Taina Säkkinen

Pilvipalvelun järjestelmämigraatio tietosuoja- ja tietoturvavaatimukset huomioon ottaen

Opinnäytetyö

Tradenomi YAMK

Yrittäjyys ja liiketoiminta-osaaminen

Syksy 2019

KAMK • University of Applied Sciences

Tiivistelmä

Tekijä: Säkkinen Taina

Työn nimi: Pilvipalvelun järjestelmämigraatio tietosuoja- ja tietoturvavaatimukset huomioon ottaen

Tutkintonimike: Tradenomi YAMK, Yrittäjyyden ja liiketoimintaosaamisen koulutus

Asiasanat: pilvipalvelu, tietosuoja, tietoturva, riskienhallinta

Tämän opinnäytetyön tavoite on uudistaa pilvipohjainen tallennusratkaisu, jossa otetaan huomioon tietosuoja ja tietoturva vaatimukset. Tietosuoja siten, että vain tietoa tarvitsevalla on pääsyoikeudet henkilötietoihin. Tietoturva siten, että teknistä suojausta ja käytettävyyttä parannetaan. Uusi pilvipohjainen tallennusratkaisu rakennetaan Google Driven Business -versioon, Jaetun Driven puolelle. Kehittämistyön tarkoitus on saada selvitettyä, millaisiin ryhmiin henkilökunta saadaan jaettua järjestelmämigraatiota varten, sekä luoda uusi kansiorakenne. Muutokseen on tarve, sillä henkilöstössä on tapahtunut muutoksia kuluneen vuoden aikana. Henkilöillä on saatavilla liikaa tietoa.

Opinnäyteyön teoreettinen viitekehys koostuu pilvipalveluista, tietosuojasta, tietoturvasta, sisäisestä valvonnasta, riskienhallinnasta sekä muutoksen johtamisesta. Tutkimusstrategiana käytetään konstruktiivista tutkimusta. Tutkimusmenetelmänä käytetään mixed methodsia. Tutkimusmetodeina käytetään teemahaastattelua ja kyselyä kohdeorganisaation henkilöstölle. Anonyymi kysely tehdään poikittaistutkimuksena Google Formsilla. Ryhmien muodostamista varten lähetetään kaikille erillinen kysely työtehtävistä. Haastattelu tehdään Adobe Connectilla kahdelle henkilölle. Haastattelut tallennetaan ja litteroidaan. Aineiston analysointimenetelmänä käytetään sisällönanalyysiä.

Kehittämismenetelmänä oli työryhmä. Kyselyn tuloksien perusteella saatiin tehtyä ryhmäjaottelu ja ryhmien oikeudet uutta järjestelmää varten sekä kansiorakenteen suunnitelmat. Muutoksen piti olla valmis syksyllä, mutta uudet ominaisuudet Google saa valmiiksi alkuvuodesta. Sen jälkeen järjestelmämigraatio voidaan tehdä loppuun. Kyselyiden ja haastatteluiden avulla saatiin selville tietoturvaan liittyviä kehityskohteita. Tietoturva koulutuksien sisältö suunnitellaan kyselyn tulosten perusteella. Koulutusta lisäämällä saadaan tietoturva-asioita kerrattua henkilöstölle. Haastatteluissa saatiin kartoitettua sisäisen valvonnan ja riskienhallinnan nykytilanne. Esimiehille tehdään tietopaketti sisäisestä valvonnasta.

Tutkimusongelmaan ja tutkimuskysymyksiin saatiin vastaukset. Kohdeorganisaatio pääsee hyödyntämään kehittämistyön tuloksia heti opinnäytetyön julkaisemisen jälkeen. Kehittämistyö merkitsee yritykselle paljon, saadaan iso järjestelmämuutos tehtyä, jonka suunnitteluun henkilökunnan mielipiteitä on kysytty ja otettu huomioon. Tietoturva koulutukset saadaan aloitettua ja esimiehille tietopaketti luotua sisäisestä valvonnasta. Jatkotutkimushaasteena voisi tutkia miten uuden järjestelmän käyttöönotto on sujunut esimerkiksi vuoden päästä.

Abstract

Author: Säkkinen Taina

Title of the Publication: Cloud Service System Migration Considering Data Privacy and Data Security Requirements

Degree Title: Master of Business Administration, Entrepreneurial and Business Competence

Keywords: cloud services, data privacy, data security, risk management

The aim of this thesis is to modernize the cloud-based system, which takes into account the data privacy and data security requirements. Privacy means that only the person who needs the information has access to the personal data. Security is gained by improving technical security and usability. The new cloud-based system is being built for the Google Drive Business, Shared Drive. The purpose of the development work is to find out which groups of staff can be shared for system migration and to create a new folder structure. There is a need for change, because staff changes have taken place over the past year. There is too much information available to staff.

The theoretical framework of the thesis consists of cloud services, data privacy, data security, internal control, risk management and change management. Constructive research was used as the research strategy. The research method includes mixed methods, i.e. theme interviews and questionnaires for the personnel of the target organization. An anonymous survey was conducted as a cross-study on Google Forms. In order to form groups, a separate job inquiry was sent to everyone. The interview was conducted with two people using Adobe Connect. Interviews were recorded and transcribed. Content analysis was used as the method of data analysis.

The working method was the development method. Based on the results of the survey, a grouping and group permissions for the new system and plans for the folder structure were made. The change was supposed to be ready in the fall, but Google will be completed with the new features at the beginning of next year. Then the system migration can be completed. The surveys and interviews revealed data security related development targets. The content of the data security training is planned based on the results of the survey. By increasing training data security information can be shared with staff. The interviews provided an overview of the current state of internal control and risk management. The supervisors will have an information package on internal control.

Answers were given to the research problem and research questions. The target organization will have access to the results of the development immediately after the publication of the thesis. The development work means a lot to the company, a major system change can be made, and the opinions of the staff have been sought and taken into account in the planning. Information data security training can be started and the information package for supervisors is created from internal control. The challenge of further re-search could be to examine how the implementation of the new system has progressed, for example, with-in a year.

Extended Abstract

This development task was commissioned by a private adult education company. It provides labour training and expert services nationwide. There are currently about 150 staff. At the beginning of the year, the number of personnel was over two hundred. This change has affected the job description of many, so it was time to switch to the cloud. The role of the researcher in the development task is to be involved in the process of change, both in development and implementation. The target organization uses Google Drive's cloud-based storage system to store data. The research problem was that the cloud-based storage system had to be re-placed. The main reason for the change involves changes in the staff's job responsibilities, as well as the impracticality and security of the current folder structure. The storage and processing of personal data should be made safe and appropriate. As job descriptions change, information is available too broadly. Too much information is available, as job tasks have changed.

The Personal Data Protection Regulation (GDPR) contributes to the need to modify the data storage systems to ensure the safe and lawful storage and processing of personal data. The target organization is storing data in the cloud system, but currently it is unable to make the necessary changes. What is needed is a new cloud-based storage system, i.e., a system migration that can better into account the data protection and security settings. The topic of the development work was chosen from the needs of working life. There is a lot of data in the organization and access to data should be more strictly limited to new legislation. Also, not everyone needs access to modify or delete files. Finding information needs to be made smoother than it is now, which means changing the folder structure to the new system.

The target company has two goals in redesigning its cloud-based storage solution. 1) Data privacy, that is the development of the protection of personal data so that only the person who needs the information has access to the personal data. 2) Data security, that is the development of technical security of data and the improvement of its usability. The new cloud-based storage solution is being built for Google Drive Business, on the side of Shared Drive. The purpose of the development work is to find out which groups in a cloud-based storage system will be able to distribute staff for the system migration. It also renews the folder structure so that security issues will be taken into account when making the change.

The development task will seek answers to the following questions:

- What groups of employees are assigned to the new storage system?
- How should data privacy and data security be taken into account in enterprise cloud services?
- How is the organisation's internal control and risks managed from the manager's perspective?

Constructive research was used as the research strategy. The research method included mixed methods, or method triangulation, which means many research methods. It combines qualitative research with quantitative research. The material acquisition, so research methods, was a theme interview and an online survey. The survey was a cross-sectional survey of 70 employees on Google Form, which collected data from several respondents at the same time. The theme interview will be was conducted with Adobe Connect for two people.

The survey was used to chart user expectations for the new cloud-based storage system. The job survey was intended to identify changes in job roles that affect access and usability due to organizational change. The interview explained how the current internal control and risk management are organized, and how data privacy and data security was sought for more information.

Content analysis was used as a method of analysing the development material after transcription. Job response answers were used to plan the group breakdown needed for Shared Drive. The purpose of the interviews was to find out how internal control and risk management are currently implemented within the target organization. The development method was based on interviews and questionnaire materials used in a development team workshop. The content of the job had a significant impact on the formation of the groups, based on which the data sharing rights of the new system were granted to the files. The materials were used to make a plan for group distribution for system migration. The researcher is involved in a development team that plans folder levels and their permissions to staff. From the current folder structure, the files will be moved to the correct locations in the new system. The result of the development work is system migration, where data privacy and data security are taken into account.

Chapter 2 deals with the theory framework for cloud-based system migration, which is limited to studying cloud-based information systems, data privacy, data security, internal controls, and risk management. The chapter also considers change management during digitalization and competence management. Addressing these topics is an essential part of making such changes in an organization where changes occur both externally and internally. Chapter 3 deals with research and development methods. Chapter 4 covers the empirical section, the development section, which details the target organization and the company that will support the system changeover, as well as another type of M-Files that provides metadata storage. This chapter reviews the research results. The final one, chapter 5, discusses the conclusions and the consideration.

The survey was conducted using the Google Forms program and was addressed to the staff of the target organization. The sample consisted of 70 respondents out of 120. They represent the entire population. The survey was conducted as an anonymous query, meaning that the respondents cannot be identified. The topic of the survey concerned data security and cloud services. There were 27 questions. The answers highlighted the issues that had been dealt with in the theoretical framework. In conclusion, generally speaking, there are data security policies, updates and monitoring of the company, including security incidents. The thing that needs to be changed is the implementation of the information and making it known to the staff. The supervisor and the management team were well aware of information security is-sues. They go through them several times a year at their meetings. Other employees, on the other hand, felt insecure in using the systems and finding information. It was felt that it was known that information existed somewhere, but it was not found.

