Kemi Tornion ammattikorkeakoulu

Käyttöoikeusprosessin yhtenäistäminen

Case Kirkon palvelukeskus, Kipa

Nina Heikkinen

Kaupan ja kulttuurin toimialan opinnäytetyö
Liiketalouden koulutusohjelma
Tradenomi

TORNIO 2013

TIIVISTELMÄ

KEMI-TORNION AMMATTIKORKEAKOULU, Kaupan ja kulttuurin toimiala

Koulutusohjelma: Liiketalouden koulutusohjelma
Opinnäytetyön tekijä: Nina Heikkinen
Opinnäytetyön nimi: Käyttöoikeusprosessin yhtenäistäminen
Sivuja (joista liitesivuja): 43
Päiväys: 27.5.2013
Opinnäytetyön ohjaajat: Helena Ranta-Saarela, Satu Valli
Tämän opinnäytetyön tavoitteena oli määrittää käyttöoikeusprosessiin valvontakeinoja, joiden avulla Kirkon palvelukeskuksella on mahdollisuus valvoa käyttöoikeuksien ajantasaisuutta ja sitä, ettei vaarallisia työyhdistelmiä pääse syntymään. Vaarallisilla työyhdistelmillä tarkoitetaan työrooleja, joita on yhdistelty siten, että riskimielessä syntyy vaarallisia käyttöoikeusyhdistelmiä. Lisäksi opinnäytetyön tavoitteena oli tehdä ohjeistus Kirkon palvelukeskuksen asiakkaille siitä, miten tehdä käyttöoikeuspyyntöjä käyttöoikeuksien hallintajärjestelmässä. Opinnäytetyö toteutettiin kvalitatiivisena tapaustutkimuksena. Tiedonkeruumenetelminä olivat teemahaastattelut, havainnointi, keskustelut ja lähdemateriaali. Opinnäytetyö koostui teoriaosuudesta ja empiriatutkimuksesta. Teoriaosuudessa hyödynsin kirjallisuutta ja sähköisiä lähteitä. Empirian pohjana olivat haastattelut. Tietoa keräsin myös havainnoimalla, keskustelemalla ja toimeksiantajan dokumentteihin tutustumalla. Opinnäytetyön tuloksena tein käyttöoikeuspyyntöohjeen Kirkon palvelukeskukselle ja määrittelin eri keinoja käyttöoikeuksien valvontaan. Käyttöoikeusprosessi on tärkeä osa yrityksen tietoturvallisuutta, sillä käyttöoikeuksien hallinnalla voidaan suojata yrityksen tietojen saatavuus, luottamuksellisuus ja eheys. Käyttöoikeuksien valvonnalla voidaan seurata, että yrityksen käyttöoikeustiedot ovat ajan tasalla ja, että sovittuja käytäntöjä noudatetaan. Vaaralliset työyhdistelmät estetään työtehtävien eriyttämisellä ja käyttöoikeuksien valvonnalla. Opinnäytetyöni tulokset ovat salaisia, sillä ne sisältävät toimeksiantajan salaista, luottamuksellista tietoa. Luottamukselliset tiedot luovutetaan vain Kirkon palvelukeskukselle.
Avainsanat: käyttöoikeusprosessi, käyttöoikeuksien valvonta, vaaralliset työyhdistelmät, työtehtävien eriyttäminen

ABSTRACT

KEMI-TORNIO UNIVERSITY OF APPLIED SCIENCES, Business and Culture

Degree programme: Business Administration

Author: Nina Heikkinen

Thesis title: Harmonization of the access rights process

Pages (of which appendixes): 43

Date: 27.5.2013

Thesis instructors: Helena Ranta-Saarela, Satu Valli

The objective of this thesis was to delineate ways to control the access rights process allowing Kirkon palvelukeskus, i.e. the service center of the Evangelical Lutheran Church of Finland, to ensure that access rights are up-to-date and that no unsafe working procedures occur. Unsafe working procedures mean such situations in which combining working roles bring about the risk of emergent unsafe combinations of access rights. The objective of the thesis was also to compile instructions for the clients of Kirkon palvelukeskus on how to create access rights requests in the access rights management system.

The thesis was carried out as a qualitative case study. Data collection methods comprised theme interviews, observation, discussions and source materials. The thesis consists of the theory part and the empirical part. In the theory part, I utilized literature and electric sources. Interviews were the basis for the empirical part. I also collected data by observing, discussing and getting acquainted with the service center's internal documents.

I compiled the access rights request instructions for Kirkon palvelukeskus and delineated the process for monitoring the access rights procedures as a result of the thesis. The access rights process is an important part of the organization's information security as access rights management allows ensuring the availability, confidentiality and integrity of the organization's information. Monitoring access rights makes it possible to follow up that the organization's access rights information is up-to-date and that agreed procedures are followed. Unsafe working combinations can be prevented with the differentiation of tasks and by monitoring the access rights. The results of this thesis are confidential as they include the assignor's classified and confidential information. The information which is classified is submitted only to Kirkon palvelukeskus.

Key words: access rights process, monitoring the access rights, unsafe working procedures, differentiation of tasks

SISÄLLYS

1 JOHDANTO

Voidakseen taata tietojensa koskemattomuuden, on yrityksen tietoturvan oltava kunnossa. Tietoturvassa on kysymys niistä toimenpiteistä, joilla yritys suojaa tärkeät tiedot ulkopuolisilta. Tietoturvalla halutaan saavuttaa tietojen luottamuksellisuus, eheys, kiistämättömyys, pääsynvalvonta, saatavuus ja tarkastettavuus. (Tietoturva 2013, hakupäivä 19.1.2013.) Tietoturvallisesti määritellyiksi käyttöoikeudet voidaan katsoa silloin, kun käyttäjillä on vain ne oikeudet, joita käyttäjät työtehtäviensä tekemiseen tarvitsevat. (KPMG 2012, 4).

Käyttöoikeuksien hallinnalla tarkoitetaan prosessia, jossa myönnetään käyttöoikeudet valtuutetulle henkilölle yrityksen tai organisaation tietoon, toimintoon tai palveluun ja vastaavasti rajataan oikeudet ei-valtuutetuilta henkilöiltä. Käyttöoikeuksien hallinnalla suojataan tiedon luottamuksellisuus, eheys ja saatavuus. (UCISA 2013, hakupäivä 25.1.2013, 1.)

KPMG:n tietoturvaraportin (2012, 2, 4) mukaan yksi vuoden 2011 kymmenestä yleisimmistä suomalaisten organisaatioiden kohtaamista tietoturvaongelmista oli käyttövaltuushallinnan ongelmat. Raportin mukaan käyttöoikeuksien hallintaan liittyy useita haasteita. Ensimmäisenä haasteena nähdään käyttöoikeusprosessin myöntämisprosessi. Myöntämisprosessin tulisi olla riittävän nopea ja kevyt työn joustavuuden kannalta, mutta tarpeeksi jäykkä pyydettyjen oikeuksien tarpeellisuuden varmistamiseen ja sen varmistamiseen, ettei ristiriitaisia käyttöoikeusyhdistelmiä, esimerkiksi oikeus luoda ja maksaa laskuja omalle tilille, käyttäjän olemassa oleviin käyttöoikeuksiin ole. Myös useamman henkilön käyttämät yhteiset tunnukset asettavat haasteita. Näin on erittäin hankalaa varmistaa, kuka tunnuksia milloinkin käyttää ja ketkä kaikki tietävät tunnuksen. Yhteiskäyttöiset tunnukset hankaloittavat tuntuvasti väärinkäytösten selvittämistä. Kolmantena ongelmana on raportilla mainittu ylläpito-oikeuksien myöntäminen liian kevein perustein. Ylläpito-oikeuksilla käyttäjä pääsee halutessaan asentamaan uusia ohjelmia koneelleen ja mahdollisesti näin voi asentaa haitallisen ohjelman tai kytkeä virustorjunnan pois päältä.

Opinnäytetyöni aiheen sain Kirkon palvelukeskuksessa suorittamani työharjoittelun aikana. Kirkon palvelukeskus on aloittanut palvelutuotantonsa 1.9.2012 ja uutena organisaationa toimintaa kehitetään voimakkaasti ja prosesseja otetaan käyttöön. Aiheeni on

ajankohtainen, sillä Kirkon palvelukeskuksessa on meneillään käyttöoikeuksien hallintajärjestelmän käyttöönottohanke, jonka aikana prosessia automatisoidaan ja jatkossa asiakkaat tekevät kaikki käyttöoikeuspyynnöt käyttöoikeuksien hallintajärjestelmässä.

1.1 Kirkon palvelukeskus

Vuoteen 2017 mennessä siirtyy Suomen seurakuntien taloushallinto Kirkon palvelukeskuksen, Kipan, hoidettavaksi. Tällä muutoksella pyritään säästämään vuosittain seitsemän miljoonaa euroa. Muutos on iso ja vaatii ihmisiltä sekä tietojärjestelmiltä joustoa ja yhteistyötä. Jos kuntaliitokset eivät vaikuta seurakuntien määrään, palvelukeskuksen asiakkaina tulee olemaan 295 seurakuntataloutta. (Koivu 2013, 2.)

Vuoden 2010 toukokuussa kirkolliskokous hyväksyi Kirkkolakiin ja Kirkkojärjestykseen muutokset, joiden myötä kirkkohallitus hoitaa seurakuntien, seurakuntayhtymien, hiippakuntien ja kirkon keskusrahaston kirjanpidon, palkanlaskennan sekä niihin liittyvän maksuliikenteen, siten kuin kirkkojärjestyksessä on erikseen säädetty ja taloushallinnon ja henkilöstöhallinnon tehtäviä hoitaa kirkkohallituksen yhteydessä toimiva kirkon kirjanpidon ja palkanlaskennan palvelukeskus. Kirkon palvelukeskuksen perustamista edeltäneen kirkon henkilöstö- ja taloushallinnon kehittämishankkeessa (HETA) on määritelty Kirkon palvelukeskuksen tarjoamien palvelujen laajuus. Kirkon palvelukeskus on kirkkohallituksen erillisyksikkö, joka tarjoaa laadukkaita ja kustannustehokkaita taloushallinnon ja henkilöstöhallinnon sähköisiä palveluratkaisuja asiakkailleen. Kirkkohallituksen täysistunto teki kokouksessaan 22.2.2011 päätöksen Kirkon palvelukeskuksen ensimmäisen toimipisteen perustamisesta Ouluun. Pääpaikan Oulun lisäksi toimipisteet avataan myös Lahteen ja Kuopioon. Ruotsinkielinen toimipiste avataan Porvooseen. (Kirkkohallituksen yleiskirje Nro 8/2011, 201; Kirkkohallituksen yleiskirje Nro 19/2012, 1: Kirkon palvelukeskus, hakupäivä 6.12.20012.)

Kirkon palvelukeskuksen verkkosivujen (hakupäivä 6.12.20012, 6.4.2013) mukaan palvelukeskuksen palvelutuotanto käynnistyi 1.9.2012, jolloin 13 ensimmäistä seurakuntataloutta otti käyttöön palvelukeskuksen palvelut. Palvelukeskuksen tarjoamia talous- ja henkilöstöhallinnon palveluja ovat

Taloushallinnossa

- kirjanpito, tilinpäätökset ja konsernitilinpäätökset
- käyttöomaisuus
- maksuliikenne
- menojen ja tulojen käsittely
- viranomaistilitykset, tilastot sekä raportit
- pääkäyttäjäpalvelut
- asiakastuki.

Henkilöstöhallinnossa

- palkat ja palkkiot
- palelusuhdetiedot
- vuosilomat ja poissaolot
- viranomaistilitykset, tilastot ja raportit
- matka- ja kululaskupalvelut
- henkilö- ja palvelusuhderekisteri
- pääkäyttäjäpalvelut
- asiakastuki.

Palvelukeskuksen tuottamia talous- ja henkilöstöhallintopalveluja asiakkaat käyttävät palvelukeskuksen sähköisen työpöydän Kipan Akkunan kautta. Palvelukeskuksen palvelutuotanto toteutetaan monitoimittajamallia käyttäen. Järjestelmätoimittajina ovat

- Fujitsu Finland Oy – Ydinratkaisu, SAP
- Lociga Oy – Palkat
- Basware Oyj – Maksuliikenne
- Atos IT Solutions an Services Oy – Portaali- (SAP) ja matka- ja kulujärjestelmä (SAP)
- eTaika Oy – Henkilö- ja palvelusuhderekisteri. (Kirkon palvelukeskus 2013, hakupäivä 6.4.20013.)

1.2 Opinnäytetyön tavoitteet ja rajaus

Tämän opinnäytetyön tavoitteena on määritellä Kirkon palvelukeskukselle käyttöoikeuksien hallintaan keinoja, joiden avulla palvelukeskuksella on mahdollisuus valvoa käyttöoikeuksien ajantasaisuutta ja sitä, ettei vaarallisia työyhdistelmiä pääse syntymään. Opinnäytetyön tavoitteena on myös luoda palvelukeskuksen asiakkaille selkeä ohjeistus, miten tehdä käyttöoikeuksien haku-, muutos- ja poistamispyyntöjä.

Opinnäytetyön tutkimus- ja alakysymykset ovat seuraavat:

1. Miten palvelukeskus valvoo käyttöoikeuksia?
    - Miten palvelukeskus valvoo käyttäjien käyttöoikeuksia ja sitä, ettei vaarallisia työyhdistelmiä pääse syntymään?

