että tarpeettomien tietojen tuhoaminen hoidetaan tiedon salaisuusasteen mukaisesti.

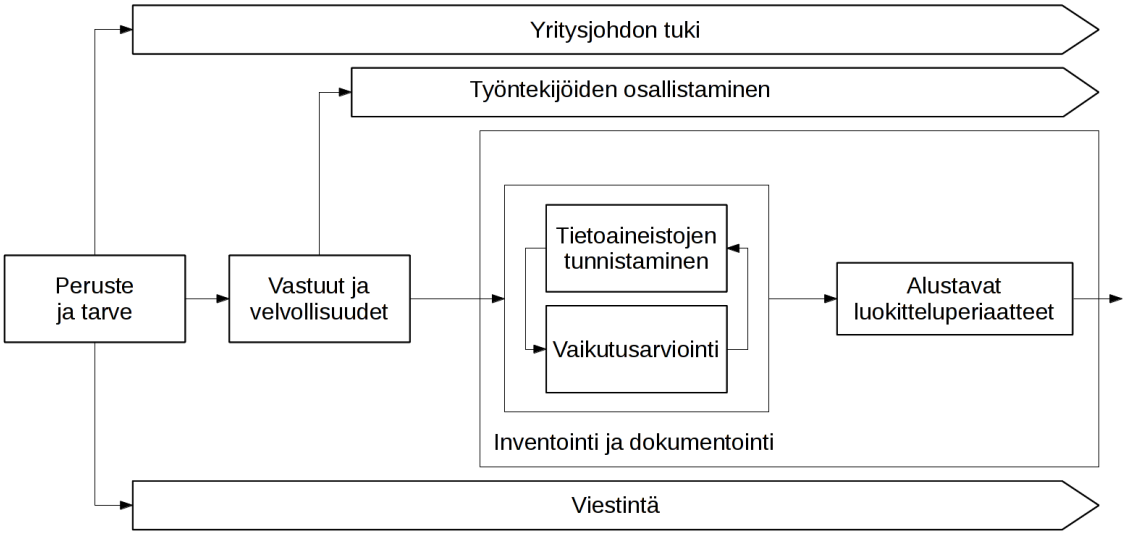
Muita tiedon käsittelyyn ja luokittelun ohjeistamiseen liittyviä aineistoja ei tunnistettu. Haastateltavien vastaukset olivat puolestaan ristiriitaisia muuhun tutkimusaineistoon verrattuna:

”Käytännössä meillä ei ole ohjeita.”, H3.

”Ohjeistus on olemassa, mutta sitä ei ole otettu käyttöön.”, H4.

4.2 Menetelmä julkisuusluokittelun aloittamiseksi

Toisen osatutkimuksen aikana kehitettiin menetelmä julkisuusluokittelun aloittamiseksi. Menetelmä koostuu yhdeksästä vaiheesta: 1) tunnista tarve, 2) osoita yritysjohdon tuki, 3) määritä vastuut ja velvollisuudet, 4) viestitä tarkoitus, tavoitteet ja hyödyt, 5) osallista työntekijät, 6) dokumentoi ja inventoi, 7) tunnista tietoaineistot, 8) toteuta vaikutusarviointi, 9) määrittele luokittelukategoriat ja luokittele tietoaineistot. Kuviossa 3 on esitetty menetelmän eri vaiheista muodostettu kokonaiskuva.



Kuvio 3: Menetelmä julkisuusluokittelun aloittamiseksi

Kuten kuviosta 3 huomataan, iteraatio on tärkeä osa menetelmän suorittamista. Kaikki vaiheet eivät myöskään pääty, vaan jatkuvat koko menetelmän suorittamisen ajan. Seuraavissa alaluvuissa on esitelty menetelmän vaiheet järjestyksessä. Järjestys on kuitenkin vain suositus. Tärkeämpää on kaikkien vaiheiden läpikäynti.

Suunnittelututkimuksessa toteutettavan, tutkimusongelman ratkaisevan lopputuloksen toteuttaminen vaatii teoriatiedon ohella jonkin verran luovuutta (Hevner & Chatterjee 2010, 31; Hevner ym. 2004, 81; Vaishnavi & Kuechler 2008, 21). Tästä johtuen menetelmän eri vaiheiden selostukset sisältävät myös omia kommenttejani ja huomioitani, jotka on kuitenkin pyritty perustelemaan teoreettisen viitekehyksen mukaisesti.

Tietojen luokittelu ei ole yksittäinen projekti vaan käyttöön jäävä toimintamalli. On kuitenkin suositeltavaa, että menetelmän käyttämiseksi perustettaisiin projekti. Näin kokonaisuuden hallinta on helpompaa ja organisoidumpaa. (Mukaillen Whitman & Mattord 2014, 15–17.)

Isommissa organisaatioissa luokitteluprojekti kannattaa rajata aluksi esimerkiksi yhteen liiketoimintayksikköön, jolloin menetelmää voidaan testata käytännössä pienemmässä viitekehyksessä. Smallwood (2012, 189) suosittelee kertomaan, miten projekti on edennyt ja osoittamaan siitä saadut hyödyt ennen kuin siirrytään luokittelemaan seuraavaa yksikköä.

Kokonaisen tietojen luokittelumallin käyttöönotto muuttaa lopulta työntekijöiden tapaa työskennellä. Tästä johtuen menetelmän käytön tueksi kannattaa harkita muutosjohtamisen työkaluja. On myös hyvä kysyä muilta samalla alalla toimivilta, miten he ovat toteuttaneet vastaavan muutosprojektin (Peltier & Tompkins 2014, 301).

4.2.1 Tunnista tarve

Menetelmä käynnistetään tarpeen tunnistamisella. Ilman tarpeen määrittelyä ei välttämättä tiedetä, mitä luokittelulla ollaan tavoittelemassa (Tudor 2001, 45).

Organisaatioilla on eri syitä luokittelun aloittamiseksi. Tietoaineistojen tietoturvallisuustason selvittäminen, kustannusten oikea kohdistaminen (Peltier & Tompkins 2014, 298), kilpailuedun tavoittelu, julkisuuskuvan parantaminen (Calder 2005, 57–58) sekä yleinen liiketoiminnan riskienhallinnasta huolehtiminen (Whitman & Mattord 2014, 283) ovat päteviä perusteluita. Vaatimustenmukaisuusvelvoitteiden hoitaminen on myös yleinen tarve luokittelun aloittamiseksi (Boyer 2003, 1-2).

4.2.2 Osoita yritysjohdon tuki

Yritysjohdon tulee osoittaa olevansa mukana tukemassa luokittelutoimintaa. Tukea voi osoittaa eri tavoin. Yksi tapa on se, että yritysjohto asettaa luokitteluprojektin. Toinen vaihtoehto on tehdä erillinen tiedon luokittelupolitiikka tai ottaa se esimerkiksi osaksi organisaation tietoturvapolitiikkaa.

Luokittelupolitiikka on hyödyllinen dokumentti, koska se sitouttaa sekä yritysjohdon että työntekijät (Calder 2005, 58; Greene 2006, 120–121). Boyer (2003, 3) kuitenkin huomauttaa, että politiikan pitää olla nimenomaan yritysjohdon toteuttama eikä esimerkiksi IT-yksikön. Muuten luokittelutoiminta voi saada liian teknisen näkökulman työntekijöiden keskuudessa.

On tärkeää, että puhutaan yritysjohdon tuen osoittamisesta eikä tuen hankkimisesta. Hyvä ja kattava tarpeen kuvaus osoittaa luokittelun tärkeyden. Yritysjohto ymmärtää sen ja osoittaa olevansa mukana. Mikäli tukea pitää erikseen hakea, niin viestintätyö voi olla jo epäonnistunut.

4.2.3 Määritä vastuut ja velvollisuudet

Evans ja Price (2014, 117) havaitsivat tutkimuksessaan, että tietoaineistoihin liittyvät vastuut ja velvollisuudet ovat usein määrittämättä yrityksissä. Jotta projekti etenisi mahdollisimman hyvin ja luokittelumenetelmä tukisi projektin jälkeistä toimintaa, vastuut ja velvollisuudet määritellään heti alussa. Tässä menetelmässä vastuut ja velvollisuudet on jaettu neljälle eri taholle: yritysjohdolle, tiedon omistajille, luokittelutiimille sekä vaihtuville asiantuntijoille.

Yritysjohto on se taho, joka omistaa kaikki yrityksen tiedot ja lopulta päättää tietojen suojaamisesta sekä niiden käsittelystä. Yritysjohto voi kuitenkin osoittaa tiedon omistajuuteen, suojaamiseen ja luokitteluun liittyviä tehtäviä erillisille tiedon omistajille, luokittelutiimille sekä muille työntekijöille.

Tiedon omistaja on se henkilö tai taho, jonka yritysjohto on valtuuttanut huolehtimaan tiedon käsittelystä ja turvallisuudesta. Omistaja voi olla esimerkiksi liiketoimintayksikön johtaja tai yksittäisestä toiminnosta vastaava esimies (Peltier & Tompkins 2014, 298). Whitmanin ja Mattordin (2014, 280) mukaan jokaisen esimiestason henkilön tulisi keskittyä riskien alentamiseen, joten on luonnollista, että he ovat tiedon omistajia. Raggad (2010, 71) puolestaan toteaa, että omistaja on se henkilö, joka tuntee tiedon liiketoiminta-arvon. Käytännössä tiedoston luoja voi myös olla omistaja, koska hän tietää luomansa dokumentin sisällön luottamuksellisuuden. Organisaatiossa on hyvä määritellä tiedon omistajuuteen liittyvät vastuut ja velvollisuudet.

Luokittelutiimi toteuttaa luokittelua yhdessä tiedon omistajien ja muiden työntekijöiden kanssa. Luokittelutiimi vastaa projektin etenemisestä, mutta tiimi ei ole yksin vastuussa luokittelusta. Tiimi voi koostua esimerkiksi ydintiimistä ja vaihtuvista asiantuntijoista. Calder (2005, 59) suosittelee, että organisaation tietoturvavastaava johtaa tiimin toimintaa. Muita olennaisia jäseniä ovat esimerkiksi lakiasiantuntija ja esimiestason henkilö (Furness 2005, 4; Boyer 2003, 11).

Asiantuntijat osallistuvat luokittelutiimin toimintaan omalta asiantuntijuusalueeltaan. Heidät valitaan tapauskohtaisesti luokittelutoiminnan kohteena olevan liiketoimintayksikön työntekijöistä. Asiantuntijat ovat tiedon omistajia ja aktiivisesti luokittelun kohteena olevien tietojen kanssa työskenteleviä henkilöitä, jotka tuntevat tiedon luottamuksellisuustarpeet.

4.2.4 Viestitä tarkoitus, tavoitteet ja hyödyt

Henkilöstölle kerrotaan aikaisessa vaiheessa, miksi luokittelutoimintaa ollaan tekemässä (Smallwood 2012, 190). Hyvin perusteltu tarvenäkökulma ja toiminnasta saatavat hyödyt ovat

olennaisia viestittäviä asioita. Paton ja McCalman (2008, 50,54) korostavat positiivisen ja kaksisuuntaisen kommunikoinnin tärkeyttä. Bruckman (2008, 214–217) puolestaan suosittelee aktiivisesti huomioimaan henkilöiden omia mielipiteitä muutokseen liittyen.

Ymmärtämällä henkilöiden syitä muutostahdolle tai -vastarinnalle, voidaan muutosta viestiä ja viedä eteenpäin tehokkaammin. Huono viestintä saattaa puolestaan johtaa epäluottamukseen koko muutosprojektia vastaan (Widmark, Tishelman, Gustafsson & Sharp 2012, 6).

4.2.5 Osallista työntekijät

Ottamalla työntekijät mukaan luokitteluprojektiin pyritään kolmen hyödyn saavuttamiseen. Ensinnäkin heillä on paras näkemys aiheesta päivittäisen työnteon kannalta. He tietävät mikä on luottamuksellista tietoa ja mikä vaatii suojausta (Smallwood 2012, 190).

Toiseksi, työntekijöiden on saatava merkittävissä määrin osallistua luokitteluprojektin toteuttamiseen, jotta he kokisivat sen omakseen (mukaillen Lakos & Phipps 2004, 358). Hamel (2000, 190) toteaakin, että iso osa muutoksesta on aktiivisten työntekijöiden ansiota, ei yritysjohdon.

Kolmas tavoiteltu hyöty on ymmärryksen lisääminen. Kun työntekijät ovat alusta asti mukana toiminnassa, he ymmärtänevät kokonaisuuden paremmin. Ymmärryksen lisäämisellä pyritään siihen, että työntekijöiden kuva luokittelutoiminnasta olisi positiivisempi ja motivaatio luokittelun tekemiseksi kasvaisi (mukaillen Svärd 2014, 13–14). Porvari (2012, 221) pitää osallistuvaa ja verkostomaista toimintaa koulutustakin tehokkaampana tapana lisätä henkilöstön tietoturvatietoisuutta ja motivaatiota tietoturvakäytäntöjen noudattamiseen.

4.2.6 Dokumentoi ja inventoi

Luokittelumenetelmän toteuttamisen aikana kerätyt tiedot dokumentoidaan ja inventoidaan. Ensin tulee kuitenkin pohtia, mitä tietoja myöhemmin tarvitaan. Tässä ehdotetussa menetelmässä kannattaa dokumentoida ainakin tiedon omistaja, vaikutusarvioinnin tulos, käsiteltävien dokumenttien sisältö lyhyesti sekä dokumentin luokittelukategoria.

Käyttötarkoituksesta riippuen myös muita tietoja voi dokumentoida. Esimerkiksi Whitman ja Mattord (2014, 87) suosittelevat dokumentoimaan tiedoston luojan, säilytyspaikan ja varmuuskopiointikäytännöt. Fowler (2003, 6) lisää edellisiin myös tiedon suojaustavat ja tiedon hyödyntäjät. Mainittuja tietoja voi hyödyntää esimerkiksi riskianalyysissä ja jatkuvuudenhallinnassa (Greene 2006, 139).

4.2.7 Tunnista tietoaineistot

Tietoaineiston tunnistamisvaiheessa tarkastellaan luokittelun kohteena olevan toiminnon, esimerkiksi IT-yksikön, tietoaineistoja. Tarkoituksena on tunnistaa ja dokumentoida suojattavien tiedostojen sijainti, tiedostojen sisältö sekä omistaja. Menetelmän seuraavan vaiheen, vaikutusarvioinnin, voi myös toteuttaa samaan aikaan tietoaineistojen tunnistamisen kanssa. Boyerin (2003, 5) mukaan tietoaineistojen tunnistaminen on yksi luokittelutoiminnan hankalimmista vaiheista, koska tietoa on monessa eri paikassa. Kaikkia tiedostoja ei tarvitse kuitenkaan tunnistaa samalla kertaa. Riittää, että luokittelutoiminnan saa käyntiin. (Calder 2005, 60.)