To improve this situation, small training sessions on data security should be held several times a year. Employees need a reminder of where to find instructions and actions. A review of working methods is also in place. Many teams meet weekly, but for example once a month they could discuss important issues. Small changes would increase the skills of the employees and improve the smooth running of the work. It is expected that the new system will not pro-vide information as extensively as it currently is.

For the development work, a theme interview was conducted with two people. The interviewees were sent a small background questionnaire prior to the interview via Google Forms. A separate theme interview was conducted with Adobe Connection. The recordings of inter-views were transcribed. The transliteration model was used for transcription. The transcribed texts, the original

phrases, contained so many trade secrets that they could not be added to the thesis. The transcripts were eight pages of Word text (including questions). The questions were formulated successfully, because the answers were good.

After the transcript was completed, the data was transferred to Excel, where an array for content analysis was built. In the content analysis, the first column was compiled of raw text, basic phrases. In the second column, a simplified expression was created from the raw text. A subclass was with the content of a condensed expression, and upper class was placed with a subject or words to describe the subclass in a concise manner. Generalization in the column was collected by theme breakdown of the most repetitive word in the upper class. The interview included questions on four themes: data security, cloud services, internal control and risk management.

A separate job inquiry was sent to almost all staff, about 120 employees. The survey was made on Google Forms. A small survey asked about the tasks for the group division needed in the new Shared Drive. A total of 40 replies were received, with one third responding to this questionnaire. The purpose of the survey was to find out what information the staff needed to be able to manage their work. The part was divided into main tasks. The respondent had the opportunity to choose as many alternatives as needed.

The materials from interviews and questionnaires were reviewed in a workshop. Based on the new research results, a grouping of personnel was planned. Internal control and risk management theory will be communicated to supervisors and management. The results of the study will also be made available to the aforementioned groups. The team provided background support for the researcher throughout the process. The researcher made a note of each meeting and wrote down things.

Respondents are aware that guidance on data security exists, but information is not always found. Many of them require minor training in data security. The working group will take the training into account. Training will be offred for staff, either through team weekly meetings or separately organised webinars. Respondents to the anonymous survey asked for a new system for storing data. In the current system, there is a risk that important files will be deleted by individuals. On the side of the new cloud system, the company owns the data, not the individual, so they cannot delete the data.

From the interview responses, it can be stated that risk factors have been taken into account, guidance is in place and risks have been assessed. The conclusion of the interviews could be that the staff needs small training sessions on practical security issues several times a year. They can help maintain a good level of data security. The quality site has been found to have up-to-date guidelines, but employees should be reminded of its existence and refer them to the site.

With the help of a job survey, the team was able to group the staff together. The grouping is ready and will be changed as the staff changes. There is a plan for the folder structure and permissions and file transfers will be made when Google get ready to share subfolders of files. Moving entire folders takes time, testing was done in May 2019. Many channels will inform staff in advance of the start of transfers.

Surveys and interviews provided important insights into corporate data security and the folder organization in the cloud services. The staff has been consulted and wishes have been taken into account in the development work. The interviews provided an update on the organisation's internal controls and risk management. Folder structures, permissions and group partitioning can improve data security. In the surveys, data security training was highlighted as an important issue, so more training will be provided. The surveys also revealed that data security was at a very good level in the target organization. Information exists, but in the middle of a hectic everyday life, you can't go back to information when you can't find directions. These will be improved by training and raising awareness on data security. Small changes can contribute to a smoother working day and successful work experiences for everyone.

The research part of the development work provided a solution to the research problem. In data security, staff are trained more often, briefly and systematically. Staff were divided into groups for the new cloud service system. There is a plan for the folder structure. The state of internal control and risk management was surveyed.

Alkusanat

Opintojemme ensimmäisenä päivänä meille sanottiin, että te valmistutte, vaikka väkisin, kun teette kaikki annetut tehtävät. Tämä laajojen asiakokonaisuuksien pilkkominen pienempiin osiin on saanut työmäärät hallittavampaan muotoon ja olen edennyt systemaattisesti tehtävä tehtävältä kohti deadlinejä. Keväällä kaikki kurssit olikin saatu tehtyä ja oli aika keskittyä opinnäytetyöhön. Töiden ohessa opiskellessa on aika rajallista ja suurimmat kiitokset kärsivällisyydestä saakin perheeni. He ovat jaksaneet tukea minua tavoitteessani. Opinnäytetyön tekeminen on vaatinut vahvaa itsensä johtamista ja koko elämän tarkkaa aikatauluttamista.

Kiitokset saavat tottakai ohjaava opettajani Heli Itkonen sekä kohdeorganisaation kaksi kommentaattoria ohjaustuokioista ja oikean suunnan hahmottamisessa. Kiitoksia, että sain tehdä tämän kehittämistyön. Pilvipalvelun järjestelmämigraatio on hyödyllinen ja ajankohtainen muutos jatkuvasti kehittyvässä organisaatiossa. Aihe oli mielenkiintoinen ja sitä oli antoisaa tutkia. On ilo olla mukana sekä seurata nykyaikaista ja ketterästi toimivaa päätöksentekoa hajautetun hallinnon organisaatiossa.

1.12.2019 Taina Säkkinen

Sisällys

1 Johdanto

Yhä useampi organisaatio, kohdeorganisaation tavoin, käyttää tietojensa tallennuspaikkana pilvipohjaisia ratkaisuja, joissa tieto on nopeasti saatavilla. Digitalisaatio on tulossa osaksi nykyaikaisia ja kehittymishaluisia organisaatioita. Yrityksissä tapahtuu kuitenkin muutoksia kaiken aikaa, jonka vuoksi tehtävänkuvia joudutaan yhdistelemään ja muuttamaan. Tällöin on vaarana, että tallennettua tietoa on saatavilla liian laajoina asiakokonaisuuksina työnkuvaan nähden. Henkilötietojen käsittelyä säätelevä tietosuoja-asetus GDPR (General Data Protection Regulation) tuli voimaan 25.5.2018, jota sovelletaan kaikissa EU-maissa. Tietosuoja-asetuksen avulla voi suojata henkilötietoja paremmin ja siitä saa tietojen käsittelyn hallintaan enemmän keinoja. Organisaatioissa oli ryhdyttävä uuden asetuksen mukaisiin toimenpiteisiin yhdenmukaistaakseen henkilötietojen käsittelyä ja parantaakseen yksityisyydensuojaa. (Tietosuojavaltuutetun toimisto 2019.) Dataa kertyy organisaatioihin paljon, joten tiedon tulisi olla helposti käytettävissä ja vain niiden henkilöiden saatavilla, jotka sitä työtehtävissään tarvitsevat, sekä tarpeettomat tiedostot tulee hävittää turvallisesti.

Kehityksen kärjessä olevat yritykset pyrkivät pysymään jatkuvassa muutoksessa mukana, kehittämällä toimintatapojaan ja käyttämiään järjestelmiä. Pilvipohjaisia tallennusjärjestelmiä on markkinoilla moniin erilaisiin tarpeisiin myös yrityksille. Digitalisaation myötä tieto tallennetaan yhä useammin pilvipohjaisiin järjestelmiin. Tiedon säilytys pilvipalvelussa on huomattavasti edullisempaa konesaliratkaisuihin verrattuna. Yrityksen ei tarvitse investoida kalliisiin ja fyysisiin laitteistoihin. Organisaatioiden rakenteiden muuttuessa on syytä tarkastella myös niiden käyttämiä järjestelmiä. Muutoksien tullessa johtaminen korostuu, jotta työntekijät pysyvät muutoksessa mukana. Muutoksiin voi valmistautua ja hyvällä johtamisella muutosvaiheista päästään joustavasti eteenpäin. Kehittämistehtävälle on tarvetta, sillä lainsäädäntö on muuttunut ja tehtävänkuvia on muutettu.

Kohdeorganisaatiossa on tarve tehdä muutos pilvipalvelun tallennusjärjestelmään vaihtamalla järjestelmä toiseen, eli tehdään pilvipalvelun järjestelmämigraatio. Teoriaviitekehyksessä selvitetään mitä asioita tulee ottaa huomioon muutosta tehtäessä niin tietosuojan kuin tietoturvan näkökulmasta. Teoriaviitekehyksessä perehdytään myös sisäiseen valvontaa ja riskienhallintaan. Muutoksen läpivientiin tarvitaan tietoa myös muutoksen johtamisesta, joka on oleellinen osa prosessia.

1.1 Lähtökohta opinnäytetyölle

Tässä opinnäytetyössä tutkimusongelmana on, että kohdeorganisaation henkilöstössä on tullut paljon muutoksia kuluneen vuoden aikana, jolloin myös tehtävänkuvat muuttuivat monilla. Työtehtäviä on yhdistelty ja työnkuvaan nähden tietoa on saatavilla liian laajoina asiakokonaisuuksina. Henkilötietojen tietosuoja-asetus GDPR osaltaan vaikuttaa siihen, että tiedon tallennusjärjestelmiä tulee muuttaa, jotta henkilötietojen säilytys ja käsittely on turvallista ja lainmukaista. Myös tämän vuoksi yrityksessä on ryhdytty toimenpiteisiin tiedon turvaamiseksi. Kohdeorganisaatio tallentaa tietoja pilvijärjestelmään, mutta nykyisellään se ei taivu tarvittaviin muutoksiin. Kehittämistyön aihe tuli työelämän tarpeista. Organisaatiossa on paljon tietoa ja tietoihin pääsyä tulee rajata tarkemmin koskemaan uutta lainsäädäntöä. Kaikkien ei tarvitse myöskään päästä muuttamaan tai poistamaan tiedostoja. Tietojen löytäminen tulee tehdä sujuvammaksi kuin mitä se on tällä hetkellä, eli kansiorakennetta tulee muuttaa uuden järjestelmän puolelle.

