Tampereen yliopisto

Laura Karintaus

LUOTTAMUKSELLISEN TIEDON KÄYTTÖOIKEUKSIEN HALLINNAN JOHTAMINEN SUURESSA YRITYKSESSÄ

Tekniikan ja luonnontieteiden tiedekunta
Kandidaatintyö
Huhtikuu 2019

TIIVISTELMÄ

Laura Karintaus: Luottamuksellisen tiedon käyttöoikeuksien hallinnan johtaminen suuressa yrityksessä
Kandidaatintyö
Tampereen yliopisto
Tietojohtaminen
Huhtikuu 2019

Tieto synnyttää yritykselle sekä arvoa että riskejä. Käyttöoikeuksien hallinnalla yritys jakaa tietoa ja toisaalta suojaa liiketoiminnan kannalta kriittistä tietoa vääriin käsiin joutumiselta. Erilaisten tietokokonaisuuksien käyttöä hallitaan niiden luottamuksellisuustason edellyttämien vaatimusten mukaisesti. Käyttöoikeuksien hallinnan organisoimista ohjaa tietoturvallisuuspolitiikka ja -päätöksenteko.

Tutkimuksen tavoitteena ja siten päätutkimuskysymyksenä oli selvittää, miten luottamuksellisen tiedon käyttöoikeuksien hallintaa tulisi johtaa suuressa yrityksessä. Aiheen tutkimisessa keskityttiin erityisesti yrityksen tiedon käyttöoikeuksien hallinnan prosesseihin, toimintaa ohjaavaan tietoturvallisuuspolitiikkaan ja yrityksen eri toimijoiden vastuisiin näiden parissa. Tietoa hankittiin alan tietokirjallisuudesta ja uudemmista tutkimusartikkeleista. Tieteellisen aineiston lisäksi hyödynnettiin kansainvälistä tietoturvallisuuden ISO-standardia. Eri lähteistä saatua tietoa vertailtiin ja yhdisteltiin, ja tuloksena muodostettiin eri tutkimusalueet kattava kokonaiskuva aiheesta.

Tutkimusaineistoista selvisi, että yrityksen eri toimijoiden ja käyttöoikeuksien hallintaan liittyvän prosessin vastuualueiden yhteensovittaminen aiheuttaa usein haasteita etenkin suurissa yrityksissä. Tärkeimpänä tuloksena tälle kandidaatintyölle muodostettiin kokonaiskuva johtamismallista, joka yhdistää luottamuksellisen tiedon käyttöoikeuksien hallinnan politiikan ja prosessit sekä näiden piirissä toimivat tahot. Tutkimuksen seurauksena voidaan vetää johtopäätös, että yrityksen käyttöoikeuksien hallinnan systeemiä toimijoineen tulisi tarkastella kokonaisuutena jo sen suunnitteluvaiheessa.

Tutkimusaihe saatiin kirjoittajan työnantajayritykseltä, jossa tutkimuksen tuloksia käytetään esiselvityksenä käyttöoikeuksien hallinnan johtamisen kehittämisessä. Tutkimuksen tuloksena muodostettua johtamismallia voidaan verrata yrityksessä käytössä oleviin toimintamalleihin ja etsiä mahdollisia ongelma- ja kehityskohteita.

Avainsanat: käyttöoikeuksien hallinta, luottamuksellinen tieto, tietoturvallisuus

ALKUSANAT

Tämä tutkimus on tehty kandidaatintyönä Tampereen yliopiston tietojohtamisen koulutusohjelmaan kevätlukukaudella 2019. Tutkimuksen aiheen valinta tehtiin yhdessä työnantajayritykseni Metson kanssa. Tämän kandidaatintyön on tarkoitus toimia esiselvityksenä Metson IAM-prosessien kehittämiselle tulevaisuudessa. Aiheen valintaa tuki myös oma kiinnostukseni tietoturvallisuuteen ja käyttöoikeuksien hallintaan sen osana.

Haluan kiittää ohjaajaani ja kandidaatintyöni tarkastajaa Miikka Palvalinia, jolta sain todella hyvää ohjausta läpi koko kandidaatintyöprojektin. Hänen ansiostaan työni tavoitteet selkenivät ja punainen lanka löytyi aina uudelleen jokaisen ohjaustuokion jälkeen. Lisäksi haluan kiittää työnantajayritystäni Metsoa ja Metsolta erityisesti Kari Nousiaista ja Kari Mikkolaa, joiden kautta sain tutkittavakseni erittäin mielenkiintoisen aiheen. Metsolla tuettiin minua työn aikana paljon ja tulinkin kuluttaneeksi työn kirjoitusvaiheessa paljon Metson Tampereen toimiston kahvikoneen antimia. Haluan kiittää myös samassa seminaariryhmässä olleita kanssaopiskelijoitani, joilta saadusta opponointipalautteesta oli paljon apua. Hanna Tahvanaista haluan kiittää erityisesti avusta lähdeviittausten hionnassa sekä vertaistuesta ja hajoilemisseurasta vaikeina hetkinä. Lisäksi haluan kiittää perhettäni ja Henri Kasurista mittavasta henkisestä tuesta, jota sain heiltä läpi projektin.

Tampereella, 17.4.2019

Laura Karintaus

KESKEISET KÄSITTEET

Seuraavassa listauksessa esitellään ja avataan kandidaatintyössä käytettäviä keskeisiä käsitteitä.

Eheys on tiedon ominaisuus, johon sisältyy tiedon virheettömyys, oikeellisuus ja kattavuus (ISO 27000:2017). Tiedon eheyttä ylläpidetään esimerkiksi tiedon säännöllisillä päivityksillä ja tarkastuksilla sekä sillä, että tietoa ei päästä muokkaamaan ilman lupaa.

IAM eli "Identity access management" tarkoittaa uniikkeihin henkilöiden identiteetteihin perustuvaa käyttöoikeuksien hallintaa (Martin & Waters 2018).

ISO 27000:2017 on kansainvälisen standardoimisliiton (International Organization for Standardization) asettama standardi informaatio- ja turvallisuusteknologioille ja tietoturvallisuuden hallintajärjestelmille (ISO 27000 2017).

IT-osasto on organisaation yksikkö, joka vastaa yrityksen tietohallinnosta, tietotekniikasta ja tietojärjestelmistä sekä näiden ylläpidosta ja kehittämisestä (Sofigate, 2019). Vastaa kaikista tietoja käsittelevistä järjestelmistä, palveluista tai infrastruktuureista ja fyysisistä tiloista, joissa nämä sijaitsevat (ISO 27000:2017).

Käyttöoikeuksien hallinta eli "Access management" tarkoittaa prosesseja ja teknologioita, joita käytetään tiedon käytön rajoittamisessa, luvituksessa ja valvonnassa (Martin & Waters, 2018). Käyttöoikeuksien hallinnalla varmistetaan, että omaisuuteen pääsevät käsiksi vain valtuutetut tahot ja että pääsyä rajoitetaan liiketoiminta- ja turvallisuusvaatimusten perusteella (ISO 27000:2017).

Luottamuksellinen tieto on tietoa, johon luvattomilla henkilöillä, tahoilla tai prosesseilla ei saa olla pääsyä, eikä tietoja luovuteta tällaisille tahoille (ISO 27000:2017). Käsittää kaiken tiedon jonka käyttöä rajoitetaan jollakin tavalla (Yrityksen oma dokumentaatio 2018).

Metatieto on tietoa tiedosta. Se kuvaa, selittää ja paikantaa tietoa sekä helpottaa sen hakemista, käyttämistä ja hallitsemista. (Viljanen 2013-2018) Metatietoa ovat esimerkiksi tiedot tietyn tietoartikkelin omistajasta, luottamuksellisuudesta, sijainnista ja sallituista käyttäjistä.

Politiikka tarkoittaa niitä toimintaperiaatteita, jotka organisaation johto on luonut esittämään organisaation tarkoitusta ja suuntaa (ISO 27000:2017). Politiikassa määritellään tiettyyn organisaation toimintaan, kuten tietoturvaan, liittyvät yhteiset ohjeistukset, joita yrityksen kaikkien toimijoiden tulee noudattaa.

Prosessi tarkoittaa toisiinsa liittyviä tai vaikuttavia toimintoja, jotka muuttavat panokset tuotoksiksi (ISO 27000:2017).

Saatavuus on tiedon ominaisuus, joka tarkoittaa, että valtuutetulla taholla on tarvepohjainen pääsy- ja käyttöoikeus kohteeseen (ISO 27000:2017).

Tiedon luokitus tarkoittaa tietoartikkelille annettavaa arvoa, joka kuvaa sen salaustarvetta ja jonka mukaan sitä käsitellään jatkossa. Esimerkiksi työnantajayrityksessä on käytössä arvot: ”Public”, ”Restricted, ”Confidential” ja ”Secret”. (Yrityksen oma dokumentaatio 2018)

Tietoturvallisuuden johtaminen tarkoittaa järjestelmää ja prosesseja, joilla organisaation tietoturvatoimenpiteitä ohjataan ja valvotaan (ISO 27000:2017).

Tietoturvallisuus tarkoittaa tiedon saatavuuden, eheyden ja luottamuksellisuuden turvaamista. Tietoturvallisuus sisältää ajatuksen myös prosesseista ja politiikoista, joiden avulla sen toteutumiseen voidaan päästä. (Springer 2017)

Tiedon omistaja on henkilö tai taho, joka omistaa tiedon ja on siten vastuussa sen kontrollista ja turvallisuudesta (Whitman & Mattord 2014, s. 535). Tiedon omistaja tekee päätökset liittyen tiedon luokitteluun ja sitä suojaaviin käyttökontrolleihin ja määrittelee tiedon sallitut käyttäjät (Tipton & Krause 2004, s. 721). Tiedon omistaja ohjeistaa tiedon hallitsijaa toimittamaan tekniset ratkaisut tiedon suojelemiseksi tietoturvapolitiikan mukaan (Barman 2001).

Tiedon vartija on henkilö tai taho, joka vastaa niistä säädöksistä ja politiikoista, joiden mukaan yrityksessä organisoidaan ja valvotaan tietoa ja sen käyttöä (Hebbar 2017). Tiedon vartija on vastuussa siitä, millaisia käytäntöjä ja sääntöjä yrityksessä käytetään pääsynhallinnan ratkaisuissa. Tiedon vartijan vastuulla on myös valvoa, että näitä käytäntöjä ja sääntöjä noudatetaan. (Barman 2001)

Tiedon hallitsija on henkilö tai taho, joka toimii operatiivisena osana käyttöoikeuksien hallinnan prosessia. Käyttöoikeuksien hallinnan palveluiden ja prosessien ylläpito, organisointi ja käyttö ovat tämän tahon vastuulla. Tämä taho vastaa tiedon organisoinnista ja järjestelmistä, joita siihen käytetään, mutta hänen vastuullaan ei ole päättää kenelle mitäkin tietoa luvitetaan. Tiedon hallitsijan tulee saada tiedon vartijalta selkeä ohjeistus työnteossa noudatettavista prosesseista ja politiikoista ja tiedon omistajalta tieto siitä, kuka tietoa saa käyttää. (Whitman & Mattord 2011)

SISÄLLYSLUETTELO

TAULUKKOLUETTELO

KUVALUETTELO

1. JOHDANTO

Johdantoluvussa lukija johdatellaan aiheeseen tutkimuksen taustan, lähtökohtien ja perustelujen esittelyllä. Tämän jälkeen esitetään tutkimuskysymykset, jotka tämä tutkimus pyrkii ratkaisemaan. Johdannon lopuksi kerrotaan vielä kandidaatintyön rakenteesta.

1.1 Tutkimuksen tausta, lähtökohdat ja perustelut

Yritykset luovat, käyttävät ja hankkivat monenlaista tietoa, ja erilaisia informaatiotyyppejä tulee kohdella niiden vaatimilla tavoilla. Erilaisia tietoartikkeleita pyritään luokittelemaan niiden luottamuksellisuuden mukaan, jotta niitä voitaisiin suojella tarvittavalla tasolla (Tipton & Krause 2004, s. 715). Suurissa yrityksissä tieto siitä, kenellä pitäisi olla pääsy mihinkäkin tietoon on usein kuitenkin jakautunut ympäri organisaatiota (Bradford et al. 2014). Siispä sillä, kuka näitä käyttöoikeuksia jakaa ja valvoo, on suuri merkitys sille, miten hyvin yritys onnistuu tietoturvallisuuteen ja tehokkuuteen liittyvissä tavoitteissaan.

Käyttöoikeuksien hallinnalla todennetaan, kontrolloidaan ja valvotaan sitä, mitkä käyttäjät saavat käyttää, tarkastella ja muokata mitäkin informaatiota. Käyttöoikeuksien hallinta suurissa yrityksissä on usein haastavaa niiden monimutkaisen ja monimuotoisen informaatioarkkitehtuurin vuoksi. (Bradford et al. 2014) Käytössä on paljon erilaisia järjestelmiä, joissa kaikissa on ylläpidettävää ja valvottavaa tietoa. Käyttöoikeuksien hallinnan pääasiallisena tehtävänä on huolehtia tietoturvallisuudesta estämällä tiedon luvaton käyttö. Lisäksi käyttöoikeuksien hallinta palvelee yrityksen toiminnan tehokkuutta, kun yrityksen työntekijöille pyritään tarjoamaan pääsy heidän tarvitsemaansa tietoon mahdollisimman sujuvasti (Bradford et al. 2014).

Käyttöoikeuksien hallinnan systeemin, eli IAM-systeemin, organisointi yrityksissä koostuu IAM-politiikasta, IAM-prosesseista ja niissä käytettävistä teknologiosta (Whitman & Mattord 2011). Käyttöoikeuksien hallinnan politiikka määrittelee ne säännöt, joiden mukaisesti tietoa luokitellaan ja käyttöoikeuksia jaetaan erityyppisiin tietoartikkeleihin (Whitman & Mattord 2014). Prosesseilla tarkoitetaan niitä päätösten, tehtävien ja teknologisten toimintojen sarjoja, joita tiedon käyttöoikeuksien kontrolloinnissa ja jakamisessa käytetään (esimerkiksi tiedon luokittelu ja autorisointi) (Whitman & Mattord 2011, ss. 421-422). Politiikan ja prosessien onnistunut toteutuminen vaatii sitä, että yrityksen työntekijöiden vastuut ja roolit prosessien ja politiikan toteuttamisessa on suunniteltu ja ohjeistettu (Barman 2001, s. 26).

Tämän kandidaatintyön aiheena on luottamuksellisen tiedon käyttöoikeuksien hallinnan johtaminen suuressa yrityksessä. Työssä perehdytään luottamuksellisen tiedon käyttöoikeuksien hallinnan prosessiin ja sitä ohjaavaan tietoturvapolitiikkaan sekä prosessin roolien- ja vastuunjakoon. Aihe tähän kandidaatintyöhön valikoitui yhdessä kirjoittajan työnantajayrityksen kanssa. Yrityksen näkökulmasta kandidaatintyö on esiselvitys uusien käyttöoikeuksien hallinnan prosessien muodostamiselle. Tavoitteena on, että tutkimuksesta saatuja tuloksia voidaan hyödyntää tulevaisuuden toiminnan suunnittelussa.

Tämän kandidaatintyön tavoitteena on ratkaista, miten suuressa yrityksessä voidaan johtamisen avulla varmistaa, että vain oikeilla ihmisillä on pääsy informaatioon. Aiemmin työnantajayrityksen toiminta on perustunut pitkälti paikallisiin järjestelmiin, joiden pääsynhallinta on hoidettu lokaalisti. Yrityksellä on useita eri liiketoiminta-alueita, jotka toimivat toisistaan hyvinkin irrallaan osittain omissa järjestelmissään. Yrityksen IT-osasto palvelee kuitenkin näitä kaikkia samaan aikaan pyrkien huolehtimaan sekä tietoturvan että operatiivisen tehokkuuden varmistamisesta. Nyt toiminta on kehittymässä siihen suuntaan, että kaikki yrityksen työntekijät ympäri maailmaa käyttävät samoja järjestelmiä ja työskentely siirtyy pitkälti globaaleihin virtuaalitiimeihin. Tämä aiheuttaa usein haasteita, sillä tietohallinnossa ei voida tietää, kenen tulee saada käyttää mitäkin tietoa, kun käyttäjiä on tuhansia ja he sijaitsevat eri puolilla maailmaa. Samalla myös hallittavan tiedon määrä lisääntyy digitalisaation myötä, joten kysymys siitä, kuka voi käyttää mitäkin informaatiota ja miksi, korostuu entisestään. Prosessin piirissä toimivien tahojen toimintaympäristö laajenee ja monimutkaistuu jatkuvasti ja siksi on erityisen tärkeää tutkia juuri prosessin vastuun ja roolien jakamista.

1.2 Tutkimusongelma ja rajaukset

Tärkeimpänä tutkimusongelmana ja päätutkimuskysymyksenä tässä kandidaatintyössä on:

- **Miten luottamuksellisen tiedon käyttöoikeuksien hallintaa voisi suuressa yrityksessä johtaa?**

Tätä kysymystä voidaan tarkastella monesta eri näkökulmasta, mutta tässä työssä keskitytään erityisesti tietoturvallisuuteen ja prosessin ja sen piirissä toimivien ihmisten johtamiseen. Tarkoituksena on tutkia etenkin sitä, millaisia rooleja ja vastuunjakoja luottamuksellisen tiedon käyttöoikeuksien hallinnassa kannattaisi hyödyntää. Olennaista on pohtia erityisesti sitä, kuka valvoo mitäkin tietoa ja kuka on vastuussa tiedon käytöstä. Kandidaatintyössä pyritään tunnistamaan sellainen toimintamalli, jota noudattamalla yrityksen tiedonkulku on mahdollisimman joustavaa ja tehokasta, mutta tietoa ei kuitenkaan päädy vääriin käsiin. Päätutkimuskysymykseen vastataan tutkimuksen viidennessä luvussa.