2. Miten ohjeistetaan palvelukeskuksen asiakkaat käyttöoikeuspyyntöprosessin osalta?
    - Miten käyttöoikeuspyyntöjä voidaan tehdä?
    - Mitä oikeuksia voidaan hakea?

Opinnäytetyössäni en käsittele pääsynhallintaa. Sisäisen valvonnan näkökulman olen tuonut esille ainoastaan käyttöoikeushallinnan näkökulmasta.

1.3 Tutkimusmenetelmä

Toteutan opinnäytetyöni laadullisena tapaustutkimuksena. Aineiston keruun teen työympäristössä. Tiedonhakumenetelminä käytän teemahaastatteluja ja osallistuvaa havainnointia. Tietoa haen myös aiheeseen liittyvistä Kirkon palvelukeskuksen dokumenteista. Laadullinen tutkimusmenetelmä sopii parhaiten tilanteessa, jossa halutaan saada ilmiöstä syvällinen näkemys, luoda uusia teorioita ja luoda ilmiöstä hyvä kuvaus. Laadullista tutkimusmenetelmää käyttämällä voidaan sekä tarkentaa että luoda uutta teoriaa. Myös prosessin kuvaukseen sanallinen kuvaus sopii määrällistä ilmaisua paremmin. (Kananen 2010, 41, 42.)

Osallistun käyttöoikeuksien hallintaan työssäni välittämällä käyttöoikeuspyyntöjä vastuuhenkilöille. Teen päivittäin yhteistyötä käyttöoikeuksien hallinnasta vastaavien henkilöiden kanssa. Olen myös havainnoimalla kerännyt tietoa Kirkon palvelukeskuksen käyttöoikeuskäytänteiden nykytilasta. Tutkijan ollessa mukana tutkimustilanteessa on kyse osallistuvasta havainnoinnista. Tutkija osallistuu toimintaan ja näin tukija pääsee syvälle kiinni tutkittavaan ilmiöön. Kun tiedetään havainnoinnin tarkoitus, voidaan kiinnittää huomio havainnoitavaan ilmiöön. Havainnot tulee kirjoittaa mahdollisimman tarkasti muistiin ja tehdä jatkuvaa analysointia. Jokaisen havainnointikerran jälkeen tulee tutustua aineistoon ja tehdä siitä tiivistelmä. Laadullisessa tutkimuksessa aineiston keruuta ja analysointia tehdään samanaikaisesti ja saadaan koko ajan käsitystä ilmiöstä. Tämä auttaa paremmin löytämään osa-alueet, joilla ratkaistaan tutkimusongelma. (Kananen 2010, 50, 51.)

Teemahaastattelu käydään keskusteluna, johon on etukäteen mietitty teemat. Teemahaastattelussa erittäin tärkeää on, että haastattelun kulku ja rakenne pysyvät haastattelijan hallinnassa. Aina teemojen käsittelyjärjestyksellä ei ole ratkaisevaa merkitystä, sillä keskustelun luonteva kulku määrää käsittelyjärjestyksen. Tutkimusongelman kuitenkin niin vaatiessa asiat on käsiteltävä teemahaastattelussa etukäteen määrätyssä järjestyksessä. Teemahaastattelussa aineisto muodostuu haastateltavan henkilön kokemuksista, eikä tutkijan etukäteen mietityt vastausvaihtoehdot aina rajaa kertyvää aineistoa. (Teemahaastattelu, hakupäivä 28.1.2013.)

Opinnäytetyöhöni liittyvät haastattelut toteutan teemahaastatteluina. Kanasen mukaan (2010, 48, 49) mukaan kvalitatiivisessa tutkimuksessa haastattelut ja dokumentit ovat tärkeitä tiedonkeruumenetelmiä. Haastattelen palvelukeskuksen taloushallinnon palvelupäällikköä, tietohallintopäällikköä sekä käyttöoikeuksista vastaavaa sovellusasiantuntijaa. Laadullisessa tutkimuksessa tehdään usein pieni määrä haastatteluja, joita analysoidaan perusteellisesti. Tällöin tieteellisyyden kriteeri ei ole määrä vaan laatu, eikä tutkimuksen onnistumisen kannalta aineiston koolla ole välitöntä vaikutusta tai merkitystä. Osa haastatteluista voidaan nauhoittaa ja niiden aikana tehdään muistiinpanoja. Aineistoa kerätään ja sitä käsitellään tarpeen mukaan tutkimuksen edetessä. Toisin kuin kvantitatiivisessa tutkimuksessa, jossa aineiston kerääminen, käsittely ja analyysi ovat omia vaiheitaan, laadullisessa tutkimuksessa voidaan aineistoa kerätä, käsitellä ja analysoida koko tutkimusprosessin ajan (Koivula, Suihko & Tyrväinen, 2002, 37; Eskola & Suoranta 2008, 18, 62.)

2 ORGANISAATION PROSESSIT JA KYPSYYSTASOMALLIT

Kipa toimii prosessiorganisaationa, jonka strategisiin päämääriin sisältyy myös prosessien kehittäminen ja asiakkaan prosessien kehittämisen tukeminen. (Kirkon palvelukeskus 2013, hakupäivä 12.3.2013.) Organisaation prosessien jokaisessa vaiheessa on otettava huomioon myös tietoturvallisuus. Tässä luvussa tarkastelen opinnäytetyöni aiheeseen käyttöoikeusprosessiin liittyvää käsitettä prosessi sekä organisaation kyvykkyyttä ja kypsyystasomalleja, joiden avulla organisaation prosessien kypsyyttä voidaan mitata ja näin kehittää organisaation toimintaa.

2.1 Prosessit

Laamanen ja Tinnilä (2009, 121, 122) määrittelevät Prosessijohtamisen käsitteet – kirjassa prosessin joukoksi toimintoja ja niiden toteuttamiseen tarvittaviksi resursseiksi, jotka liittyvät toisiinsa ja joiden avulla syötteet muutetaan tuotoksiksi. Toimintaa tai kehityskulkua voidaan kuvata prosessina. Organisaation kannalta kiinnostavia ovat prosessit, jotka ovat kriittisiä organisaation menestymisen kannalta. Näitä kutsutaan usein liiketoimintaprosesseiksi, pääprosesseiksi tai avainprosesseiksi. Asiakkaille suoraan arvoa tuottavat prosessit ovat ydin- tai myös liiketoimintaprosesseja. Edellytykset ulkoisille asiakkaille arvoa tuottaville prosesseille luovat tukiprosessit. Termejä johtamisprosessi ja ohjausprosessi voidaan käyttää strategisen suunniteluun sekä toiminnan suunnitteluun ja seurantaan. Laaja prosessi voidaan jakaa prosessikokonaisuuksiin, jolloin käytetään käsitteitä osaprosessi tai aliprosessi.

Prosessilla kuvataan se, miten työ tehdään ja arvo tuotetaan organisaatiossa. Sen avulla kuvataan toimintojen logiikkaa ja kehitetään toimintoja. Prosessien avulla voidaan organisaation kulttuuria muuttaa. Prosessien avulla pyritään löytämään eri yksiköiden tai toimijoiden väliseen yhteistyöhön yhteisen asiakkaan parhaaksi oikeat menettelytavat. Prosessia kehittäessä prosessi on ensin tunnistettava, jonka jälkeen prosessi voidaan kuvata. Kuvaamisen jälkeen prosessi viedään käytäntöön, jonka jälkeen prosessia tulee jatkuvasti parantaa. Prosessiajattelussa tarkoitus on parantaa yrityksen suorituskykyä

samalla ottaen huomioon asiakkaan ja sidosryhmien tarpeet. Prosessijohtaminen (Business Process Management, BPM) tarkoittaa prosessikokonaisuuden tai yksittäisen prosessin johtamisessa noudatettavia periaatteita ja sopimuksia. (Paunia 2013, hakupäivä 6.4.2013.)

Prosessin kuvauksessa tulee olla mukana prosessin oleelliset tekijät, kuten resurssit, henkilöstö, menetelmät ja työkalut, tuotos, ympäristökuvaus sekä liittymäpinnat muihin prosesseihin. Prosessin kuvauksessa esitetään siis ne kriittiset toiminnot ja muut määrittelyt, jotka ovat prosessin ymmärtämisen kannalta tärkeitä. Liiketoiminnan prosessille tulee prosessiajattelun mukaan nimetä omistaja, jolla on operatiivinen vastuu prosessista. Prosessin omistajan vastuulla on myös tietoturvallisuuden huomioiminen prosessin jokaisessa vaiheessa. (Laaksonen, Nevasalo & Tomula 2006, 134; Laamanen, Tinnilä 20009, 123.)

2.2 Kyvykkyyksien ja kypsyystasojen mittaaminen

Kyvykkyydellä tarkoitetaan kykyä toimia tarkoituksenmukaisesti käytännön tilanteissa. Organisaation kyvykkyydestä tai tietämyksestä puhuttaessa viitataan toimintamalleihin ja prosesseihin, joita organisaatiossa on omaksuttu tai osaamisen kasvattamiseen liittyviin investointeihin. Organisaation kyvykkyyksiä on mahdollista mitata mm. kypsyysmallien avulla. Perusajatuksena kypsyysmalleissa on se, että kehittäminen tapahtuu tietyssä järjestyksessä. Tällöin kyvykkyydet rakentuvat toistensa varaan ja kypsyysmallin avulla nähdään kehityspolku. Kypsyystasomallien perusidea on se, että siinä vaiheessa, kun on kypsyystason kaikki alemmat vaatimukset täytetty, voidaan päästä korkeammalle kypsyystasolle. Siihen, mitä kypsyystasoa yritys tavoittelee, vaikuttaa toimiala, omat tavoitteet ja ulkoiset vaatimukset, eikä kaikkien prosessien tarvitse olla samalla kypsyystasolla. Kypsyysmalli auttaa myös valitsemaan kulloiseenkin kehitysvaiheeseen tehokkaan parantamisstrategian. Prosessien kypsyystasot mitataan pääsääntöisesti prosessien läpikäymisellä ja haastatteluilla. (Laaksonen ym. 2006, 274, 275; Laamanen & Tinnilä, 2009, 92, 93.)

Kypsyysmallien avulla kypsyyden eli toiminnan määrämuotoisuutta mitattaessa tulee ottaa huomioon, ettei toiminnan tai prosessin saattaminen korkealle kypsyystasolle merkitse vielä sitä, että itse toiminnan tulos on hyvä tai laadukas. Tämän lisäksi tarvitaan itse lopputuloksen tai tehokkuuden mittaamista. Suurin osa kypsyystasoa soveltavista malleista käyttää kypsyystason osoittamiseen viisi-kuusiportaista asteikkoa. Yleensä kypsyysmallien asteikko on alla olevassa kuvassa (kuva 1) mukainen, joskin eri mallien välillä voi olla pieniä vaihteluita, mutta periaate on kaikissa sama. (Laaksonen ym. 2006, 274.)

Taulukko 1. Kypsyysmallien asteikko (Laaksonen ym. 2006, 274.)

0	Ei – olemassa – Kyseistä prosessia ei ole ollenkaan.
1	Alustava / tapauskohtainen – Organisaatio on tunnistanut kyseiseen prosessiin liittyvät asiat ja tarpeet. Kyseistä prosessia ei kuitenkaan virallisesti ole olemassa ja asiat hoidetaan tapauskohtaisesti.
2	Toistettava – Prosessi on siinä määrin määrämuotoinen, että samat tehtävät tulevat samalla tavalla suoritetuksi vaikka suorittaja vaihtuisi. Prosessista ei ole formaalisti tiedotettu, eikä henkilöitä ole koulutettu siihen.
3	Määritelty – Prosessi on määritelty ja formaalisti dokumentoitu. Kaikki henkilöt joita prosessi koskettaa ovat tietoisia siitä ja heidät on asianmukaisesti koulutettu. Itse toimintatapoja ei ole pyritty kehittämään, vaan on lähinnä kuvattu olemassa olevat toimintatavat.
4	Hallittu – Prosessin toimivuutta ja tilaan voidaan seurata ja mitata. Prosessin epäkohtiin on mahdollista puuttua. Prosessit ovat jatkuvan kehityksen alaisia ja toimintatavat edustavat alan parhaita käytäntöjä. Automaattisia työkaluja käytetään, mutta niiden käyttö on rajoittunutta.
5	Optimoitu – Prosessi on hioutunut jatkuvan parantamisen seurauksena ja edustaa alansa huippua. Menetelmät ja työvälineet on integroitu muihin välineisiin ja prosesseihin.

Tietyn kypsyystason omaavan toiminnan osalta hyvyys ja tuloksellisuus on mitattava erikseen, prosessin kypsyystaso ei mittaa sitä. Formaalit ja optimoidut prosessit tuottavat todennäköisimmin ei määrämuotoisia prosesseja parempaa lopputuotetta. Toiminnan tuloksellisuutta on mahdollista mitata esimerkiksi ajan tasalla olevien järjestelmän käyttöoikeuksien perusteella. Tärkeää on huomata, että tarkoitus on nimenomaan toiminnan lopputuloksen laadun parantaminen, jonka vuoksi hyvin mittareidenkin tulee mitata lopputuotoksen laatua tai muutosta siinä. (Laaksonen ym. 2006, 276.)