Kohdeyrityksellä on kaksi tavoitetta pilvipohjaisen tallennusratkaisun uudistamisessa. 1) Tietosuoja, eli henkilötietojen suojauksen kehittäminen siten, että vain tietoa tarvitsevalla on pääsyoikeudet henkilötietoihin. 2) Tietoturva, eli tietojen teknisen suojauksen kehittäminen ja käytettävyyden parantaminen. Uusi pilvipohjainen tallennusratkaisu rakennetaan Google Driven business -versioon, Jaetun Driven puolelle. Opinnäytetyön tarkoitus on saada selvitettyä, millaisiin ryhmiin pilvipohjaisessa tallennusjärjestelmässä henkilökunta saadaan jaettua järjestelmämigraatiota varten. Sekä uudistaa kansiorakenne ja oikeuksienjako niihin, siten että tietoturva-asiat otetaan huomioon muutosta tehdessä. Opinnäytetyössä etsitään vastauksia seuraaviin tutkimuskysymyksiin:

- Millaisiin ryhmiin työntekijät jaetaan uutta tallennusjärjestelmää varten?
- Miten tietosuoja ja tietoturva tulisi ottaa huomioon yrityksen pilvipalvelussa?
- Miten organisaation sisäinen valvonta toteutetaan ja riskejä hallitaan esimiehen näkökulmasta?

Aikaisempia tutkimuksia on järjestelmämigraatiosta muun muassa Hakalan Annin tekemä työ vuodelta 2011 *Sampo Pankki Oyj:n mediajulkisuus*, siinä Sampo Pankki ja Danske Bank toteuttivat vuonna 2008 järjestelmämigraation. Pilvipalvelun järjestelmämigraatiosta ei löytynyt juurikaan aikaisempia tutkimuksia. Raunion (2013) Tietojenkäsittelyn koulutusohjelman opinnäytetyössä

Koepalvelun näkymien koostaminen digitaaliseen oppimisjärjestelmään sivuttiin hieman pilvipalvelun järjestelmämigraatiota kertomalla, että tällaista on olemassa, mutta aiheeseen ei syvennytty tarkemmin. Tutkimuksia pilvipalvelusta on erittäin paljon tehty viimeisen kymmenen vuoden aikana. Järjestelmämigraatiosta löytyi vain viisi tieteellistä tutkimusta.

1.2 Tutkimusmenetelmät

Tutkimusstrategiana käytetään konstruktiivistatutkimusta. Tutkimusmenetelmänä käytetään mixed methodsia eli menetelmätriangulaatiota. Siinä kvalitatiivista eli laadullista tutkimusta, sekä kvantitatiivista eli määrällistä tutkimusta yhdistetään. Aineiston hankinta eli tutkimusmetodeina ovat teemahaastattelu ja kysely verkossa. Kysely tehdään poikittaistutkimuksena Google Form:lla 70:lle työntekijälle, eli kerätään aineistoa samaan aikaan useilta vastaajilta. Teemahaastattelu tehdään Adobe Connect:lla kahdelle henkilölle. Haastattelu on kvalitatiivisen tutkimuksen puolelta ja kysely on kvantitatiiviselta puolelta.

Aineiston analysointimenetelmänä käytetään litteroinnin jälkeen sisällönanalyysia. Työtehtäväkyselyn vastauksien avulla suunnitellaan ryhmäjaottelu, jota tarvitaan Jaetun Driven puolella. Haastatteluiden avulla on tarkoitus selvittää miten sisäinen valvonta ja riskienhallinta on kohdeorganisaatiossa toteutettu tällä hetkellä ja niiden päivittäminen. Kehittämismenetelmänä käytetään haastatteluista ja kyselystä saatuja materiaaleja, joita käytetään kehittämisryhmän työpajassa. Materiaalien avulla tehdään suunnitelma ryhmäjaosta järjestelmämigraatiota varten. Tutkija on mukana kehittämisryhmässä, jossa suunnitellaan kansiotasoja ja niiden oikeuksia henkilöstölle. Tarkoitus on luoda kokonaan uudenlaisen kansiorakenne Jaetun Driven puolelle. Nykyisestä Drivestä tarvittavat tiedostot tullaan siirtämään uuteen järjestelmään. Tietoturva kyselyllä selvitetään yrityksen tietoturva-asioiden nykytilanne. Kehittämistyön tuloksena on järjestelmämigraatio, jossa tietosuoja ja tietoturva on otettu huomioon. Tutkija on muutosprosessin toteutuksessa mukana.

Tämän kehittämistehtävän toimeksiantajana on yksityinen aikuiskoulutusalan yritys. Se järjestää työvoimakoulutuksia ja asiantuntijapalveluita valtakunnallisesti. Yrityksen hankkija-asiakkaina toimii Elinkeino-, liikenne- ja ympäristökeskukset (ELY) sekä Työ- ja elinkeinotoimistot (TE-toimisto). Koulutuksissa opiskelevat työttömät tai työttömyysuhanalaiset henkilöt. Henkilökuntaa on noin 150 tällä hetkellä. Alkuvuodesta henkilöstön määrä oli reilu kaksisataa. Tämä muutos on vaikuttanut monien työnkuvaan, jonka vuoksi pilvipalvelun vaihtoon oli aika ryhtyä.

2 Pilvipohjaiset tallennusjärjestelmät

Pilvipalveluiden avulla on mahdollista saavuttaa kilpailuetu yrityksissä. Ne, jotka eivät lähde pilvipalveluita käyttämään tulevat menettämään kilpailuetunsa. Pahimmillaan organisaatiossa on käytössä vanhentunut heterogeeninen laitekanta, jossa on vanhentuneet sovellukset, kalliit huoltosopimukset, hitaat verkkoyhteydet, eikä lainkaan mobiili- tai etätyönmahdollisuuksia. Mikäli tilanne on edellä kuvaillun kaltainen, on organisaation ennuste heikko ja tulevaisuudessa kannattavuus laskee. Pilvipalveluilla voidaan korvata sähköposti-, sovellus- ja tiedostopalvelimet. Kiinteät kustannukset laskevat, hallittavuus parantuu, toiminta tehostuu, liikkuvuus kasvaa, prosessit nopeutuvat, henkilöstö ja asiakkaat ovat tyytyväisempiä, sekä liiketoiminnan kannattavuus paranee. (Salo 2012, 174-175.)

Suomen etu pilvipalveluiden palvelinkeskusten sijaintipaikkana on viileä ilmasto, yheiskuntarauha, korkea koulutustaso ja sähkönjakeluverkoston toimintavarmuus. Googlella on palvelinkeskus Haminassa entisessä paperitehtaassa, CSC on rakentanut omansa Kajaaniin. Facebookin uusi palvelinkeskus rakennettiin Ruotsiin. Palvelinkeskukset työllistävät vähän, mutta niiden merkitys on merkittävä pilvipalveluiden runkona. Suomi pienenä kansantaloutena olisi hienoa nähdä Euroopan parhaimpana palvelinkeskuksien sijaintipaikkana. (Salo 2012, 186-187.)

Gartner listaa vuosittain strategisia tekniikoita, joissa pilvipalvelut ovat olleet kymmenen parhaan joukossa vuodesta 2008. (Gartner on ICT-alan kansainvälinen tutkimus- ja konsultointiyritys Connecticutissa. (Gartner 2019).) Cloud computin käsitteenä on yleistynyt vuonna 2007 ja lyhyen historiansa aikana se on lunastanut paikkansa ja havainnollistanut pilvipalvelu-konseptiin liitetyt hyödyt. Pilvipalveluiden analogia on telekommunikaatiossa, jossa verkon topologiaa kuvataan pilvi kuvalla. Pilvipalvelulle ei ole olemassa universaalia yhden virkkeen pituista määritelmää, vaan se edustaa trendiä, jossa tietotekniikkaa käytetään palveluna. (Salo 2014, 92.)

Nykyaikana ympäristön tila aiheuttaa huolta. Kaikista päästöistä tietotekniikan osuus on pieni. Pilvipalveluiden käytöllä on suuret välilliset positiiviset ympäristövaikutukset. Mikäli etätyömahdollisuudet parantuvat, tulevat työmatkakulut vähenemään ja työtiloja ei tarvita niin paljoa. Tämän tyylinen kehitys säästäisi fossiilista polttoainetta, toimitilojen rakentaminen ja ylläpito säästäisi luonnonvaroja. Työn tuottavuudennousu lisää taloudellista hyvinvointia yleisesti ja merkittävin tekijä talouskasvussa on työn tuottavuuden kasvu. (Salo 2010, 148-149.)

2.1 Pilvipohjaiset tietojärjestelmät

Pilvipalvelut ovat yleiskielessä internetistä hankittuja sovelluksia, tietokonekapasiteettia ja palvelinsuoritteita. Ilmiössä on kyse täysin uudesta toimintatavasta ja uusita palveluista. Cloud computingista puhutaan myös toimintamallina, jonka kautta fyysisitä konesaleista voidaan luopua. (Heino 2010, 32.) Pilvipalvelu on nimitys verkossa oleville tiedontallennuspalveluille. Pilvipalveluiden tarkoituksena on vähentää palveluntarjoajan työmäärää ja alentaa palvelun tuottamisen kustannuksia. Pilvipalveluiden avulla on mahdollisuus tarjota erilaisia työskentelyalustoja ja ohjelmiston osia. (Finanssiala ry, 2009.)

Pilvipalvelu eli cloud computing -termi tulee puhelin- ja tietoliikenneverkkojen dokumentointitavasta. Pilvisymbolia on käytetty jo 1980-luvulla asiakkaan ja puhelinoperaattorin laitteiden välillä. Verkot ovat monimutkaisia ja sisältävät monia yksittäisiä laitteita, joten niiden piirtäminen kuvaksi on haasteellista. Yksinkertaistaakseen tätä verkkoa esitetäänkin se pilvisymbolina. Nimitys ’pilvi’ on tästä peräisin. Pilvipalveluita on jo yli kymmenen vuotta ollut olemassa. Pilvitoimintamallilla tarkoitetaan uudenlaista tarjontaa it-palveluvyöhykkeille. Yritysten kannalta pilvitoimintamallissa on kyse kyvystä mukautua muutoksiin sekä rahasta. (Heino 2010, 9-10, 32.)

Pilvipalveluiden käytössä on otettava huomioon jatkuva muutos, sillä kehitys on todella nopeaa. Asenteelliseen muutokseen on panostettava, sillä uusia asioita tulee opetella jatkuvalla syötöllä pienissä erissä. Viiden vuoden välein pidettävät kurssitukset eivät toimi pilvipalveluiden kanssa, parikin vuotta on toisinaan jo liikaa. (Salo 2014, 115.)