Päätutkimuskysymys jakautuu useampaan alatutkimuskysymykseen. Vastaamalla näihin kysymyksiin luodaan konteksti ja perustelut päätutkimuskysymykseen vastaamiselle. Seuraavassa listauksessa esitellään alatutkimuskysymykset ja kerrotaan missä vaiheessa kandidaatintyötä niihin vastataan.

- **Miten luottamuksellisen tiedon käyttöoikeuksia hallitaan?**
- **Millaisia rooleja ja vastuita liittyy luottamuksellisen tiedon käyttöoikeuksien hallintaan?**

Ensimmäinen alakysymys perehtyy luottamuksellisen tiedon käyttöoikeuksien hallintaan. Tähän kysymykseen vastaamisen tavoitteena on selittää millaisilla keinoilla luottamuksellisen tiedon käyttöoikeuksien hallintaa tehdään erityisesti johtamisen näkökulmasta. Kysymykseen vastataan tämän kandidaatintyön kolmannessa luvussa. Käyttöoikeuksien hallinta on hyvin tekninen prosessi, johon liittyy monia tietoteknisiä komponentteja ja palveluita. Pääsynhallinnan järjestelyitä ovat esimerkiksi kulunvalvonta, varmenteet, asiakirjojen säilytys ja jako sekä tietojen salaus (Bradford et al. 2014). Kuitenkin käyttöoikeuksien hallinnassa on pitkälti kyse myös yrityksessä käytettävistä tiedon jakamisen politiikoista ja siitä, miten vastuu eri palveluiden käyttöoikeuksien hallitsemisesta on jaettu. Tässä kandidaatintyössä ei käsitellä valittavia teknologioita tai niiden käyttöä, sillä aihetta halutaan tarkastella erityisesti johtamisen näkökulmasta. Ensimmäiseen tutkimuskysymykseen vastataan tutkimalla käyttöoikeuksien hallinnan toteuttamiseen käytettäviä prosesseja ja tiedon käsittelyä ohjaavaa tietoturvapolitiikkaa etenkin luottamuksellisen tiedon näkökulmasta.

Toinen alakysymys keskittyy käyttöoikeuksien hallinnan piirissä työskenteleviin ihmisiin ja heidän vastuisiinsa. Tähän kysymykseen vastataan kandidaatintyön neljännessä luvussa. Käyttöoikeuksien hallinta on koko yrityksen läpileikkaava toiminto, joka koskettaa jokaista yrityksen työntekijää (Bradford et al. 2014). Siksi prosessin onnistumisessa ja politiikkojen noudattamisessa erittäin suuri rooli on myös jokaisella yksilöllä, jonka vastuulla jokin osa prosessia on. Tästä syystä toimintaa suunniteltaessa on erittäin tärkeää, että eri tahojen työtehtävät ja vastuualueet määritellään tarkkaan (Barman 2001, s. 26). Tässä kandidaatintyössä keskitytään ihmisten johtamisen osalta erityisesti vastuunjakoon ja toiminnan johtamismalliin. Vastuita tarkastellaan etenkin tietoturvallisuuden toteutumisen näkökulmasta. Tämä tutkimus ei kuitenkaan keskity siihen, miten prosessit ja politiikka implementoidaan osaksi ihmisten jokapäiväistä toimintaa. Tutkimustuloksena saadun johtamismallin käyttöönotto voisi kuitenkin olla mahdollinen jatkotutkimusaihe.

1.3 Tutkimuksen rakenne

Johdannon jälkeen tutkimuksen toisessa luvussa esitellään tutkimuksessa käytetty tutkimusmenetelmä ja tutkimusaineisto. Kolmas luku aloittaa aiheen varsinaisen käsittelyn. Luvun alussa perehdytään luottamukselliseen tietoon yrityksessä ja tiedon luokitteluun. Sen jälkeen perehdytään yrityksen käyttöoikeuksien hallinnan prosessiin ja prosesseja ohjaavaan tietoturvallisuuspolitiikkaan. Neljännessä luvussa perehdytään erilaisiin toimijoihin, joita käyttöoikeuksien hallinnan piiriin kuuluu ja eritellään heidän tehtäviään ja vastuitaan. Myös toimijoiden välisiä suhteita arvioidaan.

Viidennessä luvussa esitellään tutkimuksesta saadut tulokset ja niiden perusteella muodostettu luottamuksellisen tiedon käyttöoikeuksien hallinnan johtamismalli. Lopuksi yhteenvetoluvussa arvioidaan tutkimuksen onnistumista ja tutkimustulosten merkitystä ja hyödyntämismahdollisuuksia.

2. TUTKIMUSMENETELMÄN JA -AINEISTON ESITTELY

Kandidaatintyön tutkimusmenetelmänä on kirjallisuuskatsaus. Tavoitteena oli löytää kirjallisuudesta ja alaan liittyvistä ohjeistoista kattavaa perustietoa siitä, miten käyttöoikeuksien hallintaa tulisi organisoida yleisellä tasolla, ei organisaatiospesifisti. Aineistoja analysoitiin pitkin kandidaatintyötä, ja lopullisessa tulosvaiheessa päätelmät saatiin vertailemalla eri tutkimusaineistoja toisiinsa. Aineistojen analysoinnissa ja tutkimuksen suunnittelussa hyödynnettiin Tampereen teknillisen yliopiston Kalle Vaismaan (2009) tukipakettia opinnäytetöiden tutkimusprosessiin.

Tietoa etsittiin Tampereen yliopiston kirjaston tarjoamista tiedonhakupalveluista, kuten kirjastosta ja verkkoarkistoista. Verkosta löydetyt tutkimusaineistot tallennettiin RefWorks-palveluun, jonka avulla kerättyjä lähdeaineistoja hallinnoitiin työn edetessä. Tiedonhankintapalveluista hyödynnettiin Scopus-, Andor-, Science-direct -hakukoneita ja Tunilib-tietokantaa. Koska tutkimusalaan liittyvä aineisto on hyvin usein englanninkielistä, tietoa haettiin pääasiassa englanniksi. Tutkimuksessa hyödynnetyistä artikkeleista suurin osa löydettiin hakusanoilla ”Identity access management” ja "Identity access management" AND ”confidential”. Tärkeimmäksi hakukoneeksi valikoitui lopulta Tunilib-tietokanta, sillä sieltä löytyi eniten hyödyllistä aineistoa. Aiheen ja tutkimuskysymysten pohjustamisessa hyödynnettiin myös kirjoittajan omaa työelämässä hankittua tietoa käyttöoikeuksien hallinnasta. Kaikki tutkimusaineistona hyödynnetyt kirjat saatiin Tampereen yliopiston käyttöoikeuksien hallintaan perehtyneeltä tutkijalta. Käsitemäärittelyissä hyödynnettiin myös tietoturvallisuusalan yritysten verkkosivuilta saatua tietoa.

Taulukossa 1 esitellään tiedonhaun alkuvaiheessa hyödynnettyjä hakusanoja ja niillä eri tietokannoista saatujen osumien määriä. Hakutulokset on rajattu koskemaan tieteellisiä ja vertaisarvioituja artikkeleita, jotka ovat saatavilla verkossa kokonaisuudessaan. Ensimmäisiä hakuja tehtäessä aihetta ei oltu vielä rajattu koskemaan erityisesti luottamuksellisen tiedon käsittelyä. Taulukossa 2 on hakutuloksia täsmentyneemmillä hakusanoilla siinä vaiheessa, kun tutkimusaihe ja -kysymykset olivat jo tarkentuneet lopulliseen muotoonsa.

Taulukko 1. *Eri hakulauseilla tietokannoista saadut osumat tutkimusprojektin alkupuolella*

Hakulause	Scopus	Andor	Tunilib-tietokanta	Science-direct
"Identity access management"	4	68	420	78
"Identity access management" AND "security"	3	62	1	73
"Access management" AND "security"	127	1791	2797	1190
"Identity access management" AND "guideline"	1	11	16	9

Taulukko 2. *Eri hakusanoilla tietokannoista saadut osumat tutkimusprojektin loppupuolella*

Hakulause	Scopus	Andor	Tunilib-tietokanta	Science-direct
"IAM" AND "responsibilities	2	3639	984	235
"Identity access management" AND "confidential"	6	9	80	0

Kuten taulukoista 1 ja 2 nähdään, aiheeseen liittyvää aineistoa oli tarjolla melko paljon. Aiheen kannalta täysin irrelevanttia aineistoa löytyi kuitenkin taulukoissa esitetyillä hakusanoilla paljon, etenkin tutkimuksen alkuvaiheessa. Hakusanojen täsmentäminen aiheen täsmentyessä auttoi jo paljon. Työssä hyödynnettävien lähteiden valinnassa oltiin kriittisiä. Aineistojen valinnassa arvioitiin tutkimustiedon tuoreutta, luotettavuutta ja relevanttiutta aiheen kannalta. Suurimmaksi haasteeksi tutkimusaineistojen valinnassa osoittautui tiedon riittävän tuoreuden arvioiminen. Todella suuri osa aineistoista rajautui pois myös käyttöoikeuksien hallintaan liittyvissä aineistoissa hyvin usein käytetyn erittäin teknologialähtöisen tarkastelunäkökulman vuoksi.

Kirjallisuustutkimus keskittyi lopulta erityisesti tietoturvallisuusalan kirjoihin, joista löytyi perustietoa kaikkien käsittelylukujen taustaksi. Kirjat käsittelivät yrityksen tietoturvallisuuden johtamista kokonaisvaltaisesti useammista eri näkökulmista. Nämä kirjat valittiin, koska niistä löytyi erittäin kattavasti tietoa käyttöoikeuksien hallinnan eri-osa-alueista. Ne myös käsittelivät kaikkia asioita erityisesti tietoturvallisuuden näkökulmasta, mikä oli tässä tutkimuksessa erityisen tärkeää. Kirjoja ei luettu kannesta kanteen, mutta niistä löytyneet aiheen kannalta relevantit luvut luettiin kokonaan.

Tutkimusaineiston kirjoista vanhin, Scott Barmanin ”Writing Information Security Policies” (2001), oli suuressa roolissa etenkin vastuu- ja roolikysymysten tutkimisessa. Teos on jo suhteellisen vanha, joten sen ajankohtaisuutta tuli arvioida kriittisesti. Kirjasta löytyi kuitenkin aiheeseen liittyvää tietoa erittäin kattavasti, ja vaikutti kuitenkin siltä, että tieto oli linjassa myös uudemman kirjallisuuden kanssa. Teknologiaan ja digitalisaatioon liittyvä kirjallisuus vanhenee yleensä hyvin nopeasti, mutta tutkimusta tehtäessä arveltiin, että ihmisten vastuisiin ja johtamiseen liittyvä tieto pysyy ehkä relevanttina hieman pidempään.

Koska osa käytetyistä kirjoista oli hieman vanhempia, niiden rinnalla haluttiin käyttää tietoa tuoreemmista tieteellisistä artikkeleista. Artikkelien läpikäynti aloitettiin silmäilemällä läpi noin parikymmentä artikkelia, jotka vaikuttivat otsikon ja tiivistelmän perusteella sopivilta. Näistä valittiin tutkimuksessa käytettäväksi noin viisi parhaalta vaikuttavaa artikkelia. Hyödynnettäviksi valittiin sellaisia mahdollisimman tuoreita artikkeleja, jotka käsittelivät käyttöoikeuksien hallintaa teknisen tarkastelun sijaan erityisesti johtamisen ja tietoturvallisuuden näkökulmista. Erityisesti Bradford et al. (2014) artikkeli oli hyödyllinen, sillä siinä tarkasteltiin käyttöoikeuksien hallinnan systeemiä kokonaisuutena ja suuren yrityksen kontekstissa. Artikkeleista löytyi erityisen hyvin tietoa erilaisista käyttöoikeuksien hallinnan prosesseista ja organisointitavoista. Näissä käsiteltiin asioita hyvin teknisestä näkökulmasta, joten hallinnollisen näkökulman löytäminen oli hieman haasteellisempaa. Vastuunjakokysymyksiin liittyvää tietoa oli vaikeaa löytää tuoreista artikkeleista, mutta siihen liittyviä kirjoja löydettiin monta. Artikkeleihin tutustuttaessa huomattiin, että erityisesti aiheen teknisempään tarkasteluun olisi todennäköisesti löytynyt huomattavasti enemmän tuoretta tietoa. Vaikuttaisikin siltä, että alan tutkimus keskittyy tällä hetkellä enemmän prosessien ja teknologisten ratkaisujen tarkasteluun kuin ihmisten organisointiin. Muutamasta teknispainotteisesta artikkelista löydettiin kuitenkin työssä hyödynnettäväksi käyttöoikeuksien hallintaan liittyviä haasteita.

Tieteellisten kirjojen ja artikkelien lisäksi työssä hyödynnettiin kansainvälistä tietoturvallisuuteen liittyvää ISO-27000:2017 -standardia, jonka tarkasteleminen oli mahdollista Tampereen yliopiston tarjoaman SFS Online -portaalin avulla. Standardista saatiin paljon tietoa vaatimuksista ja tavoitteista, joita yrityksen käyttämän käyttöoikeuksien hallinnan systeemin tulee vähintään täyttää. Standardin käytössä tutkimuslähteenä oli se hyvä puoli, että siinä käsiteltiin valittavien toimintatapojen ja sääntöjen merkitystä hyvin laajasti. Lisäksi standardin merkitys tunnistetaan hyvin laajasti kansainvälisestikin, kun lukuisat yritykset ympäri maailmaa pyrkivät toimimaan sen asettamien tavoitteiden mukaisesti. Siksi on perusteltua, että myös tämän tutkimustyön tuloksena koottavan johtamismallin rakentamisessa hyödynnetään tätä standardia. (ISO 27000:2017)

3. LUOTTAMUKSELLISEN TIEDON KÄYTTÖOIKEUKSIEN HALLINTA

Luottamuksellisen tiedon käyttöoikeuksien hallinnalla kontrolloidaan ja valvotaan tiedon käyttöä ja määritellään, minkä sääntöjen ja toimintatapojen mukaisesti käyttöoikeuksia annetaan käyttäjille (Bradford et al. 2014). Tämän luvun tavoitteena on perehtyä syvällisemmin tutkimuksen ensimmäiseen alatutkimuskysymykseen: Miten luottamuksellisen tiedon käyttöoikeuksia hallitaan? Aluksi perehdytään luottamukselliseen tietoon ja sen luokitteluun, minkä jälkeen perehdytään yrityksen käyttöoikeuksien hallinnan politiikasta ja prosesseista koostuvaan IAM-systeemiin. Aiheita tarkastellaan erityisesti suuren yrityksen kontekstissa.

Kolmannen luvun tärkeimpinä tutkimusaineistoina toimii ISO 27000:2017-standardi ja Whitmanin ja Mattordin (2011; 2014) sekä Tiptonin ja Krausen (2004) ohjekirjat tietoturvallisuuden johtamiseen. Näistä saadun pohjatiedon vastapainoksi on nostettu uutta tietoa tuoreemmista artikkeleista.

3.1 Tiedon luokittelu ja luottamuksellinen tieto organisaatiossa

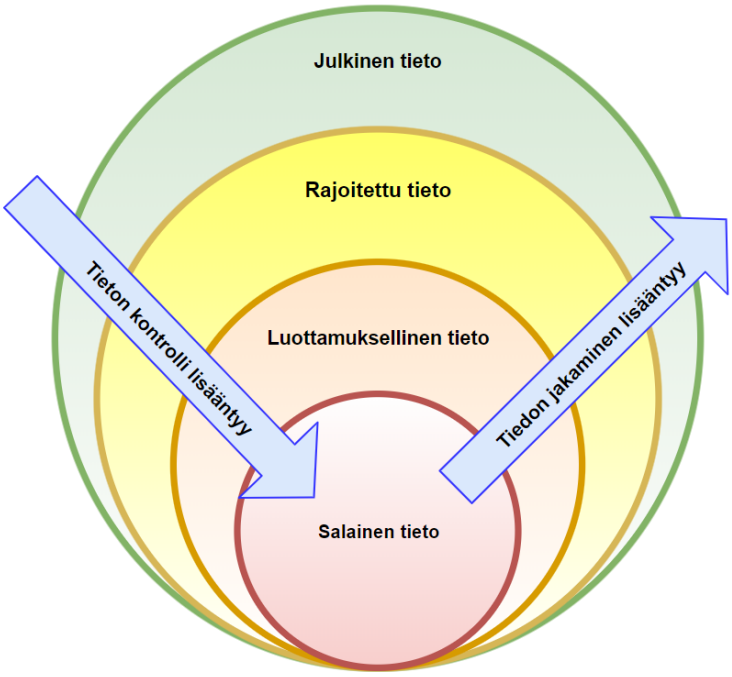
Kaikki yritykset keräävät, käsittelevät, säilyttävät ja välittävät monenlaista tietoa. ISO 27000:2017-standardi toteaa, että tieto ja siihen liittyviä prosesseit, järjestelmät, verkot ja työntekijät ovat yrityksille arvokasta suojattavaa omaisuutta, jonka avulla yrityksen tavoitteet saavutetaan. Tähän omaisuuteen kohdistuu monia riskejä, jotka voivat jollain tavalla uhata yritystä, sen ihmisiä tai lliiketoimintaa. Tieto-omaisuutta pyritään suojelemaan näiltä uhilta tietoturvallisuuden hallinnan keinoin. (ISO 27000:2017) Yksi näistä keinoista on tiedon jakaminen luottamuksellisuusluokkiin niiden suojaustarpeen mukaan.