Alla olevassa kuvassa (kuva 2) on esimerkki Capability Maturity Model – kypsyystasomallista (CMM), jolla voidaan kuvata toiminnan ja prosessien kypsyyttä. CMM-kypsyystasomalli on alkujaan kehitetty ohjelmistokehitysprosessien kypsyystasomalliksi, mutta sitä hyödynnetään nykyään myös monien muiden prosessikokonaisuuksien kehittämisessä. CMM-mallissa on yhteensä viisi porrasta, jossa aina ylempään portaaseen on sisällytettynä kaikkien aikaisempien portaiden toimintatavat ja tavoitteet. (Julkisen hallinnon kokonaisarkkitehtuuri 2011, 7.)

Seuraavassa kuvassa esitetään CMM-mallin portaat, joista kullekin malli antaa joukon keinoja, joilla kehittää toimintaa seuraavalle portaalle. Organisaatiossa mallin tietylle portaalle voidaan sijoittaa tietyn rajatun kokonaisuuden prosessit. Tasot, joille tyypillisesti prosessin kehittämisessä tähdätään, ovat kolme ja neljä. Prosessit on määritetty ja otettu käyttöön tasolla kolme. Tasolla neljällä otetaan käyttöön jatkuvan kehittämisen prosessit, joilla voidaan arvioida tason kolme aikana määriteltyjä prosesseja ja niiden toimivuutta. Tasolla neljä myös arvioidaan tasolla kolme määriteltyjen prosessimallien noudattamista ja kehitetään prosesseja havaintojen perusteella. (Julkisen hallinnon kokonaisarkkitehtuuri 2011, 7.)

Kuva 1. Kypsyystasomallin portaat (Julkisen hallinnon kokonaisarkkitehtuuri 2011, 7)

3 TIETOTURVALLISUUS

Laaksonen ym. (2006, 151) määrittävät kirjassaan käyttöoikeuksien hallinnan yhdeksi keskeisimmistä tietoturvallisuuden prosesseista. Selvitän tässä luvussa tietoturvallisuuden määritelmää ja, miten lainsäädäntö on otettava huomioon käyttöoikeuksien hallinnan yhteydessä käsiteltävissä henkilötiedoissa. Käsittelen tässä luvussa myös tietoturvapolitiikkaa, -suunnitelmaa ja tietoturvallisuuden johtamista. Tietoturvallisuus, muutoin kuin käyttöoikeuksien hallinnan osalta ei kuulu opinnäytetyöni tavoitteisiin.

Kirkkohallituksen lokakuussa 2011 antama päätös kirkon tietoturvamäärityksistä on julkaistu Kirkon säädöskokoelmassa Nro 109 (2011). Kirkon yleiset tietoturvamääräykset 2012 –asiakirjassa annetaan kirkon tietoturvamääräykset, joissa on vaatimukset mm. käyttöoikeuksien tietoturvallisuuden tasosta. Kirkon palvelukeskus on laatinut tietoturvasuunnitelman, joka on linjassa Kirkon tietoturvamääritysten kanssa. Kyseinen tietoturvasuunnitelma tarkastetaan vuosittain tai tarvittaessa.

3.1 Tietoturvallisuuden määritelmä

Hakalan, Vainion ja Vuorisen (2006) mukaan tietoturvallisuuden määritelmä lähtee ajatuksesta, että organisaation tärkein omaisuus on tieto, joka halutaan pitää luotettavana, oikeassa muodossa ja ainoastaan oikeiden henkilöiden saatavilla. Hakalan ym. mukaan (2006) perinteinen tietoturvallisuuden määritelmä koostuu luottamuksellisuudesta, käytettävyydestä ja eheydestä. Nykyisin tätä määritelmää pidetään riittämättömänä ja laajennettu tietoturvallisuuden määritelmä käsittää perinteisen määritelmän osatekijöiden lisäksi kiistämättömyyden ja pääsynvalvonnan. Luottamuksellisuudella (confidentiality) tarkoitetaan sitä, että tietoja on vain niihin oikeutettujen henkilöiden oikeus käyttää, säilyttää ja tuhota. Saatavuudella (availability) taas varmistetaan se, että tieto on saatavissa tietojärjestelmistä oikeassa muodossa ja riittävän nopeasti. Eheydellä (integrity) tarkoitetaan sitä, että tietojärjestelmien tiedot ovat paikkaansa pitäviä, eikä niissä ole tahallisia tai tahattomia virheitä. Kiistämättömyydellä (non-repudiation) varmistetaan, että tiedon siirtoon tai käsittelyyn osallistuneiden käyttäjien tunnistamista valvotaan ja

pääsynvalvonta (access control) tarkoittaa niitä toimia, joilla käyttäjien tietojärjestelmään käsiksi pääsyä rajoitetaan.

3.2 Lainsäädäntö

Laaksosen ym. (2006, 18) mukaan lainsäädäntö asettaa suoria ja epäsuoria velvoitteita yritysten ja muiden yhteisöjen tietoturvallisuudesta huolehtimiselle. Määritellyt velvoitteet ovat usein yleisluonteisia. Myös käytännön toteutus ja riittävän tietoturvallisuuden tason määritteleminen on jätetty yritykselle. Yrityksen kannalta tärkeää on kartoittaa tietoturvansa kannalta pakottavat yksittäiset säädökset ja myös tunnistaa sopimuksiin perustuvat tietoturvavelvoitteet ja oikeudet.

Suomessa ei ole erillistä kaikkia tietoturvavelvoitteita kokoavaa tietoturvalakia vaan velvoitteet on määritelty osana jonkin muun lain sisältöä, esimerkiksi osana henkilötietolakia. Perustuslaissa (731/1999) on velvoitettu säätämään henkilötietojen suojasta lailla. Tätä toteuttavat henkilötietolaki (523/1999) ja laki yksityisyyden suojasta työelämässä (759/2004). Nämä lait sisältävät keskeisimmät säädökset työelämässä tapahtuvasta henkilötietojen käsittelystä. Henkilötietolaki (523/1999) on työelämässä tapahtuvan henkilötietojen käsittelyä koskeva yleislaki, jota sovelletaan yritysten, viranomaisten, järjestöjen sekä muiden yhteisöjen ja rajoitetusti myös yksityishenkilöiden suorittamaan henkilötietojen käsittelyyn. Henkilötietolaki (523/1999), jonka edeltäjä oli henkilörekisterilaki, tuli voimaan 1999. Lakia sovelletaan yrityksissä, joissa käsitellään yksittäisen henkilön henkilötietoja, kuten nimeä tai henkilötunnusta. Kaikki työelämässä tapahtuvat henkilötietoihin liittyvät toimenpiteet, henkilötietojen luovuttamisesta tietojen poistamiseen, katsotaan henkilötietojen käsittelyksi. Henkilötietolainsäädäntö sovittaa yhteen työtekijän perusoikeuksia ja työnantajan intressit. (Koskinen, Alapuranen & Heino & Salli 2006 11, 16; Laaksonen ym. 2006, 18, 31).

Henkilötietolaki (523/1999) edellyttää henkilötietojen suojaamista, tietojen tarpeellisuus- ja virheettömyysvaatimuksen sekä käyttötarkoitussidonnaisuuden vaatimuksen

huomioon ottamista. On myös otettava henkilötietolain muut henkilötietojen käsittelyä koskeva vaatimukset huomioon. Jotta näitä vaatimuksia voidaan noudattaa ja sitä valvoa, on käyttöoikeuksien määrittely tehty asianmukaisesti henkilötasolla ja käyttöä on mahdollista myös jälkikäteen valvoa. Käyttöoikeudet muodostavat henkilölaissa mainitun henkilörekisterin, jota koskevat henkilötietolain vaatimukset. Tämä tarkoittaa sitä, että käyttäjärekisteriä koskevat myös henkilötietolaissa mainitut suojaamis- ja huolellisuusvelvoitteet. (Valtiovarainministeriö 2006, 11, 12.)

Lähtökohtana laissa on, että tietoturvan tason määrittää rekisterinpitäjä itse, sillä riittävää tietoturvan tasoa ei ole määritelty kattavasti lain tasolla eikä oikeustapaustenkaan perusteella. Käsiteltävien henkilötietojen laatu vaikuttaa rekisteriltä vaadittavaan tietoturvan tasoon. Tapauksissa, joissa tietojärjestelmiin on tallennettu pelkästään henkilön yhteystiedot, tietoturvan tason ei tarvitse olla sama, kuin käsiteltäessä lain sallimissa puitteissa arkaluonteisia tietoja, kuten henkilötunnuksia. Se, miten laajasti henkilötietoja käsitellään, tulisi rekisterinpitäjän huomioida käyttöoikeuksien määrittelyssä ja hallinnassa. Kaikkien ei tarvitse päästä käsiksi palkkatietoihin, joten on tärkeää, että käyttöoikeudet vastaavat riittävällä tasolla työntekijöiden työnkuvaa. Käyttöoikeudet onkin luontevinta määritellä rooliperusteisesti eli työntekijän työtehtävien perusteella. (Laaksonen ym. 2006, 42, 43, 45.)

Arkistolain (831/94) säännöksien mukaiset säilytysajat käyttövaltuushallintoon liittyvien tietojen ja asiakirjojen sekä järjestelmän lokitietojen säilytysaikojen osalta on määriteltävä. Säilytysajan jälkeen hävitettävien tietojen on tapahduttava siten, että tietosuoja ja tietoturvallisuus on varmistettu. (Valtiovarainministeriö 2006, 30.)

3.3 Tietoturvapolitiikka ja -suunnitelma

Organisaation tärkein tietoturvakäytäntöjä ja tietoturvallisuusprosessia ohjaava dokumentti on yrityksen tietoturvapolitiikka (Information security policy). Yrityksen tietoturvasuunnittelun yksi tavoite on luoda organisaatiolle tietoturvapolitiikka. Tietoturva-

politiikka muodostuu käytännöistä, joilla haluttu tietoturvallisuuden taso saavutetaan. Käytäntöjen tulee olla organisaation ylimmän johdon hyväksymiä. Johto määrittelee tietoturvapolitiikan avulla tietoturvatoiminnan tavoitteet, vastuut sekä toimintalinjat. Organisaation toiminnan tarkoitus ja strategia, riskianalyysi, lait ja määräykset ohjaavat tietoturvapolitiikan luomista. Tietoturvapolitiikka määrittelee kunkin erillisen liiketoimintaprosessin tai liiketoiminnan kannalta erityisen tärkeän tietojärjestelmän käytännön. Käytäntö määritellään menetelmäkokonaisuudeksi, joka muodostuu useasta eri käytänteestä. Esimerkiksi palkkahallinnossa käytäntö voi määritellä sen, että työntekijöiden henkilötietoihin pääsyä rajoitetaan vain palkanlaskijoilta ja näiltä vaaditaan käyttäjäntunnistus. Se, miten rajoittaminen ja autentikointi tapahtuu, muodostuu taas useammasta teknisestä ja hallinnollisesta käytänteestä, ja ovat jo tietoturvasuunnitelmaan kuuluva alue. (Hakala ym, 2006 7, 8; Vahti 3/2007, 25.)

Kirjalliseen muotoon laadittavan tietoturvapolitiikan tarkoitus on toimia keskipitkän, n. 5 vuotta, ja pitkän, n. 10 vuotta, aikavälin ohjeena tietojärjestelmien suunnittelijoille sekä liiketoimintaprosessien vastuullisille esimiehille. Vaikka politiikka laaditaan useammalle vuodelle, tulee tarkistaa vähintään vuosittain, että se vastaa organisaation nykyistä toimintaa ja turvallisuustarpeita. (Hakala ym. 2006, 7.)

Tietoturvasuunnitelmassa on kuvattu ne käytänteet, joilla haluttu tietoturvataso saavutetaan. Kirjallisessa muodossa on määritelty järjestelmissä käytetyt työmenetelmät ja tekniset ratkaisut. Tietoturvasuunnitelma tulee laatia keskipitkälle, 2-5 vuotta, aikavälille, mutta suunnitelma on syytä tarkistaa vähintään vuosittain. Tietoturvasuunnitelma tulee tarkistaa aina, kun yrityksen tietojärjestelmissä tai työmenetelmissä tapahtuu olennaisia muutoksia, sillä organisaation toimintaprosesseissa tapahtuvat muutokset ja uusi käyttöön otettu teknologia edellyttävät, että tietoturvasuunnitelmaa päivitetään. Tietoturvasuunnitelmassa on kuvattu käytettäviä menetelmiä ja teknisiä ratkaisuja tietoturvapolitiikkaa yksityiskohtaisemmin, jonka vuoksi suunnitelma luokitellaan luottamukselliseksi tai salaiseksi. (Hakala ym. 2006, 9.)

3.4 Tietoturvallisuuden johtaminen ja hallinnointi

Laaksosen ym. (2006, 115, 116) määritelevät tietoturvan johtamisen tarkoittavan suppeasti määritettynä tietoturvallisuudesta huolehtimista lain vähimmäisvaatimusten edellyttämällä tavalla ilman, että selkeää suunnitelmaa tai vastuuta on määritelty. Laajemmin käsitettynä tietoturvan johtaminen tarkoittaa nimettyä tietoturvapäällikköä, jonka tehtävä on hallinnoida yrityksen tietoturvaa kokonaisuudessaan. Laajimmillaan käsitettynä se on yritysjohdon uusi tehtäväkokonaisuus, joka koskettaa liiketoiminnan johtamista sekä tietohallinnon johtamista.