Pilvipalveluita voi ostaa vuorokausi- tai kuukausihinnoittelulla, joten aloitus ja lopetus on tehty helpoksi. Tilaa pilvipalvelusta voidaan ostaa luottokortilla. Pilvipalvelussa kaikki käyttävät samaa multitenant -ympäristöä, jossa kaikkien käyttäjäryhmien ja käyttäjien kesken tietojenkäsittelykapasiteetti on yhteiskäytössä ja data on käyttäjäryhmä tai käyttäjä kohtainen. (Heino 2010, 40-42.)

Pilvipalveluille ominaisinta on käyttöpaikan ja päätelaitteen riippumattomuus. Käyttäjä tarvitsee vain verkkoyhteyden laitteeseensa, jonka avulla kirjautuminen pilvipalveluun onnistuu selaimen tai erillisen sovelluksen avulla. Paikkariippumattomuuden vuoksi työn tekeminen on mahdollista mistä päin maailmaa tahansa, huomioon tarvitsee ottaa vain maakohtaiset tietoliikenneyhteydet. Päätelaiteriippumattomuuden vuoksi pystytään tukemaan useita laitteita, kun eri työasemille ei tarvitse sovittaa yksittäisiä omia sovelluksia. Päätelaite- ja paikkariippumattomuus mahdollistaa palveluiden yhtäjaksoisen ja jatkuvan käytön verkossa. Jatkuva käyttö on mahdollista, kun tietoliikenneverkkojen välille on rakennettu roaming-ominaisuuksia. (Heino 2010, 45-47.)

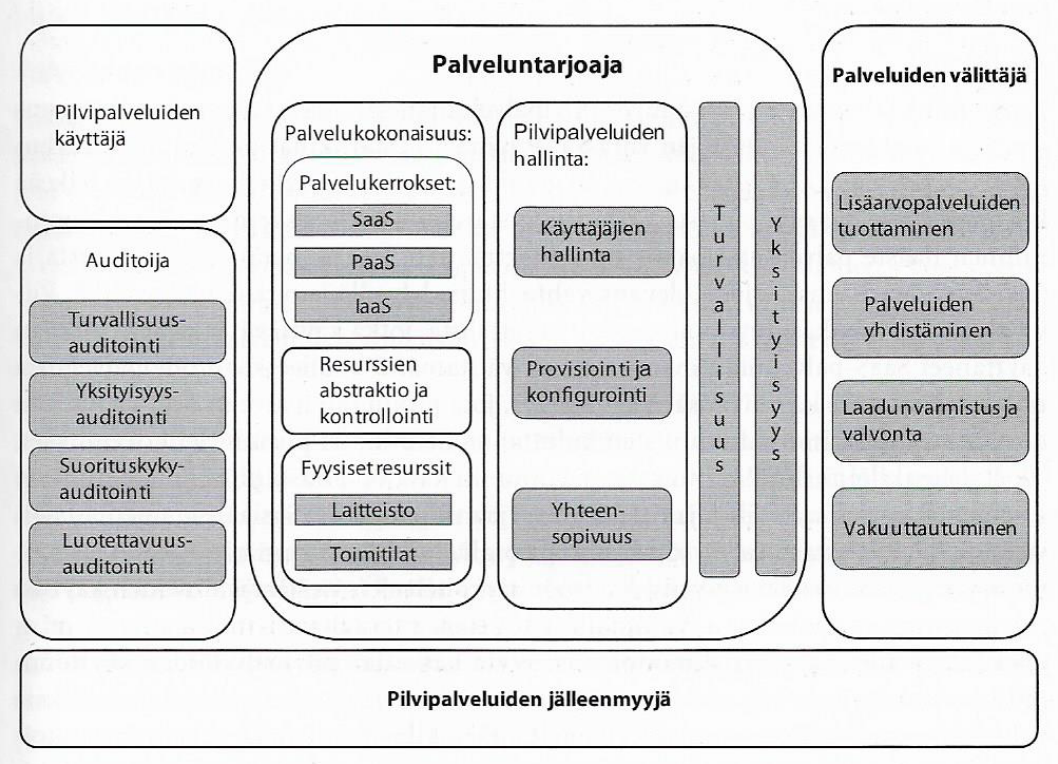
Pilvipalvelu (cloud computing) käsitteelle ei ole olemassa yleistä määritelmää. Käsitettä pilvi (cloud) käytetään kielikuvana, joka viittaa internettiin ja pilvipalveluilla tarkoitetaan eri tietotekniikkaresurssien muodostamia malleja, joita tarjotaan verkon kautta käyttäjille. Tietotekniikkaresursseja ovat palvelut, sovellukset, tietoliikenneyhteydet ja tallennuskapasiteetti. Käyttäjien ei tarvitse tietää resurssien sijaintia, eikä ottaa vastuuta toiminnasta ja ylläpidosta. Pilvipalveluiden eniten siteeratttu määritelmä on Yhdysvaltojen julkishallinnon standardeja suunnittelevan NIST:n (National Institute of Standards and Technology), joka on paikallinen elinkeinoministeriön alainen: ”Pilvipalvelut on toimintamalli, joka mahdollistaa pääsyn vapaasti konfiguroitaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön tai poistaa käytöstä helposti ja nopeasti.” (Salo 2012, 16-17.)

Pilvipalveluita käytetään innokkaasti verkkotallennukseen, mutta Suomessa se on kielletty joka kolmannella työpaikalla pilvipalvelu Evernoten kyselyn mukaan, joka on tehty helmikuussa 2014 Pohjoismaihin. Suomalaisten suosituin tietotyössä käyttämä pilvipalvelu on Google Drive, jota käyttää yli puolet kyselyyn vastanneista. Toiseksi suosituin on Dropbox ja Microsoftin OneDrive. Sen sijaan Evernoten sovellusta töissä ei käyttänyt Suomessa kukaan. Kyselyn perusteella yli sadan työntekijän yrityksissä pilvipalveluiden sovellukset on kielletty yli 40 prosentissa toimistoja. (Lehto, Tekniikka & Talous 2014.)

Pilvipalvelut toimivat erilaisten sovellusten päähankintakanavina. Tulevaisuudessa pilvipalveluiden rooli tulee todennäköisesti vain kasvamaan myös suuryrityksissä. Asiakas pääsee pilvipalvelussa käsiksi tarvitsemiin sovelluksiin internetin välityksellä paikasta ja ajasta riippumatta. Samaa sovellusta käyttää useampi eri palveluntarjoajan asiakas. Palveluntarjoaja on tällöin vastuussa sovellusten toiminnasta, kehityksestä ja päivityksestä. Keskitetty toiminta mahdollistaa merkittäviä mittakaavaetuja, mikä näkyy käyttäjäyrityksille yleensä edullisena käyttöön perustuvana hintana. Kokonaiskustannuksiltaan pilvipalveluiden käyttö voi olla jopa 50 – 80 prosenttia edullisempaa kuin perinteisten lisenssivaihtoehtojen käyttö. Hinnoittelu voi määräytyä esimerkiksi käytettävien moduulien tai sovellusten lukumäärän, käyttäjämäärän, kapasiteetin tai tapahtumavolyymien mukaan. (Mäkitalo 2017, 22-23.)

Nykyisin dataa tallennetaan pilveen fyysisesti itse hallitun konesalin tai palvelimen sijasta. Suuria etuja pilvessä on automaattinen skaalautuminen miljoonien laitteiden datavirroille ja erittäin edullinen tallennustila. Pilvipalveluja on saatavilla erilaisia. Suunniteltuja nimenomaan teolliseen internettiin, joissa datavaraston lisäksi on analytiikan, laitehallinnan ja visualisoinnin työkalut. Datan käsittelyn ja tallennuksen paikkana pilvi ei ole kaikissa tapauksissa paras valinta, usein kuitenkin hinnan perusteella se on järkevin valinta. Tietoturvasyistä on perusteltua datan varastointia

paikallisesti, mutta analysoinnissa on siivottu pois tietosuojan kannalta kriittiset osiot. Datavarastona pilvi ei ole vaihtoehto, mikäli datan käyttötarve ei salli mahdollista verkkoyhteyden pätkimistä tai pilvenväistämätöntä latenssia. Esimerkkinä tällaisista tapauksista on koneet, jotka tuottavat sekunnissa satoja tietueita, joissa havaituista poikkeamista tieto täytyy saada nopeasti. (Collin & Saarelainen 2016, 202.)



Kuva 1. Pilvipalvelun arkkitehtuuri. (Salo 2012, 29.)

Yllä olevassa kuvassa (Kuva 1) on pilvipalvelun arkkitehtuuria. Siinä kuvataan pilvipalvelumarkkinoita kokonaisuudessaan. Pilvipalvelumarkkinoiden kokonaisarkkitehtuuri koostuu viidestä toimijasta: asiakkaista, palveluntarjoajista, palveluiden välittäjistä, palveluiden jälleenmyyjistä ja auditoijista. Asiakkaisiin kuuluu palveluita käyttävät organisaatiot ja yksityiset ihmiset. Palveluntarjoajat tuottavat palveluita ja myyvät niitä loppuasiakkaille suoraan tai välikäsien kautta. Välikäsinä ovat jälleenmyyjät tai palveluiden välittäjät. Auditoijat toimivat palveluiden laadunvarmistuksessa. (Salo 2012, 29-30.)