Tietoa luokitellaan luottamukselliseksi käyttäen tiedon ominaisuuksiin perustuvia mittareita. Eri tietoresurssien käyttötarkoitukset, arvo ja liiketoimintaan kohdistuvat riskit yritykselle ovat keskenään hyvin erilaisia (Tipton & Krause 2004, s. 715). Tiedon luottamuksellisuusluokittelulla pyritään määrittelemään kunkin tiedon salattavuustarve ja tarvittavat suojauskeinot (Whitman & Mattord 2011, s. 430). Luottamuksellisen tiedon suojelemisella varmistetaan, että tietoon pääsevät vain sellaiset tahot, joilla on siihen liiketoiminnallinen tarkoitus ja annettu käyttöoikeus (Whitman & Mattord 2011, s. 478). Tiedon luokittelulla pyritään myös ohjaamaan tiedon suojelemiseen käytössä olevat resurssit sinne, missä niitä eniten tarvitaan, ja parantamaan tiedon käsittelyyn liittyvää päätöksentekoa (Tipton & Krause 2004, s. 715).

Joskus tiedon arvo saadaan sen saatavuuden kautta. Tällöin käyttöoikeuksien hallinta pyritään toteuttamaan niin, että tietoa tarvitseva taho saa tiedon käyttöönsä

mahdollisimman joustavasti ja tehokkaasti. Kuitenkin esimerkiksi todella salaisen tiedon kohdalla tietoturvallisuus ja käyttöoikeuksien jakamisen täsmällisyys on usein joustavuutta tärkeämpää. Tiedon luokittelu on tiedon arvon määrittelyä, riskienhallintaa ja tasapainoilua saatavuuden ja riittävän suojan välillä (Tipton & Krause 2004, ss. 715-719). Tiedon analysoiminen useammilla eri mittareilla auttaakin yritystä luokittelemaan tietoa ja asettamaan sen käytölle kontrolleja juuri sen tyyppiselle tiedolle toimivimmalla tavalla.

ISO 27000:2017-standardi määrittelee luottamuksellisen tiedon tarkoittavan yrityksen kaikkea sellaista tieto-omaisuutta, johon luvattomilla henkilöillä, tahoilla tai prosesseilla ei saa olla pääsyä, ja siksi sen käyttöä rajataan jollakin tavalla. Suojattavaa tieto-omaisuutta voivat olla esimerkiksi taloudellinen tieto, aineeton omaisuus, työntekijöiden henkilötiedot ja asiakkaiden tai kolmansien osapuolten organisaatiolle antamat tiedot. (ISO 27000:2017) Luottamuksellinen tieto voi jakautua useampaan alalajiin sen perusteella, kuinka paljon sen käyttöä on tarpeen rajata. Esimerkki tiedon luokitushierarkiasta on kohdeyrityksen käytössä oleva luokitus salaisuusjärjestyksessä: salainen tieto, luottamuksellinen tieto ja rajoitettu tieto (Yrityksen oma dokumentaatio 2018). Tämä on yksi arviointiasteikko monien joukossa, ja sama luokitusjärjestelmä ei todennäköisesti sovi kaikkiin yrityksiin. Olennaista tiedon luokittelussa on se, että yritys määrittelee itselleen sopivan arviointiasteikon, jonka mukaan se voi määritellä omat tietoresurssinsa mahdollisimman yksiselitteisesti. Kuvassa 1 on esitettynä esimerkki tiedon luottamuksellisuusluokittelusta. Nuolet kuvaavat sitä, miten tiedon kontrollointitarve kasvaa sen salaisuusasteen mukana ja sitä miten tiedon jakaminen korostuu vähemmän salaisen tiedon suuntaan mentäessä.

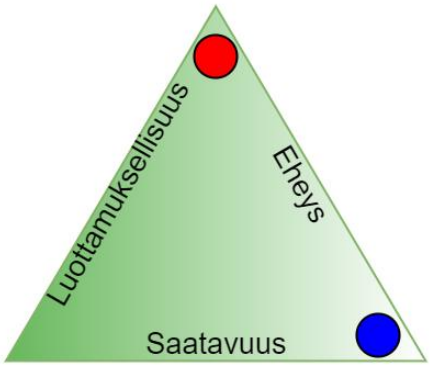


Kuva 1. *Tiedon luottamuksellisuusluokituksen yhteys tiedon jakamiseen ja kontrollointiin (Yrityksen oman dokumentaation 2018 pohjalta)*

Tiptonin ja Krausen (2004) mukaan tiedon luokittelusääntöjen tulee olla osa yrityksen tietoturvallisuuspolitiikkaa, ja politiikan tulee määrittää kaikki kriteerit, joiden mukaan tietoa luokitellaan. Politiikan tulee esittää jokaisen tietoluokan kuvaus, kuhunkin luokkaan kuuluvan tiedon suojelemiseen liittyvät vähimmäisvaatimukset sekä roolit ja vastuut, joita tiedon käsittelyyn ja politiikan käytännön toteutukseen liittyy. Tiedon käsittelyn vaatimusten tulee käsittää tiedon koko elinkaari ja olla yhtenäisiä sen luomisesta tallentamiseen ja tiedon tuhoamiseen. (Tipton & Krause 2004, s. 717) Tietoa käsitellään sen elinkaaren aikana monissa järjestelmissä ja monien henkilöiden toimesta, joten on todella tärkeää, että samoja luokittelusääntöjä noudatetaan kaikissa järjestelmissä.

Tipton ja Krause (2004) esittävät työkaluksi tiedon luokitteluun tiedon käytön liiketoiminnallisten riskien analyysin. Analyysiä varten tulee selvittää, mitä uhkia esimerkiksi tiedon luottamuksellisuuteen, saatavuuteen tai yhtenäisyyteen liittyy. Käytännössä tämä tarkoittaa sitä, että määritellään, mitä seurauksia esimerkiksi tiedon menettämisellä olisi suoraan yrityksen liiketoiminnalle, esimerkiksi laillisista tai kilpailullisista syistä. Joissain tilanteissa puolestaan riskejä syntyy, jos tarvittavaa tietoa ei saada riittävän nopeasti. (Tipton & Krause 2004, s. 718) Luottamuksellisen tiedon luovuttaminen useampien tahojen käsiin on aina riski, mutta tietoa luokiteltaessa on tehtävä päätökset siitä, mitä riskejä voidaan ottaa tiedon saatavuuden kustannuksella.

Myös puutteet tiedon eheydessä voivat aiheuttaa tietoturvallisuusriskejä. Eheydellä tarkoitetaan tiedon oikeellisuutta, virheettömyyttä ja kattavuutta (ISO 27000:2017). Esimerkiksi sellainen tilanne, jossa yrityksen tieto omista aktiivisista työntekijöistään on vanhentunutta tai muuten virheellistä, aiheuttaa tietoturvallisuusriskin. Tällöin käyttöoikeuksia saattaa jäädä sellaisille henkilöille, joilla ei enää sellaisia kuuluisi olla. Tiedon luottamuksellisuuden, eheyden ja saatavuuden suhdetta toisiinsa voidaan kuvata CIA-kolmiolla (engl. Confidentiality, integrity, availability) (Rouse, 2014). Kolmio havainnollistaa, kuinka esimerkiksi tiedon luottamuksellisuus voi heikentyä korkeamman saatavuuden suuntaan siirryttäessä (Phoenix TS 2012). CIA-kolmio on esitettynä kuvassa 2. Punainen ympyrä on esimerkki tietoartikkelista, jonka kohdalla on erityisen tärkeää pitää huolta tiedon oikeellisuudesta ja salassapidosta. Tällaisia tietoartikkeleja voivat olla esimerkiksi yrityksen jättämät tarjoukset, jotka eivät saa päätyä kilpailijoiden käsiin. Sinisen ympyrän kuvaaman tiedon kohdalla on tärkeää, että tieto on virheetöntä ja helposti saatavilla. Tällaista tietoa voisi olla esimerkiksi sellaisten henkilöiden yhteystiedot, joita tarvitaan hätätilanteissa nopeasti.



Kuva 2. *CIA-kolmio: Luottamuksellisuuden, saatavuuden ja eheyden välinen suhde (Rouse 2014 pohjalta)*

Tipton ja Krause (2004) näkevät tiedon onnistuneesta luokittelusta ja sitä kautta kontrolloinnista yritykselle paljon suoria hyötyjä. Suunnitelmallisesti asetetut kontrollit lisäävät tiedon luottamuksellisuutta, eheyttä ja saatavuutta. Kun kriittinen suojattava tieto erotetaan vähemmän kriittisesti tiedosta, tiedon suojaamiseen käytössä olevat resurssit, kuten henkilöstö- ja raharesurssit, voidaan hyödyntää siellä missä niitä eniten tarvitaan. Kun kaikkialla yrityksessä käytetään ja tunnistetaan yhteisiä toimintatapoja ja periaatteita, on myös niiden mukaisesti tehdyt päätökset yleensä laadukkaampia. (Tipton & Krause 2004).

3.2 Käyttöoikeuksien hallinnan systeemi

Käyttöoikeuksien hallinta on erittäin kriittinen osa yrityksen tietoturvallisuutta, koska sillä määritellään ne säännöt ja toimintatavat, joilla sen tietoresursseihin päästään käsiksi (Whitman & Mattord 2011, s. 433). Käyttöoikeuksien hallinta on suuri osa yritysten tietohallinnon infrastruktuuria ja sen prosessit läpileikkaavat yrityksen kaikkia toimintoja. Bradford et al. (2014) mukaan suurissa ja keskisuurissa yrityksissä on perinteisesti käytössä käyttäjien uniikkeihin identiteetteihin perustuva ”IAM” (Identity Access Management) infrastruktuuri. Uusia IAM-prosesseja ja -infrastruktuureja implementoidaan yritysten käyttöön jatkuvasti ja niiden tavoitteena on luoda entistäkin turvallisempia ja määräystenmukaisempia kokonaisuuksia. (Bradford et al. 2014)

IAM-systeemi on osa ISO 27000:2017-standardin määrittelemää yrityksen tietoturvallisuuden hallintajärjestelmää, jolla organisaation tietoturvatoimenpiteitä ohjataan ja valvotaan. Hallintajärjestelmän avulla luodaan politiikat ja tavoitteet, sekä prosessit, joilla nämä organisaation tietoturvallisuuteen liittyvät tavoitteet saavutetaan. (ISO 27000:2017) Hummer et al. (2016) mukaan yritysten käyttöoikeuksien hallinnan systeemi rakentuu yleensä kolmen peruspilarin varaan. Näitä peruspilareita ovat yrityksen IAM-politiikka, -prosessit ja -teknologiat. (Hummer et al. 2016) Koska IAM-teknologiat on rajattu tästä tutkimuksesta ulos, keskitytään seuraavaksi tarkastelemaan käyttöoikeuksien hallintaan liittyvää politiikkaa ja prosesseja.

3.2.1 Käyttöoikeuksien hallintaa ohjaava politiikka

Käyttöoikeuksien hallintaan valittavia käytäntöjä ja niiden toteuttamiseen kohdistuvia vaatimuksia ohjaa yrityksen IAM-päätöksenteko. IAM-systeemiin liittyvien päätösten perustana toimii yrityksen tietoturvatavoitteiden ja -vaatimusten määrittelyn pohjalta rakennettu tietoturvapolitiikka. ISO 27000:2017-standardin mukaan politiikan tavoitteena on koordinoida ja yhdistää yrityksen prosesseja ja toimintoja näiden tavoitteiden ja vaatimusten täyttämiseksi. Rakentamalla kaikki yrityksen järjestelmät kattavan ja kaikkia yrityksen toimintoja ja liiketoimintaa palvelevan tietoturvallisuuspolitiikan yritys voi määritellä ja toteuttaa tieto-omaisuutensa suojaamisen perusedellytykset. (ISO 27000:2017)

Yrityksillä on yleensä käytössään useita eri tasoisia politiikkoja ja ohjeistuksia. Tasot eroavat toisistaan käsittelyn laajuuden ja yksityiskohtaisuuden osalta. Esimerkiksi työnantajayrityksessä käytössä on kolmen tason ohjeistuksia. Kaikista laajimman tason ohjeistukset ovat politiikkoja ja hieman yksityiskohtaisemmat ”guidelinet” eli suuntaviivat ovat hieman yksityiskohtaisempia. Näiden lisäksi on vielä yksityiskohtaisempia tiettyihin toimintoihin keskittyneitä ohjeistuksia (Yrityksen oma dokumentaatio 2018). Tässä kandidaatintyössä käytetään kuitenkin yksinkertaistamisen vuoksi sanaa politiikka kuvaamaan kaikentasoisia ohjeistuksia.

Kun yritys luokittelee tietoa ja luo IAM-prosessejaan, tulisi kaikkien päätösten ja käytäntöjen pohjautua yrityksen tietoturvallisuuspolitiikkaan. Käyttöoikeuksien hallinnan politiikka, eli IAM-politiikka, on se osa yrityksen tietoturvapolitiikkaa, jossa määritellään yrityksen säännöt ja vaatimukset liittyen käyttöoikeuksien hallintaan. Whitman ja Mattord (2011) määrittelevät, että politiikan tavoitteena on varmistaa, että kaikkia tietotyyppejä suojellaan ja jaetaan juuri näiden luottamuksellisuustasolle sopivilla keinoilla. Barman (2001) puolestaan korostaa, että politiikoissa tulisi määritellä myös yrityksen eri tahojen ja henkilöiden tietoturvallisuuteen ja käyttöoikeuksien hallintaan liittyvät vastuut. Tämä on kannattavaa, koska pelkillä toimivilla teknisillä komponenteilla tai prosesseilla ei voida vielä taata, että liiketoiminnan ja tietoturvallisuuden tavoitteet käyttöoikeuksien hallinnalle saavutetaan. IAM-systeemi rakentuu sen parissa toimivien ihmisten varaan ja siksi heidän merkityksensä kannattaa tunnistaa jo toimintaa suunniteltaessa ja sitä ohjaavia sääntöjä asetettaessa. (Barman 2001, s. 26)

Barman (2001) toteaa myös, että tietoturvallisuuspolitiikkojen rakentamisessa on tärkeää, että ne laaditaan tukemaan yrityksen liiketoimintaa. Jos politiikan vaatimat toimintatavat tai vastuunjaot estävät tai merkittävästi hidastavat yrityksen tekemää liiketoimintaa, sitä ei todennäköisesti noudateta. Tästä syystä on erittäin tärkeää, että politiikkaa valmistelemassa on sellaisia henkilöitä, jotka tuntevat yrityksen liiketoiminnan ja sen tarpeet tiedon käytölle (Barman 2001, s. 11) Kuten luvussa 3.1 kävi ilmi, tiedon käsittelyyn liittyy vahvasti myös riskienhallinta. Vaikka tietoturvallisuus toteutuukin parhaiten kontrollien määrää ja vahvuutta lisäämällä, ei maksimaalisen kontrollimäärän

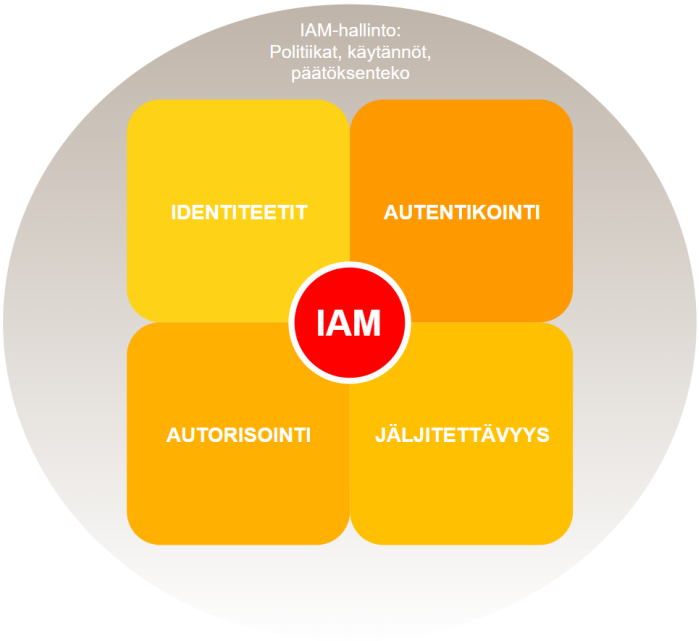
asettaminen kuitenkaan ole aina tarkoituksenmukaista. IAM-politiikkaa rakennettaessa täytyy tietää, minkälaisia riskejä voidaan ottaa tiedon saatavuuden ja matalampien kontrolloimisesta syntyvien kustannusten vuoksi. Politiikan tulee antaa tiedon käsittelyyn niin hyvät ohjeet, että yrityksen työntekijöiden ei tarvitse tehdä riskienhallinnallisia päätöksiä (Tipton & Krause 2004).