Tietoaineistoja voi tunnistaa eri tavoilla. Esimerkiksi Smallwood (2012, 189–190) ja Fowler (2003, 5) suosittelevat haastattelemaan työntekijöitä. He tietävät itse parhaiten, missä heidän päivittäin käyttämät tiedot sijaitsevat ja mitkä niistä vaativat suojausta. Whitmanin ja Mattordin (2014, 286) mukaan esimiehet ovat vastuussa tietojen tunnistamisesta, koska he tuntevat parhaiten oman toimintonsa kokonaisuutena. Myös IT-järjestelmiä voi hyödyntää tietoaineistojen automaattisessa tunnistamisessa. Järjestelmät kertovat esimerkiksi, missä kaikkialla tiedostoja on tallennettuna, ja kuka tiedostot on luonut.

4.2.8 Toteuta vaikutusarviointi

Vaikutusarviointivaiheessa pohditaan, mitä seurauksia siitä on, jos arvioinnin kohteena oleva tietoaineisto paljastuu ulkopuolisille tahoille. Aiheutuuko paljastumisesta haittaa esimerkiksi yrityksen asiakkaille, työntekijöille, liiketoiminnalle tai maineelle. Viimeistään tässä vaiheessa on myös oltava tiedossa, millaisia vaatimuksia laki ja muut mahdolliset vaatimustenmukaisuusvelvoitteet asettavat kyseisen tietoaineiston luottamuksellisuudelle (Greene 2006, 122,124).

Vaikutusarvioinnin toteuttamiseksi on olemassa eri tapoja. VAHTI (2010, 54,57) esimerkiksi ohjeistaa käyttämään tapaa, jossa arvioidaan, aiheutuuko tiedon paljastumisesta haittaa tai vahinkoa. Pohdinnassa voi käyttää apuna myös arvioita siitä, onko tieto tarkoitettu julkisesti jaettavaksi, organisaation sisäiseen jakeluun tai vain pienen ryhmän käyttöön.

Organisaatio voi hyödyntää myös ennalta määritettyjä dokumenttirakenteita, jolloin vaikutusarviointi helpottuu. Jos tiedosto sisältää esimerkiksi hinnoitteluun liittyviä elementtejä, niin vaikutusarvioinnin tulos merkitään automaattisesti haittaa aiheuttavaksi (mukaillen Eloff ym. 1996, 59–61).

Manuaalisessa vaikutusarvioinnissa luokittelutiimin kokoonpano ja luokittelutyöhön osallistuvien työntekijöiden kokemus ovat avainasemassa. Ryhmässä on oltava alan asiantuntijoita ja liiketoimintaa ymmärtäviä henkilöitä, jotta kokonaisuutta voitaisiin arvioida luotettavasti.

Vaikutusarvioinnin lopputuloksena on arvio tietoaineiston paljastumisesta aiheutuvista seurauksista. Tulokset dokumentoidaan myöhempää käyttöä varten.

4.2.9 Määrittele luokittelukategoriat ja luokittele tietoaineistot

Menetelmän viimeisessä vaiheessa analysoidaan vaikutusarvioinnin tulokset. Ennen tähän vaiheeseen siirtymistä on tietojen tunnistus- ja vaikutusarviointivaihetta toistettava useita kertoja. Analyysin perusteella pohditaan, montako luokittelukategoriaa organisaatiolla olisi hyvä olla (Whitman & Mattord 2014, 287).

Vaikutusarvioinnista saattaa paljastua esimerkiksi tietoaineistoja, joita saa, tai ei saa jakaa julkisesti. Ei-julkisia tietoaineistoja voi olla tarpeen erotella vielä useampaan kategoriaan vaatimustenmukaisuusvelvoitteiden perusteella. Tietoaineistot luokitellaan vaikutusarvioinnin tulosten perusteella siihen kategoriaan, joka parhaiten kuvaa tietoaineiston luottamuksellisuuden tasoa. Toimenpidettä on havainnollistettu taulukossa 3. Vaikutusarvioinnista on voinut ilmaantua esimerkiksi kolmenlaisia tuloksia, joten niitä varten luodaan kolme eri luokittelukategoriaa.

Vaikutusarvioinnin tulos	**Luokittelukategoria**
Ei haittaa	Julkinen
Haittaa	Sisäinen
Vahinkoa	Luottamuksellinen

Taulukko 3: Vaikutusarvioinnin tuloksia vastaavat luokittelukategoriat

Luokittelukategorioiden määrittelyvaiheen sijainti luokittelumenetelmässä on tulkinnanvarainen. Esimerkiksi Fowler (2003) määrittelee ensin luokittelukategoriat sekä niitä suojaavat tietoturvamekanismit ja luokittelee tiedot vasta sitten eri kategorioihin. Whitman ja Mattord (2014, 287) puolestaan toteuttavat luokittelukategoriat sen mukaan, millaisia suojaustarpeita jo tunnistetuilla tietoaineistoilla on.

Jättämällä kategorioiden määrittelyn menetelmän loppupäähän mahdollistetaan kategorioiden teko vaikutusarvioinnin tulosten perusteella. Jos kategoriat on määritetty tiukasti etukä-

teen, voi vaikutusarvioinnista paljastua tietoaineistoja, jotka eivät sovi tarpeeksi hyvin mihinkään kategoriaan. Toisaalta vaikutusarvioinnissa käytetyt arviointimenetelmät ohjaavat jo osittain kategoriamäärittelyä. Kategorioista on siis hyvä olla alustava hahmotelma, mutta se ei saa liikaa rajata vaikutusarvioinnin toteuttamista ja lopullista luokittelua.

Menetelmän lopputuloksena muodostuvat alustavat luokitteluperiaatteet. Organisaatiolla pitäisi olla nyt käytössään tietoa siitä, miten eri tyyppisiä dokumentteja jatkossa luokitellaan.

4.3 Julkisuusluokittelun aloitusmenetelmän testaus ja kehitys

Menetelmän toiminta todennettiin soveltamalla menetelmää käytännössä. Ennen laajempaa toteutusta testasin menetelmän toimivuuden teoriassa sekä omassa henkilökohtaisessa työympäristössäni. Tutustuin myös kahden muun vastaavan organisaation tietojen luokittelun dokumentaatioon.

Alkuvalmisteluiden jälkeen toteutettiin laajamittaisempi testaus. Seuraavassa alaluvussa on kuvattu testiympäristö. Sen jälkeen kuvataan menetelmän soveltaminen organisaation IT-yksikössä. Kuvaus sisältää myös soveltamisvaiheessa havaitut organisaatiokohtaiset kehittämiskohteet. Viimeinen alaluku sisältää kuvauksen menetelmän kokonaisuuden kehitysprosessista, miten menetelmä luotiin ja miten sen vaiheita muutettiin arvioinnin tuloksena.

4.3.1 Testiympäristö

Testiympäristönä toimi, rajauksen mukaisesti, organisaation IT-yksikkö. Vaikka menetelmä oli suunniteltu IT-yksikköä varten, niin koko IT-yksikön laajuista testiä ei toteutettu. On järkevämpää edetä pienistä palasista kohti kokonaisuutta (Smallwood 2012, 189). Pahimmassa tapauksessa, mahdollisesti toimimaton, testiversio menetelmästä olisi voinut luoda negatiivisen kuvan koko luokittelutoiminnasta. Tämä olisi vaikeuttanut menetelmän myöhempää laajamittaista käyttöä.

Riskien minimoimiseksi, mutta käytännön testin mahdollistamiseksi, menetelmää testattiin neljässä erillisessä pienryhmässä. Yksittäinen pienryhmä edusti tiettyä IT-yksikön sisäistä toimintoa, kuten esimerkiksi palvelinylläpitoa tai IT-tukea. Jokaisessa ryhmässä oli lisäkseni 1-3 henkilöä.

Tarkoituksena on saada mahdollisimman valmis menetelmä hyödynnettäväksi koko IT-yksikölle, joten pienemmät testiryhmät tukivat paremmin tavoitetta. Käyttämällä pienryhmiä saatiin myös toteutettua useita testikierroksia.

4.3.2 Menetelmän soveltaminen IT-yksikössä

Menetelmää testattiin pienryhmissä, joten menetelmän vaiheita sovellettiin sen mukaisesti. Kaikki menetelmän vaiheet käytiin kuitenkin läpi käytännön testissä. Osaa vaiheista toteutettiin yhtä aikaa ja vaiheita myös iteroitiin tarvittaessa.

Alkuvalmistelut
Organisaatio haluaisi hyödyntää tietojen luokittelua pilvipalveluiden käytön ohjeistamisessa sekä salassapidon huomioimisessa tiedon elinkaaren eri vaiheissa. Tarve luokittelulle oli selvä.

Osatutkimuksen tarkoitus, tavoitteet ja tarve esiteltiin Oppimisympäristöpalvelut-yksikön päällikölle. Hän koki asian tarpeelliseksi, hyödylliseksi ja toimintaa kehittäväksi. Päällikkö osoitti tukensa menetelmän käytännön testaamiselle.

Käytännön testien ajaksi vastuut ja velvollisuudet määriteltiin seuraavasti. Oppimisympäristöpalvelut-yksikön päällikkö valtuutti minut testaamaan menetelmää käytännössä. Sain osallistuttaa IT-asiantuntijoita menetelmän testaamiseen. Luokittelutiimi koostui minusta ja luokittelun kohteena olevan sisäisen toiminnon asiantuntijoista.

Sähköiset dokumentit, joita luokiteltiin, olivat toimintojen tuottamia dokumentteja. Asiantuntijat tiesivät parhaiten dokumenttien sisällöt, joten he toimivat samalla tietojen omistajina. Tunnistettavista tietoaineistosta päätettiin dokumentoida tiedoston tekijä eli omistaja ja päivämäärä, tiedoston sisältö lyhyesti, tiedoston sijainti, vaikutusarvioinnin lopputulos ja myöhemmässä vaiheessa tehtävä luokittelukategoria.

Haasteita viestinnässä
Tarkoituksen, tavoitteiden ja hyötyjen viestintää lähestyttiin henkilökohtaisten yhteydenottojen kautta. Valituille eri toimintojen asiantuntijoille esiteltiin aihe lyhyenä tietoiskuna, jonka jälkeen heille tarjottiin mahdollisuutta osallistua testiin. Mikäli asiantuntijat kiinnostuivat aiheesta, heille lähetettiin erillinen kokouskutsu.

Varsinaisessa tapaamisessa asiantuntijat saivat vielä toisen tietopaketin itse menetelmästä sekä sen testaamisesta. Ensimmäisen iteraatiokierroksen jälkeen ilmeni tarve tapaamisessa esitettävän viestintämateriaalin parantamiselle. Toiminnasta saatavia hyötyjä oli kuvattava paremmin. Materiaalia korjattiin palautteen perusteella. Toisessa ja kolmannessa iteraatiossa hyödyt pystyttiin osoittamaan konkreettisemmin IT-asiantuntijoille.

Menetelmän toteuttamisen jälkeisen lopputilanteen kuvaaminen aiheutti myös kysymyksiä. Osalle asiantuntijoista jäi epäselväksi, mitä menetelmään kuuluu ja mitä ei. Viestintämateriaalia parannettiin myös tältä osin.

Tietoaineistoja tunnistettiin yhdessä IT-asiantuntijoiden kanssa. Toimintaan osallistuneet asiantuntijat näyttivät, missä heidän käsittelemiään tietoja sijaitsee. Tämän jälkeen dokumenttien sisältöön tutustuttiin yhdessä ja dokumentille tehtiin vaikutusarviointi.

Ensimmäisellä kierroksella vaikutusarviointia tehtiin seuraavan kysymyksen pohjalta: ”jos tämä dokumentti päätyisi julkiseen levitykseen, niin aiheutuisiko siitä esimerkiksi jonkinlaista haittaa tai vahinkoa?”. Kysymyksen asettelulla pyrittiin siihen, että asiantuntija joutuisi pohtimaan voiko dokumentti olla julkinen.

Termit ”haittaa” ja ”vahinkoa” aiheuttivat keskustelua, jonka perusteella termien tarkoitusta pitäisi avata enemmän. Toisella iteraatiokierroksella termien tueksi otettiin käyttöön kuvaus ”voidaan julkaista organisaation sisällä” sekä ”tarkoitettu vain rajatulle henkilöryhmälle.” Tämä helpotti vaikutusarvioinnin tekemistä.

Menetelmän käytännön testaamisen perusteella viestintä on yksi niistä asioista, joka pitää hoitaa erittäin huolellisesti, kun luokittelumenetelmää hyödynnetään laajemmassa mittakaavassa. Toimintaan osallistuvien henkilöiden on tiedettävä asiasta jo ennen kuin heille osoitetaan aiheeseen liittyviä tehtäviä tai esimerkiksi kokouskutsuja. Lisäksi vaikutusarviointiin liittyvät termit tulee valita ja kuvata niin, että ne ymmärretään helposti.

Lopputulokset
Taulukossa 4 on havainnollistettu pieni määrä iteraatiokierrosten aikana kerättyä inventaariotietoa. Osa dokumentaatiosta, kuten tiedostojen omistajat ja päivämäärät, on jätetty pois tästä raportista.

Taulukossa listattu dokumentin tyyppi kertoo hyvin yleisellä tasolla, millaisesta dokumentista on kyse. Tiettyjä dokumentteja tunnistettiin useita samanlaisia, joten ne on esiteltynä taulukossa monikkomuodossa.

Menetelmän aikana kerätystä dokumentaatiosta huomaa, että IT-yksiköllä on vaikutusarvioinnin näkökulmasta ainakin kolmenlaisia dokumentteja: ei haittaa aiheuttavia, haittaa aiheuttavia sekä vahinkoa aiheuttavia. Näiden perusteella toteutettiin alustavat ja suuntaa antavat luokittelukategoriat julkinen, sisäinen ja luottamuksellinen. Luokittelukategorioiden nimeämisessä sovellettiin VAHTI-ohjeistusta (2010), kuitenkin niin, että ohjeessa mainittu kategoria ”käyttö rajattu” muutettiin muotoon ”sisäinen”. Testivaiheessa arvioitiin, että käsite ”sisäinen” ymmärretään helpommin.