Monet tietoturvallisuuden vaatimukset tulevat laeista, joiden mukaisesti tietoturvan tulee olla riittävällä tasolla. Tietoturva on otettava huomioon organisaation kaikissa yksiköissä osana päivittäistä johtamista ja jokaisen työntekijän toimintaa. Toiminnan luonne, liiketoiminnan vaatimukset sekä muut ulkoiset vaatimukset ovat ne tekijät, jotka määrittävät tietoturvallisuuteen liittyvät painotukset. (Laaksosen ym. 2006, 115, 116)

Tieto on yrityksessä pyrittävä suojaamaan siten, että tietoturvallisuuden perusvaatimukset eli saatavuus, eheys ja luottamuksellisuus säilyvät. Yrityksen eri toiminnoissa voi perusvaatimusten tärkeys vaihdella. Tietoturvallisuutta suunniteltaessa on huomioitava ja tunnettava organisaation nykytilanne, vahvuudet ja heikkoudet sekä järjestelmät, joiden avulla kriittistä tietoa käsitellään. Perustana tietoturvallisuudelle on organisaation varsinaiseen liiketoimintaan tiiviisti liitetty tietoturvallisuus sekä täsmällinen johtaminen, joka perustuu määrätietoiseen ja organisoituun toimintaan. (Laaksonen ym. 2006, 116, 117.)

4 KÄYTTÖOIKEUSPROSESSI

Käyttöoikeuksien hallintaprosessilla tarkoitetaan niitä toimia, jotka liittyvät järjestelmän käyttäjä- ja käyttöoikeustietojen sekä käyttövaltuuksien ylläpitoon. Hallintaprosessi edellyttää määrittelyn, kuvaamisen ja ylläpidon. Määrittelyssä tulee kiinnittää huomiota siihen, että prosessit ovat kattavia ja riittävän turvallisia. Prosessit ylläpidetään ajantasaisilla kuvauksilla sekä ohjeistuksilla. Prosesseille ja suojattaville kohteille tulee nimetä vastuuhenkilöt, jotka päättävät oikeuksien myöntämisestä. Lisäksi kaikkien prosessiin osallistuvien organisaatioyksiköiden sekä henkilöiden vastuut, velvollisuudet ja valtuudet tulee olla selkeästi määriteltyjä. (Valtiovarainministeriö 2006, 16.)

Käsittelen tässä luvussa käyttöoikeuksien hallintaa, hallintajärjestelmää, provisiointia eli käyttöoikeuksien automaattista siirtoa palvelujärjestelmiin sekä roolipohjaisia käyttöoikeuksia. Lopuksi kuvaan palvelukeskuksen käyttöoikeuspyyntöihin liittyvää nykytilannetta.

4.1 Käyttöoikeuksien hallinta

Käyttöoikeuksien hallinnalla tarkoitetaan käyttöoikeuksien luomista, muutoksia, poistoa ja seurantaa. Tietojärjestelmissä on huomioitava, kenellä on käyttöoikeudet järjestelmiin. Työntekijöillä tulee olla käyttöoikeudet vain niihin järjestelmiin, joita henkilö työssään tarvitsee. Henkilön vaihtaessa työtehtäviä tai lähtiessä yrityksessä on käyttöoikeuksien hallinnan toimittava siten, ettei tarpeettomia oikeuksia jää järjestelmiin. Kun käyttöoikeuksia ei enää tarvita, oikeudet poistetaan välittömästi. Tärkeää on myös määritellä käytännöt tilanteisiin, joissa tarvitaan varamiestä. (Laaksonen ym. 2006, 151; Ahokas 2012, 122.)

On tärkeää huomioida tarvitseeko henkilö katseluoikeudet, oikeudet muokata tietoa vai järjestelmän ylläpito-oikeudet. Ylläpito-oikeuksia ei tulisi olla kuin vain rajatulla joukolla henkilöitä. Järjestelmän tai tiedon omistajan tulisi hyväksyä käyttöoikeudet. Perustuen hyväksyntään konkreettinen käyttöoikeuksien lisäämisen tekee järjestelmiin yleensä tietohallinnon tai järjestelmän ylläpitäjä. Heillä tulee olla tieto siitä, kenellä on oikeus pyytää käyttöoikeuksien lisäämistä kuhunkin tietojärjestelmään. Järjestelmän käyttäjien

käyttöoikeuksista tulee pitää dokumentaatiota, jota myös tulee tarkistaa säännöllisin väliajoin. (Laaksonen ym. 2006, 151; Ahokas 2012, 122.)

Laaksonen ym. (2006, 151, 152) suosittavat käyttöoikeuksiin liittyviin pyyntöihin lomakkeen tai mieluummin sovelluksen tekemistä, jolla käyttöoikeuksiin liittyvät pyynnöt tehdään. Joissain tapauksissa eri järjestelmille on hyvä tehdä erilliset lomakkeet. Helpoin tapa on pyrkiä määrittämään eri käyttäjäryhmille roolit ja tietylle roolille määritellään tarpeelliset käyttöoikeudet. Tällöin käyttöoikeudet tarvitseva käyttäjä voidaan lisätä tarvittavaan rooliin, ja hän saa roolin mukaiset oikeudet. Kullekin roolille on hyvä olla omistaja. Hyväksytyt ja mahdollisesti myös hylätyt käyttöoikeuksien lisäämispyynnöt tulee keskitetysti arkistoida.

4.2 Käyttöoikeuksien hallintajärjestelmä

Valtiovarainministeriön ohjeessa (2006, 24, 26) on kuvattu käyttöoikeuksien hallintajärjestelmän muodostuvan

- osajärjestelmästä, joka toteuttaa automaattisen luvitusprosessin eli käyttöoikeuksien haku-, hyväksymis- ja luontiprosessin. Osajärjestelmään on liittymät käyttäjätietoja tuottavista lähdetietojärjestelmistä. Tätä käyttävät palvelujärjestelmien käyttäjät ja käyttöoikeuksien hyväksyjät
- keskitetystä käyttäjä- ja käyttöoikeusvarastosta
- automaattisesta käyttöoikeustietojen provisiointijärjestelmästä.
- jäljitettävyys- ja raportointitoiminnoista.

Käyttöoikeuksien hallintajärjestelmän automatisoinnilla tarkoitetaan työnkulkujen määrittely ja automatisointi –toiminnallisuutta. Toiminnallisuuden ohjaamana tapahtuvat käyttöoikeuksien määrittely- ja hyväksymisprosessit. Prosesseihin tulee olla myös määriteltynä jäljitettävyysvaatimusten edellyttämät lokikirjaustoiminnot. Hallintajärjestelmän avulla on mahdollista toteuttaa automatisoitu käyttöoikeuksien haku-, hyväksymis- ja luontiprosessi. Tällöin syötteet tulevat henkilötietoja tuottavista järjestelmistä tai muutostietoja itsepalveluna lisääviltä käyttäjiltä. Tietyissä tilanteissa järjestelmään käyttöoikeusvastaavat tai hallintajärjestelmän järjestelmävastaavat voivat syöttää manuaalisesti tietoja järjestelmiin. Tärkeimmät tekniset vaatimukset hallintajärjestelmälle

ovat varmistettu ympärivuorokautinen käyttö ja toimivat varajärjestelyt poikkeustilanteisiin, korkein mahdollinen sisäinen tietoturvallisuus sekä skaalautuvuus eli laajennettavuus määrällisesti ja maantieteellisesti. (Valtiovarainministeriö 2006, 25, 30.)

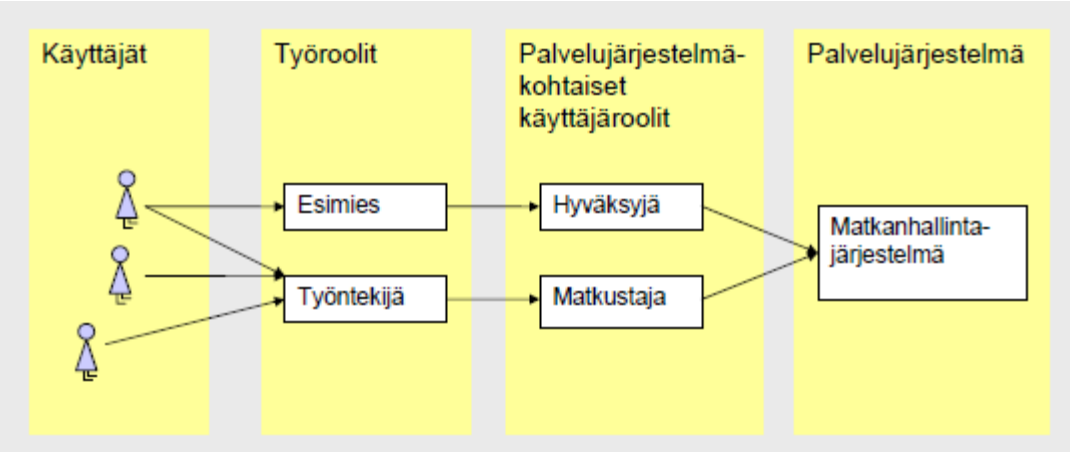
4.3 Käyttöoikeuksien provisiointi

Valtiovarainministeriön ohje (2006, 26) määrittelee käyttöoikeuksien provisioinnilla tarkoitettavan uusien ja muuttuneiden käyttäjä- ja käyttöoikeustietojen automaattista siirtoa organisaation palvelujärjestelmiin. Kuljettuaan hallintajärjestelmässä luvitusprosessin läpi käyttöoikeustapahtumat siirretään automaattisesti kohdejärjestelmiin. Tämä voi tapahtua joko heti tapahtuman synnyttyä tai ajastettuna. Jotta voidaan verrata käyttöoikeuskannassa olevia tietoja tietojärjestelmän käyttöoikeustietoihin, on hyvä siirtää tietoa myös tietojärjestelmistä käyttöoikeuskantaan. Näin voidaan havaita nopeasti mahdolliset yritykset antaa käyttöoikeuksia virallisen prosessin ohi sekä mahdollisesti provisioinnin aikana tapahtuneet tekniset virheet. Provisioinnissa ongelmana on, ettei tietojen kohdejärjestelmiin syöttämiseen tarvittavia rajapintoja ole standardoitu, jonka vuoksi provisiointiliitäntöjä täytyy räätälöidä.

4.4 Roolipohjainen käyttöoikeus

Käyttöoikeuksia määriteltäessä ei ole järkevää tarkastella yhtä käyttäjää. Sen sijaan tulee luoda käyttäjäryhmät**,** jossa yhden ryhmän käyttäjillä on kaikilla samantyyppiset työtehtävät. Samaan ryhmään kuuluvilla käyttäjillä on samanlainen toiminnallinen rooli eli työrooli, tarkoittaen samanlaisia tietotarpeita ja toimintavaltuuksia. Käyttöoikeuksia on perinteisesti hoidettu luomalla tietojärjestelmiin erilaisia käyttöoikeusyhdistelmiä, joita kutsutaan järjestelmien käyttäjärooleiksi. Käyttäjärooleihin on sijoitettu yksittäiset käyttäjät. Tämä on johtanut siihen, että tarpeiden muuttuessa rooleja on jouduttu määrittelemään aina lisää kussakin palvelujärjestelmässä. Tehokkaampaa käyttöoikeuksien hallinnan kannalta on erottaa toisistaan käyttäjien työroolit ja palvelujärjestelmien mahdollistamat käyttäjäroolit. Tällöin työroolit kytketään järjestelmän rooleihin. (Valtiovarainministeriö 2006, 17, 18.)

Yhdellä henkilöllä voi olla useampi rooli samanaikaisesti. Rooleja voivat olla esimerkiksi käyttäjän kuuluminen johonkin organisaatioryhmään tai esimiesasema. Alla (kuva4) on kuvattuna rooliin perustuvan valtuutuksen malli, jossa esimerkkinä on käytetty matkanhallintajärjestelmän oikeuksia. Kuvassa käyttäjinä ovat työntekijä ja esimies, joille on annettu työroolit työntekijä ja esimies. Esimiehellä on palvelujärjestelmäkohtaisena käyttäjäroolina hyväksyjä ja vastaavasti työntekijällä matkustaja. Molemmilla käyttäjärooleilla kyseiset käyttäjät pääsevät eri valtuuksin matkanhallintajärjestelmään. Esimiehellä voi olla molemmat roolit eli hän voi toimia sekä esimiehen että työntekijän asemassa käyttäen matkanhallintajärjestelmää joko matkustajan tai hyväksyjän ominaisuudessa. (Linden 2007, 12; Linden 2012, 31.)