Whitmanin ja Mattordin (2011) mukaan tiedon käyttöoikeuksien hallintaan käytettävien kontrollien asettamisen tulee yrityksen kaikissa järjestelmissä perustua IAM-politiikkaan. Politiikka määrittelee miten eri käyttäjille ja käyttäjäryhmille annetaan pääsyjä tietoartikkeleihin. Rakennettavan IAM-politiikan täytyy olla sellainen, että sitä voidaan noudattaa yhtä hyvin kaikissa yrityksen IAM-infrastuktuurin osissa. Vaikka prosessit ja teknologiat ovat erilaisia, on erittäin tärkeää, että tietoa käsiteltäessä kaikkialla yrityksessä noudatetaan samoja sääntöjä ja yhtä tarkasti. (Whitman & Mattord 2011, s. 433) Esimerkiksi tiedon luottamuksellisuusluokittelu ei voi olla järjestelmäkohtainen. Tilanne, jossa kaikkiin järjestelmiin luodaan oma luokitusjärjestelmä aiheuttaa ongelmia esimerkiksi silloin, kun tietoa siirretään järjestelmästä toiseen. Politiikan toteutumista koko kompleksisessa IAM-infrastruktuurissa täytyy valvoa, sillä politiikkojen implementoiminen näin suuren systeemin toimintaan voi olla joskus vaikeaa (Hummer et al. 2016).

Hummer et al. (2016) esittelevät artikkelissaan haasteita, joita yritykset kohtaavat IAM-politiikkoja muodostaessaan. Yrityksen tietoturvallisuustarpeet muuttuvat nopeasti digitalisaation ja toimintaympäristön muutoksen seurauksena. Myös liiketoiminnan tarpeet tiedon käsittelyyn elävät jatkuvasti. Siksi yrityksen käytössä olevat ohjeistukset usein vanhenevat tai muuttuvat epäkäytännöllisiksi hyvin nopeasti. Tämä johtaa helposti siihen, että yrityksen politiikkoja aletaan kiertää omin päin. Yrityksen tuleekin huolehtia siitä, että sen ohjeistuksia on mahdollista päivittää ja hallita ketterästi ja nopeasti. (Hummer et al. 2016)

3.2.2 Käyttöoikeuksien hallinnan prosessin osa-alueet

IAM-infrasturuktuurissa on paljon erilaisia organisoitavia osa-alueita. IAM-vaatimukset määritellään yrityksen tietoturvapolitiikassa ja valittavat toimintatavat ja teknologiat muodostavat IAM-prosessin. ISO 27000:2017-standardin mukaan IAM-prosessin teknisillä, loogisilla, fyysisillä ja hallinnollisilla toimintatavoilla tai näiden tapojen yhdistelmillä varmistetaan, että yrityksen tieto-omaisuuteen pääsevät käsiksi vain siihen valtuutetut tahot ja että pääsyä rajoitetaan liiketoiminta- ja turvallisuusvaatimusten perusteella (ISO 27000:2017). Tässä alaluvussa perehdytään IAM-prosessin osa-alueisiin ja niiden erityispiirteisiin luottamuksellisen tiedon käyttöoikeuksien hallinnan kannalta. Kuvassa 3 nähdään osa-alueet, joista käyttöoikeuksien hallinnan prosessit koostuvat Whitmanin ja Mattordin (2011) mukaan.



Kuva 3. *IAM-prosessiin liittyviä osa-alueita (Whitman & Mattord 2011 pohjalta)*

Whitman ja Mattord (2011) jakavat käyttöoikeuksien hallinnan neljään suuremaan osa-kokonaisuuteen. Uniikkien identiteettien avulla muodostetaan virtuaalisia projektioita luonnollisista henkilöistä, jotka esitellään järjestelmille. Autentikointi yhdistää ja todentaa reaaliaikaisesti läsnäolevan käyttäjän määriteltyyn identiteettiin ja tälle identiteetille luvattuihin käyttöoikeuksiin. Autentikoinnin vaatimukset, kuten kaksi- tai useampivaiheinen tunnistautuminen, saadaan pitkälti siitä, kuinka salaiseksi järjestelmässä sijaitseva tieto on luokiteltu. Autentikointi tapahtuu erilaisin teknisin ratkaisuin käyttämällä esimerkiksi salasanoja, tunnistekortteja tai sormenjälkiä. Autentikointi perustuu siihen, että jokainen identiteetti pystytään tunnistamaan yksiselitteisesti. Käyttäjien ja heidän suorittamiensa toimintojen yhdistäminen, eli jäljitettävyys, on myös osa käyttöoikeuksien hallintaa. Monissa yrityksissä käyttäjien järjestelmissä tekemistä toimista kerätään niin kutsuttua lokitietoa (Whitman & Mattord 2011, ss. 421-427). Tämä tarkoittaa käytännössä sitä, että esimerkiksi järjestelmissä tapahtuneet tiedon lisäykset, muokkaukset, ja poistot, liitetään lokitiedon avulla ne suorittaneeseen käyttäjään. (Bradford et al. 2014) Tietojen kerääminen ei itsessään vielä riitä, vaan tarvitaan myös lokitiedon säännöllistä tarkkailemista. Käyttäjien seuraaminen voikin auttaa yritystä selvittämään toimiiko sen käyttöoikeuksien hallinnan prosessit kuten on suunniteltu. (Whitman & Mattord 2011, s. 427)

Bradford et al. (2014) mukaan autorisoinnilla tarkoitetaan sitä prosessia, jossa autentikoidulle identiteetille luvataan käyttöoikeuksia erilaisiin tietoartikkeleihin. Autorisoinnin toteuttamiseen on monia tapoja, joiden valinta on usein haastavaa. Whitman ja Mattord (2011) esittelevät käyttäjien autorisointiin useita tapoja. Autorisointi voidaan tehdä yksittäin jokaiselle tietoartikkelille ja käyttäjälle, perustuen käyttäjän ryhmäjäsenyyksiin tai organisatoriseen rooliin tai käyttäen keskitettyä käyttöoikeuksien

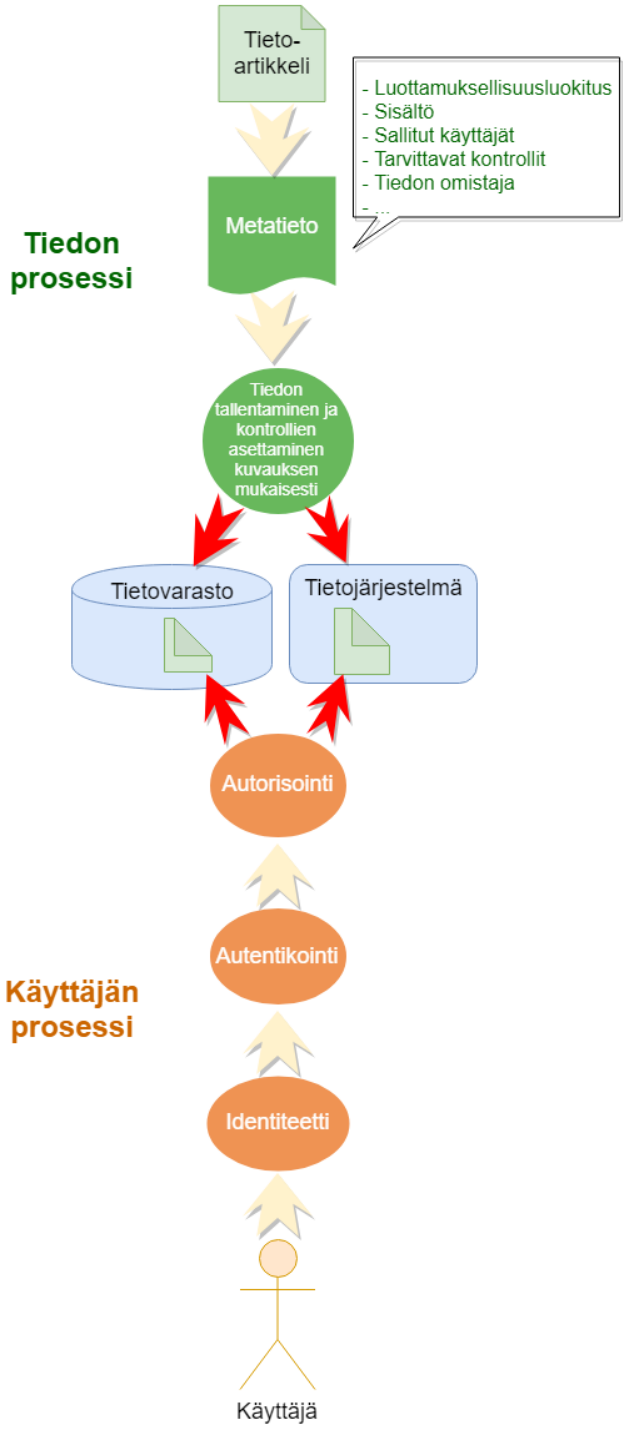
hallinnan järjestelmää. Tietoartikkeleiden autorisointitavan valinnassa erityisen merkityksellistä on valita jokaiselle tiedon luottamuksellisuusasteelle sellainen toimintamalli, joka suojaa tietoa riittävällä tasolla, mutta ei kuitenkaan estä sen tarkoituksenmukaista käyttöä. (Whitman & Mattord 2011, s. 427) Tästä syystä myös rakennettavien IAM-prosessien on tunnistettava erilaiset tietotyypit ja osattava kunnioittaa niiden vaatimuksia.

Jotta tietoa voidaan käsitellä ja kontrolloida oikein, on sitä käsittelevien tahojen tiedettävä mitä erityispiirteitä kyseiseen tietoon liittyy. Metatiedolla tarkoitetaan tietoa tiedosta. Metatieto kuvaa, selittää ja paikantaa tietoa ja helpottaa sen hakemista, käyttämistä ja hallitsemista (Viljanen 2013-2018). Metatietoon kuuluvat esimerkiksi tiedon luottamuksellisuusluokitus, sallitut käyttäjät ja tiedon omistaja. Whitman ja Mattord (2011) kertovat tiedon käyttöä hallittavan käyttökontrollien asettamisella. Käyttökontrollit muodostuvat tietoturvallisuuspolitiikan ja käytössä olevan prosessin sekä teknologioiden yhdistelmästä. Kukin kontrolli muodostaa protokollan tietyn tietotyypin tai -artikkelin suojaamiseksi ja saavuttamiseksi. (Whitman & Mattord 2011, ss. 428-230) Käytännössä jokaiselle tietoartikkelille on siis olemassa tietty polku, mitä pitkin käyttäjä voi saavuttaa oikeuden sen käyttämiseen. Erilaisia kontrollityyppejä voivat olla esimerkiksi roolien tai ryhmäjäsenyyksien mukana saatava automaattinen hyväksyntä, tarpeen ilmetessä tapahtuva hyväksyntä ja moniportainen hyväksyntä. Joskus käyttöoikeuksia voidaan jakaa myös suoraan tiedostoihin jakamiskutsujen muodossa.

IAM-prosessin tulee kattaa tiedon käytön kaikki ulottuvuudet ja sen koko elinkaari (Bradford et al. 2014). Näihin kuuluvat esimerkiksi tiedon määrittely, luominen, implementointi, käyttö, varastointi, jakaminen, varmuuskopiointi, vanhentuminen ja tuhoaminen. On tärkeää, että tiedon käyttöoikeuksia valvotaan sen koko elinkaaren ajan ja että kaikki sen esiintymät on turvattu yhtä huolellisesti. (Whitman & Mattord 2011, s. 231) Esimerkkejä epäonnistumisista voisivat olla esimerkiksi suojaamattomat varmuuskopiovarastot tai käytöstä poistuneissa järjestelmissä vanhoilla työntekijöillä olevat käyttäjätunnukset, joilla näkee yhä jotakin rajoitettua tietoa.

Kuvassa 4 esitetään rautalankamalli käyttäjän ja tiedon prosesseista luottamuksellisen tiedon käyttöoikeuksien hallinnassa. Vihreällä värillä kuvataan tiedon prosessia. Ennen kuin tietoa voidaan varastoida järjestelmiin, on tiedosta tiedettävä monia asioita. Tiedon kuvaus eli metatieto sisältää tiedon esimerkiksi siitä, millaista tietoa tietoartikkeli sisältää ja millaisin perustein ja kenen luvalla sitä saadaan jakaa. Myös tiedon luottamuksellisuusluokitus kuuluu metatietoon. Metatiedon perusteella tietoa voidaan varastoida ja kontrolloida sen vaatimilla tavoilla. Oranssilla värillä on kuvattu prosessi, jossa käyttäjä saa identiteetin, joka tunnistetaan autentikoinnin avulla oikeaksi käyttäjäksi. Jotta hän pääsee käsiksi tietoon, hänelle täytyy autorisoida käyttöoikeuksia järjestelmiin ja tietovarastoihin joissa tietoa säilytetään. Mikäli käyttäjälle on annettu käyttöoikeus kyseiseen tietoon, pääsee hän tarkastelemaan sitä järjestelmässä.

Hetkiä, jolloin käyttäjä saa pääsyn tietoon kuvataan punaisilla nuolilla. Punaisia nuolia on molemmilla puolilla prosessia, sillä varsinainen käyttöoikeus tietoon voidaan saavuttaa kaikissa näissä vaiheissa. Käyttöoikeus voi syntyä käyttäjän saadessa oikeuden tietojärjestelmään tai silloin, kun tieto tallennetaan järjestelmään, jota käyttäjä jo käyttää. On tärkeää, että koko kokonaisuus, sekä kuvan ylä- että alapuoli, toteutuu sääntöjen mukaisesti. Kuten Bradford et al. (2014) toteavat, jonkun osaprosessin epäonnistuminen on aina uhka tiedon turvallisuudelle tai saatavuudelle.



Kuva 4. *Käyttäjän ja tiedon prosessit käyttöoikeuksien hallinnassa (Whitman & Mattord 2011; Bradford et al. 2014 pohjalta)*

4. TOIMIJAT TIEDON KÄYTTÖOIKEUKSIEN HALLINNASSA

Barman (2001) korostaa, että erinomaisesti rakennetut IAM-prosessit ja -politiikat eivät vielä yksinään takaa luottamuksellisen tiedon onnistunutta turvaamista ja käsittelyä. Suuria lisähaasteita tilanteeseen tuovat kaikki ne ihmiset, joiden toimintaan prosessit ja politiikat tulee implementoida. Tästä johtuen suunnitteluvaiheessa on erittäin tärkeää määritellä tarkkaan kaikki roolit ja vastuut, joita tarvitaan tavoitteiden toteutumiseksi. (Barman 2001, s. 26)

Tässä luvussa perehdytään erilaisiin IAM-systeemiin kuuluviin toimijoihin. Luvun tavoitteena on vastata tutkimuksen toiseen alatutkimuskysymykseen: Millaisia rooleja ja vastuita liittyy luottamuksellisen tiedon käyttöoikeuksien hallintaan? Tarkempaan käsittelyyn on valittu neljä vastuutahoa: yrityksen johto, tiedon omistaja, tiedon käsittelijä ja tiedon vartija. Jokaisella taholla on prosessissa omat tehtävänsä ja vastuualueensa. Tehtäviä ja vastuukysymyksiä tarkastellaan erityisesti tietoturvallisuuden toteuttamisen näkökulmasta ja eri roolien välisiä suhteita havainnollistetaan kaaviokuvilla. Lopuksi tehdään vielä yhteenvetokuva toimijoiden muodostamasta kokonaisuudesta ja pohditaan muiden yritykseen liittyvien henkilöiden rooleja luottamuksellisen tiedon käsittelyssä. Tämän luvun tärkeimpänä tutkimusaineistona on hyödynnetty Scott Barmanin (2001) opasta tietoturvallisuuspolitiikkojen rakentamiseen. Oppaassa kerrotaan erityisen kattavasti tiedonkäsittelyyn liittyvistä vastuullisista rooleista. (Barman 2001)

4.1 Yrityksen johto

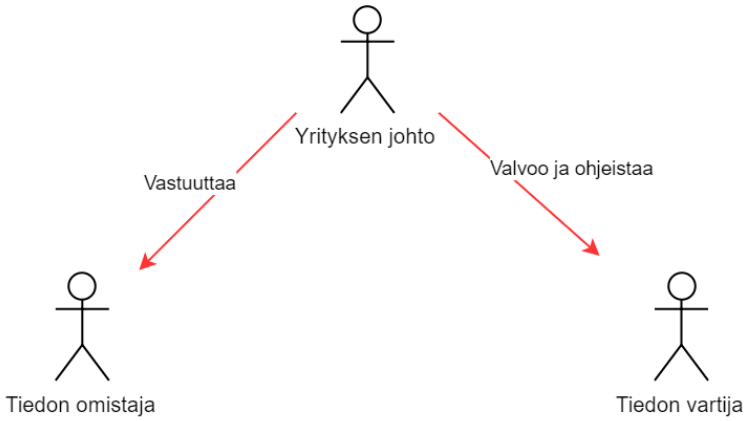
Yrityksen johdon roolia tietoturvallisuustavoitteiden, kuten luottamuksellisen tiedon käytön valvonnan, onnistumisessa ei voida liikaa korostaa. ISO 27000:2017-standardissa todetaankin, että johdon näkyvä tuki ja sitoutuminen tietoturvallisuuteen kaikilla tasoilla, erityisesti ylimmässä johdossa, on ratkaisevaa koko tietoturvan hallintajärjestelmän menestyksen kannalta.Vaikka yrityksen johdolla ei todennäköisesti ole mitään aktiivista roolia käyttöoikeuksien hallinnan ja luvittamisen prosessissa, on erittäin tärkeää, että komento ja vaatimukset luottamuksellisen tiedon huolelliseen suojaamiseen saadaan yrityksen ylimmältä johdolta (Barman 2001, s. 27).