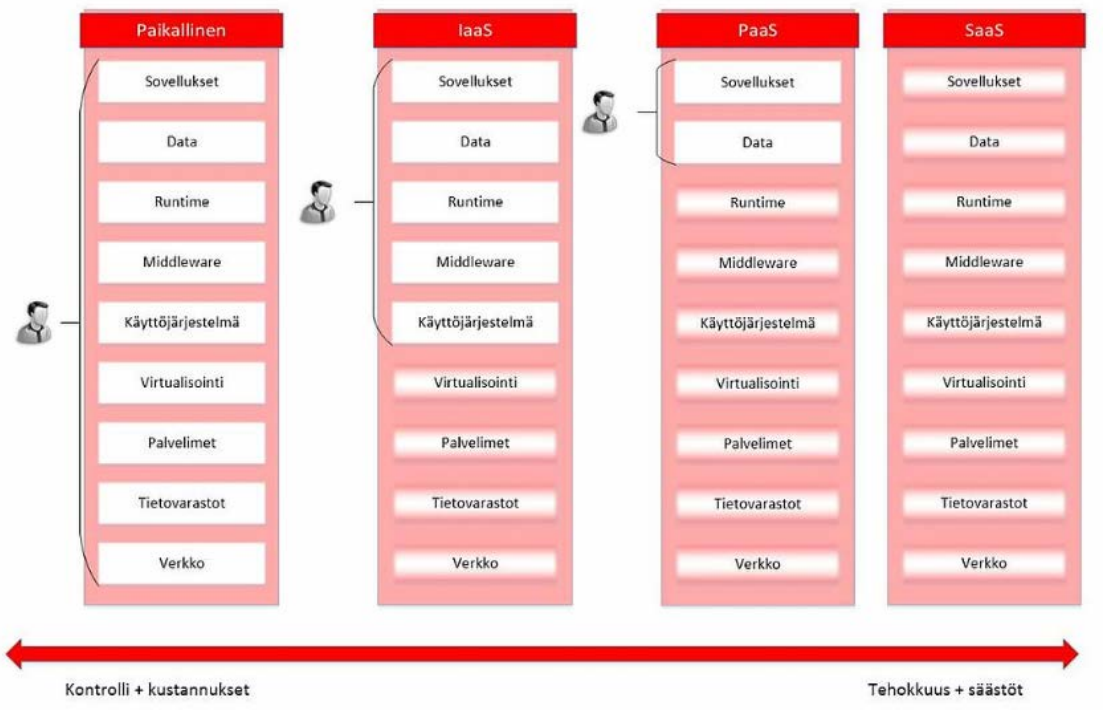
Pilvipalveluihin liittyviä riskialueita ja huolenaiheita on seuraavia: **dataan** liittyvät huolet, eli yksityisyys, tietosuoja, tietojen pysyvyys ja saavutettavuus; **käyttäjähallintaan** liittyvät huolet, eli turvallisen yhteyden muodostaminen; suorituskykyyn liittyvät huolet, eli luotettavuus, saavutettavuus, ennakoitavuus, suorituskyvyn tasaisuus ja responsiivisuus; **hallintaan** liittyvät huolet, eli

kontrolli, läpinäkyvyys ja mitattavuus; **sopimusehtoihin** liittyvät huolet, eli poikkeustilanteet, mahdolliset muutokset tulevaisuudessa, palvelutasosopimuksen sisältö, lukittuminen palveluntarjoajaan, vastuukysymykset ongelmatilanteissa; **tekniseen toteutukseen** liittyvät huolet, eli dokumentoimattomat ilmiöt, muutoksista ilmoittaminen ja pitkän aikavälin tuki; **palveluntarjoajaan** liittyvät huolet, eli toimitilat, henkilöstö, vikatilanteesta toipuminen ja tiedottaminen; **säännöksiin ja sääntöihin** liittyvät huolet, eli standardit, asiakkaiden ja toimitilan vaatimukset ja lainsäädäntö. (Salo 2012, 37.)

Pilvipalveluiden riskeihin varautuessa kannattaa miettiä palvelukohtaisesti, miten toimitaan, jos palvelu on hetkellisesti tai pidemmänkin aikaa pois käytöstä, tai jos halutaan siirtää palvelun käyttö toisaalle. Palveluntarjoajat eivät ole tehneet helpoksi pilvipalvelun vaihtamista toiselle palveluntarjoajalle. Siirtäminen voi olla jopa mahdotonta, sillä kukaan muu ei tarjoa vastaavaa palvelua erityisominaisuuksien tai lisäarvopalveluiden vuoksi. (Salo 2014, 112-113.)

2.1.1 Pilvipalvelumallit

Pilvipalvelumalleja on kolme, joita ovat IaaS (Infrastructure as a Service) eli Infrastruktuuri palveluna, PaaS (Platform as a Service) eli Palvelualusta ja SaaS (Software as a Service) eli Ohjelmisto palveluna. Nämä kolme päämallia ovat eri tyyppisille käyttäjille. (AWS Amazon 2019.) Seuraavassa kuvassa (Kuva 2) on kuvattu paikallisen tallennusratkaisun ja pilvipalveluiden arkkitehtuuria. Mallit ovat paremmuusjärjestyksessä, vasemmalla tehottomin ja oikealla tehokkain ratkaisu. Paikallisella tasolla kontrolli ja kustannukset ovat suuret, kun taas SaaS pilvipalvelumallissa tehokkuus ja säästöt ovat maksimaaliset.

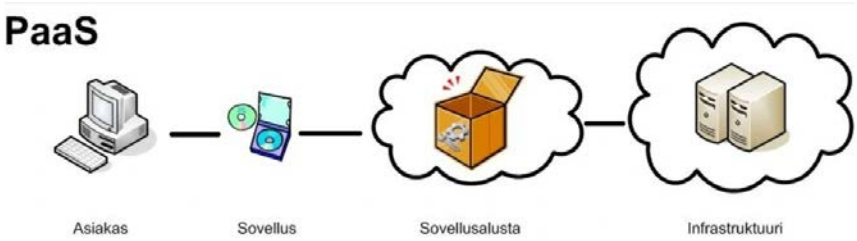


Kuva 2. Pilvipalvelumallien arkkitehtuuri. (Koppinen 2014.)

IaaS on palvelimien ulkoistamista. IaaS palvelu on suunnattu organisaatioille (Kuva 3). Palveluntarjoaja ylläpitää ja omistaa laitteiston. Tämä palvelumalli tarkoittaa internetin välityksellä tarjottavaa säilytystilaa, laskentatehoa ja verkkoinfrastruktuuria. Päätehtävänä IaaS palvelumallissa on laskentatehon ja tallennustilan tarjoaminen palveluiden asiakkaille. Yksi suurimmista IaaS palveluntarjoajista on Amazon Web Services, muita ovat Windows Azure, HP ja IBM. (Finanssiala, 2019; Koppinen 2014.)

Kuva 3. IaaS Pilvipalvelumalli. (Fandom 2017.)

PaaS palvelu on sovelluskehittäjille suunnattu, jotka haluavat siirtää järjestelmien hallintaa PaaS palveluntarjoajille (Kuva 4). PaaS tarkoittaa palvelualustan ulkoistamista. Palveluntarjoaja tuottaa palvelunaan sovellusalustoja, jotka käyttäjällä ovat helposti käyttöön otettavissa. Kehitysalustat mahdollistavat alustan helpon kehittämisen ja laajentamisen. PaaS palveluilla tehdään mobiili- ja websovelluskehitystä. Kehityskomponentit ovat valmiiksi ylläpidettyjä ja konfiguroituja. PaaS palveluita tarjoavasta alustasta esimerkkinä on Windows Azure Cloud Services, Google App Engine, Red Hat OpenShift. (Finanssiala, 2019; Koppinen 2014.)

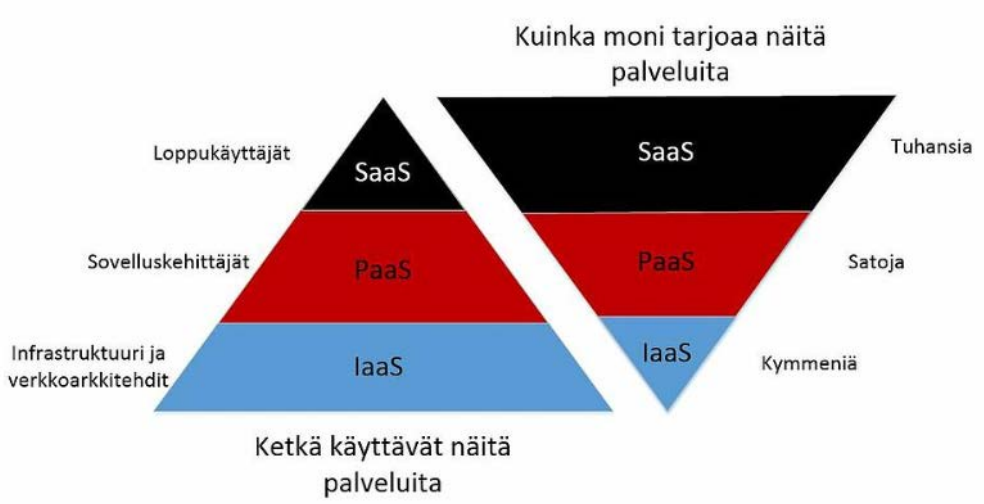


Kuva 4. PaaS pilvipalvelumalli. (Fandom 2017.)

SaaS palvelu on suunnattu loppukäyttäjille, joissa on mahdollista käyttää ohjelmia kuukausimaksua vastaan. SaaS palvelumallissa internetin välityksellä hankitaan jokin ohjelmisto palveluna (Kuva 5). SaaS mallissa ei asenneta erillisiä sovelluksia, vaan sitä käytetään internet-selaimella. Palvelun tarjoajan vastuulla on huolehtia palvelun toimivuudesta, turvallisuudesta ja saatavuudesta. SaaS:n käyttöön tarvitaan ainoastaan internetyhteys. Tuhannet käyttäjät voivat käyttää SaaS tyyppistä pilvipalvelua samaan aikaan, esimerkiksi Google Docs on tällä tekniikalla toteutettu. Muita palveluntarjoajia on Microsoft, Salesforce, SAP, Adobe, Cisco. (Finanssiala, 2019; Koppinen 2014.)

Kuva 5. SaaS pilvipalvelumalli. (Fandom 2017.)

Alla olevassa kuvassa (Kuva 6) on kuvattu pilvipalvelumalleja, joita on kolme: IaaS, PaaS ja SaaS. Vasemman puoleisessa kolmiossa on kuvattu palveluita käyttävien määrät. Vastaavasti oikean puoleisessa ylösalaisin olevassa kolmiossa palveluita tarjoavien määrä. IaaS palvelua käyttävät infrasfruktuuri ja verkkoarkkitehdit ja palvelua tarjoavien määrä on kymmeniä. PaaS palvelua käyttävät sovelluskehittelijät ja tarjoajia on satoja. SaaS palvelua käyttää loppukäyttäjät ja palvelun tarjoajia on tuhansia.