Dokumentin tyyppi	Sijainti	Vaikutusarvioinnin tulos	Luokittelukategoria
Tietojärjestelmän dokumentit tekniselle pääkäyttäjälle	Digitaalinen työtila	Vahinkoa	Luottamuksellinen
Tietojärjestelmän palvelin-konfiguraatiot	Digitaalinen työtila	Vahinkoa	Luottamuksellinen
IT-infrastruktuurin kuvaukset	Verkkolevy	Vahinkoa	Luottamuksellinen
Järjestelmäkohtainen yleis-ohje	Digitaalinen työtila	Haittaa	Sisäinen
Perehdyttämismateriaalia si-säiseen käyttöön	Verkkolevy	Haittaa	Sisäinen
Vaatimusmäärittely, kesken-eräinen	Verkkolevy	Haittaa	Sisäinen
IT-tuen yhteystiedot	Verkkolevy	Ei vaikutusta	Julkinen

Taulukko 4: Inventaariotietoa IT-yksikön dokumenteista

Taulukosta 4 huomaa, että laajat IT-infrastruktuurin rakennetta kuvaavat dokumentit, jotka on suunnattu vain rajatulle käyttäjämäärälle, arvioitiin vahinkoa aiheuttaviksi ja näin ollen luottamuksellisiksi. Samaa tulkintaa voi soveltaa myös syvällisiin, yksittäisen järjestelmän pääkäyttäjätason dokumentteihin.

Haittaa aiheuttaviksi arvioitiin puolestaan IT-yksikön sisäiseen käyttöön tarkoitetut ohjeistukset ja dokumentit. Julkisiksi luokiteltiin esimerkiksi pelkkiä yhteystietoja sisältävät dokumentit, koska sama tieto oli saatavilla myös organisaation verkkosivustolta.

Tunnistetuista dokumenttityypeistä ja niiden vaikutusarvioinnin tuloksista voidaan johtaa alustavat luokitteluperiaatteet. Yleistettynä voidaan esimerkiksi todeta, että IT-infrastruktuuriin liittyvät dokumentit tulee lähtökohtaisesti luokitella luottamuksellisiksi. Lopputulokseen vaikuttaa myös vaikutusarvioinnin tulos. Laajempia ja yleiskäyttöisempiä koko IT-yksikön laajuisia luokittelukriteereitä ei määritelty vielä tämän osatutkimuksen aikana.

4.3.3 Menetelmän kehitysprosessi

Menetelmän kehitysprosessi koostui kahdesta erillisestä vaiheesta. Ensimmäiseksi rakennettiin menetelmän ensimmäinen versio kirjallisuudesta kerättyjen tietojen pohjalta. Löydetyt teemat yhdistettiin isoksi kokonaisuudeksi luvussa 3 kuvatulla tavalla. Ensimmäisen version kehittämisessä oli olennaista oikean tiedon löytäminen ja sen järjestäminen loogiseen järjestykseen.

Toisessa vaiheessa menetelmää kehitettiin käytännön testien perusteella. Tämä kuvastaa suunnittelututkimuksen ydintä. Olemassa olevan kehittäminen on oppimista tekemällä (Nunamaker ym. 1991, 100).

Testikierroksia oli yhteensä kolme. Ensimmäiselle iteraatiokierrokselle osallistui kaksi pienryhmää. Muille kierroksille osallistui yksi pienryhmä. Ensimmäisellä iteraatiokierroksella saatiin palautetta itse menetelmän sisältöön. Toisella kierroksella tarkennettiin termejä. Kolmannella iteraatiokierroksella menetelmän runko ja sisältö koettiin yleisesti hyväksi ja toimivaksi.

Ensimmäisellä testikierroksella saatiin kaksi olennaista palautetta. Ne arvioitiin yhdessä palautteen antajan kanssa. Lopputulos oli se, että menetelmään tehtiin kaksi isoa muutosta.

Ensimmäinen muutos liittyi tietoaineiston käsittelyä koskevien tietoturvallisuusasioiden määrittelyyn; miten tietoa saa käsitellä esimerkiksi sähköpostissa tai pilvipalveluissa. Alun perin teema oli osana viimeistä vaihetta. Käytännössä tietoturvatarpeiden määrittely olisi ollut iso tehtäväkokonaisuus, joka ei tiukasti tulkittuna kuulu enää julkisuusluokitteluun vaan luokkien käytännön hyödyntämiseen. Osatutkimuksen rajauksesta johtuen teema siirrettiin menetelmän toteuttamisen jälkeiseen hetkeen.

Toinen iso muutos oli se, että lainsäädännön asettamien vaatimusten selvittäminen sisällytettiin osaksi ensimmäistä vaihetta, tarpeen tunnistamista. Aikaisemmin vaatimuksille oli oma vaiheensa.

4.4 Julkisuusluokittelun hyödyntäminen IT-yksikössä

Kolmannessa osatutkimuksessa selvitettiin, miten IT-yksikkö voi hyödyntää julkisuusluokittelua päivittäisessä toiminnassaan. Tuloksina saatiin potentiaalisia hyödyntämiskohteita. Niitä ovat tärkeiden tietojen tunnistaminen ja hallinta, tietojärjestelmien ja palveluiden suunnittelu ja käyttöönotto, pääsynhallinta ja tietoturvamekanismien toteuttaminen, vastuiden ja velvollisuuksien selkeyttäminen sekä riskienhallinta ja jatkuvuuden suunnittelu. Lisäksi arvioitiin, että julkisuusluokittelua voisi hyödyntää myös viestinnässä, perehdyttämisessä ja lain vaatimusten täyttämisessä.

Tutkimusaineistoittain tulokset jakautuivat seuraavasti. Suorissa haastatteluvastauksissa IT-yksikön työntekijät painottivat tärkeiden dokumenttien tunnistamista ja niiden käsittelyn ohjeistamista. Koko haastatteluaineiston analyysin perusteella potentiaalisiksi hyödyntämiskohteiksi tunnistettiin tietojärjestelmien suunnittelu sekä dokumentteihin liittyvien vastuiden ja velvollisuuksien selkeyttäminen. Olennaisimmat havainnoimalla tunnistetut hyödyntämiskohteet liittyivät puolestaan dokumenttien hallintaan, pääsynhallintaan ja riskienhallintaan.

Seuraavissa alaluvuissa on kuvattu kolmannen osatutkimuksen päätulokset tarkemmin. Yksittäiset hyödyntämiskohteet on koottu kokonaisuuksiksi, koska hyödyntämiskohteet ovat osittain päällekkäisiä ja toisiinsa linkittyviä. Viimeisessä alaluvussa esitellään myös muut tutkimusaineistosta tunnistetut, vähemmälle huomiolle jääneet hyödyntämiskohteet.

4.4.1 Tärkeiden tietojen tunnistaminen ja hallinta

Haastateltavat haluavat paremmin tunnistaa ne tiedot, joita ei ole tarkoitettu julkiseen jakeluun. Erityisesti kollegan tuottamien dokumenttien julkisuusluokan tunnistaminen aiheuttaa haastetta. Julkisuusluokittelussa käytettävä luokittelumerkintä helpottaisi päivittäistä toimintaa.

Eri julkisuusluokan dokumentteja havaittiin useissa eri tietojärjestelmissä. Havainnointitilanteessa henkilöt myös totesivat, etteivät ole osanneet ajatella, kuinka paljon suojattavaa tietoa dokumenteissa voi olla. Henkilöt kokivat, että heidän pitää jatkossa pohtia tarkemmin, mitä kaikkia tietoja tiedostoihin tulee laittaa. Alustavasta luokittelusta olisi potentiaalisesti hyötyä jo dokumenttien luontivaiheessa.

Luokittelua hyödynnettäisiin tärkeiden dokumenttien käsittelyn ohjeistamisessa. Käsittelyllä haastateltavat viittasivat esimerkiksi tiedon säilyttämiseen, jakamiseen ja tuhoamiseen. Ohjeistus kattaisi eri työvälineet sekä ulkopuoliset palvelut.

”Tästä saisimme samalla myös ohjeet siihen, kuinka eri tavalla luokiteltuja tietoja tulisi käsitellä, kun niitä säilytetään, varmuuskopioidaan, tulostetaan, jätetään työpöydälle jne. ”, H1.

4.4.2 Tietojärjestelmien ja palveluiden suunnittelu ja käyttöönotto

Haastateltavat mainitsivat kaksi olennaista tietojärjestelmiin liittyvää kokonaisuutta, jossa luokittelua voitaisiin hyödyntää: suunnittelutyö sekä uusien palveluiden käyttöönotto. Kun tiedetään, millaisia tietoja järjestelmässä tai palvelussa tullaan käsittelemään, voidaan se toteuttaa toimintaa tukevalla tavalla. Järjestelmät on mahdollista rakentaa alusta alkaen tietosuoja ja -turva huomioiden. H4 kiteyttää tarvelähtöisen suunnittelun kahteen kommenttiin:

”IT on muutakin kuin tekniikkaa.”, H4
”Pääsääntöisesti järjestelmissä käsitellään informaatiota, joka on eritasoista” H4

Luokittelu mahdollistaa myös uusien palveluiden suunnitelmallisemman käyttöönoton. Palveluiden käytöstä voidaan antaa ohjeistuksia luokitteluun perustuen. Esimerkiksi H3 lähestyy aihetta käänteisesti. Hän mainitsee pilvipalveluiden osalta seuraavaa: ”Jos emme luokittele, emme oikein voi ottaa kantaa edes käyttöön.”, H3.

4.4.3 Pääsynhallinta ja tietoturvamekanismien toteuttaminen

IT-yksikön tietojärjestelmissä olevia dokumentteja suojataan osittain jo nyt julkisuusluokittelun mukaisesti. Tämä ilmenee pääsynhallinnan ja käytössä olevien tietoturvamekanismien näkökulmasta. Havaintojen ja haastatteluiden perusteella dokumentteihin liittyvä pääsynhallinta vaihtelee kohteittain.

Päästäkseen käyttämään tiettyjen sisäisten palveluiden dokumentteja, on työntekijällä oltava tieto dokumentin sijainnista, pääsyn mahdollistavat välineet ja tarvittavat käyttöoikeudet. Lisäksi työntekijän tulee tunnistautua asianmukaisella tavalla.

”Asemani organisaatiossa määrää sen, mitä näen.”, H3.

4.4.4 Vastuiden ja velvollisuuksien selkeyttäminen

Luokittelusta toivotaan apua dokumentteihin liittyvien vastuiden ja velvollisuuksien selkeyttämiseen. Työntekijät tietäisivät paremmin, kuka tai ketkä ovat vastuussa tietyn tietoaineiston elinkaaresta ja turvallisuudesta.

”Turhan vastuunottamisen tarve vähenisi.”, H2

Luokittelulla voitaisiin myös osoittaa, että työntekijä käsittelee omassa tehtävässään paljon luottamuksellista tai salaista tietoa. Toisaalta, luokittelu auttaisi työntekijää ymmärtämään omat velvollisuutensa, kun hän käsittelee luottamuksellisia dokumentteja.

4.4.5 Riskienhallinta ja jatkuvuuden suunnittelu

Riskejä vähentävä toiminta ilmenee käytännössä dokumenttien tallentamisena eri järjestelmiin. Havainnointitilanteen keskusteluiden mukaan tärkeät dokumentit sijoitetaan aina tiettyyn järjestelmään, koska se on tekniseltä toteutukseltaan yksinkertaisempi kuin muut järjestelmät. Näin ollen kohteen suojaaminen ja toiminnan jatkuvuuden varmistaminen on helpompaa. Lisäksi pääsy kohteessa oleviin tietoihin on rajattu työtehtävien mukaan. Myös haastatteluvastauksista oli tunnistettavissa vastaava kommentti:

”-- luokittelu parantaisi yksikön toimintavarmuutta ja toipumista.”, H2

4.4.6 Muut hyödyntämiskohteet

Päätulosten lisäksi haastatteluista tunnistettiin myös muita potentiaalisia hyödyntämiskohteita. Luokittelua voidaan hyödyntää viestinnässä, perehdyttämisessä ja lain vaatimusten täyttämisessä.

Luokittelun hyödyntämisellä viestinnässä tarkoitettiin sitä, että projekteissa olisi helpompi kuvata tarpeita ja ratkaisuja luokitteluun perustuen:
”Jotkin asiat olisi helpompi viedä eteenpäin. Useasti on todettu että luokittelu puuttuu.”, H3.

Perehdyttämisessä luokittelu auttaisi kertomaan uudelle työntekijälle, mikä tieto on tärkeää ja missä tieto sijaitsee. Lisäksi käytännön perehdyttämistyö olisi kevyempää ja mahdolliset virhetilanteet vähenisivät. H2 antaa esimerkin luokittelun puuttumisesta aiheutuvasta perehdyttämistilanteesta: ”Tässä kansiossa olevat saa julkaista. Tässä kansiossa olevia ei saa. Erehtymisen vaara on suuri.”

Luokittelun uskottiin helpottavan lain vaatimusten täyttämisessä. Käsittelysäännöt ohjaisivat dokumenttien käsittelyä lain mukaisella tavalla. Luottamuksellisten dokumenttien sijainti tunnettaisiin, jolloin ne olisi mahdollista suojata paremmin.

Varsinaisten hyödyntämiskohteiden lisäksi haastatteluista oli tunnistettavissa muutamia yleisiä hyötyjä. Niitä olivat toiminnan selkeyttäminen, luottamuksen kasvattaminen. Selkeyttämisellä tarkoitettiin sitä, että käsittelyyn liittyvä asioita ei tarvitsisi aina pohtia uudelleen ja toimintaan olisi yhteiset linjaukset. Asianmukaisella dokumenttien käsittelyllä viestitetään toiminnan laadusta. Sitä kautta voidaan saada luottamusta. H4 kuvaa hyötyjä seuraavasti:

”Asiakas voi luottaa meidän toimenpiteisiin paremmin.”, H4.
”Kaupallisessa toiminnassa luottamus on elinehto.”, H4.

5 Pohdinta

Tässä luvussa pohditaan opinnäytetyön tuloksia ja laatua. Luku rakentuu seuraavasti. Ensimmäiseksi arvioidaan tuloksia osatutkimuksittain sekä kokonaisuuden kannalta. Toisessa alaluvussa pohditaan osatutkimusten laatua, reliabiliteettia ja validiteettia. Arvioinnin kohteena ovat käytetyt menetelmät, aineiston keräys ja analysointi, tutkimusprosessi, tulosten oikeellisuus ja yleistettävyys sekä roolini osatutkimuksissa.

Laatua käsittelevissä luvuissa on käsitelty myös osatutkimusten tekemiseen liittyviä rajoitteita, haasteita ja ongelmia. Viimeisessä alaluvussa esitetään jatkotutkimusaiheita.

5.1 Tulosten arviointi

Tässä alaluvussa vastataan tutkimuskysymyksiin ja pohditaan tuloksia yleisesti. Lisäksi pyritään arvioimaan osatutkimusten tavoitteiden saavuttamista, tulosten merkitystä ja hyödyntämistä eri yhteyksissä sekä esittämään tuloksiin perustuvia johtopäätöksiä, implikaatioita.

Arviointia tehdään myös opinnäytetyön kokonaisuuden kannalta. Lopuksi esitellään uusi julkisuusluokittelun kokonaiskuva, joka on muodostettu koko opinnäytetyön perusteella.