Barman (2001) kertoo, että valmiita tietoturvallisuuspolitiikkoja voidaan hyvin harvoin ottaa sellaisenaan käyttöön missä tahansa yrityksessä. Politiikan ja valittavien käytäntöjen tulee tukea ja suojella yrityksen liiketoimintaa ja siksi niitä suunniteltaessa on todella tunnettava yrityksen liiketoiminta ja sen erityispiirteet. Tästä syystä tietoturvapolitiikkojen tulee olla yrityksen johdon kanssa yhteistyössä valmisteltuja. Tämä osoittautuu joskus ongelmalliseksi, sillä yritysten johdon henkilöt eivät yleensä ole tietoturva-alan ammattilaisia, minkä vuoksi he saattavat suhtautua tällaiseen vastuuseen varautuneesti. Heidän roolissaan ei kuitenkaan tarvitse ymmärtää miten IAM-prosessit

teknisesti toimivat. Heidän vastuullaan on varmistaa, että liiketoiminnan prosessit ja tavoitteet on toteutettavissa valittavien sääntöjen puitteissa. (Barman 2001, ss. 27-28)

Barmanin (2001) mukaan yrityksen johdon tehtäviin kuuluu määritellä, ne säännöt, joiden mukaan tietoa yrityksessä käsitellään, esimerkiksi millaisilla perusteilla tietoa tulee yrityksessä määritellä luottamukselliseksi. Kuten aiemmin todettiin, tiedon luottamuksellisuusluokitus perustuu siihen, miten tiedon arvo saadaan. Tiedon luokittelu on käytännössä riskienhallintaa, jossa tasapainoillaan tiedon suojelemisen ja saatavuuden välillä. (Barman 2001, s. 28) Päätös siitä, millaisia riskejä voidaan tietoturvallisuuden kustannuksella ottaa tiedon saatavuuden turvaamiseksi kuuluu yrityksen johdolle. (Whitman & Mattord 2011, s. 115). Tietoon liittyvien päätösten tekeminen voi olla haastavaa pelkästään tietoturvallisuuden teknisen ulottuvuuden parissa työskenteleville henkilöille, sillä päätökset liittyvät usein suoraan liiketoimintaan. Siksi päätöksentekijöillä on oltava todella hyvä ymmärrys siitä, mistä minkäkin tiedon liiketoiminnallinen arvo koostuu. Tästä johtuen on erittäin tärkeää, että yrityksen johto ottaa vastuun näistä päätöksistä. (Barman 2001, s. 28)

Tiedon käsittelyä koskevien sääntöjen määrittelyn lisäksi yrityksen johdolla on johtajan ja esimerkin rooli, kun IAM-prosesseja ja -politiikkoja asetetaan ja otetaan käyttöön. Tiedon omistajien ja tiedon vartijoiden tulee ymmärtää vastuunsa yrityksen johdon asettamien tiedon käsittelyn perussääntöjen pohjalta. Perussääntöjen asettamisen lisäksi yrityksen johdon vastuulla on varmistaa tiedon vartijoiden kautta, että yrityksen toimintatapoja päivitetään liiketoiminnan muutosten tahdissa. (Barman 2001, ss. 27-28) Yrityksen johto asettaa vastuut IAM-systeemin osien rakentamiseen, määrittelyyn ja valvontaan (Barman 2001, ss. 199). Johdon tulee tehdä kaikille yrityksen tietoa käsitteleville tahoille selväksi, miten tärkeä resurssi tieto yritykselle on ja ohjata kaikkia noudattamaan yhteisiä sen käsittelyyn liittyviä sääntöjä. (Barman 2001, s. 28) Kuvassa 5 esitellään yrityksen johdon vastuita liittyen muihin IAM-systeemin toimijoihin.

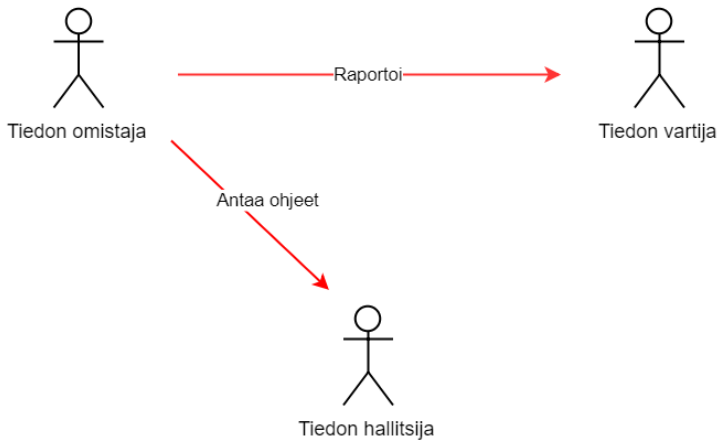


Kuva 5. *Yrityksen johdon rooli IAM-systeemissä (Barman 2001 pohjalta)*

4.2 Tiedon omistaja

Barmanin (2001) mukaan IT-keskeisissä tietoturvamalleissa vastuu tiedosta ja sen kontrolleista on perinteisesti ollut tietojärjestelmien ylläpitäjillä. Tämä on kuitenkin haastavaa, sillä tietohallinnon työntekijöiden vastuulla on usein suurissa yrityksessä todella paljon erilaisten järjestelmien ylläpitotehtäviä ja laajoja tietokokonaisuuksia. Pitääkseen jonkinlaista järjestystä yllä, nämä henkilöt joutuvat usein tekemään politiikkojen implementoinnin sillä tavalla, joka tekee heidän omasta toiminnastaan mahdollisimman sujuvaa. Vastuun jäädessä järjestelmäylläpitäjille he vastaavat tiedon käyttöoikeuksien kontrollien asettamisesta ja luottamuksellisuusluokittelusta. Tämä on ongelmallista, sillä järjestelmäasiantuntijat eivät voi mitenkään tuntea kaikkea heidän hallitsemissaan järjestelmissä olevaa tietoa. Näissä tilanteissa ei siis voida mitenkään taata, että päätökset käyttöoikeuksien jakamisesta tehdään sääntöjen mukaisesti, sillä päätökset perustuvat ylläpitäjän parhaisiin arvauksiin siitä, kuinka salaista tieto on ja kenelle tiedon käyttöoikeus kuuluu. Tästä syystä jokaiselle tiedolle tulisi määritellä omistaja, jonka vastuulla on huolehtia, että sen käsittely tapahtuu juuri tämän tietotyypin asettamien vaatimusten mukaisesti. (Barman 2001, ss. 28-29)

Tiptonin ja Krausen (2004) mukaan tiedon omistajan tehtävänä on päättää ja antaa ohjeet siihen, miten tietoa tulee yrityksen järjestelmissä kohdella. Käytännössä tämä tarkoittaa, että hän määrittelee omistamansa tiedon suojaamiseen tarvittavien kontrollien tason ja sen kuka ja millä perusteilla saa tietoa tarkastella. (Tipton & Krause 2004, s. 721) Tiedon omistaja voi luottaa kontrollien teknisessä toteutuksessa tiedon hallitsijaan, mutta vastuu tiedosta pysyy silti hänellä. Hän määrittelee tietoa hallitseville tahoille kaikki sellaiset tavat, joilla kyseistä tietoa saadaan käsitellä. Näihin tapoihin voivat kuulua esimerkiksi tiedon tarkastelu, muokkaus, jakaminen ja poisto. (Whitmann & Mattord 2014, s. 535) Tiedon omistajan tulee olla tiiviisti mukana päättämässä, millainen prosessi käyttäjän tulee läpäistä, että hän pääsee tietoon käsiksi (Barman 2001, ss. 28-29). Joskus tiedon omistaja antaa itse käyttäjille käyttöoikeuksia manuaalisia pyyntöjä vastaan, joskus IAM-päätökset koskevat suurempia käyttäjäryhmiä tai automaattisia prosesseja. On kuitenkin tärkeää, että tiedon omistaja on näissä päätöksissä aina mukana. Näin voidaan taata, että jokaisen tiedon käsittelytavoista päätettäessä tiedetään tiedon käsittelyn todelliset tarpeet. (Tipton & Krause 2004, s. 721) Tiedon omistajan suhdetta muihin toimijoihin esitetään kuvassa 6.



Kuva 6. *Tiedon omistajan rooli IAM-systeemissä (Barman 2001 pohjalta)*

Tiptonin ja Krausen (2004) mukaan tedon omistaja vastaa kaikista yksittäiseen tietoon kohdistuvista päätöksistä, esimerkiksi tiedon luottamuksellisuusluokittelusta ja tiedon metadatan määrittelystä. Hänen tehtävänsä on myös valvoa, että näitä päätöksiä päivitetään ja tarkastellaan uudestaan riittävän usein, jotta toiminta vastaisi aina liiketoiminnan sen hetken tarpeita. (Tipton & Krause 2004, s. 721) Tiedon omistajan on kaikkia päätöksiä tehdessään oltava tietoinen yrityksen tietoturvallisuuspolitiikasta ja käytännöistä. Vaikka hänen ei tarvitsekaan olla teknisen prosessin asiantuntija, on hänen myös hyvä ymmärtää miten IAM-prosessit pääpiirteittän toimivat. Tätä varten hänen tulee kommunikoida aktiivisesti sekä tietoturvasta vastaavien tiedon vartijoiden että tietojärjestelmistä vastaavien tiedon hallitsijoiden kanssa. Näin varmistetaan, että tietoa käsitellään sekä tiedon omien vaatimusten että koko yrityksen tietoturvallisuusvaatimusten mukaisesti. (Barman 2001, ss. 28-29)

Tiedon omistajan määritteleminen ei ole helppoa ja roolin ymmärtäminen on joillekin työntekijöille hankalaa. Barmanin (2001) mukaan suurimmat haasteet tiedon omistajan määrittelyssä liittyvät usein siihen, että näin suurta vastuuta ei haluta ottaa tai siihen, että omistajuus voitaisiin jakaa kompleksisessa järjestelmäinfrastruktuurissa lukuisilla tavoilla. Tiedon omistajan vastuun määritteleminen oikein on kuitenkin erittäin tärkeää tietoturvallisuuden toteutumisen kannalta. Nyrkkisääntönä voidaan ajatella, että jokainen liiketoimintayksikkö omistaa oman toimintansa tuottaman tiedon. (Barman 2001, s. 29) Tiedon omistajan roolissa toimivan tahon tulee siis olla osa tietoa tuottavaa liiketoimintaa. Tipton ja Krause (2004) perustelevat tämän sillä, että jos tiedolle kävisi jotakin, sen vaikutukset koettaisiin erityisesti siinä osassa yritystä. Tiedon koko olemassaolon tarkoitus on palvella tätä osaa yrityksestä, joten on ehdottoman tärkeää, että siihen liittyvät päätökset tehdään liiketoiminnan näkökulmasta. (Tipton & Krause 2004, s. 721) Näin ollen tiedon omistajuus ei kuulu esimerkiksi tietojärjestelmäylläpitäjälle.

Barman (2001) toteaa, että tiedon omistajuutta ei välttämättä tule jokaisessa yrityksen osassa organisoida samalla tavalla. Omistajuuden jakamisen tulee perustua laajaan

tietämykseen siitä, millaista tietoa yrityksessä on. Tiedon omistajan tehtävä on erittäin vastuullinen tehtävä ja siksi vastuunjako tulee tehdä niin, että se tukee liiketoiminnan tekemistä eikä päinvastoin. On todella tärkeää, että tiedon omistajien kanssa keskustellaan omistajuutta määriteltäessä, jotta heidän huolensa ja huomionsa liittyen tiedon käsittelyyn tulevat huomioiduiksi, jolloin koko järjestelmä saadaan rakennettua paremmin. (Barman 2001, s. 30) On myös huomioitava, että vaikka tiedon omistajan konseptiin perustuva tiedon koordinointi onkin hyvä toimintatapa monille yrityksille, ei se kuitenkaan välttämättä toimi kaikissa yrityksissä. Esimerkkejä tällaisista yrityksistä voivat olla esimerkiksi pienemmät yritykset ja sellaiset yritykset, joiden kaikki tieto on vahvasti integroituna ympäristöön. (Barman 2001, s. 29)

Suuressa yrityksessä tulee analysoida myös sitä, minkä verran tiedon omistajia voi olla. Toisaalta jos tiedon omistajia on liikaa, heidän johtamisestaan ja valvonnastaan tulee vaikeaa (Barman 2001, s. 30). Toisaalta jos omistajuudet kasautuvat liian pienelle määrälle henkilöitä, eivät he voi enää tuntea riittävän hyvin kaikkea omistamaansa tietoa. Tiptonin ja Krausen (2004) mukaan yksi ratkaisu suuren yrityksen tapaukseen on useamman tason omistajahierarkia. Tällöin jokaisella liiketoimintayksiköllä on yksi vastaava tiedon omistaja, joka kommunikoi ja vastaa tiedosta tiedon vartijalle ja tiedon hallitsijalle. (Tipton & Krause 2004, s. 724) Hänellä voi kuitenkin samanaikaisesti olla alaisuudessaan pienempien tietokokonaisuuksien omistajia, joita tämä ohjaa parhaan tietonsa mukaan. Barman (2001) muistuttaa, että suuren yrityksen tulee myös sisällyttää toimintatapoihinsa oikea tapa kiertää tiedon omistaja tarvittaessa. Tämä on tärkeää, koska tiedon omistaja ei välttämättä ole aina saatavilla ja jos oikeaa ja ohjattua tapaa hänen ohittamiseensa ei ole, syntyy hänen kiertämiseensä helposti hallitsemattomia tapoja. Toimivia tapoja voivat olla esimerkiksi sijaisen nimeäminen ja tarkka dokumentaatio. Tiedon hallinnan ja luokittelun on oltava mahdollista muutenkin kuin tiedon omistajan henkilökohtaisilla tunnuksilla. (Barman 2001, s. 30)

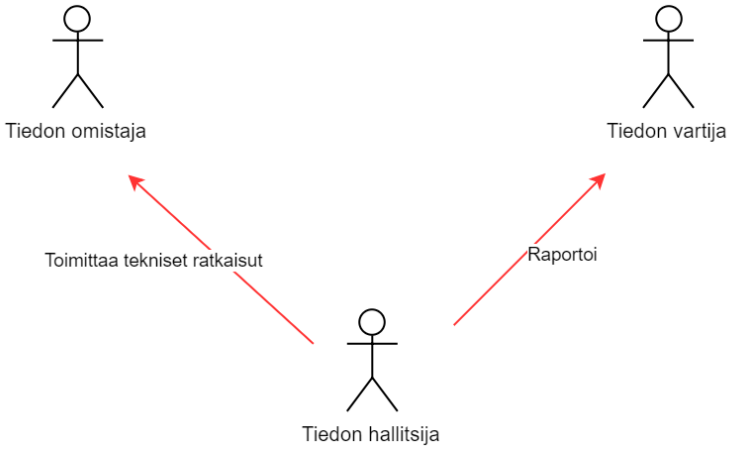
4.3 Tiedon hallitsija

Tiedon hallitsija vastaa tiedon ja sen hallinnan teknisestä ulottuvuudesta. Tiedon hallitsija on tyypillisesti IT-työntekijä, jonka työtehtävänä on tiettyjen tietojärjestelmien tai tietovarastojen ylläpitäminen. Hän suorittaa yrityksen IAM-prosesseihin liittyvän päivittäisen tason työn operoimalla niitä työkaluja ja prosesseja, joilla käyttöoikeuksien hallintaa yrityksessä tehdään (Whitman & Mattord 2011, s. 51). Näitä prosesseja ovat esimerkiksi autorisointiin tai identiteettien hallintaan käytettävien teknisten palveluiden ylläpito. Tiedon hallitsijan tehtävänä on tarjota tekninen osaaminen ja prosessit, joiden avulla tietoa hallitaan tiedon omistajan määrittelemien ohjeiden ja IAM-politiikkojen ja -prosessien mukaisesti (Tipton & Krause 2004, s. 715).

Tiedon hallitsijan tehtävät keskittyvät erityisesti siihen tekniseen ympäristöön, jossa tietoa yrityksessä säilytetään. Tehtäviin kuuluu tiedon varastointi, ylläpito, suojaaminen ja varmuuskopiointi (Whitman & Mattord 2014, s. 64). Hänen tehtäviinsä kuuluu myös

varmistaa, että liiketoiminnan tieto- ja käyttötarpeet hänen järjestelmänsä osalta täyttyvät. Lisäksi tiedon hallitsija huolehtii tiedon päivittäisestä turvallisuusvalvonnasta ja tietoon kohdistuvista käyttöoikeuspyynnöistä tietoturvapolitiikkojen ja tiedon omistajan ohjeiden mukaisesti. Hän myös valvoo jatkuvasti, että tietoa käsittelee vain sellaiset tahot, joilla siihen on oikeus. (Tipton & Krause 2004, s. 722)

Tiedon hallitsija saa tiedon vartijalta tietoturvapolitiikkaan perustuvat ohjeet prosessien rakentamiseen ja tiedon suojaamiseen. Whitman ja Mattord (2011) toteavat, että on todella tärkeää, että yrityksellä on yhtenäinen politiikka käyttöoikeuksien hallinnalle, sillä ilman politiikkaa järjestelmien ylläpitäjät voivat toteuttaa sellaisia pääsynhallinnan ratkaisuja, jotka eivät ole linjassa yrityksen kokonaistavoitteiden ja tietoturvallisuusvaatimusten kanssa. Politiikka sisältää tiedon siitä, miten käyttöoikeudet, niiden hakeminen ja muutokset tulee yrityksessä toteuttaa. (Whitman & Mattord 2011, s. 433) Mikäli tiedon hallitsija havaitsee turvallisuusuhkia tai rikkomuksia, hän välittää niistä tietoa tiedon vartijalle (Tipton & Krause 2004, s. 722). Tiedon hallitsijan tehtäviä suhteessa muihin toimijoihin on esitelty kuvassa 7.