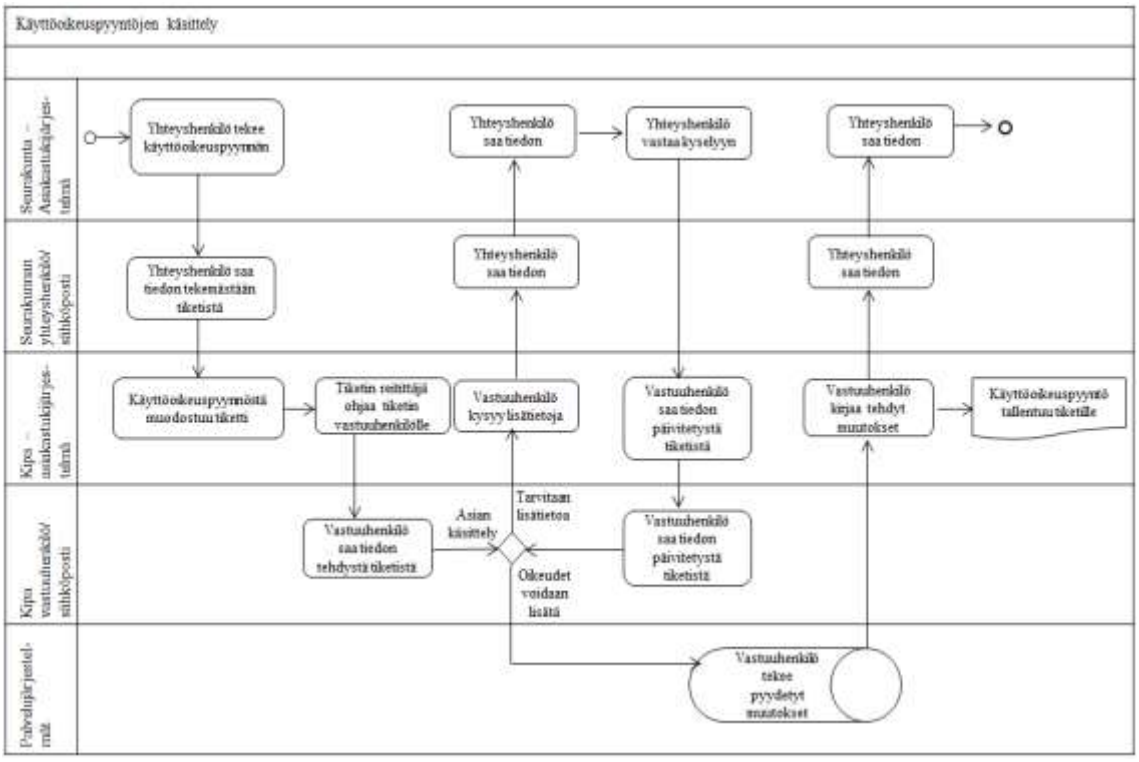
Kuva 2. Rooliin perustuvan valtuutuksen viitemalli esim. matkanhallintajärjestelmä (Linden 2007, 12)

4.5 Palvelukeskuksen nykyinen käyttöoikeusprosessi

Palvelukeskuksessa on meneillään käyttöoikeuksien hallintajärjestelmän käyttöönottohanke. Hankkeen aikana käyttöön otetaan käyttöoikeuksien hallintajärjestelmä, jossa seurakunnat tekevät käyttöoikeuspyynnöt palvelukeskuksen palvelutuotantojärjestelmiin. Jatkossa kaikki käyttöoikeuspyynnöt palvelukeskukseen tehdään käyttöoikeuksien hallintajärjestelmässä. Hankkeen ensimmäisen vaiheen tavoitteena on, että käyttöoikeusjärjestelmässä tehty käyttöoikeuspyyntö lähetetään sähköpostitse suoraan palvelukeskuksen käyttöoikeuksista vastaaville henkilöille. Lisäksi viesti lähetetään asiakastukijärjestelmään, jossa palvelukeskus hallinnoi asiakkaiden tuki- ja palvelupyyntöjä. Käyttö-

oikeuksien hallintajärjestelmään sekä tulevaan käyttöoikeusprosessiin liittyvät tiedot ovat salaisia ja niihin liittyvät tiedot luovutetaan vain toimeksiantajalle.

Siirtyessään palvelukeskuksen asiakkaaksi seurakunnat toimittavat tarvittavien käyttöoikeuksien osalta Excel-listat, joista löytyy tiedot käyttäjistä, heille lisättävistä oikeuksista ja rooleista sekä tiedot järjestelmistä, joihin käyttöoikeudet tarvitaan. Listan perusteella käyttöoikeudet lisätään palvelukeskuksen järjestelmiin. Tämän jälkeen seurakuntien yhteyshenkilöt tekevät uudet käyttöoikeuspyynnöt alla olevassa kuvassa esitetyn (kuva 4) mukaisesti. Yhteyshenkilöt tekevät käyttöoikeuksiin liittyvät pyynnöt asiakastukipyyntöjärjestelmän kautta tiketillä. Tiketti tarkoittaa asiakastukijärjestelmässä tehtyä palvelu- tai tukipyyntöä. Palvelukeskuksessa vastuuhenkilö lisää pyydetyt käyttöoikeudet ja tarvittaessa pyytää seurakunnan vastuuhenkilöltä lisätietoja asiakastukipyyntöjärjestelmän kautta. Kun käyttöoikeudet on lisätty, ilmoittaa vastuuhenkilö asiasta asiakastukipyyntöjärjestelmän välityksellä seurakunnan yhteyshenkilölle. Seurakunnan yhteyshenkilöiden tekemistä käyttöoikeuspyynnöistä jää dokumentti asiakastukipyyntöjärjestelmään tiketille. Käyttöoikeuksien muutos- ja poistopyynnöt hoidetaan ja dokumentoidaan kuten uudet käyttöoikeuspyynnöt.



Kuva 3. Palvelukeskuksen nykyinen käyttöoikeuspyyntöjen käsittelyprosessi

Käyttäjät lisäävät sijaisuusoikeudet seurakunnissa ensisijaisesti itse. Tarvittaessa sijaisuudet voivat asettaa vastuuhenkilöt palvelukeskuksessa, jolloin sijaisuusoikeudet pyydetään kuten muutkin käyttöoikeudet.

Palvelupäälliköt pyytävät sähköpostitse tai suullisesti vastuuhenkilöltä palvelukeskuksen työntekijöiden käyttöoikeudet. Näin toimitaan myös sijaisuuksien käyttöoikeuksissa. Käyttöoikeudet lisännyt vastuuhenkilö ilmoittaa oikeuksien myöntämisen jälkeen asiasta käyttäjälle sekä palvelupäällikölle joko suullisesti tai sähköpostitse. Käyttöoikeuksien muutos- ja poistopyynnöt hoidetaan kuten uudet käyttöoikeuspyynnöt. Palvelukeskuksen työntekijöiden käyttöoikeuksista tai käyttöoikeuksiin liittyvistä pyynnöistä ei jää dokumentoitua tietoa.

5 KÄYTTÖOIKEUKSIEN VALVONTA

Tämän opinnäytetyön toisena tavoitteena on määritellä keinoja käyttöoikeuksien valvontaan. Käyttöoikeuksien valvonta on yksi osa käyttöoikeuksien hallintaa. Tässä luvussa selvennän ensin, mitä valvontatoiminnoilla ja jäljitettävyydellä tarkoitetaan, jonka jälkeen käsittelen käyttöoikeuksien valvonnan keinoja. Tiedot palvelukeskuksen käyttöoikeuksien valvonnan osalta ovat salaisia ja ne luovutetaan vain toimeksiantajalle.

5.1 Valvontatoiminnot

Niina Ahokkaan (2012, 34) mukaan valvontatoiminnoilla tarkoitetaan politiikkoja ja menettelytapoja, joilla voidaan varmistaa, että organisaatio toimii sen johdon asettamisen tavoitteiden mukaisesti. Valvontatoiminnoilla voidaan varmistaa, että organisaatiossa ryhdytty tarvittaviin toimenpiteisiin tavoitteiden toteuttamista vaarantavien riskien tunnistamiseksi. Valvontatoimiin voidaan lukea erilaiset hyväksymiset, valtuutukset, todentamiset, täsmäytykset, toiminnan tarkastukset, omaisuuden turvaamistoimet sekä työtehtävien eriyttäminen. Niitä tulee suorittaa kaikissa organisaatiotasoissa ja toiminnoissa.

Valvontatoimintoja voidaan tehdä ehkäisevinä, paljastavina, manuaalisina, automaattisina tai johtamiskontrolleina. Ne voidaan jakaa toimintaperiaatteisiin eli politiikkoihin, jotka määrittävät mitä pitäisi tehdä ja kontrollitoimenpiteisiin, jotka ovat käytännön toimenpiteitä, joilla nämä politiikat toteutetaan. Kontrollitoimenpiteet voidaan taas jakaa ehkäiseviin ja paljastaviin tai automaattisiin ja manuaalisiin kontrolleihin. Ehkäisevät kontrollit suoritetaan virheiden ja väärinkäytösten ennaltaehkäisemiseksi, ja ovat yleensä sisäänrakennettu sisäiseen valvontajärjestelmään. Näitä ovat esimerkiksi työtehtävien eriyttäminen ja tietojen suojaaminen salasanoilla sekä rajoittamalla järjestelmien käyttöoikeuksia. Paljastavat kontrollit ovat jo tapahtuneiden virheiden ja poikkeaminen paljastamista varten sekä näiden korjaamisen varmistamiseksi. Näitä ovat esimerkiksi kirjanpidon rahatilin täsmäyttäminen pankkitiliotteisiin ja palkanmaksun oikeellisuuden tarkistus pistokokeilla. Manuaalisia kontrolleja ovat ne, joissa on osallisena henkilö ja automaattiset kontrollit ovat järjestelmän suorittamia. Käytännössä kontrollit ovat usein

semi-automaattisia kontrolleja eli esimerkiksi lokitietojen tarkastus, jossa systeemi ensin luo lokitiedot, jotka henkilö sitten tarkistaa. (Ahokas 2012, 34, 35, 36, 37.)

5.2 Jäljitettävyys ja raportointi

Kirjausketjun (audit trail) avulla voidaan Mika Lindenin (2012, 37) mukaan organisaation sisällä selvitellä ongelmia ja vikatilanteita. Kirjausketjun tarkoitus on kertoa kuka on tehnyt tietyn toimenpiteen ja mihin tämä valtuus tehdä toimenpide on perustunut. Jäljitettävyys (accountability) tarkoittaa identiteetin- ja pääsynhallinnan tapahtumien luotettavan kirjausketjun (audit trail) muodostamista. Jäljittäminen on mahdollista lokitietojen avulla, joita kerätään käyttäjän tunnistamisesta ja käyttövaltuuksien myöntämisestä ja näiden käyttämisestä. Näiden tietojen kerääminen ja eheys tulee varmistaa osana organisaation muuta lokitietojen hallintaa. Identiteetin- ja pääsynhallinnan lokitietojen hallinnassa on huomioitava henkilötietolain ja työntekijöiden lokitietojen hallinnassa myös työelämän tietosuojalain säädökset.

Käyttöoikeusprosessin avulla hallinnoituja käyttöoikeuksia tulee valvoa, jotta voidaan seurata sovittujen käytäntöjen noudattamista, käyttäjä- ja käyttöoikeustietojen ajantasaisuutta ja sitä, ettei järjestelmiin kerry tarpeettomia vanhoja määrityksiä. Käyttöoikeuksien valvonnalla tulisi voida ehkäistä käyttäjätunnusten lainaamiset sekä se, ettei useampi henkilö voi käyttää samaa tunnusta. Tärkeä osa käyttöoikeuksien hallinnointia on siihen liittyvien tietojen ja tehtyjen tapahtumisen raportoitavuus. Käyttäjien roolimäärittelyihin ja suojattavien kohteiden käyttöoikeuksiin tehdyt muutokset pitää voida jäljittää siten, että muutoksen tekoon liittyvät henkilöt pystytään selvittämään. Tämä onnistuu siten, että kaikki tapahtumat kirjataan lokitiedostoihin, jonka avulla voidaan käyttäjätietoja ja käyttöoikeuksien muutoksia seurata. Säännöllisen valvonnan avulla tulee seurata käyttöoikeustiedoissa tapahtuneita muutoksia, samoin niiden henkilöiden toimintaa, joilla on erityisen laajat käyttövaltuudet. Myös kriittisimpien kohteiden käytön osalta tulee olla säännöllinen valvonta. (Valtiovarainministeriö 2006, 21, 26; Ahokas 2012, 122.)

Käyttöoikeusvalvonnan välineitä ovat erilaiset raportointivälineet ja säännölliset katselmoinnit. Käyttöoikeuksien hallinnan lokitiedot ja hallinta- sekä palvelujärjestelmissä

olevat käyttöoikeustiedot ovat valvonnan perustana. Valvonnan järjestämisen vastuu on tietojen vastuullisilla omistajilla. Hallintajärjestelmän käyttöönottoon mennessä tulee olla sovittuna käyttöoikeuksien valvonnan organisointitavat sekä niihin liittyvät vastuut. Käyttöoikeuksien hallintajärjestelmästä tulee pystyä ajamaan raportteja, joilla saadaan tietoa käyttäjistä ja heidän käyttövaltuuksista, työrooleista, työrooliin kytketyistä käyttövaltuuksista. Raportteja tulee pystyä ajamaan käyttäjä-, työrooli- ja käyttövaltuustasolla. (Valtiovarainministeriö 2006, 21.)

Säännöllisesti, vähintään kerran vuodessa järjestettävien käyttöoikeuksiin liittyvien katselmointien tarkoitus on Valtiovarainministeriön (2006, 21) ohjeistuksen mukaan saada selville mahdolliset järjestelmissä olevat jo organisaation palveluksessa lopettaneet käyttäjät ja mahdolliset työroolit, joita ei enää käytössä. Tarkoitus on myös saada selville mahdolliset kohteet ja käyttöoikeudet, joita ei enää käytetä, mahdolliset irralliset käyttövaltuusmääritykset, liittyen käytöstä poistettuihin kohteisiin tai rooleihin sekä mahdolliset käyttäjät, joilla vaarallisia työrooli- ja käyttövaltuusyhdistelmiä. Lisäksi katselmoinneilla halutaan selvittää järjestelmien, roolien ja hallintaprosessien omistajuuksien ja niihin liittyvien toimeenpano- ja valvontavastuiden tilanne sekä hallinnointiprosessin toimivuus sovitun mukaisesti.