5.1.1 Ensimmäinen osatutkimus

Ensimmäisessä osatutkimuksessa selvitettiin, miten sähköisten dokumenttien julkisuusluokittelua voidaan ymmärtää organisaation IT-yksikössä. Julkisuusluokittelun kokonaisuus jaettiin erillisiin teemoihin teoreettisen viitekehyksen perusteella. Tutkimuskysymykseen etsittiin vastausta selvittämällä ymmärrystä yksittäisten teemojen kautta.

Tulosten perusteella julkisuusluokittelua voidaan ymmärtää kuviossa 1 kuvatun kokonaisuuden avulla. Teemakohtaisia tuloksia arvioimalla voidaan päätellä miten, ja kuinka laajasti, yksittäinen teema ymmärretään. Tuloksista voidaan johtaa kehittämiskohteita.

Taulukossa 2 osoitettujen periaatepäätösten mukaisesti IT-yksikön tavoitteena on toteuttaa tietojen luokittelu ja siihen liittyvät toimintamallit valtionhallinnon suojaustasojen mukaisesti. Osatutkimuksen tulosten perusteella voidaan tunnistaa kaksi tavoitteeseen liittyvää kehittämiskohdetta. Ensinnäkin päivittäiset työskentelykäytännöt eivät vielä täysin kohtaa taulukossa 2 kuvatun tavoitetilan kanssa. Valtionhallinnon suojaustasoihin liittyvää toimintamallia ei ole viety systemaattisesti IT-yksikön työntekijöiden tietoisuuteen. Toiseksi luokittelua ei ole osattu soveltaa vähäisen koulutuksen ja ohjeistuksen johdosta. Esimerkiksi tiedon omistajat ovat osittain epätietoisia velvollisuuksistaan tiedon luokittelun osalta. Periaatepäätösten mukaisen tavoitteen voisi saavuttaa systemaattisemmalla ja konkreettisemmalla lähestymistavalla ja työntekijöitä ohjeistamalla.

Muut tulokset viittaavat siihen, että IT-yksiköllä on tarve dokumenttien julkisuusluokittelulle. IT-yksikkö myös tunnistaa luokiteltavat tiedot ja luokitteluluokat sekä tiedostaa luokitellun tiedon merkintätavat.

Ensimmäisen osatutkimuksen tuloksista oli IT-yksikölle paljon hyötyä. Osatutkimukselle asetettu tavoite saavutettiin. Yksikköön saatiin ymmärrystä ja osaamista aiheesta kokonaisuutena, tietoa julkisuusluokittelun nykytilasta sekä selkeitä kehittämiskohteita. Käytännön tekeminen ja toiminnan johtaminen on helpompaa, kun tiedetään, mitä pitää kehittää ensimmäisenä.

Tuloksista voidaan päätellä, että laajentaakseen ja syventääkseen luokitteluun liittyvää ymmärrystä, tulisi IT-yksiköllä olla selkeä tarve ja tahto viedä luokittelutoimintaa suunnitelmallisesti ja systemaattisesti eteenpäin. Laajemmin ja yleisemmin pohdittuna tulokset viittaavat siihen, että ymmärtääkseen ja hallitakseen julkisuusluokittelun kokonaisuutta, on ymmärrettävä julkisuusluokittelun yksittäiset teemat sekä niiden väliset suhteet.

Opinnäytetyön tekemisen aikana ei havaittu muita vastaavia luokittelun ymmärtämiseen liittyviä tutkimuksia eikä luokittelun kypsyystasoa arvioivia menetelmiä. Näin ollen tämän osatutkimuksen tuloksille ei tunnistettu vertailukohdetta.

5.1.2 Toinen osatutkimus

Toisessa osatutkimuksessa selvitettiin, miten sähköisten dokumenttien julkisuusluokittelua voidaan toteuttaa organisaation IT-yksikössä. Tulosten perusteella luokittelua voidaan toteuttaa etenemällä suunnitelmallisesti ja systemaattisesti, valitun menetelmän mukaisesti.

Tutkimusongelman ratkaisemiseksi rakennettiin menetelmä julkisuusluokittelun toteuttamiseksi. Menetelmää testattiin käytännössä IT-yksikössä. Lopputuloksena havaittiin, että menetelmä toimii ja sen avulla saadaan aloitettua sähköisten dokumenttien julkisuusluokittelu.

Tässä osatutkimuksessa toteutettu menetelmä ei ole ainoa oikea vaihtoehto julkisuusluokittelun aloittamiseksi. Organisaatioiden kannattaa valita käytettävä menetelmä tarpeen mukaan. Kehitetty menetelmä antaa hyvät lähtökohdat, halusi sitten hyödyntää olemassa olevia, tai kehittää täysin omaan organisaatioon sovitettu menetelmä.

Valmiin työkalun hyödyntäminen olisi ollut järkevää, mutta sellaisen käyttämisessä arvioitiin olevan haasteita. Ei ollut täysin selvää, mitkä asiat valmiissa malleissa olivat olennaisia, ja mikä vaihtoehdoista olisi sopivin. Olisi ollut virhe olettaa, että olemassa oleva malli tai menetelmä toimisi suoraan sellaisenaan määritetyssä toimintaympäristössä (mukaillen Peltier & Tompkins 2014, 301). Tutkimusongelman näkökulmasta parhaaksi lähestymistavaksi koettiin oman, tutkimusympäristöä tukevan menetelmän toteuttaminen.

Analysoidessani eri julkisuusluokittelumalleja, menetelmiä ja kehikoita, havaitsin, että ne sisältävät olennaisia teemoja, mutta teemojen esiin tuomisessa on parannettavaa. Lisäksi teemoja painotetaan eri tavalla lähteestä riippuen. Teemojen käsittely saattoi olla myös hyvin hajanaista. Esimerkiksi Raman ym. (2014, 67.4, 67.5) käsittelevät lain vaatimuksia hyvin laajasti, mutta luokitteluun liittyvä käytännön toteuttaminen käsitellään tiiviisti. Smallwood (2012, 187,189) puolestaan mainitsee lainsäädännön kevyesti yhdessä lauseessa, mutta olennaisten dokumenttien tunnistamista käsitellään käytännön tasolla laajemmin.

Painotuksessa esimerkkinä käytän menetelmän vaihetta ”osoita yritysjohdon tuki”. Calder (2005, 56) käsittelee teeman erikseen niin, että se pyydetään huomioimaan jokaisessa organisaation tietoturvaprojektissa. Tietojen luokittelusta kertovassa osuudessa sitä ei enää mainittu, jolloin teema voi jäädä huomioimatta.

Hajanaisuuteen ja käsittelyn laajuuteen liittyvät huomiot vaikeuttavat kyseisten lähteiden hyödynnettävyyttä. Pyrin huomioimaan teemojen hajanaisuudesta ja painotuksesta johtuvat ongelmat rakentamassani menetelmässä käsittelemällä olennaisia teemoja tasapuolisesti ja ohjemuotoisesti, asia kerrallaan.

Kehitetty menetelmä voisi toisaalta olla myös kattavampi. Esimerkiksi NIST (2008) on julkaissut erittäin laajan ja kattavan ohjeen luokittelutoiminnasta. Vastaavasti VAHTI (2010) tarjoaa suomenkielisen ohjeistuksen tietoaineistojen luokittelua varten. Tarkempaa ja kattavampaa analyysiä näiden ohjeiden ja kehitetyn menetelmän eroista ei toteutettu tässä osatutkimuksessa.

Lopputuloksesta ei ollut tarkoitus tehdä kaiken kattavaa menetelmää, joka huomioisi jokaisen yksityiskohdan, mitä kirjallisuudessa on kerrottu. Sen sijaan menetelmä koostettiin eri lähteissä yleisimmin mainituista ja suositelluista asioista. Mikäli jokin yksityiskohta koettiin olennaiseksi, se lisättiin menetelmään omana vaiheenaan tai osaksi jotain toista vaihetta. Esimerkiksi Peltier ja Tompkins (2014, 301) suosittelevat selvittämään, miten muut ovat toteuttaneet vastaavan projektin ennen oman projektin aloittamista. Kyseinen teema mainittiin vain muutamassa lähteessä, mutta sisällytin sen silti osaksi oman menetelmäni alkuvalmisteluita.

Toisen osatutkimuksen tuloksista oli selkeää hyötyä IT-yksikölle. Osatutkimuksen tavoitteet saavutettiin. IT-yksikkö sai käyttöönsä menetelmän, jolla luokittelutoimintaa saatiin aloitettua. Koko organisaatio puolestaan hyötyy IT-yksikön kokemuksista ja kertyneestä osaamisesta.

Yksilötasolla hyötyivät menetelmän testaukseen osallistuneet työntekijät. He oppivat uutta ja ymmärtänevät aihetta nyt laajemmin. Heistä voi olla myös jatkossa hyötyä muutosvastarinnan hallitsemisessa. Muutosvastarinnan tunnistaminen auttanee puolestaan käytännön tekemisessä ja toiminnan johtamisessa.

Toisen osatutkimuksen tulosten ja käytännön testien perusteella näyttäisi siltä, että toteuttaakseen julkisuusluokittelua systemaattisesti ja suunnitelmallisesti, on IT-yksiköllä oltava kattava toteutusmenetelmä, jossa korostuu johtaminen, viestintä sekä työntekijöiden osallistaminen yhteistyön ja selkeiden ohjeiden avulla.

Yritysjohto on omalta osaltaan mukana tarpeen tunnistamisessa, vastuiden ja velvollisuuksien määrittämisessä sekä muiden resurssien osoittamisessa. Tarpeeksi kattavalla viestinnällä varmistetaan, että työntekijät tietävät, miksi ja miten luokittelua tehdään. Työntekijöiden osallistaminen puolestaan lisää työntekijöiden ymmärrystä aiheesta sekä helpottaa tietojen tunnistamista ja tukee muutoksen toteuttamista.

5.1.3 Kolmas osatutkimus

Kolmannessa osatutkimuksessa selvitettiin, miten sähköisten dokumenttien julkisuusluokittelua voidaan hyödyntää organisaation IT-yksikössä. Tulosten perusteella potentiaalisia hyödyntämiskohteita on useita ja niiden laajuus vaihtelee näkökulmasta riippuen. Varsinaisten hyödyntämiskohteiden lisäksi tunnistettiin myös hyötyjä, jotka saattavat toteutua, mikäli julkisuusluokittelua toteutetaan asianmukaisella tavalla.

Tulkintani mukaan riskienhallinnalla on isompi rooli hyödyntämiskohteena kuin tulokset suoraan osoittavat. Tulosten perusteella riskienhallinta ilmenee käytännössä vain dokumenttien tallentamisena eri järjestelmiin. Dokumenttien hallintaan, järjestelmien suunnitteluun, tietoturvamekanismeihin ja pääsynhallintaan liittyvillä toimenpiteillä pyritään kuitenkin siihen, ettei luottamuksellinen tieto päätyisi ulkopuolisille. Kokonaisuus kuvaa julkisuusluokittelun hyödyntämistä riskienhallinnassa laajemmin.

Verrattaessa osatutkimuksen tuloksia ulkopuolisten asiantuntijoiden haastatteluvastauksiin havaittiin muutamia eroja. IT-yksikkö tunnisti lainsäädännön noudattamisen yhdeksi potentiaaliseksi hyödyntämiskohteeksi. Ulkopuoliset tahot lähestyivät teemaa laajemmin kaikkien vaatimustenmukaisuusvelvoitteiden näkökulmasta.

IT-yksikön mainitsemat potentiaaliset hyödyntämiskohteet, pääsynhallinta ja jatkuvuuden suunnittelu, saivat ulkopuolisissa lähteissä puolestaan vähemmän huomiota. Ulkopuoliset asiantuntijat painottivat vastauksissaan, vaatimustenmukaisuuden lisäksi, tärkeiden tietojen tunnistamista sekä tiedon käsittelyn ohjeistusta ja kouluttamista.

Tuloksissa mainittiin julkisuusluokittelun hyödyntäminen osana palveluiden käyttöönottoa ja suunnittelua. Ulkoistettua tietojärjestelmää voidaan pitää palveluna, joten ne on yhdistetty saman otsikon ja teeman alaisuuteen.

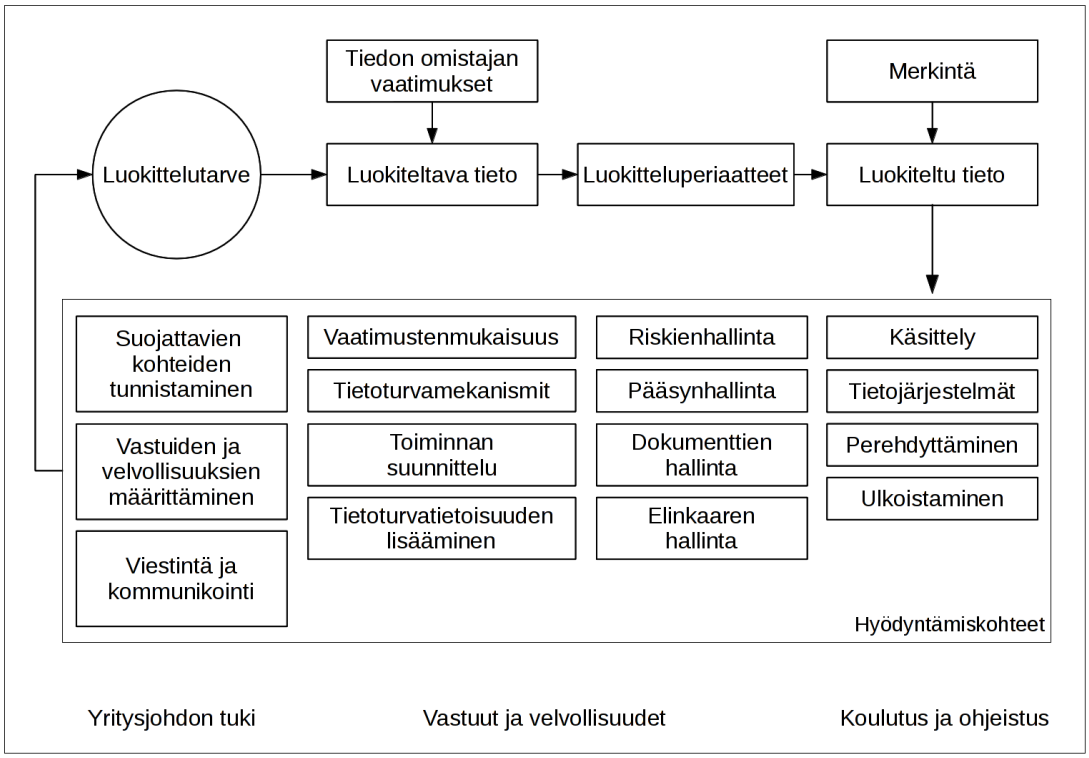
Kolmannen osatutkimuksen merkittävimpänä hyötynä pidän kattavaa listaa julkisuusluokittelun hyödyntämiskohteista. Tulokset viittaavat siihen, että julkisuusluokittelua voitaisiin hyödyntää usealla eri tavalla IT-yksikössä. Toisaalta, tulokset eivät vaikuta olevan vain IT-yksikköön sidottuja, joten tuloksia voitaneen hyödyntää myös muissa yksiköissä ja organisaatioissa. Listan myötä osatutkimuksen tavoite saavutettiin.