Kuva 7. *Tiedon hallitsijan rooli IAM-systeemissä (Barman 2001 pohjalta)*

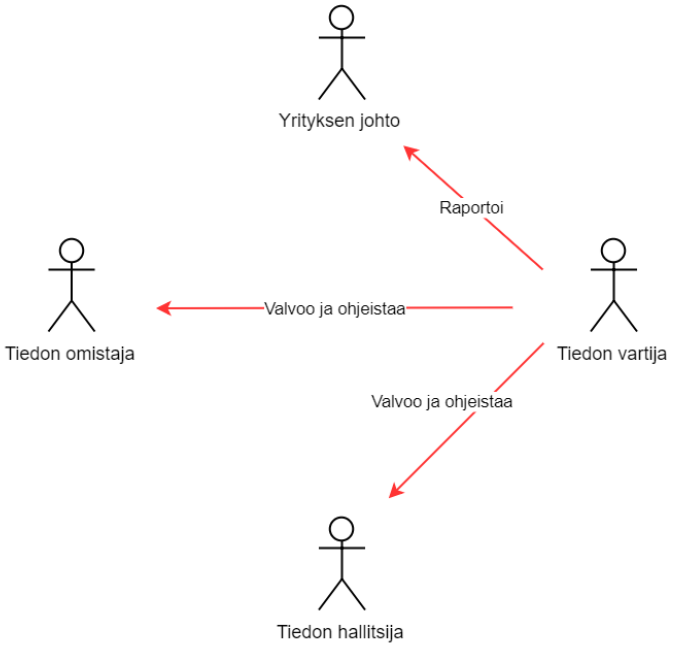
Tiedon hallitsijoita saattaa varsinkin suuressa yrityksessä olla yhden tiedon prosessin piirissä useitakin. Heidän työtehtävänsä voivat erota toisistaan ja käsitellä tiedon käsittelyn eri vaiheita tai tiedon eri ulottuvuuksia. Voidaan ajatella, että jokaisella tieto- ja kontrollityypillä tulee olla oma tiedon hallitsija (Barman 2001, s. 29). Esimerkkejä erilaisista vastuista voi olla autorisointityökalun hallinnointi ja autorisoitavan tietovaraston ylläpito ja päivittäminen. Tiedon luokitteluun ja jakamiseen liittyvät päätökset eivät saa olla tiedon hallitsijan vastuulla. Tipton ja Krause (2004) näkevät IT-osaston koko muun yrityksen toimintaa tukevana tukifunktiona, jonka tehtävänä on toimittaa määriteltyjä prosesseja. Whitmanin ja Mattordin (2011) mukaan heidän tehtävänsä on ennenkaikkea huolehtia niiden prosessien ylläpidosta ja toteutuksesta, joita liiketoiminnan ja tiedon suojelemiseksi on rakennettu. He voivat kehittää teknisiä toimintatapoja, joilla IAM-prosessia tehdään, mutta tiedon suojaamiskäytäntöihin liittyvän päätöksenteon täytyy tapahtua muualla. (Whitman & Mattord 2011, s. 51) Tämä

johtuu siitä, että tietojärjestelmäasiantuntijat eivät voi koskaan tuntea kaikkea heidän järjestelmissään hallittavaa tietoa.

4.4 Tiedon vartija

Kuten luvussa 4.1 todettiin, tiedon käsittelyn ja luokittelun reunaehdot tulisi saada yrityksen johdolta. Yrityksen johto ei kuitenkaan itse kirjoita politiikkoja tai osaa muodostaa koko toiminnan kattavia ohjeistuksia siitä, miten prosessin osat tulee toteuttaa. Hebbar (2017) määrittelee tiedon vartijan henkilöksi tai tahoksi, jonka vastuulla on huolehtia niistä säädöksistä ja politiikoista, jonka mukaan yrityksessä organisoidaan ja valvotaan tietoa ja sen käyttöä (Hebbar 2017). Tiedon vartijalta tarvitaan laajaa ymmärrystä sekä tietoturvallisuuden teknisestä ulottuvuudesta että niistä liiketoiminnallisista resursseista ja prosesseista, joita tiedon käyttöoikeuksien hallinnalla pyritään tukemaan ja suojelemaan (Barman 2001, s. 28). Suuren yrityksen prosesseissa tiedon vartijoita on tyypillisesti useita ja heidän vastuualueensa eroavat hieman toisistaan. Tiptonin ja Krausen (2004) mukaan näitä tehtäviä hoitaa yleensä yrityksen useasta henkilöstä koostuva tietoturvallisuusyksikkö, joka ei vastaa päivittäisten tietohallintopalveluiden tuottamisesta tai ylläpidosta. Eri liiketoiminta-alueiden tietoturvallisuudesta vastaavat henkilöt muodostavat virtuaalitiimin, jonka vastuulla on huolehtia IAM-systeemin tietoturvallisuustavoitteiden toteutumisesta ja valvonnasta. (Tipton & Krause 2004, s. 725)

Uudemmassa kirjassaan Whitman ja Mattord (2014) esittelevät tiedon vartijan valvontaan liittyviä tehtäviä. Myös Barmanin (2001) näkee politiikan ja prosessien noudattamisen valvonnan tärkeänä osana tiedon vartijan tehtäviä. Tiedon vartija siis valvoo toimintamalleja ja tiedon kontrollointisysteemejä yrityksen korkeimman johdon alaisuudessa ja valvomana. Hän tarkkailee, onko valitut toimintatavat ja prosessit politiikkojen mukaisia ja selvittää, miten hyvin niissä asetetuista tavoitteista todellisuudessa suoriudutaan. Hän valvoo, että tiedon hallitsijat ja omistajat suorittavat omat vastuunsa tiedon määrittelyssä, luokittelussa, varastoinnissa ja käsittelyssä. Nämä tahot myös raportoivat tiedon vartijalle mahdollisista kohtaamistaan tietoturvallisuusongelmista. (Whitman & Mattord 2014, s. 64) Tiedon vartijan tehtävänä on etsiä, valvoa ja esitellä johdolle mahdollisia riskejä, joita IAM-prosessin päivittäisessä toiminnassa kohdataan. Lisäksi tiedon vartija edustaa tietoturvallisuuden näkökulmaa koko yrityksen muutosjohtamisen prosesseissa. (Whitman & Mattord 2011, ss. 52-53) Kuva 8 esittää tiedon vartijan suhdetta muihin toimijoihin.



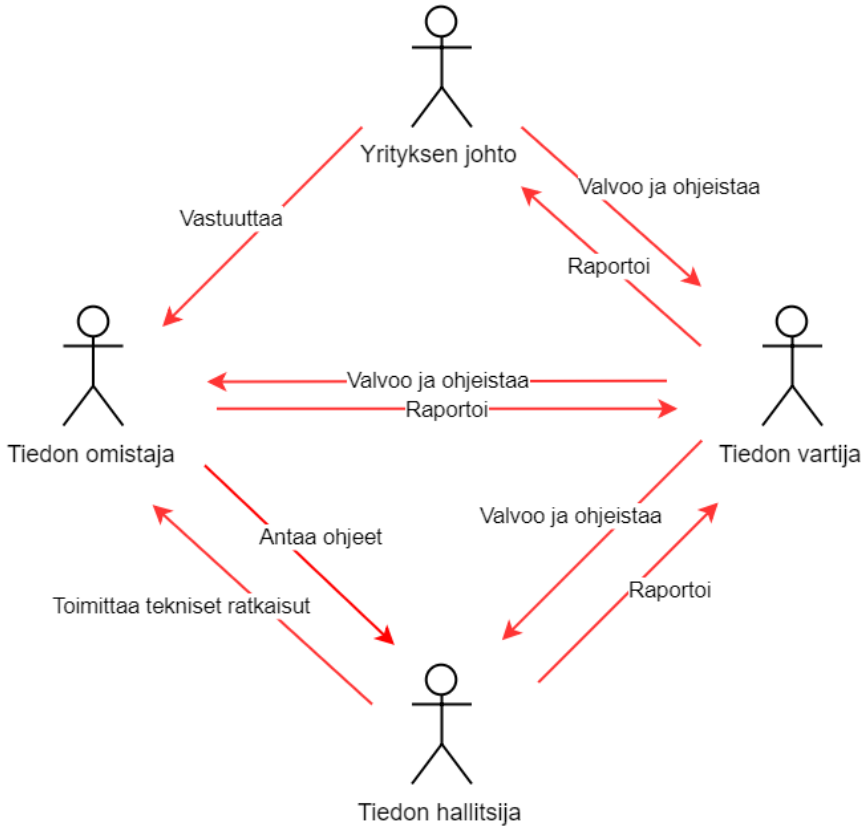
Kuva 8. *Tiedon vartijan rooli IAM-systeemissä (Barman 2001; Whitman & Mattord 2011 pohjalta)*

Barman (2001) korostaa, että on todella tärkeää, että politiikkojen käyttöönoton onnistumista arvoidaan tietoturvallisuuden teknisen ulottuvuuden lisäksi myös liiketoiminnan näkökulmasta. Tässä tehtävässä onnistuakseen tiedon vartija tarvitsee laajan ymmärryksen yrityksen koko IAM-infrastruktuurista ja yrityksen liiketoiminnasta. (Barman 2001, s. 33) Hän ei voi kuitenkaan tuntea läpikotaisin kaikkia järjestelmiä eikä kaikkea järjestelmissä käsiteltävää tietoa. Siksi hänen ei pitäisi tehdä operatiivista teknistä työtä, yksittäisiin tietoartikkeleihin liittyviä päätöksiä tai huolehtia metadatasta ja tiedon luokittelusta. Tipton ja Krause (2004) korostavat, että vastuun jakaminen on tärkeää myös tehtävien eriyttämisen takia. Tällä tarkoitetaan käytännössä sitä, että saman henkilön tai tahon ei pitäisi vastata saman prosessin rakentamisesta, määrittelystä, toteuttamisesta ja valvonnasta. (Tipton & Krause 2004, s. 725) Se, että yksilöt vastaavat itse oman toiminta valvonnasta saattaa aiheuttaa joissakin tilanteissa esimerkiksi huolimattomuutta.

Barman (2001) näkee yhdeksi yritysten suurimmaksi ongelmaksi johdon osallistumisen puutteen. Hänen mukaansa yksi tapa toteuttaa johdon osallistuminen IAM-prosessien valvontaan on perustaa yrityksen johdon ja tiedon vartijatahon henkilöiden yhteenliittymä, jonka vastuulla on valvoa yrityksen tietoturvallisuustavoitteiden toteutumista. Tämä ryhmä voi toimia siltana tietoturvan ammattilaisten ja yrityksen johdon välillä. Ryhmässä voidaan jakaa ymmärrystä liiketoiminnasta, tietoturvallisuuteen liittyvistä riskeistä ja teknisestä ulottuvuudesta. Tästä ryhmästä vastaavan henkilön pitäisi vastata yhtiön korkeimmalle taholle. (Barman 2001, s. 28)

4.5 Yhteenveto vastuukysymyksistä

ISO 27000:2017-standardin mukaan on todella tärkeää, että koko yrityksessä vallitsee yhtenäinen ohjestus, näkemys, asenne ja puitteet käyttöoikeuksien hallinnan suunnitteluun, toteuttamiseen, seurantaan, ylläpitoon ja parantamiseen. Näiden mukana saadaan yhteinen käsitys luottamuksellisen tieto-omaisuuden suojausvaatimuksista, jotka voidaan täyttää soveltamalla IAM-toimintatapoja tietoturvaohjeistuksien mukaisesti. (ISO 27000:2017) IAM-systeemin tärkeimmät vastuut kuuluvat yrityksen johdolle, tiedon omistajalle, tiedon hallitsijalle ja tiedon vartijalle. Kuvassa 9 on esitettynä näiden neljän toimijan muodostama suhdeverkosto.



Kuva 9. *Toimijoiden väliset suhteet IAM-systeemissä (Barman 2001 pohjalta)*

Vaikka tässä luvussa määriteltiinkin vain neljä erillistä roolia, on muistettava, että kaikilla organisaation luottamuksellista tietoa käsittelevillä on omat vastuunsa prosessissa. Evans ja Price (2014) korostavat, että jokainen yrityksen työntekijä tulee todennäköisesti jossakin vaiheessa käsitelleeksi luottamuksellista tietoa ja siksi on tärkeää, että kaikilla on tiedossa, miten tietoa tulee kohdella. Yrityksen onkin tärkeää huolehtia, että luottamuksellisen tiedon varjeleminen kuuluu jokaisen työntekijän työnkuvaan ja kaikki tietävät, mitkä heidän vastuunsa sen puitteissa on (Barman 2001 s. 34). Myös ISO 27000:2017-standardissa todetaan, että tietoturvallisuustavoitteiden onnistumiseksi vaaditaan sitä, että kaikki työntekijät ja muut asianmukaiset tahot tietävät tietoturvallisuuteen liittyvistä velvoitteistaan, jotka asetetaan tietoturvapolitiikassa. Heitä

on myös motivoitava toimimaan näiden velvoitteiden mukaisesti. (ISO 27000:2017) Jos pelisäännöt eivät ole kaikille selviä, voi luottamuksellinen tieto levitä hyvistä IAM-prosesseista huolimatta politiikkojen vastaisesti esimerkiksi yksittäisten työntekijöiden lähettämissä ruutukaappauksissa.

Tietoturvallisuuteen liittyviä vastuita jaettaessa on otettava huomioon, että työntekijöiden lähtökohdat ja valmiudet vastuunkantamiseen on erilaiset. Saattaa olla, että kaikki eivät pidä tietoturvallisuutta tärkeänä ja toisaalta osalle haasteita saattaa aiheuttaa heikommat tietotekniset taidot. Useammassa tutkimusaineistossa, kuten ISO 27000:2017-standardissa sekä Whitmanin ja Mattordin ohjekirjoissa (2011; 2014), todetaan, että yrityksen jokaisen toimijan tulisi kuitenkin osata kantaa oma vastuunsa yrityksen tiedon turvaamisesta. Tätä osaamista yritys voi tukea tietoturvallisuutta käsittelevällä koulutuksella, tietoisuuden lisäämisellä ja työntekijöille tarjottavalla tuella (Whitman & Mattord 2011, s. 490; Whitman & Mattord 2014; ISO 27000:2017). Viestin tietoturvallisuusosaamisen tärkeydestä tulisi tulla työntekijöille mahdollisimman korkealta taholta (Barman 2001 s. 24).

5. LUOTTAMUKSELLISEN TIEDON KÄYTTÖOIKEUKSIEN HALLINNAN JOHTAMINEN SUURESSA YRITYKSESSÄ

Tutkimuksen päätutkimuskysymys oli: Miten luottamuksellisen tiedon käyttöoikeuksien hallintaa voisi suuressa yrityksessä johtaa? Viidennessä luvussa vastataan tähän kysymykseen. Aluksi esitellään tutkimuksen tuloksena saatu johtamismalli ja käydään läpi tutkimuksen keskeisimmät havainnot. Sen jälkeen näiden havaintojen pohjalta johdetaan päätelmiä.

5.1 Kokonaiskuva käyttöoikeuksien hallinnan johtamismallista

Tutkimuksen tuloksena esitellään kuva 10, joka on aiempiin lukuihin kerätyn tutkimustiedon pohjalta muodostettu kokonaiskuva, joka yhdistää IAM-systeemin ja sen toimijat. Jo luvun 3 kuvassa 4 osittain esitelty ISO 27000:2017 standardin, Whitmanin ja Mattordin (2011) ohjekirjan ja Bradford et al. (2014) artikkelin perusteella muodostettu IAM-systeemi käsittää luottamuksellisen tiedon käyttöoikeuksien hallinnassa käytettävän IAM-prosessin ja politiikan. Kuvassa 10 mukaan on otettu IAM-systeemin piirissä työskenteleviä erilaisia toimijoita, joista jokaisen kohdalle on eritelty Barmanin (2001), Tiptonin ja Krausen (2004) sekä Whitmanin ja Mattordin (2011) ohjekirjojen mukaisesti heidän tärkeimpiä tehtäviään ja vastuitaan.