Kuva 6. Pilvipalvelumalleja. (Koppinen, 2014.)

Pilvipalvelutyyppejä on kolme erilaista, julkinen, yksityinen ja hybridi pilvi. Julkinen pilvipalvelu ja infrastruktuuri tarjotaan julkisessa verkossa. Valintana julkinen pilvi on hyvä, kun kehitetään ja testataan ohjelmistokoodeja tai kuormitushuippujen vuoksi on tarve lisätä prosessien suorituskykyä. Yksityisiä pilvipalveluita ja infrastruktuureja ylläpidetään yksityisessä verkossa. Yksityiset pilvet vaativat, että yritys ostaa ohjelmistoille ylläpidon, taatakseen korkean tason turvallisuuden ja hallinnan. Organisaation kannattaa valita yksityinen pilvi, kun se on osa teollisuutta, jolla tiukat turvallisuusvaatimukset ihmisten henkilökohtaista dataa käsiteltäessä. Hybridi pilvitekniikassa käytetään yksityistä pilveä kontrolloidusti, mutta toimintoja delegoidaan tarvittaessa julkiseen pilveen, esimerkiksi ruuhka-aikoina kannattaa siirtää sovelluksia julkisen pilven puolelle. (Sensoan 2016.)

2.1.2 Järjestelmämigraatio

Järjestelmämigraatio on prosessi, jossa liiketoimintaprosessit siirretään uudempaan ohjelmisto-alustaan. Tarkoitus on, että organisaatio pysyy ajan tasalla tekniikassa. Järjestelmän vaihto on muutos parempaan nykyisestä. Järjestelmämigraatio on ajankotainen silloin, kun entinen järjestelmä ei pysty tarjoamaan vaadittua suorituskykyä eikä pysty vastaamaan yrityksen liiketoiminnan tarpeisiin. Mikäli on tarkoitus siirtää vain ohjelmistoja ja tiedostoja, voidaan siirto-ohjelmistoilla siirto automatisoida. (Techopedia.)

Tärkeimpiä syitä järjestelmämigraatioon ovat:

- Tämän hetkinen järjestelmä ei toimi enää odotuksien mukaisesti.
- Saatavilla on uutta tekniikkaa, joka ohjaa prosesseja nopeammin.
- Nykyinen järjestelmä vanhenee ja siihen ei ole saatavilla enää kauan tukea.
- Yritys on ottamassa uuden suunnan.

(Techopedia.)

Kaikki tietojärjestelmät vanhentuvat jossain vaiheessa ja uudistuksiin on ryhdyttävä esimerkiksi vanhenevan tekniikan myötä tai käyttäjien vaatimuksesta. Järjestelmämigraatio uusien vaatimusten mukaiselle alustalle säilyttää perustoiminnallisuuden ja tietovaraston kehittyvän, uuden järjestelmän sydämenä. (Finnish Support Center.)

Organisaation liiketoiminnan kannalta kriittisiä järjestelmiä siirrettäessä uudelle alustalle, kannattaa huomioida kaksi tärkeää seikkaa: tulee kirkastaa päämäärä ja suunnitella tarkoin. Oikea tapa toteuttaa IT-remonteista kriittisin on tarkkoihin suunnitelmiin perustuva migraatio. Suunnitteluvaihe on tärkeä, jolloin parhaaseen lopputulokseen pääsee pohdinnalla, selkeillä stepeillä ja mittaamisella. Päämäärien kirkastamisella tarkoitetaan, että on pohdittava mitä uudella järjestelmällä tulevaisuudessa on tarkoitus tehdä. Onnistunut migraatio on hyvä oppimisprosessi. Suunnittelemalla mitä siirretään ja missä vaiheessa tuo onnistumisia, ettei liiketoiminta kärsi uudistuksesta. Siirrot kannattaa aloittaa pienemmistä, vähemmän liiketoimintakriittisistä järjestelmistä ja uuteen järjestelmään kannattaa siirtää vain tarpeellinen tieto. (Makkonen 2017.)

2.2 Tietosuoja

Tietosuojalla tarkoitetaan ihmisten yksityisyyden suojelemista ja kunnioittamista oikeudellisia säännöksiä noudattavin toimintakäytännöin ja periaattein. (Kuula 2006, 263). Tietosuoja on perusoikeus, jolla turvataan rekisteröidyn vapauksien ja oikeuksien toteutumista henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, millä edellytyksillä ja milloin voidaan käsitellä henkilötietoja. Tietosuojan ja tietoturvan erona on se, että tietoturva on yksi keinoista toteuttaa tietosuojaa. Tarkoitus on suojata tietojärjestelmät ja tietoaineisto. Tietoturva tarkoittaa muun muassa teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan järjestelmien käytettävyys, rekisteröidyn oikeuksien toteutuminen, tiedon eheys ja luottamuksellisuus. (Tietosuojavaltuutetun toimisto, tietosuoja.)

Käsiteltäessä henkilötietoja on aina noudatettava tietosuojaperiaatteita ja lakia. Henkilötietojen käsittelystä on kuusi eri perustetta tietosuoja-asetuksessa: sopimus, rekisteröidyn suostumus, elintärkeiden etujen suojaaminen, rekisterinpitäjän lakisääteinen velvoite, rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu sekä yleistä etua koskeva julkinen valta tai tehtävä. Lähtökohtaisesti kiellettyä on terveyttä ja etnistä alkuperää koskevien tietojen käsittely. Käsittelykieltoon säädetyt poikkeukset mahdollistavat tietojen käsittelyn. Henkilötietoja on kaikki ne tiedot, joissa henkilö on tunnistettavissa, esimerkiksi nimi, puhelinnumero, kotiosoite, sähköpostiosoite, auton rekisterinumero, henkilökortin numero, potilastiedot, henkilökortin numero, paikannustiedot, IP-osoite. (Tietosuojavaltuutetun toimisto.)

Käsiteltäessä henkilötietoja noudatetaan aina tietosuojaperiaatteita. Henkilötietoja on tietosuojaperiaatteiden mukaisesti: Käsiteltävä asianmukaisesti, lainmukaisesti ja läpinäkyvästi. Tietoa on kerättävä vain tiettyä tarkoitusta varten ja vain tarpeellinen määrä. Tietoja on päivitettävä ja säilytettävä siinä muodossa, jossa se on tunnistettavissa tarpeellisen ajan. Henkilötietoja on käsiteltävä turvallisesti ja luottamuksellisesti. (Tietosuojavaltuutetun toimisto.) Henkilötietojen käsittelyn aikana tiedot voivat kulkea monien organisaatioiden ja yritysten läpi. **Rekisterinpitäjä:** päättää henkilötietojen käsittelytavasta ja -tarkoituksesta. **Tietojenkäsittelijä:** käsittelee ja säilyttää tiedot rekisterinpitäjän puolesta. (Euroopan Unioni 2019.)

Tietosuojavastaava tulee nimittää organisaatioihin, joissa edellytetään työtehtävänä arkaluontoisten tietojen laajamittaista käsittelyä, ihmisten järjestelmällistä, säännöllistä ja laajamittaista seurantaa. Tai jos yritys toimii julkishallinnossa. Tietosuojavastaava on yrityksen sisäinen asiantuntija tietosuoja-asioissa sekä tietosuojaviranomaisen ja rekisteröityjen yhteyshenkilö. (Tietosuojavaltuutetun toimisto.)

2.2.1 Tietosuoja-asetus GDPR

Yleinen tietosuoja-asetus GDPR tulee sanoista General Data Protection Regulation. GDPR on uusi henkilötietojen käsittelyä sääntelevä laki, jota on sovellettu 25.5.2018 alkaen kaikissa EU-maissa. Tietosuoja-asetuksen avulla saa enemmän keinoja omien tietojen käsittelyyn sekä parempaa suojaa henkilötiedoille. Tavoitteena uudella lainsäädännöllä on parantaa henkilötietojen tietosuojaoikeuksia ja suojaa, yhtenäistää tietosuojakäsittelyä kaikissa EU-maissa, vastata uusiin globalisaatioon ja digitalisaatioon liittyviin tietosuojakysymyksiin, sekä edistää digitaalisten sisämarkkinoiden kehittymistä. (Tietosuojavaltuutetun toimisto.)

Uusi asetus koskee kaikkia organisaatioita, jotka keräävät, käsittelevät ja säilyttävät henkilötietoja. Lähes kaikissa yrityksissä ylläpidetään henkilörekistereitä, muun muassa jäsen- tai asiakasrekisteriä, on asetuksen soveltamisala laaja. Rikkomusten hallinnollinen sakko on maksimissaan 20 miljoonaa euroa tai 4 % yhtiön edellisen vuoden kokonaisliikevaihdosta, riippuen kumpi on suurempi. Tietosuojaviranomainen voi myös muina toimenpiteinä kieltää henkilötietojen käsittelyn. (Euroopan Unioni 2019). Organisaation tietoturvakäytännöt kannattaa dokumentoida tietoturvadokumenttiin, jossa on vastattu seuraaviin kysymyksiin: miten tietoturvasta huolehditaan, miten henkilötietoja käsitellään ja perustelut niille, miten toimitaan, jos tietomurto tapahtuu ja ketkä käsittelevät henkilötietoja. (Lianatech 2018.) Alla olevassa kuvassa (Kuva 7) on GDPR:n keskeiset peruskäsitteet.

Henkilötieto: Kaikki sellainen tieto, jolla voidaan tunnistaa ja yksilöidä henkilöitä. Näitä tietoja ovat muun muassa nimi, osoite, henkilötunnus, sähköpostiosoite sekä verkkotunnistetiedot.

Henkilörekisteri: Henkilötietoja sisältävä jäsennelty tietojoukko, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla taikka joka on järjestetty kortistoksi, luetteloksi tai muulla näihin verrattavalla tavalla siten, että tiettyä henkilöä koskevat tiedot voidaan löytää helposti ja kohtuuttomitta kustannuksitta.

Rekisterinpitäjä: Luonnollinen henkilö, yhteisö, virasto, säätiö tai joku muu, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä.

Henkilötietojen käsittelijä: Luonnollinen henkilö, viranomainen, virasto tai joku muu, joka käsittelee henkilötietoja rekisterinpitäjän lukuun, esimerkiksi uutiskirjetyökalun toimittaja.