Käytännössä tuloksia voisi hyödyntää esimerkiksi viestinnässä. Henkilöstölle voidaan kertoa, miten organisaatio ja työntekijät hyötyvät, kun tietoja luokitellaan. Henkilöstön lienee myös helpompi hyväksyä julkisuusluokittelusta johtuvat toimintamuutokset, kun uuden toiminnan hyödyt ovat selvillä.

Tulosten hyödyntämistä voisi lähestyä myös luokittelutarpeen tunnistamisen näkökulmasta. Ovatko kattavat ja laajat hyödyntämiskohteet jo sellaisenaan peruste aloittaa luokittelutoiminta?

5.1.4 Opinnäytetyö kokonaisuutena

Opinnäytetyössä koottiin yhteen kolmen osatutkimuksen kokonaisuus, joiden avulla tuotettiin yleistietoa, ymmärrystä ja osaamista tietojen julkisuusluokittelusta kohdeorganisaation IT-yksikölle. Julkisuusluokittelua lähestyttiin kuviossa 1 esitetyn kokonaisuuden kautta. Opinnäytetyön tekemisen aikana tapahtuneen ymmärryksen, osaamisen ja tiedon karttumisen sekä henkilökohtaisen oppimisen tuloksena julkisuusluokittelun kokonaiskuva laajentui. Uusi laajennettu kokonaisuus on havainnollistettu kuviossa 4.



Kuvio 4: Laajennettu julkisuusluokittelun kokonaiskuva

Laajennettu kokonaisuus etenee aikaisemmasta kuviosta tuttujen teemojen mukaisesti. Kuvioon 4 ei tuotu uusia teemoja ensimmäisen osatutkimuksen perusteella. Sen sijaan ensimmäinen osatutkimus osoitti IT-yksikölle, mitä teemoja pitää kehittää.

Kuvion 4 mukaisesti luokittelulle on oltava tarve, jotta luokittelutoiminta olisi perusteltua. Tarpeet voivat muodostua esimerkiksi lain, toimialan, standardien, kolmannen osapuolen tai organisaation omien vaatimusten kautta. Luokitellessaan tietoaineistoa tiedon omistaja huo-

mioi tarvepohjaiset vaatimustenmukaisuusvelvoitteet, luokiteltavan tiedon tietoturvavaatimukset sekä organisaation tietojen luokitteluperiaatteet. Tietoaineisto merkitään niin, että tiedon käsittelijä tietää, mihin julkisuusluokkaan tieto kuuluu.

Alustavat luokitteluperiaatteet muodostetaan toisessa osatutkimuksessa kehitetyn menetelmän avulla. Menetelmää ei sellaisenaan sisällytetty kuvioon 4, koska menetelmän ja kokonaiskuvan abstraktiotaso on eri. Sen sijaan kokonaiskuvioon lisättiin toisessa osatutkimuksessa tunnistetut yritysjohdon tuki sekä luokittelutoimintaan liittyvät vastuut ja velvollisuudet.

Yritysjohdon on osoitettava tukensa koko luokittelutoiminnalle. Alkuvaiheessa tuki voidaan ilmaista esimerkiksi luokitteluprojektin asettamisella. Luokittelu voidaan huomioida myös organisaation tietoturvapolitiikassa. Vastuiden ja velvollisuuksien määrittelyllä ja dokumentoinnilla pyritään työntekijöiden roolien selkeyttämiseen. Erityisesti tiedon omistajan rooli on olennainen. On pystyttävä vastaamaan, kuka tiedon omistajaa ja millaisia tehtäviä omistajalla on luokitteluun liittyen.

Luokittelutoiminnan tarkoitus, tavoitteet ja hyödyt sekä vastuut ja velvollisuudet saatetaan työntekijöiden tietouteen koulutuksen ja ohjeistuksen avulla. Ohjeistus kertoo työntekijälle miksi luokittelua tehdään, kuka tietoa luokittelee, miten tietoa luokitellaan ja miten luokiteltua tietoa käsitellään.

Kolmannen osatutkimuksen aikana tunnistetut hyödyntämiskohteet on lisätty kuvion 4 keskelle. Luokitellun tiedon käsittely on siirretty osaksi muita hyödyntämiskohteita, vaikka se onkin edelleen yksi julkisuusluokittelun merkittävimmistä teemoista. Käsittelyohjeiden lisäksi luokittelutietoa voidaan hyödyntää useissa eri kohteissa, kuten esimerkiksi tietoaineistojen hallinnassa, tietojärjestelmien suunnittelussa ja riskien perusteella kohdistettujen tietoturvaratkaisujen toteuttamisessa.

Kuviossa 4 hyödyntämiskohteista on johdettu nuoli takaisin luokittelutarpeeseen. Hyödyntämiskohteita on paljon ja ne ovat laajoja sekä kattavia. Voidaankin todeta, että hyödyntämiskohteet ovat jo itsessään tarpeeksi hyvä peruste luokittelun aloittamiseksi.

Alkuperäistä kokonaiskuvaa voitiin pitää karkealla tasolla kuvattuna luokittelumallina. Uusi kokonaiskuva laajentaa näkemystä. Voidaan puhua jo kokonaisesta luokittelumallista, jota on täydennetty julkisuusluokittelun hyödyntämiskohteilla.

Opinnäytetyön tuloksista hyötyvät IT-yksikkö sekä organisaatio kokonaisuutena. Organisaatioon saadaan yleistietoa, ymmärrystä ja osaamista tietojen julkisuusluokittelusta sekä sen hyödyntämisestä muussa toiminnassa. Opinnäytetyö kokoaa aiheeseen liittyvää teoriatietoa

kattavaksi kokonaisuudeksi, josta on hyötyä myös muille organisaatioille. Luokittelumalli toimii johtamisen, suunnittelun ja toteuttamisen tukena.

Opinnäytetyön perusteella julkisuusluokittelu on laaja ja monipuolinen kokonaisuus. Vaikuttaisi siltä, että siirtyäkseen kohti laajamittaisempaa tietoaineistojen luokittelua, on organisaation 1) ymmärrettävä yksittäiset teemat ja niiden muodostama kokonaisuus, 2) edettävä systemaattisesti ja suunnitelmallisesti sekä 3) viestittävä ja ohjeistettava aiheesta ymmärrettävästi.

Opinnäytetyö käsittelee julkisuusluokittelua tieteellinen näkökulma huomioiden. Tästä on hyötyä aihealueen teoreettiselle viitekehykselle, koska luokitteluun liittyviä tieteellisiä artikkeleita on julkaistu verrattaen pieni määrä tietoturva-aiheisissa julkaisuissa (Silic & Back 2014, 291). Muuta aiheeseen liittyvää kirjallisuutta on olemassa runsaasti.

Metodologisesta näkökulmasta katsottuna opinnäytetyö osoittaa, että monimenetelmällisellä etenemisellä saadaan tuloksia aikaiseksi. Suunnittelututkimuksella voidaan toteuttaa tapaustutkimuksesta tunnistettuja kehittämiskohteita.

5.2 Laadun arviointi

Tässä alaluvussa arvioidaan opinnäytetyön laatua pohtimalla osatutkimusten sisäistä ja ulkoista reliabiliteettia ja validiteettia Milesin ym. (2014, 310–315) suosituksia soveltaen. Sisäisellä reliabiliteetilla tarkoitetaan osatutkimusten toteuttamisen huolellisuutta ja toistettavuutta. Ulkoisella reliabiliteetilla viitataan toteuttamisen objektiivisuuteen ja vahvistettavuuteen. Sisäinen validiteetti kuvaa tulosten uskottavuutta ja oikeellisuutta. Ulkoisella validiteetilla tarkoitetaan puolestaan tutkimustulosten yleistettävyyttä ja laajennettavuutta tutkimusympäristön ulkopuolelle. (Miles & Huberman 1994, 278–279; Miles ym. 2014, 311–314.)

Arviointi on tehty aihealueittain. Arvioitu on käytettyjä tutkimusmenetelmiä, tutkimusdatan keräystä ja analysointia, tutkimusprosessia, tulosten oikeellisuutta ja yleistettävyyttä sekä omaa rooliani osatutkimusten toteuttamisessa. Alaluvuissa käsitellään myös osatutkimusten tekemiseen liittyviä haasteita ja ongelmia.

5.2.1 Käytetyt tutkimusmenetelmät

Tapaustutkimus oli oikea tapa suorittaa ensimmäinen ja kolmas osatutkimus, koska sen avulla saatiin kerättyä tarvittavaa tutkimusaineistoa ja tutkimuskysymyksiin saatiin vastattua. Tapaustutkimuksessa, tutkittaessa yhtä ilmiötä vain yhdessä organisaatiossa, muodostuu kuitenkin ongelmia tutkimuksen toistettavuudessa. Tutkimustilanne on usein uniikki, täysin saman-

laista tilannetta tuskin tulee samassa organisaatiossa uudelleen. Ympäristö, kuten tietojärjestelmät, henkilöt ja organisaation sosiaaliset suhteet muuttuvat jatkuvasti. Yhden kohteen tutkimus on kuin kerran tehty koe. Siitä ei voi johtaa täysin luotettavia ja yleistettäviä päätöksiä ilman kokeen toistamista. (Lee 1989, 34–35; Yin 2002, 32–33.)

Toisessa osatutkimuksessa noudatettiin Hevnerin ym. (2004) ohjeita suunnittelututkimuksen toteuttamiseksi. Käytännön toteuttamiseen sovellettiin DSRM-mallia (Peffers ym. 2008). Mallin ymmärtäminen ja soveltaminen käytäntöön oli loogista. Isompia tutkimusmenetelmän käyttöön liittyviä ongelmia ei ilmaantunut.

5.2.2 Aineiston keräys ja analysointi

Lopputulosten kannalta aineiston keräys ja analysointi olivat onnistuneita. Osatutkimuksissa sovellettiin Milesin ym. (2014, 12–14) esittelemää analysointiprosessia. Aineiston keräys, tiivistys, kuvaaminen sekä johtopäätösten tekeminen onnistuivat pääsääntöisesti hyvin. Johtopäätökset myös käsiteltiin ja varmistettiin tutkimuksen kohteena olleen IT-yksikön henkilöstön kanssa.

Ensimmäisen osatutkimuksen tutkimusaineiston luotettavuutta pyrittiin nostamaan kaksivaiheisella etenemismallilla. Ensin tutkittiin organisaation ja yksikön kirjallisia lähteitä. Tämän jälkeen toteutettiin haastattelut. Haastatteluilla pyrittiin saamaan tukea jo havaittuihin tuloksiin, mutta mahdollistettaisiin myös uuden tiedon löytäminen.

Organisaation ja IT-yksikön kirjalliset aineistot olivat jakautuneet laajalti yhteiseen intranetiin sekä IT-yksikön omassa käytössä olevaan digitaaliseen työtilaan. Tämä saattoi rajoittaa tutkimusaineiston löytymistä. Ongelmaa yritettiin pienentää käyttämällä hakutoimintoja ja tutkimalla tietorakenteita manuaalisesti.

Haastateltavien määrä suhteessa IT-yksikön työntekijöiden määrään oli melko pieni. Tämä vaikuttaa aineiston kattavuuteen. Toisaalta haastatteluaineisto tuki jo löydettyjä tuloksia ja mahdollisti tutkimuskysymyksiin vastaamisen, joten haastateltavien vähäisestä määrästä ei koettu olevan merkittävää haittaa tutkimuksen luotettavuudelle.

Tutkimusetiikan kannalta on olennaista, että haastateltavat tietävät osallistuvansa tutkimukseen (Ronkainen ym. 2013, 109), ja että he saavat osallistua siihen vapaaehtoisesti (Eriksson & Kovalainen 2008, 70). Lisäksi on huolehdittava haastateltavien anonymiteetistä ja vastausten luottamuksellisuudesta (Eriksson & Kovalainen 2008, 73–74). Mainitut asiat huomioitiin osatutkimuksissa.

Toisen osatutkimuksen lopputuloksena kehitetty menetelmä perustui vahvasti alan kirjallisuuteen. Aineiston keräämisessä hyödynnettiin perinteistä kirjallisuuskatsausta (Jesson, Matheson & Lacey 2011). Keräysmenetelmä tuki hyvin osatutkimuksen toteuttamista.

Perinteisessä kirjallisuuskatsauksessa on kuitenkin muutamia ongelmia. Jessonin ym. (2011, 75) mukaan seuraavat ongelmat ovat tyypillisiä perinteiselle kirjallisuuskatsaukselle. Katsausta ei voida toistaa, kun käytettyä menetelmää ei ole kuvattu kattavasti. Joidenkin lähdeaineistojen sisällyttämistä tai pois jättämistä ei ole perusteltu. Lähdeaineistojen määrä on vähäinen eikä täten anna tarpeeksi kattavaa näkökulmaa aiheesta. Valittujen lähteiden laadun arviointia ei ole tehty. Tämä voi aiheuttaa väärien päätelmien tekemisen.

Työn laadun ja luotettavuuden parantamiseksi edellä mainittuja ongelmia pyrittiin vähentämään seuraavasti. Kirjallisuuskatsauksen toteuttaminen kuvattiin mahdollisimman tarkasti. Lähdeaineistot valittiin perustellusti siten, että ne tukivat aihetta ja tutkimusongelman ratkaisua. Aineistoa etsittiin alan kirjallisuudesta ja laadukkaista tieteellisistä lähteistä. Lähdeaineistoa kerättiin niin kauan, kunnes aineistosta ei saanut enää uusia näkökulmia kehitettävään menetelmään. Koska lopullinen menetelmä rakennettiin alan kirjallisuuteen perustuen ja tutkimusympäristöön sovitettuna, niin lähteiden sisällyttämistä ja pois jättämistä ei ollut tarpeellista arvioida yhtä tarkkaan kuin systemaattisessa kirjallisuuskatsauksessa.

Kolmannen osatutkimuksen tutkimusaineiston luotettavuutta olisi voinut parantaa toteuttamalla kokonaan uudet haastattelut, esimerkiksi kolme vuotta julkisuusluokittelun laajamittaisen käyttöönoton jälkeen. Näin tulokset olisivat kuvanneet todellista tilannetta eikä vain potentiaalisia hyödyntämiskohteita.