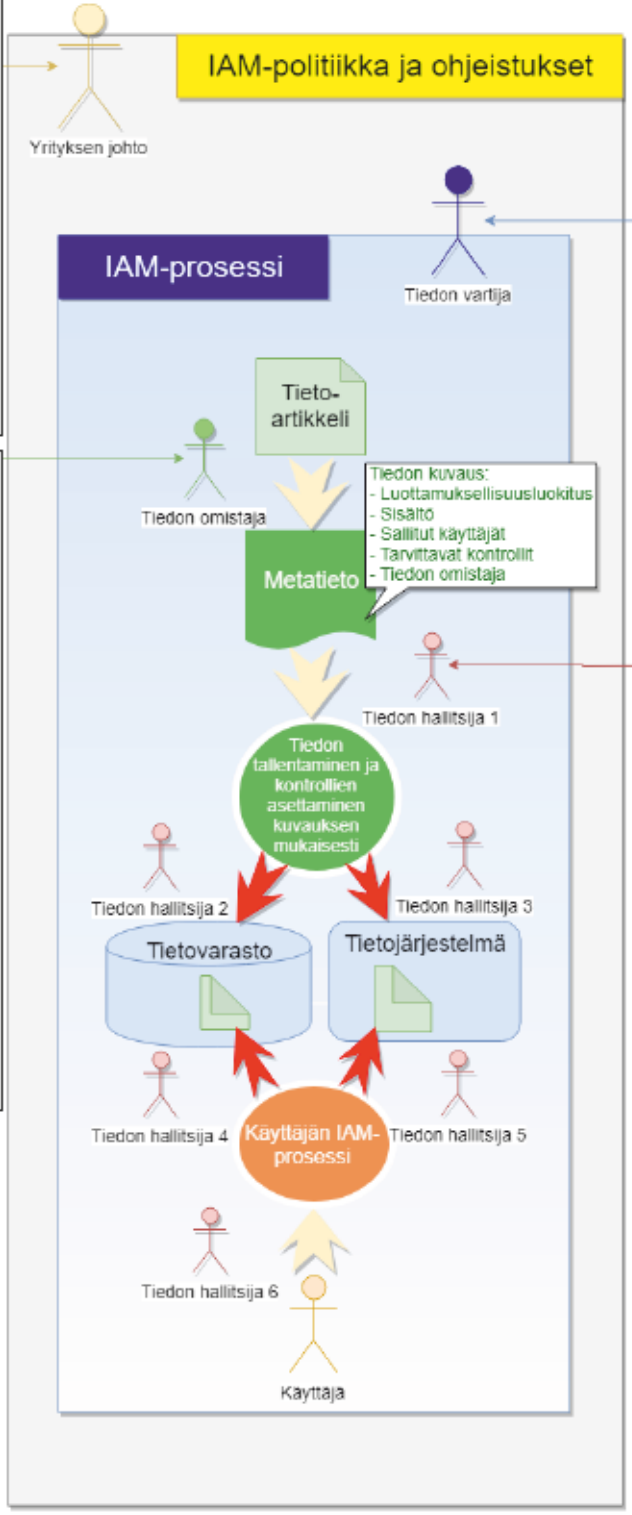
Muodostetun johtamismallikuvan keskellä nähdään kolmannessa luvussa jo esitelty IAM-prosessi, josta on otettu tarkasteluun erityisesti tiedon puoli prosessista (Whitman & Mattord 2011). Kuten aiemminkin, punaiset nuolet kuvaavat jälleen sitä vaihetta prosessista, joissa käyttäjä voi saavuttaa tiedon. Prosessin käyttäjienhallinnan puoli on tiivistetty yhdeksi osioksi, koska käyttäjien hallinta ei ole tämän tutkimuksen tuloksen kannalta olennaista. Rooleja kuvaavat hahmot on asetettu prosessissa niihin kohtiin, joista he vastaavat tutkimusaineistojen mukaan (Barman 2001; Tipton & Krause 2004; Whitman & Mattord 2011). Kuvan tiedonhallinnan teknisiä prosesseja kuvaavien nuolien luo on tuotu näistä prosesseista vastaavat tiedon hallitsijat. Tiedon omistajan hahmo on kuvassa tiedon metatiedon ja tiedon kuvauksen määrittelyn kohdalla. Metatiedon avulla jatkotoimenpiteistä vastaava tiedon hallitsija tietää, miten tietoa tulee kohdella (Tipton & Krause 2004). Prosessin kehykseen asetettu tiedon vartija kuvaa tämän roolia prosessin valvonnassa. Tiedon vartijan rooli jatkuu IAM-politiikan ja -ohjeistuksien laatimiseen ja valvontaan, joten hahmo sijaitsee näiden tasojen välissä. (Whitman & Mattord 2011) Yrityksen johto osallistuu politiikan laatimiseen ja ohjeistuksien asettamiseen ja valvoo, että ne tukevat liiketoimintaa (Barman 2001). Hänen päätyönsä on kuitenkin kuvan ulkopuolella. Tehtävälistoilla havainnollistetaan sitä, että suorittamalla nämä tehtävät, toimija hoitaa roolinsa jo melko kattavasti.

Yrityksen johto:

- On aktiivisesti mukana päätöksenteossa
  - Riskienhallinta
  - Tiedon arvon määrittely
- Huolehtii liiketoiminnan vaatimusten/tarpeiden huomioimisesta tietoturvapolitiikassa
- Valvoo tiedon vartijaa
- Viestii tietoturvallisuuden merkityksestä kaikkialle yritykseen

Tiedon omistaja:
Liiketoiminnan edustaja, tuntee tiedon sisällön ja merkityksen liiketoiminnalle

- Vastaa tiedosta ja kaikista siihen liittyvistä päätöksistä
- Luo tiedon kuvauksen
- Antaa tiedolle luottamuksellisuus-luokituksen perustuen tietoturvapolitiikkaan
- Määrittelee tiedolle tarvittavat kontrollit ja sallitut käyttäjät
- EI huolehdi teknisestä toteutuksesta



Tiedon vartija:
Yrityksen tietoturvallisuudesta vastaava henkilö/taho

- Laatii politiikan ja ohjeistuksen tiedon käsittelyyn
- Valvoo, että politiikka toteutuu yhtäläisesti kaikissa järjestelmissä
- Valvoo IAM-prosessia ja sen toimijoita
- Raportoi yrityksen johdolle esim. riskeistä
- Huolehtii prosessin päivittämisestä liiketoiminnan mukana
- EI tee prosessin operatiivista työtä

Tiedon hallitsija:
IT-työntekijä, esim. järjestelmäylläpitäjä

- Ylläpitää tietoa ja tietojärjestelmiä
- Hallinnoi teknisiä kontrollimenetelmiä
- Kehittää IAM-prosessia teknisesti
- Saa ohjeita tiedon omistajalta ja vartijalta ja raportoi tiedon vartijalle ongelmista ja riskeistä
- Huolehtii tiedon koko elinkaaresta
- EI tee päätöksiä tiedon käsittelystä

Kuva 10. *Kokonaiskuva luottamuksellisen tiedon IAM-systeemistä ja sen toimijoista (Barman 2001; Tipton & Krause 2004; Whitman & Mattord 2011; Whitman & Mattord 2014; Bradford et al. 2014; ISO 27000:2017 pohjalta)*

Digitalisaatio ja tiedon määrän kasvu lisäävät yritysten käytettävissä olevaa tietoa ja kommunikointimahdollisuuksia. Samalla kun myös turvattava tiedon määrä kasvaa, yrityksiltä vaaditaan nopeampaa ja joustavampaa tiedon hallintaa kuin koskaan ennen. (Werner et al. 2017) Luottamuksellisen tiedon turvassa pysyminen vaatii yrityksiltä yhtenäistä, mutta liiketoiminnan muutosten tahdissa pysyvää käyttöoikeuksien hallinnan systeemiä. Jotta prosessi voisi toimia sujuvasti, tulee sen tahojen tunnistaa roolinsa ja vastuunsa ja toisaalta paikkansa osana yrityksen tiedon turvaamisesta vastaavaa kokonaisuutta. Kuten Katsikogiannis et al. (2016) artikkelissa kerrotaan, nykyteknologiat mahdollistavat nopeita ja automaattisia kontrolli- ja autorisointijärjestelmiä. Rakennettavien järjestelmien tulee kuitenkin perustua yrityksen yhteisiin käytäntöihin. (Katsikogiannis et al. 2016) Tämä vaatii todennäköisesti myös prosessien ja politiikkojen parissa toimivilta henkilöiltä uudenlaista joustavuutta ja nopeampaa kommunikaatiota jokapäiväisessä työssään. Tästä syystä on erittäin tärkeää, että kaikki toimijat ymmärtävät roolinsa IAM-systeemin kokonaisuuden osana sekä suhteessa muihin toimijoihin että suhteessa IAM-politiikkaan ja teknisiin prosesseihin. Tutkimustuloksena saadun kuvan 10 arvo saadaankin siitä, että se yhdistää havainnolliseen muotoon juuri näitä ihmisten, politiikan ja prosessien välisiä suhteita.

Tutkimuksen aikana ei löydetty yhtäkään kuvan 10 kaltaista jäsennystä käyttöoikeuksien hallinnan toimijoiden ja prosessien välisestä suhteesta. Kuva muodostettiin yhdistelemällä eri aineistoista löytynyttä tietoa ja näin ollen kuva tuo aivan uudella tavalla esiin juuri osakokonaisuuksien välisiä yhtyksiä. Tutkimukseen ei myöskään löydetty yhtäkään aineistoa, joka olisi puhunut suoraa IAM-systeemin vastuunjaon onnistumisen yhteydestä luottamuksellisen tiedon suojaamisen onnistumiseen. Aihetta lähestyttiin tässä tutkimuksessa kuitenkin useasta eri tulokulmasta ja löydettyjen aineistojen yhdistämisen perusteella voitaneen todeta, että luottamuksellisen tiedon käyttöoikeuksien hallintaa tulisi johtaa niin, että yrityksen toimijoita, prosesseja ja politiikkaa tulisi johtaa kokonaisuutena.

Kuvaa voidaan pitää tutkimuksen keskeisimpänä tuloksena, koska se yhdistää yhdeksi kokonaisuudeksi kaiken, mitä tässä tutkimustyössä on käsitelty ja saatu selville. Kuva havainnollistaa aineistojen tutkimuksen perusteella muodostetun mallin siitä, miten luottamuksellisen tiedon käyttöoikeuksia tulisi johtaa. Kuvaa tarkasteltaessa tulee kuitenkin ottaa huomioon, että kuva on hyvin yksinkertaistettu. Todellisessa tilanteessa IAM-systeemiin kuuluu paljon muitakin osia ja toimijoita. Esimerkiksi osa kuvan toimijoista saattaa todellisessa suuren yrityksen tapauksessa muodostua useamman henkilön hierarkisesta järjestelmästä. Käyttöoikeuksien hallinnan toteuttamiseen on olemassa monia mahdollisia tapoja, joista tämä on yksi. On huomioitava, että vaikka tässä tutkimuksessa tulokseksi muodostui tällainen johtamismalli, voi jossakin yrityksessä silti olla perusteltua toimia eri tavalla.

5.2 Tutkimusaineistoista tehdyt havainnot ja päätelmät

Tutkimuksen ensimmäiseen alatutkimuskysymykseen vastaamisessa olennaista oli ymmärtää, että yrityksen erilaiset tietotyypit vaativat tiedon käsittelyltä erilaisia asioita. Kuten Barman (2001) sekä Tipton ja Krause (2004) totesivat, tiedon sopivan suojaustason valinta on riskienhallintaa ja tasapainoilua tiedon saatavuuden ja luottamuksellisen välillä. On tärkeää, että yrityksen tiedon luokittelussa käytetään yhtenäisiä kriteerejä, jotka saadaan tiedon liiketoiminnallisen arvon ja riskien kautta (Whitman & Mattord 2011). Tiedon luokittelua ja IAM-prosessin rakentamista ohjaa tietoturvallisuuspolitiikka ja IAM-politiikka, joissa määritellään ne tavat ja säännöt, joilla yrityksessä hallitaan, luokitellaan ja järjestellään tietoa ja käyttöoikeuksia (ISO 27000:2017). Luottamuksellisen tiedon käyttöoikeuksien hallinnan prosessit perustuvat kullekin tietotyypille sopivien kontrollien asettamiseen ja käyttäjien identifioimiseen, autentikointiin, autorisointiin ja seurantaan (Bradford et al. 2014). Prosessien määrittelyn tulee kattaa kokonaisuudessaan sekä käyttäjän että tiedon polku tietojärjestelmiin ja molempien prosessien pitää toteutua, jotta tietoturvallisuustavoitteisiin voidaan päästä (Whitman & Mattord 2011).

Toisen alatutkimuskysymyksen tarkastelun tärkeimpiä havaintoja oli, että yrityksen liiketoiminnan tulee toimia tuottamansa tiedon omistajana, koska tiedon käyttämisen arvo ja riskit kohdistuvat suorimmin tähän osaan yritystä (Barman 2001; Tipton & Krause 2004). Kuten Barman (2001) kirjassaan totesi, liiketoiminnan parista tulevien tiedon omistajien tulee vastata tiedon käyttöoikeuksien jakamiseen liittyvistä päätöksistä, kuten tiedon luokittelusta. Vastuun prosessien rakentamiseen ja ylläpitoon pitää olla tiedon hallitsijataholla, eli useimmiten yrityksen IT-osastolla. Prosessit tulee rakentaa tiedon omistajan ja tietoturvapolitiikan määrittelemien ohjeiden mukaisiksi. Myös tiedon omistajien päätökset tulee perustaa tietoturvapolitiikkaan. (Barman 2001) Tipton ja Krause (2004) määrittelivät, että tietoturvapolitiikkojen rakentamisesta vastaavat tiedon vartijat, eli tavallisesti yrityksen tietoturvallisuusosasto, joka ei vastaa prosessien operoinnista. Tiedon vartijoiden tehtävänä on myös valvoa, että tiedon omistajat ja hallitsijat hoitavat omat tehtävänsä politiikan mukaisesti. (Tipton & Krause 2004) Barmanin (2001) ohjekirjan mukaisesti yrityksen johdon tulee olla mukana politiikkaan rakennettavien sääntöjen ja ohjeiden määrittelyssä, jotta politiikka tukee yrityksen liiketoimintaa mahdollisimman hyvin. Johdolla on kattavin ymmärrys yrityksen liiketoiminnasta, ja he ymmärtävät parhaiten tiedon liiketoiminnallisen arvon ja sen, minkälaisia riskejä sen saatavuuden eteen voidaan ottaa. (Barman 2001)

Kuten myös Evans ja Price (2014) totesivat, on ensiarvoisen tärkeää ymmärtää, että vaikka kaikki yrityksen sidosryhmät ja työntekijät eivät toimita aktiivista roolia ja tehtäviä IAM-systeemissä, lähes kaikki yrityksen työntekijät ovat kosketuksissa sen luottamuksellisen tiedon kanssa. Tästä syystä kaikkien yrityksen tietoa käsittevien on ymmärrettävä oma vastuunsa tieto-omaisuuden suojelemisessa. (Evans & Price 2014) Siksi luottamuksellisen tiedon käyttöoikeuksien hallinnan johtamisella on huolehdittava

myös siitä, että tiedon ja tietoturvallisuuden merkitykset ymmärretään kaikkialla yrityksessä (ISO 27000:2017).

Tutkimuksen perusteella voidaan todeta, että IAM-systeemien rakentaminen suurissa yrityksissä on monimutkaista ja usein haastavaa. Samoja haasteita on koettu yrityksissä jo kauan, eikä tutkimuksessa täysin selvinnyt, miksi niitä koetaan yhä samanlaisina. Haasteita aiheuttavia tekijöitä ovat mahdolliset tietojärjestelmien väliset toimintatapaerot, roolien jakaminen, yksilöiden heikko tietämys tietoturvasta ja siihen liittyvistä vastuistaan sekä digitalisaation ja tiedon määrän kasvun seurauksena jatkuvasti kiristyvät vaatimukset tiedon hallinnalle. Tutkimuksen päätutkimuskysymyksen vastaukseksi voidaankin esittää, että jotta yritys voisi johtaa luottamuksellisen tiedon käyttöoikeuksien hallintaansa hyvin, on sen todennäköisesti panostettava eri toimijoiden väliseen kommunikaatioon ja siihen, että mahdollisimman monet erilaiset IAM-systeemin toimijat ja ulottuvuudet otetaan huomioon systeemiä suunniteltaessa ja johdettaessa. Käyttöoikeuksien hallinnan toimijat ja IAM-systeemi muodostavat yhdessä valtavan kokonaisuuden, jonka johtaminen vaatii kaikkien näiden osa-alueiden ja niiden välisten suhteiden ymmärtämistä. Tämän kokonaisuuden ymmärtämisen arvoa ei olla vielä välttämättä kaikkialla ymmärretty, koska siitä ei löytynyt ollenkaan tutkimusta. Kuvan 10 kaltainen kokonaisuuden jäsentäminen on ilmeisesti harvinaista, mutta tällaisten kokonaiskuvien rakentaminen voisi auttaa yrityksiä muodostamaan omia toimintamallejaan sellaisiksi, että prosessit ja toimijat saataisiin toimimaan paremmin yhdessä.

Tutkimuksen perusteella vedetään siis johtopäätös, että vaikka erilaisten IAM-systeemin osa-alueiden ja roolien tarkasteleminen erillään voi monissa tilanteissa olla hyödyllistä, niin systeemin suunnitteluvaiheessa ja sen johtamisen suunnittelussa näitä tulisi tarkastella kokonaisuutena. IAM-systeemien implementoinnin haasteet voivat johtua siitä, että politiikan ja prosessien rakennus ja työntekijöiden organisointi nähdään toisistaan erillisinä asioina. Tällöin saattaa syntyä prosesseja tai politiikkoja, joiden istuttaminen työntekiöiden arkeen on todella haastavaa. Jos kuitenkin yrityksen käyttöoikeuksien hallintaan käytettävät prosessit ja politiikat suunniteltaisiin juuri niitä suorittavien toimijoiden kautta, voisi niiden implementointi todelliseen jokapäiväiseen toimintaan olla helpompaa. On huolehdittava, että yrityksen kaikilla työntekijöillä on aikaa, osaamista ja työkaluja omien tiedon turvaamiseen liittyvien velvollisuuksiensa suorittamiseen.