Laaksonen ym. (2006, 152) pitää henkilöstöhallintoa tärkeänä yhteistyökumppanina käyttöoikeuksien hallinnassa. Henkilöstöhallinnon uusien työtekijöiden palkkaamiseen ja työsuhteen päättymiseen liittyvät prosessit tulee pyrkiä integroimaan käyttöoikeuksien hallinnan prosessiin, jotta esimerkiksi työsuhteen päättymisen yhteydessä myös käyttöoikeuksien hallinnasta vastaava taho saa automaattisesti asiasta tiedon. Käyttöoikeuksien hallinnan prosessiin on hyvä sisällyttää säännöllisesti tehtävä käyttöoikeuksien tarkastus. Tarkistus tehdään henkilöstöhallinnon tuottaman listan perusteella. Listaan on koottu yrityksen työntekijät sekä mahdolliset ulkopuoliset yrityksen järjestelmiin käyttöoikeudet omaavat henkilöt. Poistettavat käyttöoikeudet tulee merkitä käyttöoikeuksien myöntämislomakkeisiin. Tällöin käyttöoikeuslomakkeissa olevat tiedot vastaavat yrityksen järjestelmissä olevia käyttöoikeuksia.

6 VAARALLISET TYÖYHDISTELMÄT JA TYÖTEHTÄVIEN ERIYTTÄMINEN

Käyttöoikeuksia myönnettäessä ja valvottaessa tulee kiinnittää huomiota vaarallisiin työyhdistelmiin. Työtehtävien eriyttämisellä voidaan estää vaarallisten työyhdistelmien muodostuminen. Opinnäytetyön yhtenä tavoitteena on miettiä keinoja, miten valvoa, ettei vaarallisia työyhdistelmiä palvelukeskuksessa syntyisi, jonka vuoksi käsittelen asiaa laajemmin omassa luvussaan. Työtehtävien eriyttäminen on tärkeä osa sisästä valvontaa. Käsittelen sisäistä valvontaa ja riskienhallintaa tämän luvun alussa. Tässä yhteydessä kerron myös Sarbanex-Oxley Act –laista (SOX). Vaikka laki velvoittaa yhdysvaltalaisiin pörsseihin listautuneita yrityksiä, eikä sinällään kosketa Kirkon palvelukeskusta, haluan nostaa sen tässä yhteydessä kuitenkin esille, sillä lain vaikutuksesta yrityksissä on herätty huomaamaan sisäinen valvonnan tärkeys.

Kirkkolaissa ei ole mainintaa sisäisestä valvonnasta, mutta Kirkkojärjestyksessä (1055/1993 15:8 §) sisäisen valvonnan osalta mainitaan, että seurakunnan ja seurakuntayhtymän tilintarkastajan on tarkistettava, onko sisäinen valvonta järjestetty asianmukaisesti. Havaitessaan epäkohtia on tilintarkastajan ilmoitettava viipymättä kirkkoneuvostolle, yhteiselle kirkkoneuvostolle, tuomiokapitulille tai kirkkohallitukselle. Seurakuntien hallinnosta, taloudenhoidosta ja sisäisen valvonnan järjestämisestä vastaa kirkkoneuvosto, joka myös huolehtii, että järjestelmä toimii käytännössä päätösten ja annettujen ohjeiden mukaisesti. Sisäisen valvonnan ohjeet on lähetetty seurakunnille yleiskirjeessä 30/2004. (Sakasti.evl.fi 2013, hakupäivä 13.4.2013.)

6.1 Sisäinen valvonta

Sisäinen valvonta tarkoittaa organisaation eri tasoille rakennettuja toimenpiteitä ja –tapoja. Nämä muodostuvat useista osa-alueista, joita voivat olla hyväksymisvaltuudet tai työtehtävien jako. Näillä toimenpiteillä pyritään varmistamaan, että organisaatio noudattaa tavoitteitansa ja toimintaohjeitansa. Sisäisen valvonnan pyrkimys on kyetä ehkäisemään ja paljastamaan virheitä, erehdyksiä ja väärinkäytöksiä. Sisäisen valvonnan perimmäinen tavoite on saada riittävä varmuus yrityksen raportoiman taloudellisen

tiedon luotettavuudesta ja siitä, että se on yritystä koskevien lakien ja säädösten mukaista. Käsitteellä sisäinen valvonta viitataan niihin toimintaperiaatteisiin ja menettelytapoihin, joilla pyritään varmistamaan, että johdon tavoitteet saavutetaan. Sisäinen valvonta koskettaa koko organisaatiota. Sisäisen tarkastuksen tehtävänä on arvioida sisäisen valvonnan tehokkuutta. Sisäisen valvonnan tehokkuuteen kantaa ottavat sekä sisäinen tarkastus että tilintarkastaja. (Ahokas, 2012, 11 – 12, 47, 54.)

Sisäinen valvonta ja tarkastus käsitetään monesti samaksi asiaksi ja ne nivoutuvatkin monelta osaa yhteen. Käsitteinä sisäinen valvonta ja tarkastus kuitenkin voidaan erottaa. Sisäinen valvonta määritellään organisaation sisäisiksi menettely- ja toimintatavoiksi, joiden avulla toiminnan laillisuus ja tuloksellisuus halutaan varmistaa. Sisäinen tarkastus käsitteenä on helpompi rajata, sillä viitataan riippumattomaan ja objektiiviseen tarkastusorganisaatioon. Toiminnan ulottuvuus voi vaihdella organisaatioittain. (Ahokas, 2012, 12.)

Yhtiön toiminnan lainmukaisuutta pyritään ulkoisesti valvomaan lakisääteisellä tilintarkastuksella. Tilintarkastuksen suorittaa tilintarkastaja, joka ottaa kantaa sisäisen kontrollin toteutumiseen. Tilintarkastajien tulisi muodostaa riittävän luotettava kuva tarkastettavan kohteen toiminnasta, valvontajärjestelmien luotettavuudesta sekä toimivuudesta. Tarkastuksen kohteita ovat tietojärjestelmien, sisäisen laskennan ja kirjanpidon toimivuus ja luotettavuus, päätöksenteko sekä varallisuuden hoito ja valvonta. (Ahokas, 2012, 47, 50.)

Riskienhallinta tarkoittaa systemaattisia menettelyitä, joiden avulla voidaan tunnistaa ja arvioida riskejä, jotka uhkaavat toimintaa sekä määrittää toimintatavat ja keinot riskien hallitsemiseen sekä niiden raportoimiseen. Riski ovat potentiaalisia ongelmia, ja ne voidaan määritellä ei-toivotuksi epävarmaksi tapahtumaksi tai tekijäksi, joka saattaisi estää tavoitteiden saavuttamisen ja palvelutuotannon häiriöttömyyden. Olennaista sisäisen valvonnan kannalta on, että toimintaan liittyvät riskit on arvioitu ja ymmärretty. Riski tulee ottaa huomioon organisaation kokonaisuussuunnittelussa ja kaikessa päätöksenteossa. Esimiesten ja organisaation johdon on pyrittävä tunnistamaan ja hallitsemaan olennaisimmat ja todennäköisimmät palvelujen tuottamiseen, järjestämiseen sekä tavoitteiden saavuttamiseen liittyvät riskit. Kaikkien organisaatioon kohdistuvien riskien hallinta ei ole mahdollista. Syitä tähän voi olla informaation epätäydellisyys, valvonnan kiertäminen tai vilpillinen toiminta. Keskeinen periaate, jota on noudatettava sekä sisäi-

sessä valvonnassa että riskienhallinnassa, on tavoitetila kohtuullista varmuutta. Tämä tarkoittaa kohtuullista varmuutta toiminnan tuloksellisuudesta, laillisuudesta sekä varojen ja resurssien turvaamisesta ja väärinkäytösten estämisestä. Sisäinen valvonta ei hyvin toteutettunakaan voi taata toiminnan virheettömyyttä tai pysyvyyttä. Sisäisen valvonnan ja riskienhallinnan menettelyjen tulee olla suhteessa toiminnan laajuuteen ja sisältöön sekä niihin liittyvien riskien osalta asianmukaiset ja järkevät. (Raudasoja & Johansson 2009, 146 – 147, 152.)

Vuonna 2002 Yhdysvalloissa voimaan tullut Sarbanex-Oxley Act (SOX)- laki säädettiin 2000-luvun alkupuolen suurten yrityspetosten seurauksena. Petokset onnistuivat suurilta osin yritysten heikon sisäisen valvonnan vuoksi. Lain avulla on tarkoitus saada estettyä väärinkäytöksiä ja parannettua konsernien hallintotapoja. SOX velvoittaa yrityksiä, jotka on listattu USA:n osakemarkkinoita varten U.S. Securities and Exchange Commissionin (SEC) alaisessa pörssissä, niiden tytäryhtiöitä ja muita yksiköitä ulkomailla. Etenkin lain säätämisen myötä sisäiset kontrollit ovat nousseet viime vuosina keskusteluissa esille. Keskeisillä turvallisuuden ja talouden prosesseilla tulee olla tehokkaat kontrollikäytänteet. SOX:n vaatimuksesta yhtiöiden johdon on luotava ja ylläpidettävä tehokasta sisäistä valvontaa ja tämä vaikuttaa suoraan tietojärjestelmien käyttöoikeuksien hallinnan tehostamiseen.. SOX-vaatimusten mukaan it-prosessien tulee olla hyvin dokumentoituja ja jokaisella it-prosessilla on oltava hyvin suunniteltu ja dokumentoitu sisäisen valvonta, joka on hyvin toteutettu, seurattu ja valvottu. SOX-lain noudattamisen avaintekijä on tehtävien eriyttämisen (SOD) hallinta. (Khan 2007, 4; Lahti & Salminen 2008, 155; Ahokas 2012, 132; Propentus, 2013, hakupäivä 30.4.2013; Sarbanes-Oxley Act 2013, hakupäivä 2.2.2013).

SOX-lain mukaan käyttöoikeuksien hallintaprosessi pitää olla kirjallisesti dokumentoitu ja kaikista myönnetyistä käyttöoikeuksista tulee löytyä asianmukaisesti hyväksytty käyttöoikeuksien lisäämispyyntö. Tämä on hyvä käytäntö myös yrityksissä, joita laki ei kosketa. (Laaksonen ym. 2006, 151.)

6.2 Vaaralliset työyhdistelmät

Ns. vaarallisilla työyhdistelmillä tarkoitetaan niitä yhdistelmiä joita voi syntyä, jos työrooleja tai työroolien yhdistelmiä yhdistellään siten, että riskimielessä syntyy vaarallisia

käyttöoikeusyhdistelmiä. Valvonnalla voidaan välttää vaarallisten työyhdistelmien syntyminen. Lisäksi voidaan valvoa käyttöoikeusyhdistelmiä niissä tilanteissa, joissa vaarallisia työyhdistelmiä on kuitenkin myönnettävä. (Valtiovarainministeriö 2006, 20.)

Vaarallisia työyhdistelmiä ovat esimerkiksi tapaukset, jos yhdellä henkilöllä on oikeudet ostolaskun tekemiseen ja hyväksymiseen, palkkojen laskemiseen ja maksamiseen, kirjanpidon hoitamiseen ja tositteiden hyväksymiseen, kirjanpidon hoitamiseen ja laskujen maksamiseen, hinnoittelu-masterdatan ylläpitoon ja asiakaslaskutukseen, toimittaja-masterdatan ylläpitoon ja laskujen prosessointiin sekä laskujen prosessointiin järjestelmään ja laskujen maksuun. (Ahokas 2012, 37)

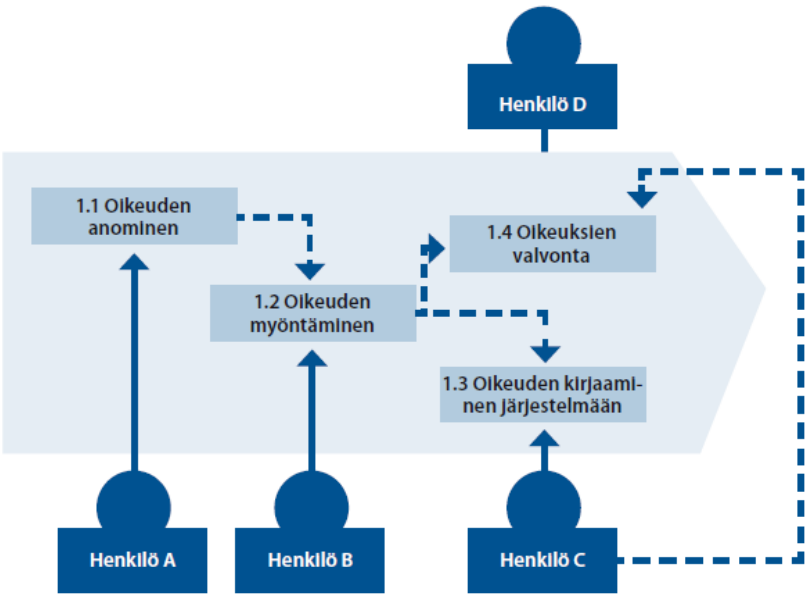
Pienemmissä yrityksissä, jossa on vähän työntekijöitä, työtehtävien eriyttäminen on usein erittäin haastavaa. Näissä tilanteissa tunnistamalla ja dokumentoimalla vaaralliset työyhdistelmät sekä kiinnittämällä huomiota jälkikäteisvalvontaan, riskiä voidaan tasata. Jälkikäteisvalvonta voidaan tehdä esimerkiksi tarkastamalla tapahtumia tai käymällä läpi käyttäjälokeja, jolla varmistetaan, ettei tietojärjestelmissä ole tapahtunut asiatonta tietojen käsittelyä. (Ahokas 2012, 38.)