Havainnoinnilla kerätyt aineistot analysoitiin jälkikäteen teemapohjaisesti. Tämä heikentää lopputuloksen luotettavuutta ja laatua. Havainnoinnin kohteet olisi voinut määritellä etukäteen, jolloin tietojen keruu ja muistiinpanojen tekeminen olisi ollut luotettavampaa ja systemaattisempaa. Toisaalta, teemapohjaisesta tietojen keruusta voi olla myös haittaa, koska teemoihin keskittyminen voi siirtää tutkijan huomion pois ennalta tunnistamattomista teemoista (Silverman 1993, 39). Lopputuloksen kannalta tällä olisi ollut suurempi vaikutus, jos kolmannessa osatutkimuksessa olisi etsitty todellisia eikä potentiaalisia hyödyntämiskohteita.

Kolmannessa osatutkimuksessa ulkopuolisten asiantuntijoiden vastausten määrän vähäisyys yllätti. Vastausten määrällä ei kuitenkaan ollut merkittävää vaikutusta kokonaisuuteen, koska aineistoa hyödynnettiin vain tulosten pohdinnan yhteydessä.

Kaikkien osatutkimusten osalta tunnistettiin kaksi isoa haastetta. Ensinnäkin julkisuusluokitteluun liittyviä, luotettavia, vertaisarvioituja tieteellisiä artikkeleita löytyy todella vähän verrattuna muihin tietoturva-alan teemoihin (Silic & Back 2014, 291). Haun rajaus vain tietoturva-aiheisiin julkaisuihin saattoi vaikuttaa lopputulokseen. Tieteellisten artikkeleiden vähäisestä määrästä johtuen SANS:n julkaisut (Boyer 2003; Fowler 2003; Furness 2005) koettiin arvokkaiksi lisätietolähteiksi, vaikka niiden laatu ei muuten olisikaan vertaisarvioitujen tieteellisten artikkeleiden tasolla. Julkaisut tukevat myös hyvin alan kirjallisuudesta löytyneitä tietoja.

Toinen haaste muodostui luokitteluun liittyvistä käsitteistä. Tietokantahakuja toteuttaessa joutui käyttämään hyvin yleisiä ja monitieteellisiä hakutermejä. Esimerkiksi alan kirjallisuudessa aiheesta puhutaan englanninkielisillä termeillä "information classification" (tiedon luokittelu) ja "asset classification" (omaisuuden luokittelu). Näiden hakusanojen käyttö tietokantahaussa tuottaa satoja hakutuloksia. Tämä oli iso haaste erityisesti toisessa osatutkimuksessa. Hakutulokset eivät välttämättä käsittele millään tavalla luokittelumallin rakentamista.

5.2.3 Tutkimusprosessi

Ensimmäisessä ja kolmannessa osatutkimuksessa ei tunnistettu suurempia tutkimusprosessin luotettavuuteen negatiivisesti vaikuttavia tekijöitä. Osatutkimusten tutkimusprosessit pyrittiin kuvaamaan niin, että tutkimukset olisi toistettavissa. Toinen tutkija päässee samoihin lopputuloksiin aineistoa tulkitsemalla.

Toisessa osatutkimuksessa tutkimusaineiston ja tutkimustulosten välisen suhteen kuvaaminen aiheutti haastetta. Tarkoituksenani oli osoittaa, missä lähteissä menetelmään valitut teemat esiintyivät.

Oikeaa lisäarvoa tuottavan taulukon rakentaminen oli kuitenkin erittäin hankalaa. Teemojen painotus vaihteli yhdestä lauseesta kokonaisiin lukuihin. Lisäksi teemojen käsittely saattoi olla jaoteltuna useaan eri osioon lähdeaineistossa.

Yksiselitteisen, luotettavan, eettisesti oikean ja lisäarvoa tuottavan analyysitaulukon esittäminen ei onnistu, joten se jätettiin tekemättä. Sen sijaan kirjallisuuskatsauksesta kertovassa luvussa on esitetty, mitä kaikkia lähdeaineistoja toisessa osatutkimuksessa hyödynnettiin.

Opinnäytetyön prosessia, tuloksia ja johtopäätöksiä käsiteltiin myös toimeksiantajan edustajien kanssa. Opinnäytetyötä arvioivat ja kommentoivat ylimmän johdon edustaja, Oppimisympäristöpalvelut-yksikön esimies sekä aihealueen asiantuntija. Osatutkimusten haastateltavilla oli myös mahdollisuus kommentoida tuloksia.

Opinnäytetyön ohjausprosessiin ja työn arviointiin Laurea ammattikorkeakoulun puolelta osallistuivat opinnäytetyön ohjaajat Pirinen (2013) ja Rajamäki (2014), joilla on paljon kokemusta työelämälähtöisen tutkimus- ja kehitystoiminnan integroimisesta osaksi korkeakouluopetusta. Opinnäytetyön laatua kehitettiin toimeksiantajan ja opinnäytetyön ohjaajien kommenttien perusteella.

5.2.4 Tulosten oikeellisuus ja yleistettävyys

Ensimmäisen osatutkimuksen tuloksia ei voida sellaisenaan yleistää kohteena olleen IT-yksikön ulkopuolelle. Tulokset kuvaavat luokittelun ymmärtämistä tietyssä IT-yksikössä ja tietyllä ajan hetkellä. Muissa toimintaympäristöissä tulokset voivat vaihdella. Tutkimusaineisto on kuitenkin selkeää ja yksiselitteistä, joten tuloksia voidaan pitää uskottavina ja oikeina.

Toisessa osatutkimuksessa toteutettu menetelmä on hyvin todennäköisesti yleistettävissä hyödynnettäväksi myös muihin toimintaympäristöihin. Niitä ovat esimerkiksi organisaation muut yksiköt ja toiset organisaatiot. Menetelmä ei ole myöskään millään tavalla sidottu Suomen olosuhteisiin.

Toimintaympäristökohtaista soveltamistarvetta voi esiintyä esimerkiksi eri maiden lainsäädännön, yrityksen toimialan ja koon mukaan. Esimerkiksi henkilöstä, joka tuntee lainsäädännön asettamat vaatimukset tiedon julkisuudelle, voi olla paljon hyötyä. Organisaation koosta huolimatta on myös järkevää hyödyntää pienryhmätyöskentelyä (Smallwood 2012, 189–190) ja näin ollen osallistaa työntekijöitä. Henkilöstön osaaminen ja osallistaminen ovat olennaisia asioita organisaation tietoturvallisuuden kehittämisessä (Porvari 2012, 221).

Toisen osatutkimuksen tulosten uskottavuutta ja oikeellisuutta on vaikea arvioida yksiselitteisesti. Menetelmän kehittäjän rooli on merkittävä eivätkä kaikki välttämättä päädy rakentamaan samanlaista menetelmää julkisuusluokittelun toteuttamiseksi. Kehitetty menetelmä on kuitenkin rakennettu tiettyä tarkoitusta varten, joten sen on todistettava arvonsa (Hevner ym. 2004, 85–86). On pystyttävä osoittamaan, vastaako lopputulos aikaisemmin määritettyjä vaatimuksia (Nunamaker ym. 1991, 100). Osatutkimuksen tavoitteet saavutettiin, joten tuloksiakin voidaan pitää oikeina ja uskottavina.

Suunnittelututkimuksen lopputuloksia voidaan arvioida myös laadun ja tehokkuuden näkökulmasta. Ne on kuitenkin pystyttävä osoittamaan tieteellisesti pätevillä keinoilla. (Gregor & Hevner 2013, 351; Hevner ym. 2004, 85–86.) Opinnäytetyön aikana ei tehty erillisiä mittauksia.

Kolmannessa osatutkimuksessa tunnistetut potentiaaliset hyödyntämiskohteet eivät ole sidottuja kohteena olleeseen IT-yksikköön. Tuloksia voitaneen soveltaa myös muissa organisaation

yksiköissä tai kokonaan toisissa organisaatioissa. Muista organisaatioista tai toisilta toimialoilta voi löytyä lisää hyödyntämiskohteita, joita ei tässä osatutkimuksessa tunnistettu.

Osatutkimuksen tulokset vaikuttavat käytännöllisiltä julkisuusluokittelun hyödyntämiskohteilta. Käytännöllisestä näkökulmasta tuloksia ei voida pitää täysin oikeellisina ennen kuin ne on käytännössä todennettu. Teoreettisesta näkökulmasta tulokset ovat oikeellisia ja uskottavia.

Tulokset koottiin koko aineiston perusteella, triangulaatiota (Dubé & Paré 2003 615; Patton 1999, 1195; Yin 2002, 97) hyödyntäen, ja lopputuloksissa painotettiin eniten huomiota saaneita teemoja. Vähemmän huomiota saaneet teemat käsiteltiin tuloksissa erikseen. Tällä pyrittiin erottelemaan uskottavammat ja oikeellisemmat tulokset muista ja samalla parantamaan koko osatutkimuksen validiteettia ja luotettavuutta.

5.2.5 Roolini osatutkimuksissa

Laadullisessa tutkimuksessa tutkijan rooli vaikuttaa aina jollakin tavalla lopputulokseen. Tutkimusprosessin taustalla on ihminen, joka lähestyy aihetta omien ennakkokäsitysten ja kokemusten kautta. (Denzin & Lincoln 2011, 11; Patton 1999, 1201–1202.) Esimerkiksi ulkoisen reliabiliteetin kannalta on olennaista tunnistaa tutkimuksen toteuttamiseen vaikuttavat tekijät (Miles ym. 311–312).

Osatutkimukset toteutettiin yhden henkilön toimesta. Tällä voi olla vaikutuksia tutkimusaineiston keräyksen ja analysoinnin luotettavuuteen (Neuendorf 2002, 12). Osatutkimusten toteuttamisen jälkeen tunnistin, että aineiston analysoinnin teoreettista osaamistani pitää kehittää. Positiivisesti tutkimusaineiston keräykseen ja analysointiin vaikutti puolestaan työhistoriani organisaatiossa sekä aikaisempi osaaminen tietoturva-alalta. Lähdeaineiston sisältöä analysoitaessa on olennaista, että asiasta tietää jotain. Muuten lopputulokset voivat olla vääristyneitä. (Neuendorf 2002, 8-9.)

Toisessa osatutkimuksessa kehitetty menetelmä perustui kirjallisuuteen, mutta menetelmän rakentamiseen vaikuttivat myös omat kokemukseni ja mielipiteeni. Tutkimusetiikan näkökulmasta on ongelmallista, jos tutkijan mielipiteet ja ennakkokäsitykset vaikuttavat tutkimuksen etenemiseen (Yin 2002, 61–62). Toisaalta tutkijan luovuus on olennainen osa suunnittelututkimuksen toteuttamista (Hevner & Chatterjee 2010, 31; Hevner ym. 2004, 81; Vaishnavi & Kuechler 2008, 21).

Mielipideasiat ja ennakkokäsitykset piti huomioida erityisen tarkasti ensimmäisessä osatutkimuksessa. Ymmärrys ei saanut muodostua omien kokemuksieni, vaan IT-yksikön tietoaineisto-

jen ja haastatteluiden pohjalta. Toisessa ja kolmannessa osatutkimuksessa etsittiin mahdollisimman kattavasti tietoa toteuttamisesta ja hyödyntämisestä, joten osallistumisellani oli vain positiivisia vaikutuksia. Pystyin paremmin arvioimaan, millainen lopputulos hyödyttää organisaatiota eniten (mukaillen Yohalem & Tseng 2015, 120).

5.3 Jatkotutkimusaiheet

Julkisuusluokittelu on aiheena laaja ja moniulotteinen. Opinnäytetyön aikana muodostui useita jatkotutkimusaiheita.

Ensimmäistä osatutkimusta vastaava tutkimus voidaan toteuttaa myös muiden organisaatioiden IT-yksiköissä. Laajemmalla tutkimuksella voitaisiin osoittaa yleisimmät aiheeseen liittyvät kehittämiskohteet. Lisäksi voisi selvittää, miten julkisuusluokittelu ymmärretään IT-yksikössä esimerkiksi kaksi vuotta luokittelun käyttöönoton jälkeen.

Toisen osatutkimuksen osalta olennaisin jatkotutkimuskohde on kehitetyn menetelmän käytännön testaaminen toisessa tutkimusympäristössä. Näin saataisiin lisätietoa menetelmän toiminnasta ja soveltamisesta myös muualla.

Kolmannen osatutkimuksen tärkein jatkotutkimusaihe on selvittää, realisoituvatko ennen luokittelua tunnistetut hyödyntämiskohteet luokittelun käyttöönoton jälkeen. Lisäksi voisi selvittää, miten eri organisaatiohierarkian tasoilla toimivat henkilöt suhtautuvat tietojen luokitteluun, sen hyödyntämiskohteisiin ja siitä saataviin hyötyihin. Onko esimerkiksi IT-henkilöllä eri käsitys saavutetuista hyödyistä ja hyödyntämiskohteista verrattuna yritysjohtoon.

Jatkotutkimusaiheita voidaan esittää myös laajemmasta näkökulmasta. Päivittäisen työnteon kannalta on olennaista selvittää, miten julkisuusluokittelun käyttöönotto vaikuttaa organisaation työntekijöiden tietoturvatietoisuuteen. Olisi myös hyvä tietää, miksi julkisuusluokittelua ei ole otettu käyttöön eri organisaatioissa, tai mitä haittaa julkisuusluokittelusta voi organisaatiolle olla.

Liitteessä 3 on alustava tiivistelmä suunnitteluvaiheessa olevasta artikkelista, joka voitaisiin toteuttaa tämän opinnäytetyön perusteella. Tiivistelmä on kirjoitettu englanniksi ja se on suunnattu tietojärjestelmien suunnittelijoille ja tietoturva-alan ammattilaisille.

6 Lopuksi

Opinnäytetyö kuvasi julkisuusluokittelutyön aloittamista organisaation IT-yksikössä. Opinnäytetyön muodostavien osatutkimusten aikana selvitettiin, miten sähköisten dokumenttien julkisuusluokittelua voidaan ymmärtää, toteuttaa ja hyödyntää IT-yksikössä. Osatutkimuksille asetetut tavoitteet saavutettiin.

Opinnäytetyö oli pitkä prosessi, mutta sen tekeminen opetti minulle paljon uutta. Tietojen luokittelu osoittautui aiheena laajaksi ja haastavaksi. Osatutkimusten ansiosta ymmärrän aihetta paremmin, ja osaan soveltaa tietoa käytännössä. Opinnäytetyön kautta muodostunut osaaminen on tärkeää, sillä jo vuosien ajan tietojen luokittelu on ollut aiheena sellainen, joka alan asiantuntijoiden tulisi hallita (Stewart, Chapple & Gibson 2015; Krutz & Vines 2003, 5-10; Srinivasan 2008, 24–26).

Koen myös omaavani aikaisempaa paremmat valmiudet oman ammattitaidon kehittämiseen ja elinikäiseen oppimiseen. Lisäksi opin hyödyntämään tehokkaammin tutkimustietoa ja -menetelmiä osana työelämän kehittämistä.