Rekisteröity: Rekisterissä oleva tunnistettava tai tunnistettavissa oleva henkilö.

Opt-in: Henkilön itsensä antama suostumus henkilötietojensa keräämiseen ja käsittelyyn.

Kuva 7. GDPR:n keskeiset peruskäsitteet. (Lianatech 2018.)

Yleisessä tietosuoja-asetuksessa organisaatioille ja yrityksille asetetaan henkilötietojen hallinnointia, keräämistä ja säilytystä koskevat tarkat vaatimukset. Vaatimuksia sovelletaan eurooppalaisten organisaatioiden lisäksi myös EU:n ulkopuolisiin organisaatioihin, jotka käsittelevät EU:n alueella asuvien ihmisten tietoja. Yleistä tietosuoja-asetusta ei sovelleta, jos rekisteröity on oikeushenkilö tai rekisteröity on kuollut tai tietoja käsittelee henkilö, joka toimii sellaisissa tarkoituksissa, jotka eivät kuulu hänen ammattiinsa, alaansa tai liiketoimintaansa. Yritykset eivät voi käsitellä henkilökohtaisia tietoja, jotka koskevat ammattiliittoon kuulumista, sukupuolista suuntautumista, rotua tai etnistä alkuperää, poliittista mielipidettä, uskonnollista tai filosofista vakaumusta, rikostuomioita tai rikkomuksia koskevia henkilötietoja (vain jos kansallinen tai EU:n lainsäädäntö tämän sallii) tai terveydellisiä, geneettisiä ja biometrisiä tietoja. (Euroopan Unioni 2019.)

2.2.2 Tietosuojaan liittyvät lainkohdat

Tietosuojaan liittyy moni laki. Seuraavaan on avattu tärkeimpiä lakeja, joita tulee ottaa huomioon tietosuojassa.

- **Perustuslaki (731/1999, 10 §)**

  Yksityiselämän suoja. ”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.” (Finlex).

- **Tietosuojalaki (1050/2018)**

  Lain tarkoitus: ”Tällä lailla täsmennetään ja täydennetään luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679 (yleinen tietosuoja-asetus), jäljempänä tietosuoja-asetus, ja sen kansallista soveltamista.” (Finlex). *Henkilötietolaki (HetiL 523/1999)* on kumottu 5.12.2018 tietosuojalailla.

- **Laki yksityisyyden suojasta työelämässä (YksL 759/2004)**

  Lain tarkoitus: ”Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä.” (Finlex).

- **Sähköisen viestinnän tietosuojalaki (516/2004)**

  Lain tarkoitus: ”Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.” (Finlex).

- **Rikoslaki (39/1889, luku 38 ja 40)**

  Luku 38. Tieto- ja viestintärikoksista.

  Luku 40. Virkarikoksista.

- **Yhdenvertaisuuslaki (1325/2014)**

  Lain tarkoitus: ”Tämän lain tarkoituksena on edistää yhdenvertaisuutta ja ehkäistä syrjintää sekä tehostaa syrjinnän kohteeksi joutuneen oikeusturvaa.” (Finlex).

- **Laki naisten ja miesten välisestä tasa-arvosta (609/1986)**

  Lain tarkoitus: ”Tämän lain tarkoituksena on estää sukupuoleen perustuva syrjintä ja edistää naisten ja miesten välistä tasa-arvoa sekä tässä tarkoituksessa parantaa naisten asemaa erityisesti työelämässä. Lain tarkoituksena on myös estää sukupuoli-identiteettiin tai sukupuolen ilmaisuun perustuva syrjintä.” (Finlex).

- **Laki sähköisistä allekirjoituksista (14/2003)**

  Lain tarkoitus: ” Tämän lain tarkoituksena on edistää sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa.” (Finlex).

2.3 Tietoturva

Kun yrityksen data siirretään maantieteellisesti jopa kauas, tietoliikenneyhteyden taakse, toisen yrityksen ylläpidettäväksi, virtuaaliseen palvelimeen, voi tietoturvasta syntyä huoli. Pilvipalvelussa asiakkaan osa suojataan monilla tietoliikenne- ja palvelintekniikan menetelmillä. Pilvipalvelukoneisto suojataan ulkomaailman pääsyltä järjestelmään palomuurilla. Pilvipalveluntarjoajan tehtävänä on ylläpitää palomuurijärjestelmää pilvikoneiston ja internetin välillä. Esimerkiksi pa-

lomuurivalmistaja on muun muassa Cisco. Pilvikoneisto suojataan myös tunkeilijan havaitsemisjärjestelmällä, josta käytetään termiä Intrustion Detection System (IDS) tai Intrustion Detection and Prevention System (IDPS). Nämä järjestelmät reagoivat hyökkäystilanteisiin ja katkaisevat hyökkääjien yhteydet. Tiedot, jotka siirretään pilvipalveluun, salataan *kryptauksen* avulla. *Koventaessa* pilvipalvelun koneistossa olevia palvelimia, niistä poistetaan kaikki järjestelmäpalvelut, jolloin ne ovat hyökkäyksiä vastaan vastustuskykyisempiä. Kryptaus ja koventaminen on yrityksen vastuulla, ei pilvipalveluntarjoajan. (Heino 2010, 92-93.)

Alla olevassa taulukossa (Taulukko 1) on esitelty pilvipalvelun tietoturvaan liittyviä riskitekijöitä. Taulukossa arvioidaan riskin todennäköisyyttä ja vaikutusta, sekä miten niitä voidaan ehkäistä ja hallita. Kolmen plussan menetelmässä mitä enemmän on plussia, sitä suurempi on todennäköisyys ja vaikutus ja yhdellä plussalla on ominaisuuden määrä vähäistä. (Heino 2010, 96.)

Riski	Todennäköisyys	Vaikutus	Ehkäiseminen tai hallinta
Tietoliikenneyhteyksien vika	++	+++	Tehdään se, mitä itse voidaan eli hankitaan yhteydet useammalta operaattorilta. Asetelma on sama kuin käyttöpalveluna hankittaessa.
Pilvipalvelun-tarjoajan ylläpidollinen virhe	+++	++	Pilvessä ajettavista instansseista tulee saada talteen varmuuskopio pilven omalla menetelmällä. Pilveen siirretyistä sovelluksista ja kapasiteetista tulisi tarpeen mukaan saada kopioita toiseen pilvipalveluun.
Pilvipalvelun-tarjoajan toiminnan loppuminen	+	++	Vaikutus arvioidaan pieneksi, sillä asiasta kuitenkin tulee asiakkaalle tietoja etukäteen ja siihen voidaan varautua.
Luonnonmullistus, ilkivalta tai muu force majeure	+	+++	Todennäköisyys on pieni, mutta seuraukset voivat olla hyvin merkittäviä.

Taulukko 1. Pilvipalvelun riskejä. (Heino 2010, 96).

Teollisuusvakoilu, tietomurrot ja haavoittuvuudet muodostavat vakavan uhkan. Internet laajentaa hyökkäyspinta-alaa paikkoihin, joissa aiemmin ei ole ollut tarvetta selvitellä kyberturvallisuuden haasteita. Aiemmat riskienhallinnan keinot eivät enää riitä takaamaan tietoturvaa. (Collin &

Saarelainen 2016, 311.) Tietoturvalla tarkoitetaan organisatorisia ja teknisiä toimenpiteitä henkilötietojen suojaamiseksi. Pyritään estämään asiattomilta pääsy tiedostoihin, sekä estämään vahingossa tai tahattomasti tapahtuvien tietojen hävittämistä, siirtämistä, luovuttamista, muuttamista tai muuta laitonta käsittelyä. (Kuula 2006, 264.)

Tietoturvallisuus kuuluu osaksi yritysturvallisuutta. Sen osa-alueet voidaan jakaa seuraavanlaisesti fyysisiin, hallinnollisiin, henkilöstö-, laitteisto-, tietoliikenne-, tietoaineisto-, ohjelmisto- ja käyttöturvallisuuteen. Fyysisellä turvallisuudella tarkoitetaan henkilö- ja aineellisten vahinkojen riskejä koskevaa turvallisuuden osa-aluetta ja käyttö-, varastointi- ja laitteistotilojen, arkistojen sekä materiaalien ja laitteiden suojaamista fyysisiltä vahingoilta ja uhilta. Hallinnollisella tietoturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla organisoidaan, ohjataan ja ohjeistetaan tietoturvallisuuteen vaikuttavia asioita. Nämä ovat turvallisuustoiminnan järjestelyjen, henkilöstön vastuiden ja tehtävien sekä koulutuksen, ohjeistuksen ja valvonnan muodostama kokonaisuus. Henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien luotettavuusriskien hallintaa. Se sisältää henkilöstön soveltuvuuden, taustojen tarkistukset, toimenkuvien ja käyttöoikeuksien määrittelyt, sijaisuuksien varmistamisen, henkilöstön turvallisuuskoulutuksen, valvonnan ja suojaamisen. (Holopainen, ym. 2010, 301, 304.)

Laitteistoturvallisuus sisältää tietojenkäsittely- ja tietoliikennelaitteiden suunnittelun, käytettävyyden, kokoonpanon, toiminnan, kunnossapidon ja laadunvarmistuksen turvallisuusominaisuudet. Tietoliikenneturvallisuus on tärkeimpiä osa-alueita tietoturvallisuudessa. Tietoa siirretään paikasta toiseen ja usein avoimessa tietoliikenneverkossa, jolloin tämänkaltaiset tietoliikenneturvallisuus riskit ovat organisaation omien kontrollitoimien tavoittamattomissa. Tiedon turvallisuudella tarkoitetaan tiedon oikeellisuutta, käytettävyyttä, saatavuutta, luottamuksellisen aineiston turvallista käsittelyä ja salassa pitämistä. Ohjelmistoturvallisuuteen kuuluu ohjelmiston pääsynvalvonta-, tunnistamis- ja varmistusominaisuudet, lokimenettelyt, tarkkailu- ja paljastustoimenpiteet sekä laadunvarmistustekniikat ja päivystykseen ja ylläpitoon liittyvät turvallisuustoimenpiteet. Käyttöturvallisuus tarkoittaa turvallisia käyttöperiaatteita, tietojenkäsittelyn ja käyttöympäristön turvallisuuteen vaikuttavien tapahtumien valvontaa ja turvaamalla toiminnan jatkuvuus. (Holopainen, ym. 2010, 305-306.)