6.3 Työtehtävien eriyttäminen (SOD)

Työtehtävien eriyttäminen (SOD, Segregation of duties) on tärkeä tekijä organisaation eri vastuujakojen ja työnkuvien käsittelyssä. Yrityksessä on olemassa erilaisia toimintoja, joita eri roolit suorittavat. Mitä kriittisempi toiminto on, sitä selvempi tulee myös tehtävien eriyttämisen olla. Työtehtävien eriyttämisellä varmistetaan, ettei virheitä pääse syntymään. Kun toiminnolla on useampi vastuuhenkilö, väärinkäytösten riski pienenee. Lisäksi työtehtävien eriyttämisellä selkiytyvät myös organisaation eri roolit ja vastuut. (Khan 2007, 1.)

Niina Ahokas (2012, 37) nimeää työtehtävien eriyttämisen yhdeksi tärkeimmistä yrityksen valvontatoiminnoista. Tällä hän tarkoittaa työtehtävien jakamista useiden henkilöiden kesken. Yksi henkilö ei tällöin ole vastuussa kaikista liiketapahtuman vaiheista. Vaiheet voidaan jaotella liiketapahtumien valtuutukseen, kirjaamiseen ja maksamiseen.

Tehtävien eriyttämisellä eli vaarallisia työyhdistelmiä välttämällä on tarkoitus ehkäistä virheitä ja väärinkäytöksiä. Turvatussa käsittelyketjussa yksi ihminen voi vastata vain yhdestä suorituksesta. Esimerkiksi tietojärjestelmissä oikeuksien saamisen prosessissa on kolme suorituksesta vastaavaa toimijaa. Kuvassa 2 on kuvattuna käyttöoikeusprosessin tehtävien eriyttäminen ja siihen liittyvä väärinkäytöksen mahdollisuus. (Vahti 2/2008, 30.) Tehtävien vaiheet on eriytetty hakuprosessia siten, että jokainen henkilö vastaa yhdestä prosessin tehtävästä. Henkilö A anoo oikeudet, jotka henkilö B myöntää ja henkilö C lisää oikeudet. Jotta virheiltä ja väärinkäytön mahdollisuudelta vältyttäisiin, käyttöoikeudet tulee esimerkiksi esimiehen ensin hyväksyä, jonka jälkeen eri henkilö lisää käyttöoikeudet ja eri henkilö hoitaa käyttöoikeuksien valvonnan.



Kuva 4. Tehtävien eriyttäminen sisältäen väärinkäytöksen mahdollisuuden (Vahti 2/2008, 30.)

6.4 Työtehtävien eriyttäminen taloushallinnon eri prosesseissa

Yrityksen uloslähtevässä maksuliikenteessä on usein suurin riski väärinkäytöksille. Yrityksestä ulospäin lähteviä maksuja ovat ostolaskujen maksut, matka- ja kululaskujen maksut, palkkojen maksut sekä verojen ja veroluoteisten erin maksut ja muut manuaalimaksut. (Lahti & Salminen 2008,111, 113.)

Ostolaskuprosessin osalta kontrollin tarve on hyvin selkeä, sillä prosessiin liittyy suuria rahamääräisiä maksutapahtumia. Jottei vaarallisia työyhdistelmiä pääsisi ostoprosessissa syntymään, tehtävät on hajautettava useammalle henkilölle. Tehtävät voidaan hajauttaa siten, ettei ostotilausten tekemisestä vastaava henkilö hoida tavaroiden vastaanottoa, ostolaskujen hyväksymistä tai maksua eikä kirjanpitoa ja tavaroiden vastaanotosta vastaava henkilö ei hoida laskujen maksua tai kirjanpitoa. Samoin on huomioitava, ettei toimittajan perustietojen, kuten pankkitilinumeron, tietojärjestelmiin syöttämisestä vastaava henkilö kirjaa laskua järjestelmiin eikä tee maksuaineistoa laskuista. Usein ostoreskontran tehtävät jaetaan kolmeen osaan kolmen eri henkilön hoidettavaksi. Eri henkilöt hoitavat toimittajarekisterin ylläpidon, laskujen käsittelyn ja maksuaineiston luomisen. Pienessä yrityksessä ei aina näin voida toimia, tällöin ohjelmasta voidaan kontrollimielessä seurata toimittajarekisterin muutoslokia, josta löytyy tieto toimittajarekisterin tietojen muuttajasta ja tieto siitä, mitä on muutettu. Maksuliikenneohjelmistoissa on mahdollista käyttää toimintoa, joka vaatii kaksoishyväksynnän siten, että maksuerä on mahdollista lähettää pankkiin vasta kun vähintään kaksi eri henkilöä on hyväksynyt sen. (Lahti & Salminen 2008, 114, 158; Ahokas 2012, 99.)

Ostolaskuprosessin käyttöoikeushallintaan liittyviä järjestelmäkontrolleja ovat esimerkiksi toimittajarekisterin ylläpidon rajaaminen käyttöoikeuksilla nimetyille henkilöille, järjestelmän lokeista saatavat tiedot toimittajarekisterin muutoksista ja muuttajista, järjestelmässä ylläpidetyt hyväksymisvaltuudet sekä kiinteät hyväksymiskierrot. Kontrolli, jossa toimittajarekisterin ylläpidon käyttökäyttöoikeudet rajataan nimetyille henkilöille, pyrkii varmistamaan, että toimittajarekisteriin on oikeus tehdä muutoksia vain tietyillä henkilöillä. Toimittajan perustamisen keskittämisellä uusien toimittajien hyväksymiset ja rekisterin eheyden ylläpito on selvemmin hallittavissa. Järjestelmän lokitietojen kontrollilla saadaan tietoa toimittajarekisterin muutoksien ja muuttajien osalta ja kontrollilla pyritään ehkäisemään väärinkäytöksiä. Järjestelmässä ylläpidettävillä hyväksymisvaltuuksilla taas hyväksymisoikeudet saaneelle henkilölle annetaan valtuus tiettyyn euromäärään asti, jota suuremmat määrät on lähetettävä hyväksyttäväksi toiselle henkilölle. (Lahti & Salminen 2008, 158 -159.)

Myyntiprosessissa on huomioitava, ettei myytävien tuotteiden käsittely, kirjanpito ja rahavarojen hoito kuulu saman henkilön toimenkuvaan. Eri henkilöt hoitavat tavaralähe-

tykset ja laskutuksen, laskutuksen ja myyntireskontran hoidon sekä myyntireskontran ja perinnän. Asiakastietojen ja hintatietojen ylläpito tulee olla vain ennalta määritellyillä henkilöillä. (Ahokas 2012, 103 – 104, 107 - 108.)

Henkilöstöhallinnossa tulee erityistä huomiota kiinnittää käyttöoikeuksien rajaamiseen, sillä henkilöstöhallinnon tietojärjestelmissä on arkaluontoista tietoa, kuten palkka- ja tilinumerotietoja. Näiden tietojen turvaamiseen tuleekin kiinnittää erityisesti huomiota sisäisen valvonnan avulla. Työntekijöistä pidetään henkilöstörekisteriä, jossa on tietoja muun muassa palkanmaksuun tarvittavia henkilötietoja, palkanmääriä ja palkkaluokka sekä tiedot luontoiseduista. Yrityksessä tuleekin määritellä erikseen ne henkilöt, joilla on valtuudet tehdä muutoksia henkilöstörekisterin tietoihin. Henkilötietojen muuttamisen osalta voidaan laatia ohjeistus, jolla esimerkiksi ohjeistetaan toimittamaan esimiehen kirjallinen hyväksyntä ennen muutoksen tekemistä järjestelmään. Järjestelmien käyttöä valvotaan käyttäjätunnusten ja salasanojen avulla, jolloin vain henkilöt, joiden toimenkuva edellyttää järjestelmän käyttöä, saavat oikeudet järjestelmään. Arkaluontoisia tietoja käsiteltäessä onkin erittäin tärkeää, että järjestelmään jää merkintä muutoksen tehneestä henkilöstä sekä muutoksen teon ajankohdasta. (Ahokas 2012, 115, 117.)

Palkkahallinnossa työtehtävien eriyttämisen osalta on kiinnitettävä huomiota, ettei saman henkilön työtehtäviin kuulu palkkojen laskeminen sekä palkkojen maksaminen. Järjestelmään on mahdollista myös luoda automaattisia kontrolleja, kuten palkkamaksimi, jolloin yhdellä kerralla ei voi maksaa tiettyä summaa suurempaa palkkaerää. Sama henkilö ei myöskään voi tehdä tietojärjestelmiin henkilötietoja koskevia muutoksia ja hyväksyä niitä. Jos yksi henkilö joutuu pienessä yrityksessä työntekijöiden vähyyden vuoksi vastaamaan palkkojen laskusta ja maksuunpanosta, tulisi tällöin kaikki palkanlaskentaan liittyvät toimenpiteet hyväksyttää toisella henkilöllä ennen maksuunpanoa. Henkilön työsuhteen päättyessä, tulee useita asioita huomioida sisäisessä valvonnassa. Näitä asioita ovat esimerkiksi työsuhteen päättyessä käyttöoikeuksien poistamisen huolehtiminen järjestelmistä. (Ahokas 2012, 118-119.)

Työntekijöiden työaikakirjanpidon tapahtumien tarkastamisesta ja hyväksymisestä vastaavan henkilön ei tulisi hoitaa palkanlaskentaan ja kirjanpitoon liittyviä tehtäviä, eikä

myöskään tulisi olla mahdollista muuttaa niitä henkilörekisteritietoja, joilla on vaikutusta palkanlaskentaan. Henkilöstörekisterin ylläpito, työntekijöiden valvontaan liittyvät tehtävät sekä palkanlaskenta tulee eriyttää palkan maksuun liittyvistä tehtävistä. Palkanlaskentaan liittyviä tehtäviä hoitava henkilö ei saisi myöskään hoitaa kirjanpitoon liittyviä tehtäviä. Henkilö, joka ei vastaa palkanlaskennasta eikä kirjanpidon tehtäviä, voi suorittaa säännöllistä kontrollien seurantaa, vertailemalla palkkalaskentajärjestelmän ja kirjanpidon tietoja keskenään. (Halonen & Steiner 2010, 373.)

Matkalaskuprosessin yksittäiset maksusuoritukset eivät ole yleensä suuria, mutta niitä maksetaan suurelle osalle työntekijöitä. Kontrolleilla pyritäänkin varmistamaan, että korvatut matkakorvaukset ovat syntyneet yrityksen matkustussäännön mukaisesti ja kululaskujen osalta se, että korvataan vain yrityksen maksettavaksi kuuluvia kustannuksia, jotka kustannuksista vastaava esimies on hyväksynyt. Matkalaskun osalta käyttöoikeushallinnan järjestelmäkontrollina toimii järjestelmässä ylläpidetyt hyväksymisvaltuudet. Kun järjestelmässä on organisaatiokaavioiden mukaiset hyväksyjät ja mahdolliset euromääräiset hyväksymislimiitit, pystytään valvomaan automaattisesti, että matka- ja kululaskut hyväksyy aina oikea henkilö. (Lahti & Salminen 2008, 161, 162.)

Yrityksen suurin riski menettää rahaa liittyy sen maksuliikenteeseen. Maksuliikenteeseen liittyvät tehtävät tulisi jakaa usealle henkilölle, jotta riskit ja mahdollisuudet väärinkäytöksille saadaan minimoitua. Riskien ja väärinkäytösten minimointiin voidaan käyttää erilaisia järjestelmäkontrolleja, joita ovat käyttöoikeushallinnan osalta hyväksynnät ja rajatut käyttöoikeudet. Hyväksyntä takaa, että maksuohjelmassa täytyy kahden eri henkilön hyväksyä maksu ennen niiden vapautumista pankkiin lähetettäväksi. Käyttöoikeuksien rajauksella taas varmistetaan, ettei sama henkilö pääse tekemään maksuja ja kirjaamaan pankin tiliotteita. (Lahti & Salminen 2008, 164.)

Veroja ja muita veroluoteisia eriä joudutaan yleensä viemään manuaalisesti rahaliikenneohjelmaan. Tavoitteena kuitenkin tulee olla, ettei manuaalisia maksutapahtumia jouduttaisi tekemään ja maksut tehdään pääsääntöisesti esijärjestelmiä ja niiden hyväksymismenettelyjä käyttäen. Tämä mahdollistaa esijärjestelmien hyväksymisrajojen ja –oikeuksien ja niiden lokitietoihin tallentuvien tietojen, joita ovat tapahtumien käsittelijät

ja hyväksymiset, hyödyntämisen maksujen kontrolloinnissa ja raportoinnissa. (Lahti & Salminen 2008, 113.)