Kokonaista luokittelumallin rakentamista ja käyttöönottoa organisaatiossa ei suoritettu, koska sellaisen toteuttaminen voi viedä vuosia. Tulosten perusteella voidaan kuitenkin arvioida, onko julkisuusluokittelun käyttöönoton jatkaminen ja laajentaminen järkevää sekä kannattavaa.

Edetäkseen kohti tietoaineistojen luokittelua, on IT-yksikössä ja koko organisaatiossa suoritettava vielä muita isoja tehtäväkokonaisuuksia. Organisaation on määritettävä luokittelukategoriaan liitettävät tietoturvavaatimukset, toteutettava tiedon merkintä- ja käsittelysäännöt, koulutettava työntekijät uuteen toimintamalliin sekä otettava käyttöön toimintaa tukevat tietoturvamekanismit. Lisäksi on harkittava tarvetta tiedon eheyden ja saatavuuden perusteella tehtävälle luokittelulle.

Organisaatiolla on nyt tarvittava yleistieto, ymmärrys ja osaaminen tietojen luokittelun toteuttamiseksi. Matka kohti tietoaineistojen luokittelua on alkanut.

Lähteet

Alparslan, E., Karahoca, A. & Bahsi, H. 2011. Classification of confidential documents by using adaptive neurofuzzy inference systems. Procedia Computer Science, 3, 1412–1417.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma.

Bayuk, J. 2009. Information Classification. Teoksessa Axelrod, C. W., Bayuk, J. & Schutzer, D. (toim.) Enterprise Information Security and Privacy. Norwood: Artech House.

Benbasat, I., Goldstein, D. K. & Mead, M. 1987. The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 11(3), 369–386.

Booysen, H. A. & Eloff, J. H. P. 1995. Classification of objects for improved access control. Computers & Security, 14, 251–265.

Boyer, B. 2003. Making use of Data Classification in the Corporate Environment (Security Essentials Certification (GSEC)). SANS. Viitattu 14.7.2015. https://www.giac.org/paper/gsec/2862/making-data-classification-corporate-environment/104832

Brand, J. C., Kruger-Van Renen, W. & Rudman, R. 2015. Proposed Practices To Mitigate Significant Mobility Security Risks. International Business and Economics Research Journal, 14(1), 199–219.

Bruckman, J. C. 2008. Overcoming Resistance to Change: Causal Factors, Interventions, and Critical Values. The Psychologist-Manager Journal, 11, 211–219.

Cabinet Office. 2014. Government Security Classification April 2014. Viitattu 2.2.2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

Calder, A. 2005. Business Guide to Information Security. London: Kogan Page.

Calder, A. & Watkins, S. 2012. IT Governance: An International Guide to Data Security and ISO27001/27002. 5. painos. London: Kogan Page.

Cazemier, J. A., Overbeek, P. & Peters, L. 2010. Information Security Management with ITIL (r) V3. Van Haren Publishing.

Council of the European union. 2013. Council Decision of 23 September 2013 on the security rules for protecting EU classified information. Official Journal of the Europen Union, 56(L274). Viitattu 2.2.2016. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2013:274:FULL&from=FI

Davison, R. M., Martinsons, M. G. & Kock, N. 2004. Principles of canonical action research. Information Systems Journal, 14, 65–86.

Denzin, N. K. & Lincoln Y. S. 2011. Introduction: The Discipline and Practice of Qualitative Research. Teoksessa Denzin, N. K. & Lincoln Y. S (toim.) The SAGE Handbook of Qualitative Research. 4. painos. Los Angeles: SAGE Publications.

Dlamini, M. T., Eloff, J. H. P. & Eloff, M. M. 2009. Information security: The moving target. Computers & Security, 28, 189–198.

Dubé, L. & Paré, G. 2003. Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations. MIS Quarterly, 27(4), 597–635.

DuraiPandian, N. & Chellappan, C. 2006. Dynamic Information Security Level Reclassification. 2006 IFIP International Conference on Wireless and Optical Communications Networks.

EBSCOhost. Viitattu 16.4.2016. https://www.ebscohost.com/

Eisenhardt, K. M. 1989. Building Theories from Case Study Research. Academy of Management Review, 14(4), 532–550.

Ellingson, L. L. 2011. Analysis and representation across the continuum. Teoksessa Denzin, N. K. & Lincoln Y. S (toim.) The SAGE Handbook of Qualitative Research. 4. painos. Los Angeles: SAGE Publications.

Eloff, J. H. P., Holbein, R. & Teufel, S. 1996. Security classification for documents. Computers & Security, 15(1), 55–71.

Eriksson, P. & Kovalainen, A. 2008. Qualitative Methods in Business Research. London: SAGE Publications.

Evans, N. & Price, J. 2014. Responsibility and Accountability for Information Asset Management (IAM) in Organisations. Electronic Journal Information Systems Evaluation, 17(1), 113–121.

Fowler, S. 2003. Information Classification - Who, Why and How (GIAC Security Essentials Certification (GSEC)). SANS. Viitattu 16.2.2016. http://www.sans.org/reading-room/whitepapers/auditing/information-classification-who-846

Furness, T. 2005. Implementing Information Classification within the Enterprise (GIAC Security Essentials Certification). SANS. Viitattu 14.7.2015. http://www.giac.org/paper/gsec/4198/implementing-information-classification-enterprise/106714

Greene, S. S. 2006. Security policies and procedures : principles and practices. Upper Saddle River, New Jersey: Prentice Hall.

Gregor, S. & Hevner, A. R. 2013. Positioning Design Science Research for Maximum Impact. MIS Quarterly, 37(2), 337–355.

Grimaila, M. R. & Fortson, L. W. 2007. Towards an Information Asset-Based Defensive Cyber Damage Assessment Process. Proceedings of the 2007 IEEE Symposium on Computational Intelligence in Security and Defense Applications (CISDA 2007), 206–212.

Hamel, G. 2000. Leading the revolution. Boston: Harvard Business School Press.

Hevner, A. R. & Chatterjee, S. 2010. Design Research in Information Systems, Theory and Practice. New York: Springer.

Hevner, A. R., March, S. T., Park, J. & Ram, S. 2004. Design Science in Information Systems Research. MIS Quarterly, 28(1), 75–105.

Huttunen, L. 2010. Tiheä kontekstointi: haastattelu osana etnografista tutkimusta. Teoksessa Ruusuvuori J., Nikander P. & Hyvärinen M (toim.) Haastattelun analyysi. Tampere: Vastapaino.

Jesson, J. K., Matheson, L. & Lacey, F. M. 2011. Doing your literature review : traditional and systematic techniques. SAGE Publications.

Julkaisufoorumi. 2015. Viitattu 2.2.2016. http://www.julkaisufoorumi.fi

Kaario, K. & Peltola, T. 2008. Tiedonhallinta : Avain tietotyön tuottavuuteen. Jyväskylä: Docendo.

Krippendorff, K. 2004. Content analysis: an introduction to its methodology. 2. painos. Thousand Oaks: SAGE.

Krutz, R. L. & Vines, R. D. 2003. Tietoturvasertifikaatti - CISSP. Suomentaja Suominen E. Helsinki: Edita Publishing.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing.

Lakos, A. & Phipps, S. 2004. Creating A Culture of Assessment: A Catalyst for Organizational Change. Portal: Libraries and the Academy, 4(3), 345–361.

Landoll, D. 2011. The security risk assessment handbook : a complete guide for performing security risk assessments. 2. painos. Boca Raton: CRC Press.

Lee, A. S. 1989. A Scientific Methodology for MIS Case Studies. MIS Quarterly, 13(1), 33–50.

Locke, L. F., Spirduso, W. W. & Silverman, S. J. 2007. Proposals that work: A guide for planning dissertations and grand proposals. 5. painos. Thousand Oaks: SAGE Publications.

March, S. T. & Smith, G. F. 1995. Design and natural science research on information technology. Decision Support Systems, 15(4), 251–266.

Microsoft. 2015. Top journals in security & privacy. Viitattu 2.2.2016. http://academic.research.microsoft.com/RankList?entitytype=4&topDomainID=2&subDomainID=2

Miles, M. B. & Huberman, A. M. 1994. Qualitative Data Analysis: an expanded sourcebook. 2. painos. SAGE Publications.

Miles, M. B., Huberman, A. M. & Saldaña, J. 2014. Qualitative data analysis: a methods sourcebook. 3. painos. Thousand Oaks: SAGE.

Mitchell, R. C., Marcella, R. & Baxter, G. 1999. Corporate information security management. New Library World, 100(5), 213–227.

Neuendorf, K. A. 2002. The Content analysis guidebook. Thousand Oaks: SAGE.

NIST. 2004. Standards for Security Categorization of Federal Information and Information Systems. FIPS Publication 199. Viitattu 3.12.2015. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

NIST. 2008. Guide for Mapping Types of Information and Information Systems to Security Categories. NIST Special Publication 800-60, Volume 1. Viitattu 3.12.2015. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

NIST. 2011. The NIST Definition of Cloud Computing. NIST Special Publication 800-145. Viitattu 16.9.2016. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Nunamaker, Jr., J. F. & Briggs, R. O. 2011. Toward a broader vision for Information Systems. ACM Transactions on Management Information Systems, 2(4).

Nunamaker, Jr., J. F., Chen, M. & Purdin, T. D. M. 1991. Systems Development in Information Systems Research. Journal of Management Information Systems, 7(3), 89–106.

Oppenheim, C., Stenson, J. & Wilson, R. M. S. 2003. Studies on information as an asset II: repertory grid. Journal of Information Science, 29(5), 419–432.

Paton, R. A. & McCalman, J. 2008. Change Management. A Guide to Effective Implementation. 3. painos. SAGE Publications.

Patton, M. Q. 1999. Enhancing the Quality and Credibility of Qualitative Analysis. Health Services Research, 34(5 osa 2), 1189-1208.

Patton, M. Q. 2002. Qualitative Research & Evaluation Methods. 3. painos. Thousand Oaks: SAGE.

Pavlov, G. & Karakaneva, J. 2011. Information Security Management System in Organization. Trakia Journal of Sciences, 9(4), 20–25.

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. 2008. A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45–77.

Peltier, T. R. 2010. Information Security Risk Analysis. 3. painos. Boca Raton: Auerbach Publications.

Peltier T. R. & Tompkins W. 2014. Asset Classification. Teoksessa Peltier, T. R. (toim.) Information Security FUNDAMENTALS. 2. painos. Boca Raton: CRC Press.

Peräkylä A. & Ruusuvuori J. 2011. Analyzing talk and text. Teoksessa Denzin, N. K. & Lincoln Y. S (toim.) The SAGE Handbook of Qualitative Research. 4. painos. Los Angeles: SAGE Publications.

Pfleeger, C. P. & Pfleeger, S. L. 2006. Security in computing. 4. painos. Prentice Hall.

Pirinen, R. 2013. Towards Realization of Research and Development in a University of Applied Sciences. Väitöskirja. Itä-Suomen yliopisto, luonnontieteiden ja metsätieteiden tiedekunta, tietojenkäsittelytieteen laitos. Kuopio. Viitattu 23.10.2016. http://urn.fi/URN:ISBN:978-952-61-1150-6

Pirinen, R. 2016. Tutkimuksen attribuutit. Sähköpostikeskustelu, Rauno Pirinen, Laurea. 12.4.2016.

Porvari, P. 2012. Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Väitöskirja. Aalto-yliopisto, sähkötekniikan korkeakoulu, elektroniikan laitos. Helsinki.

ProQuest. Viitattu 16.4.2016. http://www.proquest.com/

ProQuest Ebrary. Ebook Central. Viitattu 16.4.2016. http://www.proquest.com/products-services/ebooks-main.html

PwC. 2013. The Global State of Information Security Survey 2014. Viitattu 15.7.2015. http://www.pwchk.com/home/eng/rcs_info_security_2014.html

PwC. 2015. The Global State of Information Security Survey 2016. Viitattu 23.9.2016. http://www.pwc.com/gx/en/consulting-services/information-security-survey/download.jhtml

Raggad, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton: CRC Press.

Rajamäki, J. 2014. Studies of Satellite-Based Tracking Systems for Improving Law Enforcement: Comprising Investigation Data, Digital Evidence and Monitoring of Legality. Väitöskirja. Jyväskylän yliopisto, informaatioteknologian tiedekunta, tietotekniikka. Jyväskylä. Viitattu 23.10.2016. http://urn.fi/URN:ISBN:978-951-39-5789-6

Raman K., Beets K. & Kabay M. E. 2014. Developing classification policies for data. Teoksessa Bosworth, S., Kabay, M. E. & Whyne, E. (toim.) Computer Security Handbook. Volume 2. 6. painos. Somerset, New Jersey: John Wyley & Sons.

Reed, B. 2007. Implementing Information Lifecycle Security (ILS)*. Information Systems Security, 16(3), 177–181.

Ronkainen, S., Pehkonen, L., Lindblom-Ylänne, S. & Paavilainen, E. 2013. Tutkimuksen voimasanat. Helsinki: Sanoma Pro.

Runeson, P. & Höst, M. 2009. Guidelines for conducting and reporting case study research in software engineering. Empirical Software Engineering, 14(2), 131–164.

Ruusuvuori J., Nikander P. & Hyvärinen M. 2010. Haastattelun analyysin vaiheet. Teoksessa Ruusuvuori J., Nikander P. & Hyvärinen M (toim.) Haastattelun analyysi. Tampere: Vastapaino.

SANS. Viitattu 30.4.2016. https://www.sans.org/

SFS-ISO/IEC. 2013a. SFS-ISO/IEC 27001:2013 ”Information technology - Security techniques - Information security management systems – Requirements”. 2. painos. Helsinki: Suomen Standardisoimisliitto SFS.

SFS-ISO/IEC. 2013b. SFS-ISO/IEC 27002:2013 ”Information technology - Security techniques - Code of practice for information security controls”. 2. painos. Helsinki: Suomen Standardisoimisliitto SFS.

Siepmann, F. 2014. Managing Risk and Security in Outsourcing IT Services : Onshore, Offshore and the Cloud. Boca Raton: CRC Press.

Silic, M. & Back, A. 2014. Information security : Critical review and future directions for research. Information Management & Computer Security, 22(3), 279–308.

Silverman, D. 1993. Interpreting Qualitative Data. Methods for Analysing Talk, Text and Interaction. SAGE Publications.

Simon, H. 1996. The Sciences of the Artificial. 3. painos. Cambridge: MIT Press.

Smallwood, R. F. 2012. Safeguarding Critical E-Documents : Implementing a Program for Securing Confidential Information Assets. Somerset, New Jersey: John Wiley & Sons.

Srinivasan, M. K. 2008. CISSP in 21 Days. Birmingham: Packt Publishing.

Stamp, M. 2015. Information Security Journals : The good, the bad, and the ugly. Viitattu 2.2.2016. http://cs.sjsu.edu/~stamp/securityJournals.html

Stewart, J. M., Chapple, M. & Gibson, D. 2015. CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide. 7. painos. Indianapolis: Sybex.