6. YHTEENVETO JA TUTKIMUKSEN ARVIOINTI

Viimeisen luvussa arvioidaan tutkimuksen onnistumista ja merkitystä. Ensimmäisessä alaluvussa arvioidaan tutkimuksesta saatuja tuloksia ja sitä, miten hyvin ne vastaavat utkimuskysymyksiin. Arvioinnin kohteena ovat myös tutkimusprojektin ja tiedonhankinnan onnistuminen ja haasteet. Luvun toisessa osassa arvioidaan tutkimuksen merkitystä ja hyödyntämismahdollisuuksia sekä yleisesti että kirjoittajan ja hänen työnantajayrityksen kannalta. Myös mahdollisia tutkimuksen jättämiä tutkimusaukkoja ja jatkotutkimusmahdollisuuksia esitellään tässä luvussa.

6.1 Tulosten arviointi

Tutkimusprojekti sujui pääpiirteittäin hyvin. Kaikkiin tutkimuskysymyksiin saatiin vastattua ja niiden vastaamisen taustaksi löytyi riittävästi tietoa. Uudempaa tutkimustietoa saatiin erityisen hyvin erityisesti koskien IAM-systeemin politiikkoja ja prosesseja. Tuoretta tietoa toimijoiden vastuisiin liittyen ei löytynyt yhtä paljon, minkä vuoksi jouduttiin hyödyntämään vanhempia aineistoja. Erityisen haastavaa oli löytää tietoa joka käsittelisi tutkimusaihetta kokonaisuutena nimenomaan johtamisen näkökulmasta, sillä suurin osa aineistoista keskittyi käyttöoikeuksien hallinnan osa-alueiden erilliseen tarkasteluun. Käyttöoikeuksien hallinnan tutkimuksesta todella suuri osa vaikuttaisi keskittyvän aiheen tarkasteluun erityisesti teknisestä näkökulmasta, minkä vuoksi suuri osa alan tuoreesta tutkimuksesta jäi kokonaan tutkimuksen rajausten ulkopuolelle.

Käyttöoikeuksien hallinnan kokonaisuuden ja sen eri osakokonaisuuksien välisten suhteiden ymmärtäminen oli aluksi hankalaa, kun kokonaisuuteen keskittyneitä aineistoja ei juuri löytynyt. Eri osakokonaisuuksien tutkimisesta saadut tulokset tukivat kuitenkin hyvin toisiaan. Vaikutti siltä, että kun ymmärrys yhdestä asiasta karttui, myös muut tutkittavat osakokonaisuudet selkenivät entisestään. Kirjallisuustutkimuksen tekemisessä palkitsevaa oli se, että joissakin aineistoissa käsiteltiin tämän kandidaatintyön tutkimuskysymyksiin liittyviä osa-alueita rinnakkain. Tästä johtuen näiden aineistojen lukeminen edesauttoi merkittävästi kirjoittajan ymmärrystä aiheen kokonaiskuvasta, kuten tiedon luokittelun, tietoturvapolitiikan ja yrityksen johdon vastuun välisistä yhteyksistä. Asioiden limittyminen saattoi aiheuttaa paikoitellen toistoa lopullisen kandidaatintyön kolmanteen ja neljänteen käsittelylukuun. Tätä voidaan kuitenkin pitää todisteena siitä, kuinka suuri merkitys toimijoilla on luottamuksellisen tiedon hallinnan ja IAM-systeemin onnistumisessa. Voidaankin mahdollisesti päätellä, että esimerkiksi prosesseja ja niiden toimijoiden vastuita tulisi yrityksissäkin käsitellä ennemmin kokonaisuuksina kuin erillisinä asioita.

Tutkimuksessa tunnistettiin myös useita yleisiä haasteita ja ongelmakohtia, joita yritykset kohtaavat luottamuksellisen tiedon käyttöoikeuksien hallinnassa. Erityisen tärkeäksi huomioksi koettiin se, että monien tutkimusaineistojen mukaan samat haasteet ovat toistuneet yrityksissä jo kauan. Tutkimus onnistui löytämään tavan prosessien ja ihmisten organisointiin, mutta avoimeksi jää kuitenkin vielä se, miksi monet jo pitkään yleisesti hyvinä pidetyt toimintatavat, kuten tiedon omistajan määrittely, toteutuvat yrityksissä heikosti. Haasteille löydettiin joitakin mahdollisia selityksiä, mutta kokonaisuuden ymmärtämiseksi ongelmien juurisyitä tarvitsisi ehkä tutkia enemmänkin. Tutkimuksen tuloksena muodostettu johtamismalli ei välttämättä ota riittävissä määrin huomioon siihen kohdistuvia haasteita, koska yritysten kokemien haasteiden juurisyiden tutkiminen jäi tässä tutkimuksessa vielä spekuloinnin tasolle.

Kun tutkimusta alettiin tehdä, ei yrityksen johdolle kuuluvaa vastuuta käyttöoikeuksien hallinnan onnistumisessa oltu vielä tunnistettu tärkeäksi tutkimusalueeksi. Kirjallisuuskatsausta tehtäessä sen tärkeys hahmottui kuitenkin nopeasti, sillä sitä käsiteltiin lähes jokaisessa tutkitussa aineistossa. Tästä syystä yrityksen johdon merkityksen tutkiminen ja käsittely päätettiin ottaa osaksi tätä tutkimusta. Huomattiin, että yrityksen johdon osallistuminen luottamuksellisen tiedon käyttöoikeuksien hallintaan on suorastaan kriittisen tärkeää yrityksen tietoturvallisuus- ja liiketoimintatavoitteiden täyttämiseksi.

Mielenkiintoista tutkimuksen lopputuloksessa on se, miten tutkimuksen kaksi suurempaa kokonaisuutta, luottamuksellisen tiedon käyttöoikeuksien hallinta ja toimijat sen piirissä, saatiin yhdistettyä samaan kokonaiskuvaan. Näin aluksi toisistaan irrallisilta vaikuttaneista osa-alueista saatiin muodostettua looginen kokonaisuus, joka auttaa hahmottamaan asioiden välisiä yhteyksiä. Kirjallisuustutkimuksessa löytyneistä aineistoista lähes kaikki käsittelivät tutkimusaihetta ainoastaan yhdestä näkökulmasta, eikä missään oltu tehty tutkimuksen tuloksena muodostetun kuvan 10 kaltaista jäsennystä käyttöoikeuksien hallinnan kokonaisuudesta. Erityistä uutuusarvoa tämän tutkimuksen tuloksiin toikin se, että kaikki prosessin osa-alueet saatiin tuotua samaan kuvaan. Kokonaiskuva pystyy vastaamaan jo melko kattavasti koko tutkimuksen pääkysymykseen ja sen rakentaminen johtikin moniin tärkeimpiin tutkimusprojektin aikana saatuihin oivalluksiin.

Kirjoittajan näkökulmasta suurin tutkimuksen tuottama lisäarvo saatiin juuri luottamuksellisen tiedon käyttöoikeuksien hallinnan kokonaiskuvan hahmottumisesta. Vaikka kirjoittajalla oli jo entuudestaan tietoa tutkimusaiheesta ja sen osa-alueista, laajensi tutkimuksen tekeminen kokonaisymmärrystä erittäin paljon. Erityisesti näkökulmat tiedon liiketoiminnallisen arvon määrittelyyn ja riskienhallintaan olivat kirjoittajalle aivan uusia asioita. Tärkeä uusi oivallus oli myös yrityksen johdon osallistumisen suuri merkitys yrityksen tietoturvallisuustavoitteiden täyttymisessä.

6.2 Tutkimuksen merkitys ja hyödyntäminen

Tutkimuksen aikana todettiin, että tiedon käyttöoikeuksien hallinnan onnistuminen on yritykselle todella tärkeää sekä tietoturvallisuuden että tehokkaan toiminnan takaamiseksi. Moni tutkimusaineisto osoitti, että luottamuksellisen tiedon käyttöoikeuksien hallinta on usein haastavaa yrityksille. Näitä haasteita on ilmennyt yrityksissä jopa kahdenkymmenen vuoden ajan, joten vaikuttaisi siltä, että ongelmat vaativat vielä lisätutkimusta ja keskittymistä yrityksissä. Etenkin tiedon omistajuuteen liittyvässä vastuunjaossa onnistuminen on jostain syystä yleisesti yrityksissä vaikeaa. Vaikuttaisi siltä, että käyttöoikeuksien hallinnan päätöksenteko jää yrityksissä edelleen liikaa tietohallinnon harteille, jolloin luottamuksellisen tiedon asianmukainen käsittely vaarantuu. Tiedon luokittelun rooli- ja vastuukysymykset vaikuttaisivat olevan haastavia siksi, että liiketoimintayksiköillä ja johdolla on hankaluuksia ymmärtää ja ottaa vastuuta tiedon turvaamisesta. Voidaankin todeta, että yritysten tulisi todennäköisesti kiinnittää huomattavasti enemmän huomiota johdon sitouttamiseen ja ihmisten organisointiin tiedon turvallisuudesta puhuttaessa.

Tämän tutkimuksen jälkeen ei vielä täysin tiedetä mistä johtuu, että roolien ja vastuiden toteutuminen on usein niin vaikeaa käytännössä. Osasyy hankaluuksiin voi olla politiikan ja prosessien implementoinnissa, eli siinä, miten määritellyistä toimintatavoista ja säännöistä tulee osa yrityksen työntekijöiden jokapäiväistä toimintaa. Tästä syystä mielenkiintoinen aihe tulevaisuudessa tutkittavaksi olisikin se, miten rakennetut tietoturvallisuuspolitiikat ja tarkkaan määrittellyt vastuut ja prosessit saataisiin ihmisten johtamisen ja muutosjohtamisen avulla paremmin mukaan yrityksen jokapäiväiseen käytännön toimintaan. Tätä aihetta tutkimalla voitaisiinkin mahdollisesti vastata moniin tässä tutkimuksessa avoimeksi jääneisiin kysymyksiin. Tutkimus voisi täydentää tätä tutkimusta esimerkiksi löytämällä syitä ja ratkaisuja niihin ongelmiin, joiden olemassaolo tiedostetaan tämän tutkimuksen jälkeen.

Koska aihe tähän kandidaatintyöhön saatiin yritykseltä, pohditaan tässä vaiheessa myös tutkimuksen merkitystä yritykselle. Yrityksen kanssa käytiin keskustelua koko projektin ajan. Käytyjen keskustelujen ja yritykseltä saadun palautteen avulla tutkimusta pystyttiin ohjaamaan ja täsmentämään sellaiseen suuntaan, että se palveli yrityksen tarpeita. Yritys odotti, että tästä tutkimuksesta on apua yrityksen uudenlaisten luottamuksellisen tiedon käyttöoikeuksien hallinnan toimintatapojen ja prosessien rakentamisessa. Tämä esiselvitys voi myös auttaa yritystä erilaisten jatkokehityshankintojen harkinnassa. Tulosten pohjalta voidaan esimerkiksi pohtia, tulisiko jonkinlaisia palveluita tai prosessin osia hankkia yrityksen ulkopuolisilta toimijoilta.

Tämä tutkimus tuo yritykselle lisätietoa erityisesti siitä, miten tulevan prosessin piirissä toimivia ihmisiä kannattaisi organisoida. Tutkimuksen jälkeen vaikuttaisi siltä, että ihmisiä, politiikkaa ja prosesseja ja niiden välisiä suhteita kannattaa käsitellä ja kuvata kokonaisuutena. Voisikin olla hyödyllistä, että tutkimuksen jälkeen yrityksessä

pyrittäisiin muodostamaan tarkkoja oikeat ihmiset, järjestelmät ja prosessit kattavia kokonaiskuvia myös sen omiin tarkoituksiin. Kirjoittajan on tarkoitus jäädä yritykseen töihin kandidaatintyöprojektin jälkeen, jolloin myös hänen tutkimuksen aikana karttunutta omaa osaamista päästään hyödyntämään. Yksi mahdollinen tehtävä kirjoittajalle voisikin olla kandidaatintyössä muodostetun johtamismallin kaltaisten kokonaiskuvien muodostaminen suoraa yrityksen omien prosessien ja toimijoiden havainnollistamiseen. Kandidaatintyössä opittujen asioiden soveltaminen käytännön työhön tuleekin varmasti olemaan mielenkiintoista.

LÄHTEET

Bradford, M., Earp, J.B. & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case analysis using the Technology Organization Environment framework. International Journal of Accounting Information Systems, Volume 15, Issue 2. pp. 149-165. Saatavissa: https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S1467089514000049 (viitattu 27.1.2019).

Barman, S. (2001). Writing Information Security Policies. pp. 11-34. New Riders.

Data Governance Institute. (2013). Assigning Data Ownership. Saatavissa: http://www.datagovernance.com/assigning-data-ownership (viitattu 27.1.2019).

Evans, J. & Price, N. (2014). Responsibility and Accountability for Information Asset Management (IAM) in Organisations. June 2014. Electronic Journal of Information Systems Evaluation. Volume 17, Issue 1. pp 113-121. Saatavissa: https://search-proquest-com.libproxy.tuni.fi/docview/1555355138/fulltextPDF/A62DB11E7A5141B1PQ/1?accountid=14242 (viitattu 11.4.2019).

Hebbar, B. (2017). Who Is A Data Steward And What Are His Roles And Responsibilities? 26.9.2017. Analytics India. Saatavissa: https://www.analyticsindiamag.com/data-steward-roles-responsibilities (viitattu 27.1.2019).

Hummer, M., Kunz, M., Netter, M., Fuchs, L. & Pernul, G. (2016). Adaptive identity and access management-contextual databased policies. August 2016. EURASIP Journal on Information Security. pp. 1-16. Saatavissa: https://search-proquest-com.libproxy.tuni.fi/docview/1835626223 (viitattu 3.4.2019).

ISO 270000:2017. (2017). Information technology. Security techniques. Code of practice for information security controls. 3.3.2017. International Organization for Standardization. Saatavissa:
https://online-sfsfi.libproxy.tuni.fi/fi/index/hakutulos.html.stx (viitattu 17.2.2019).

Katsikogiannis, G., Mitropoulos, S. & Douligeris, C. (2016). An Identity and Access Management approach for SOA. Konferenssijulkaisu. IEEE/IET Electronic Library. Saatavissa: https://tuni.finna.fi/PrimoRecord/pci.ieee_s7886021. (viitattu 14.4.2019).

Kunz, M., Puchta, A., Groll, S., Fuchs, l. & Pernul, G. (2019). Attribute quality management for dynamic identity and access management. Journal of Information Security and Applications. pp. 44-79. Saatavissa: https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S2214212618301467 (viitattu 27.1.2019).

Ladley, J. (2012). Data Governance – How to design, deploy and sustain an effective data governance program. Morgan Kaufman publishers.

Lundgren, B. & Möller, N. (2017). Defining Information Security. 15.11.2017. Science and Engineering Ethics. Springer. Saatavissa: https://link.springer.com/article/10.1007/s11948-017-9992-1 (viitattu 27.1.2019).

Martin, J. A. & Waters, J. K. (2018). What is IAM? Identity and access management explained. 9.10.2018. CSO.. Saatavissa: https://www.csoonline.com/article/2120384/identity-management/what-is-iam-identity-and-access-management-explained.html (viitattu 27.1.2019).

Phoenix TS. (2012). CIA Triad (Security Triad). Video. 4.6.2012. CISSP Training Series. Saatavissa: https://www.youtube.com/watch?v=SP8cr0fg5Sg (viitattu 28.3.2019).

Sofigate. (2019). Organisaatio ja osaamisen kehittäminen. Yrityksen verkkosivut. Saatavissa: https://www.itforbusiness.org/fi/book/strategia-ja-hallinto/organisaatio-ja-osaamisen-kehittaminen (viitattu 27.1.2019).

Rouse, M. (2014). Confidentiality, integrity, and availability (CIA triad). November 2014. TechTarget. Saatavissa: https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA (viitattu 28.3.2019).

Tipton, H. & Krause, M. (2004). Information Security Management Handbook. Fifth Edition. Auerbach.

Vaismaa, K. (2009). Aiheesta analyysiin – Tukipaketti kandidaatin- ja diplomityön tutkimusprosessiin. 17.3.2009. TTY. Tiedonhallinnan ja logistiikan laitos. Saatavissa: http://www.tut.fi/verne/aineisto/aiheesta_analyysiin.pdf (viitattu 11.2.2019).

Viljanen, V. (2013-2018). Tiedostojen metatieto. Yksityisyydensuoja.fi. Saatavissa: https://www.yksityisyydensuoja.fi/tiedostojen-metatieto (viitattu 17.3.2019).

Werner, J. Westphall, C. M. & Westphall, C. B. (2017). Cloud identity management: A survey on privacy strategies. Elsevier SD Freedom Collection. Saatavissa: https://tuni.finna.fi/PrimoRecord/pci.sciversesciencedirect_elsevierS1389-1286(17)30166-4 (viitattu 14.4.2019).

Whitman M. & Mattord, H. (2014). Management of Information Security. Cengage Learning.

Whitman M. & Mattord, H. (2011). Roadmap to Information Security – for IT and InfoSec Managers. Cengage Learning.

Yrityksen oma dokumentaatio. (2018). Metso.