7 TUTKIMUKSEN TOTEUTUS

Tutkimuksen aineiston keräsin teemahaastatteluilla, havainnoinnilla, keskustelemalla sekä palvelukeskuksen käyttöoikeuksien hallintaan liittyviin dokumentteihin perehtymällä. Teemahaastattelujen teemat olivat tietoturvallisuus, käyttöoikeuksien hallinta ja käyttöoikeuksien valvonta. Haastattelin palvelukeskuksen tietohallintopäällikköä, käyttöoikeuksista vastaavaa sovellusasiantuntijaa sekä käyttöoikeusprosessista vastaavaa taloushallinnon palvelupäällikköä. Haastattelut toteutettiin työympäristössä ja ne kestivät kerrallaan 1 – 2 tuntia. Haastatteluista tein muistiinpanot, joista kirjoitin koosteet teemoittain. Koosteiden pohjalta havainnointia, keskusteluja ja palvelukeskuksen dokumentteja hyödyntäen kuvasin palvelukeskuksen käyttöoikeuksien hakuprosessin nykytilanteen, käyttöoikeuksien hallintajärjestelmän sekä käyttöoikeuksien hakuprosessin käyttöoikeuksien hallintajärjestelmässä ja käyttöoikeuksien valvonnan nykytilanteen.

Tutkimuksen teoriaosuudessa hyödynsin kirjallisia ja sähköisiä lähteitä. Teoriaa ja tutkimuksessa saamaani tietoa hyödyntäen olen saanut vastaukset tutkimuskysymyksiini ja saavuttanut opinnäytetyöni tavoitteet asetetun aikataulun mukaisesti.

8 JOHTOPÄÄTÖKSET JA POHDINTA

Opinnäytetyöni tavoitteena oli luoda ohje palvelukeskuksen asiakkaille käyttöoikeuspyyntöjen tekemiseen käyttöoikeuksien hallintajärjestelmässä ja määritellä keinot käyttöoikeuksien valvontaan ja siihen, että vaarallisia työyhdistelmiä ei synny. Aiheeni on ajankohtainen, sillä palvelukeskuksessa on meneillään käyttöoikeuksien hallintajärjestelmän käyttöönottohanke, joka muuttaa nykyisiä käyttöoikeuksien hallintakäytäntöjä. Käyttöönottohankkeen aikana palvelukeskuksessa otetaan käyttöön käyttöoikeuksien hallintajärjestelmä, jossa jatkossa hallinnoidaan palvelukeskuksen palvelujärjestelmien käyttöoikeudet. Organisaatiossa ei vielä ole valmiita, systemaattisia prosesseja käyttöoikeuksien hallintaan. Opinnäytetyöni käsittelee myös sisäistä valvontaa työtehtävien eriyttämien näkökulmasta, joka myös on ajankohtainen aihe, sillä sisäiseen valvontaan ja sen kehittämiseen on alettu organisaatioissa kiinnittää yhä enemmän huomiota.

Vastauksena tutkimuskysymyksiin, miten palvelukeskus valvoo käyttöoikeuksia ja, miten ohjeistetaan palvelukeskuksen asiakkaat käyttöoikeuspyyntöprosessin osalta, määrittelin keinoja palvelukeskukselle valvoa käyttöoikeuksia ja tein Kirkon palvelukeskukselle käyttöoikeuspyyntöjen hakuohjeen. Kirkon palvelukeskukselle tehdyt käyttöoikeusohjeet ja määritellyt valvontakeinot käyttöoikeuksien valvonnan nykytilan kuvaus ja tiedot käyttöoikeuksien hallintajärjestelmän osalta ovat salaisia ja ne luovutetaan vain toimeksiantajalle. Tässä luvussa käsittelen yleisellä tasolla opinnäytetyöni tuloksia käyttöoikeuksien ohjeistukseen ja käyttöoikeuksien valvontakeinoihin liittyen.

Ohje käyttöoikeuspyyntöjen tekemiseen on tehty hankkeen ollessa vielä kesken, jonka vuoksi käyttöoikeuspyyntöohjetta päivitetään vielä tarvittavilta osin muutosten osalta käyttöoikeuksien hallintajärjestelmän käyttöönottohankkeen edetessä. Ohje on kuitenkin pääosin valmis ja palvelukeskus käyttää ohjetta käyttöoikeuksien hallintajärjestelmän käyttöönotossa.

Käyttöoikeuksien valvonnalla varmistetaan se, että käyttöoikeustiedot ovat ajantasaiset ja organisaatiossa toimitaan sovittujen käytäntöjen mukaisesti. Teoriaan ja keräämääni tietoon perustuen tutkimustuloksena esitän valvontaan keinoja, joiden perustana ovat

käyttöoikeus- ja lokitiedot sekä raportit ja katselmoinnit. Säännöllisesti ajettavien käyttöoikeusraporttien ja katselmointien perusteella tehdyillä päivityksillä varmistetaan, että käyttöoikeustiedot ovat ajantasaiset. Lokitietojen perusteella voidaan myös seurata, että organisaatiossa toimitaan sovittujen käytäntöjen mukaisesti. Palvelukeskuksen tulisi jatkossa kehittää myös käyttöoikeustietojen dokumentointia ja siihen liittyviä ohjeistuksia

Vaaralliset työyhdistelmät voidaan estää työtehtävien eriyttämisellä ja käyttöoikeuksien valvonnalla. Työtehtävien eriyttämisellä voidaan myös selkeyttää organisaation rooleja ja vastuita. Työtehtävien eriyttämisellä voidaan varmistaa, ettei virheitä pääse syntymää ja väärinkäytösten riski pienenee. Jos on tarvetta kriittisten työyhdistelmien käytölle, näiden osalta järjestelmien käyttöä tulisi palvelukeskuksessa valvottava tehostetusti. Palvelukeskuksen tulisi tarkistaa ja kuvata työntekijöiden vastuut ja työnkuvat sekä näihin liittyvät käyttöoikeudet. Myös työnkuvien, vastuiden ja työyhdistelmien dokumentointia tulisi palvelukeskuksessa jatkossa kehittää.

Palvelukeskuksen tietoturvasuunnitelma on tarkistettava ja tarvittaessa päivitettävä käyttöoikeuksien hallintajärjestelmän ja käyttöoikeusprosessin osalta. Palvelukeskuksen dokumentoinnin, prosessien ja sisäisen valvonnan kehittäminen ovat tärkeitä toiminnan laadun ja tehokkuuden parantamiseksi.

Opinnäytetyöni aihe oli laaja ja mielenkiintoinen. Tutkimusta tehdessäni ammatillinen osaamiseni on kasvanut. Haasteita opinnäytetyöni tekemiseen toi käyttöoikeuksien hallintajärjestelmän käyttöönottohanke, joka jatkuu edelleen. Meneillään olevasta hankkeesta johtuen käyttöoikeusprosessiin liittyvät asiat muuttuivat ja kehittyivät työni edetessä. Hankkeen aikana on myös uusia tarpeita noussut esille. Käyttöoikeuksien hallintajärjestelmän käyttöönottoprojekti on ollut haaste myös palvelukeskukselle. Opinnäytetyöni työni tulokset ovat selkiyttäneet palvelukeskuksen käyttöottohankkeeseen liittyviä tarpeita. Tutkimukseni tuloksena määrittelemiäni käyttöoikeuksien valvontakeinoja ja tekemiäni kehitysehdotuksia hyödynnetään palvelukeskuksessa käyttöoikeushallinnan jatkokehitysprojektissa.

Tärkeänä jatkotutkimusaiheena näen sisäisen valvonnan kehittämisen. Myös kypsyystasomallien hyödyntäminen prosessien kehittämisessä on mielenkiintoinen jatkotutkimusaihe. Sisäisen valvonnan sekä prosessien ja dokumentointien kehittämiseen tekemäni kehitysehdotukset toimeksiantaja huomioi jatkokehityksessään, jonka jatkotoimista päättää palvelukeskuksen johto.

LÄHTEET

Ahokas, Nina 2012. Yrityksen sisäinen valvonta. Jyväskylä: Bookwell Oy.
Eskola, Jari & Suoranta, Juha 2008. Johdatus laadulliseen tutkimukseen.
Hakala, Mika & Vainio, Mika & Vuorinen, Olli 2006. Tietoturvallisuuden käsikirja. Jyväskylä.
Halonen, Kaarina & Steiner, Maj-Lis 2010. Tilintarkastusprosessi käytännössä.
Julkisen hallinnon kokonaisarkkitehtuuri 2011. Julkisen hallinnon KA-kypsyystasomalli. Valtiovarainministerö. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20110407Luonno/06_JHKA_Kypsyystasomalli_20110404.pdf
Kananen, Jorma 2010. Opinnäytetyön kirjoittamisen käytännön opas.. 2010.
Khan, Nuzhat 2007. Segregation of Duties – SoD. HCL Technologies. 2007. http://www.sdn.sap.com/irj/scn/go/portal/prtroot/docs/library/uuid/f02855c9-2091-2a10-8682-af41abe087ba?overridelayout=true
Kirkkohallituksen yleiskirje Nro 8/2011. Suomen evankelis-luterilainen kirkko. 28.2.2011. http://sakasti.evl.fi/sakasti.nsf/0/0F61D00B4BB4204DC2257824002D1BD6/$FILE/2011-08.pdf
Kirkkohallituksen yleiskirje Nro 19/2012. Suomen evankelis-luterilainen kirkko. 2.11.2012. http://sakasti.evl.fi/sakasti.nsf/0/1BC606B379F69758C2257976004527BB/$FILE/2012-19.pdf
Kirkkojärjestys 8.11.1991/1055.
Kirkon palvelukeskus, 2012. Hakupäivä 6.12.2012 http://sakasti.evl.fi/sakasti.nsf/sp?open&cid=Content3D0098
Kirkon säädöskokoelma Nro 109, 2011.Suomen evankelis-luterilainen kirkko. Hakupäivä 26.2.2013 http://sakasti.evl.fi/sakasti.nsf/0/0F61D00B4BB4204DC2257824002D1BD6/$FILE/2011-22-%20liite%201.pdf
Koivu, Pirkko 2013. Kirkko keskittää taloushallinnon. NET. Nro 1/2013, 20.
Koivula, Ulla-Maija & Suihko, Kristiina & Tyrväinen, Jari 2002. Mission: Possible, Opas opinnäytteen tekijälle. Pirkanmaan ammattikorkeakoulun julkaisusarja C. Oppimateriaalit Nro 1.
Koskinen Seppo & Alapuranen, Leena & Heino, Anna-Maija & Salli, Minna 2005. Henkilötietojen käsittely työelämässä. Edita Publishing Oy. Tallinna 2005.
KPMG 2012. Tietoturvaraportti 2012. http://www.kpmg.com/FI/fi/Ajankohtaista/Uutisia-ja-julkaisuja/Neuvontapalvelut/Documents/KPMG-Tietoturvaraportti-2012.pdf
Laaksonen, Mika & Nevasalo, Terho & Tomula, Karri 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy. Helsinki.
Laamanen, Kai & Tinnilä, Markku 2009. Prosessijohtamisen käsitteet. Espoo 2009.
Lahti, Sanna & Salminen, Tero 2008. Kohti digitaalista taloushallintoa. Helsinki.
Linden, Mikael, 2007. Käyttäjähallinnon käsitteitä ja periaatteita. Tieteen tietotekniikan keskus CSC. 12. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20080924Virtuk/011_20071112_linden1.pdf
Linden, Mikael, 2012. Identiteetin- ja pääsynhallinta. Luentomoniste. http://www.cs.tut.fi/~linden/iam-pruju.pdf
Paunia, 2013. Hakupäivä 6.4.2013. http://www.paunia.fi/prosessit-ja-laatu/

Propentus 2013. Hakupäivä 30.4.2013. Yrityspetokset identiteetinhallinnan taustalla http://www.propentus.com/fi/propentus_united_identity/yrityspetokset_identiteetinhallinnan_taustalla.html

Raudasoja, Kaisa & Johansson, Marja-Leena 2009. Esimies talouden johtajana julkishallinnossa. WSOpro.

Sakasti.evl.fi 2013. Hyvien johtamis- ja hallintotapojen sekä sisäisen valvonnan kehittäminen. Hakupäivä 23.4.2013. http://sakasti.evl.fi/sakasti.nsf/sp2?open&cid=Content2E72F1

Sarbanes-Oxley Act, 2013.Hakupäivä 2.2.2013 https://www.appsecinc.com/solutions/sarbanesoxley/index.shtml

Teemahaastattelu, 2013. Hakupäivä 28.1.2013. http://www.stat.fi/virsta/tkeruu/04/03/

Tietoturva, 2013. Mitä on tietoturva? Suomen Internetopas. Hakupäivä 19.1.2013. http://www.internetopas.com/yleistietoa/tietoturva/

UCISA 2013. ITIL – A guide to access management. Hakupäivä 25.1.2013. http://www.ucisa.ac.uk/~/media/Files/members/activities/ITIL/service_operation/access_management/ITIL_a%20guide%20to%20access%20management%20pdf

Vahti 3/2007. Tietoturvallisuudella tuloksia. Valtionvarainministeriö. Helsinki 2007. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20071128Tietot/vahti3_07_netti.pdf

Vahti 2/2008. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Valtionvarainministeriö. Helsinki 2008. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20080218Taereki/Vahti2_08low.pdf

Valtiovarainministeriö 2006. Käyttövaltuushallinnon periaatteet ja hyvät käytännöt 2006. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20061122Kaeyttoe/vahti_9_06.pdf