Svärd, P. 2014. The impact of information culture on information/records management : A case study of a municipality in Belgium. Records Management Journal, 24(1), 5–21.

Tankard, C. 2015. Data classification - the foundation of information security. Network Security, 2015(5), 8–11.

Tong, A., Sainsbury, P. & Craig, J. 2007. Consolidated criteria for reporting qualitative research (COREQ): a 32-item checklist for interviews and focus groups. International Journal for Quality in Health Care, 19(6), 349–357.

Tudor, J. K. 2001. Information Security Architecture. An Integrated Approach to Security in the Organization. Boca Raton: CRC Press.

VAHTI. 2006. VAHTI 5/2006 Asianhallinnan tietoturvallisuutta koskeva ohje. Viitattu 27.2.2016. https://www.vahtiohje.fi/web/guest/5/2006-asianhallinnan-tietoturvallisuutta-koskeva-ohje

VAHTI. 2008. VAHTI 8/2008 Valtionhallinnon tietoturvasanasto. Viitattu 27.2.2016. https://www.vahtiohje.fi/web/guest/8/2008-valtionhallinnon-tietoturvasanasto

VAHTI. 2010. VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Viitattu 27.2.2016. https://www.vahtiohje.fi/web/guest/2/2010-ohje-tietoturvallisuudesta-valtionhallinnossa-annetun-asetuksen-taytantoonpanosta

Vaishnavi, V. K. & Kuechler, W. 2008. Design Science Research Methods and Patterns : Innovating Information and Communication Technology. Boca Raton: Auerbach Publications.

Whitman, M. E. & Mattord, H. J. 2014. Management of Information Security. 4. painos. Stamford, CT USA: Cengage Learning.

Widmark, C., Tishelman, C., Gustafsson, H. & Sharp, L. 2012. 'Information on the fly': Challenges in professional communication in high technological nursing. A focus group study from a radiotherapy department in Sweden. BMC Nursing, 11(10).

Yin, R. K. 2002. Case Study Research: Design and Methods. 3. painos. SAGE Publications.

Yin, R. K. 2014. Case Study Research: Design and Methods. 5. painos. Thousand Oaks: SAGE Publications.

Yohalem, N. & Tseng, V. 2015. Commentary: Moving From Practice to Research, and Back. Applied Developmental Science, 19(2), 117–120.

Kuviot

Kuvio 1: Hahmotelma julkisuusluokittelun kokonaiskuvasta 11
Kuvio 2: Kuvaus opinnäytetyön kokonaisuudesta..... 21
Kuvio 3: Menetelmä julkisuusluokittelun aloittamiseksi 36
Kuvio 4: Laajennettu julkisuusluokittelun kokonaiskuva 54
Figure 5: Classification model as proposal with furthered utilization targets 77

Taulukot

Taulukko 1: Tutkitut tietoturva-alan julkaisut 27
Taulukko 2: IT-yksikön perusteet dokumenttien luokittelulle 33
Taulukko 3: Vaikutusarvioinnin tuloksia vastaavat luokittelukategoriat 41
Taulukko 4: Inventaariotietoa IT-yksikön dokumenteista..... 45
Taulukko 5: Opinnäytetyön attribuutit..... 74

Liitteet

Liite 1: Opinnäytetyön attribuutit 73
Liite 2: Haastattelukysymykset 75
Liite 3: Studies of information asset classification in a University of Applied Sciences 76

Liite 1: Opinnäytetyön attribuutit

Taulukossa 5 on kuvattu opinnäytetyön attribuutteja Piriseltä (2016) saatua attribuuttilistaa mukaillen. Attribuuttien tarkoituksena on auttaa ulkopuolista henkilöä arvioimaan opinnäytetyön metodologista täsmällisyyttä ja perusteellisuutta (Dubé & Paré 2003). Pirinen (2016) on muodostanut listan eri lähteiden (Davison, Martinsons & Kock 2004; Dubé & Paré 2003; Locke, Spirduso & Silverman 2007; Miles & Huberman 1994) perusteella.

Attribuutti	**Kuvaus**
Opinnäytetyön otsikko	Kohti tietoaineistojen luokittelua ammattikorkeakoulussa
Tutkimuskysymykset	Kolme eri osatutkimusta, joissa tutkittiin, miten sähköisten dokumenttien julkisuusluokittelua voidaan ymmärtää, toteuttaa ja hyödyntää organisaation IT-yksikössä?
Tutkimuslupa	Suullinen sopimus
Analysointiyksikkö	Julkisuusluokittelu
Tarpeellisuus	Tulokset ovat tärkeitä toimeksiantajalle tietojen luokittelun edistämiseksi.
Tutkimusmetodologia	Tapaustutkimukset (Yin 2002) ja suunnittelututkimus DSRM-mallia (Peffers ym. 2008) soveltaen. Aineistona haastattelut, kirjallisuuskatsaus, käytännön testauksen tulokset ja havainnointi.
Analysointi	Laadullinen analysointi, teemoittelu, triangulaatio.
Tutkimuksen luonne	Deskriptiivinen (1. ja 3. osatutkimus) sekä eksploratorinen (2. osatutkimus).
Lähestymistapa	Pääosin deduktiivinen.
Konstruktioiden määrittely	Tietojen luokittelu, turvallisuusluokittelu, julkisuusluokittelu.
Keskeinen teoria	Alan asiantuntijoiden tuottama kirjallisuus, tieteelliset artikkelit, kansainvälisesti tunnustetut tietoturvastandardit sekä kansalliset ja kansainväliset ohjeistukset.
Ensimmäinen tutkimustavoite	Tietojen luokittelun yleistiedon, ymmärryksen ja osaamisen kerääminen.
Toinen tutkimustavoite	Organisaatiokohtaisten kehittämiskohteiden tunnistaminen ja luokittelun aloittaminen.
Tulosten vertailu	Ensimmäisen ja kolmannen osatutkimuksen tuloksia ei vertailtu systemaattisesti muihin lähteisiin, koska täysin vastaavia tutkimuksia ei tunnistettu. Toisen osatutkimuksen tulos perustui kirjallisuudessa esitettyihin malleihin.

Tutkimusasetelma	Tapaustutkimukset soveltaen Yinin (2002) mallia ja suunnittelututkimus soveltaen Peffersin ym. (2008) DSRM-mallia.
Tutkimusaineiston keräys	Ensimmäisessä osatutkimuksessa IT-yksikön työntekijöiden haastattelut (n=4) sekä organisaation ja IT-yksikön dokumentit (n=18). Toisessa osatutkimuksessa kirjallisuuskatsaus ja kehitetyn menetelmän testaus käytännössä (n=4). Kolmannessa osatutkimuksessa IT-yksikön työntekijöiden haastattelut (n=4), käytännön testauksen havainnointi (n=4) ja ulkopuoliset tiedonantajat (n=4).
Aineiston ja tulosten välinen logiikka	Ensimmäisessä ja kolmannessa osatutkimuksessa kirjallisuuteen ja aineistoon perustuva. Toisessa osatutkimuksessa kirjallisuuteen perustuva.
Aineiston analysoinnin teoria	Ellingson 2011; Krippendorff 2004; Miles & Huberman 1994; Miles, Huberman & Saldaña 2014; Patton 2002
Haastattelut	Yksilöhaastatteluita (n=4), joissa puoli-strukturoidut kysymykset kartoittivat aihetta IT-yksikön näkökulmasta. Haastateltavien toiveiden mukaisesti haastatteluja ei nauhoitettu. Haastatteluvastaukset dokumentoitiin tekstinä.
Teemoittelu	Aineisto teemoiteltiin kirjallisuudesta muodostettujen teemojen perusteella (mukaillen Miles & Huberman 1994).
Muistiinpanot	Osatutkimusten tutkimusaineiston keruun yhteydessä tehtiin muistiinpanoja.
Tutkijoiden määrä	n=1
Tärkeimmät tulokset	Julkisuusluokittelun nykytilan ja kehittämiskohteiden tunnistaminen organisaatiossa, menetelmä julkisuusluokittelun toteuttamiseksi sekä lukuisia potentiaalisia julkisuusluokittelun hyödyntämiskohteita.
Merkittävin implikaatio	Vaikuttaisi siltä, että siirtyäkseen kohti laajamittaisempaa tietoaineistojen luokittelua, on organisaation 1) ymmärrettävä yksittäiset teemat ja niiden muodostama kokonaisuus, 2) edettävä systemaattisesti ja suunnitelmallisesti sekä 3) viestittävä ja ohjeistettava aiheesta ymmärrettävästi.
Roolit	Opinnäytetyön tekijän roolin merkitys vaihteli osatutkimuksittain. Haastateltavat ja käytännön testaukseen osallistuneet henkilöt olivat organisaation työntekijöitä.

Taulukko 5: Opinnäytetyön attribuutit

Liite 2: Haastattelukysymykset

Jokaisen kysymyksen ohessa kysyttiin myös ”miksi” -pohjaisia lisäkysymyksiä, joilla pyrittiin saamaan haastateltavalta lisätietoja.

Miten luokittelu näkyy päivittäisessä toiminnassa?

Miten dokumenttien julkisuusluokittelu näkyy IT-yksikön dokumenteissa?

Miten hyvin luokittelu on IT-yksiköllä tiedossa? Miksi se on hoidettu, kuten kuvasit? Voisiko sitä kehittää jotenkin? Miten?

Miksi IT-yksikön pitäisi luokitella tietoja?

Vaatiiko jokin taho tietojen luokittelua? Perustele.

Millaista hyötyä tai haittaa luokittelun tekemisestä voisi IT-yksikölle olla?

Millaisia dokumentteja IT-yksikön tulisi luokitella ja millä perusteella?

Miten IT-yksikön kannattaisi luokitella dokumenttinsa?

Missä vaiheessa dokumentti kannattaisi luokitella?

Miten luokittelua tulisi ohjata?

Kuka tai mikä taho vastaa dokumentin luokittelusta?

Millaista ohjeistusta aiheeseen on olemassa? Tai pitäisi olla?

Miten julkisuusluokitteluun suhtaudutaan? Tai pitäisi suhtautua?

Muuta aiheeseen liittyvää kommentoitavaa?

Liite 3: Studies of information asset classification in a University of Applied Sciences

This appendix includes a preliminary abstract of furthered manuscript for an appropriate conference or journal in information systems. The study is addressed to the contribution of design theory of information systems and audience of security expertise in the context of objects and document classification. The paper will comprise the thesis work by Laakso, M. and its results for professional audience. Abstract authors: Laakso M., & Pirinen R.

Studies of information asset classification in a University of Applied Sciences (UAS)

The primary objective of this study was to achieve common understanding and realization knowledge about the information asset classification in a higher education institution domain. A case and design research studies were conducted to form basic understanding of asset classification and development in the information technology unit of a UAS. An applied method for starting classification was developed using design science research methodology with an additional case study which was conducted to reveal potential ways to utilize classified information assets according to achieved understanding.

Main results revealed that classification model must be systematically built and implemented. Results indicate that classified information can be utilized in planning, designing and building more secure information systems. In this first realization case, personnel were placing sensitive documents in a specific location, such as in directory; however in future the sensitive documents can be imported to the data base, digital library or content manager. This enables the improvement of protection of documents from outsiders and better versioning and recovery procedures if a critical information system failure occur. For example document metadata information could be used to recognize and recover most sensitive documents in first phase of recovery functions and in sense of continuity management.

In addition, personnel also recognized that many of their documents include too much sensitive information which is not mandatory for the document. It was understood that authors must plan the document structure and contents more carefully. Thinking more widely this could also be beneficial for planning information system data structures, data modeling and metadata enabled services based on the classification of information.

Asset classification model as proposal is presented in the Fig.5.

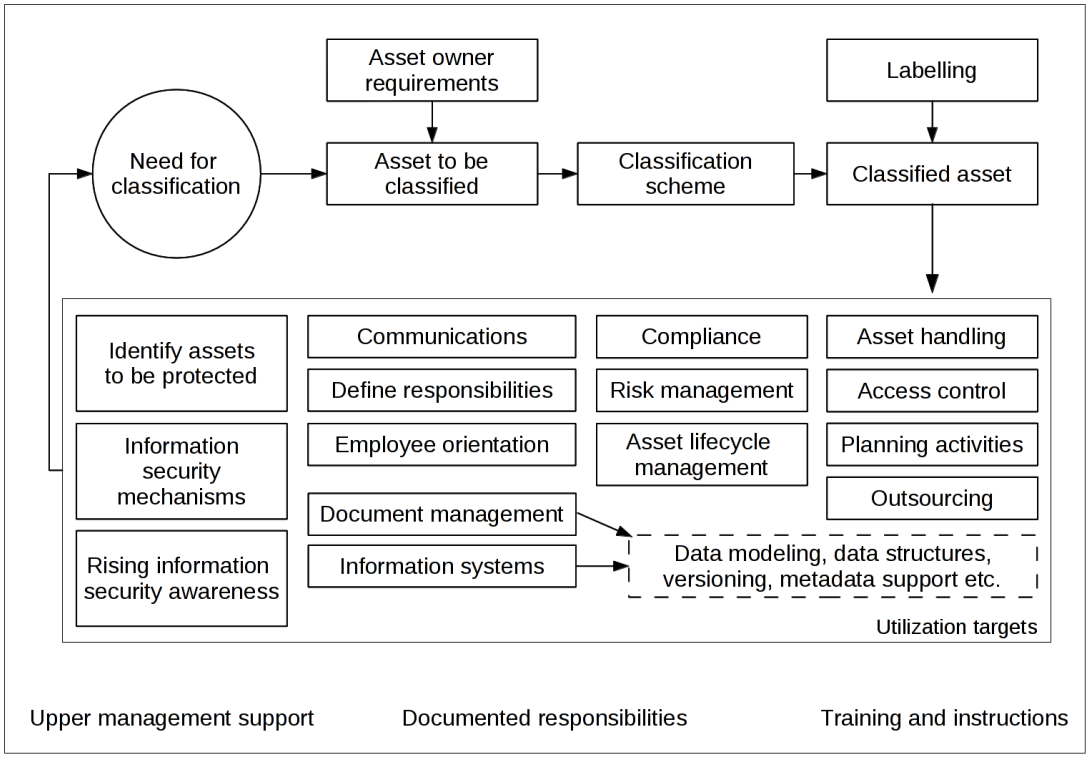


Figure 5: Classification model as proposal with furthered utilization targets

Fig.5 describes that classification starts by identifying the need to classify assets, for example compliance requirements. Asset owners classify the information according to information security requirements specified by the owner and the organization, compliance requirements and classification scheme. Classified information is labeled with appropriate label which reflects the classification scheme. In Fig.5 information systems and document management are seen as utilization targets for classified assets. Targets may include sub targets such as like data modeling, data structures, versioning and metadata support. Upper management support, documented responsibilities, training and instructions are seen as important components of the classification implementation model.