Tietoturvaohjeistuksen tarkastuksessa varmistutaan muun muassa siitä, että käytännön toiminta vastaa ohjeita ja valvotaan niiden noudattamista. Tietojen varmistamisella tarkoitetaan, että tiedostoista on tehty kopiot ja tiedot ovat palautettavissa, jos alkuperäiset tiedot menetetään. Tulee varmistua myös siitä, että tiedot säilyvät myös varmistusvälineellä riittävän kauan. Tietojen käytön valvonnalla kontrolloidaan, että tietoihin ja tietojärjestelmiin sallitaan vain luvallinen pääsy.

Fyysiseen turvallisuuteen kuuluu kulkuoikeuksien asianmukaisuutta ja ajantasaisuutta. Tietojen luokitukseen ja käsittelyyn kuuluu muun muassa salassapitovelvollisuus työsuhteen aikana ja sen päätyttyä. Tarkistuksessa varmistutaan, että järjestelmäkehityksen, käyttäjien ja käytön välinen työnjako on selkeästi määritelty. (Holopainen, ym. 2010, 306-309.)

Teollisen internetin käsite on käännös englannista Industrial Internet. Ensimmäisenä sen esitti 8.6.2000 yhdysvaltalainen konsultti- ja analyytikkoyhtiö Frost & Sullivan julkaisemassaan raportissa. Käsite vaipui unholaan pitkäksi aikaa, mutta vuonna 2012 se otettiin taas käyttöön yhdysvaltalaisen General Electric -yhtiön (GE) tuotekehitysyksikön toimesta. Teollisen internetin käsitettä on helppo mieltää merkitsemään ainoastaan teollisuuden internettiä. GE:n määrittelyssä teollisella viitataan siihen tunnuksenomaiseen piirteeseen, jolla ohjelmistopohjainen äly sisältyy laitteisiin ja koneisiin, jotka valmistetaan teollisesti. (Collin, ym. 2016, 29-30.)

”Jos ottaa esiin teollisen internetin valtavat tietoturvahaasteet, saa äkkiä otsaansa juhlien pilaajan leiman”. Ralph Langner, Langner Communications, omistaja. Hän on teollisuuden kontrollijärjestelmien tietoturvan huippuasiantuntija. Langner tuli kuuluisaksi oivaltaessaan, että tuhoa Iranin uraanirikastamoissa aiheuttanut Stuxnet-haittaohjelma liittyy teollisuusautomaatiojärjestelmiin. Hänen huolensa liittyy teollisen internetin tietoturvaan ja siihen kuuluviin laiminlyönteihin. Tietoturvan sivuuttaminen on todellista, kyse ei ole pelkästään riskistä. Monissa kyselyissä teollisen internetin pahimmaksi esteeksi on noussut tietoturva. Usein ensimmäisiä askelia järjestelmien verkottamiseksi ei uskalleta ottaa, sillä vakavien tietoturvariskien toteuttamisen pelko saa lamaantumaan. (Collin, ym. 2016, 241-242.)

Turvatakseen omat järjestelmät tietoturva tulee hoitaa kuntoon ennen teollisen internetin ratkaisujen käyttöönottamista. Lähtökohtana on kartoittaa yrityksen laitteet ja järjestelmät yksityiskohtaisesti ja muodostaa niistä kattava malli verkkotopologiasta. Sisäistä dokumentointia varten kannattaa teettää tietoturvan ja verkkojen auditointi. Yritysten kannattaisi tehdä järjestelmistään datavirroista verkkokaavioita. Suunnitelmassa tulee käydä ilmi, miksi tehdään ja millä tavalla tehdään, jotta luotettavuus, ylläpidettävyys ja valvottavuus olisi mahdollista. Teollista internettiä ja teollisuuden verkkoja koskee samat lainalaisuudet kuten muutakin tietoturvaa. Tarvitaan muun muassa monen kerroksen suojausta, palomuureja, tietoturvapolitiikkaa, päivitysten hallintaa. Sallittuja ovat ainoastaan valtuutetut ja tunnistautuneet käyttäjät. Suurena apuna tietoturvassa ovat protokollat, modernit standardit ja arkkitehtuurit. (Collin, ym. 2016, 245-247.)

Tietoturvauhkina nähdään suojaamattomat protokollat, sillä niistä moni siirtää salasanoja ja tunnuksia selväkielisenä sekä luvaton kuunteleminen verkkoliikenteessä. Uhkakuvia ovat myös tunnusten kalastelu, käyttäjien koneille asentuvat ei-toivotut ohjelmat (vakoiluohjelmat), palvelun ylikuormittaminen sekä identiteettivarkaudet. (Suvilehto 2011, 18-21.) Seuraavassa muutamia teknisiä ratkaisuja tietoturvauhkiin. Palomuuri ohjelmiston avulla voidaan säädellä liikennettä yksittäisen koneen ja muun verkon välillä. Palomuuri yksistään ei riitä turvaamaan verkossa olevia koneita, vaan niiden tulee olla suojattuna ulkomaailmaa vastaan. Käyttämällä kahta tai useampaa autentikaatiota saadaan vahva tunnistautuminen järjestelmiin. Vahva salasana on riittävän pitkä ja sisältää isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä ja vaihtoväli on tarpeeksi usein. Salauksella suojataan tiedon luottamuksellisuutta ja tiedon eheyttä suojataan sähköisellä allekirjoituksella. Tiedon siirron aikana kryptografia on suojana. (Suvilehto 2011, 24-38.)

2.3.1 Tietoturvallisuuden hallintajärjestelmä

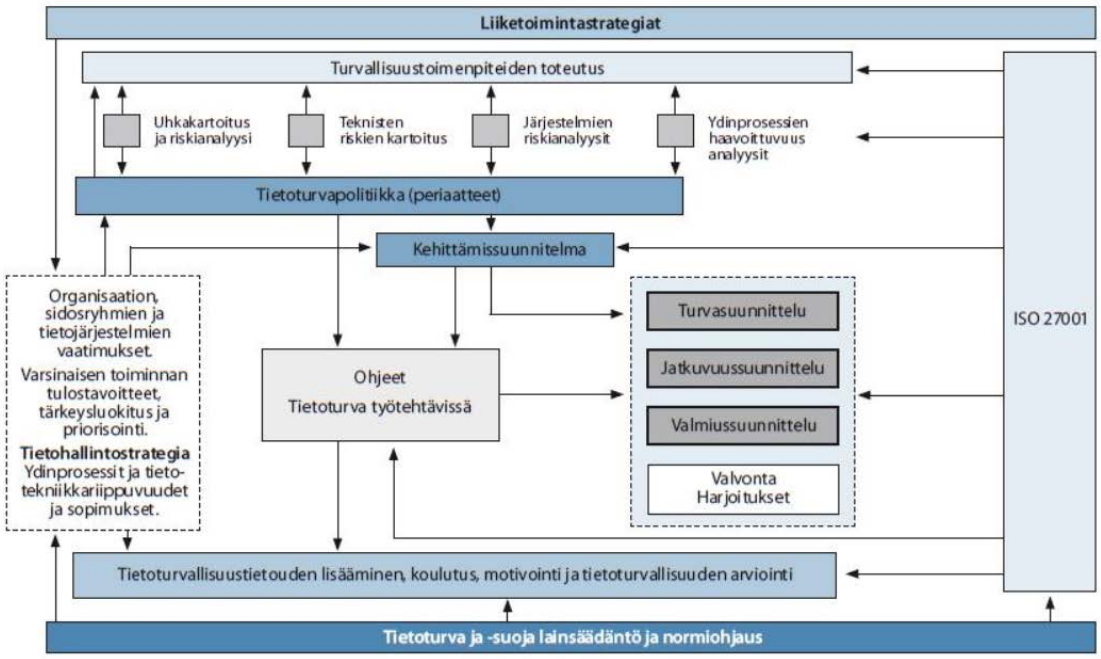
Tietoturvallisuuden ja riskienhallinnan kehittäminen on jatkuva prosessi, jossa painopiste on tuloksellisuuteen, tieto-omaisuuden turvaamiseen, laillisuuteen ja tietoturvapoikkeamien luotettavaan raportointiin liittyvien tavoitteiden edistämistä. Tietoturvallisuus tulee sisällyttää osaksi yrityksen toimintaprosesseja toteutuakseen käytännössä. Toimintaprosesseihin sulauttaminen vaatii hyvää yhteistyötä usealta taholta. Prosesseja suunniteltaessa turvallisuutta lisäävät toimenpiteet on otettava huomioon, jotta täytetään turvallisuusvaatimukset. (Vahti 9/2009.)

Tietoturvallisuuden hallintajärjestelmä koostuu muun muassa seuraavista dokumenteista ja toimintamalleista:

- tietoturvakäytännöt ja -periaatteet,
- tietoturvallisuuden perus- ja lisäohjeistus,
- tietoturvapolitiikka ja -strategia,
- tietoturvallisuuden kehittämissuunnitelma,
- tietoturva-arkkitehtuurit,
- pelastus-, jatkuvuus- ja valmiussuunnitelmat,
- tietoturvaraportointi johdolle,
- auditointisuunnitelma ja

- toimintaan liittyvät tietoturvaprosessit.

Hallintajärjestelmä toteuttaa yrityksen strategiaa ja kattaa tietoturvallisuuden yksityiskohtaisen suunnittelun, organisoinnin, vastuut, politiikat, prosessit, resurssit ja menettelytavat. Kehittämällä järjestelmää jatkuvasti, parantaa se yrityksen valmiuksia tietoturva-asioiden systemaattiseen hallintaan. (Vahti 9/2009.)

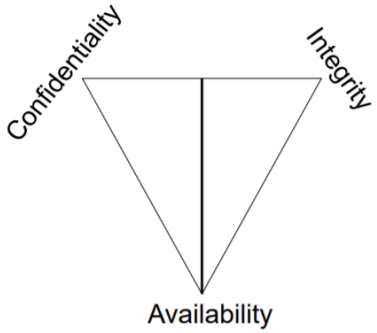


Kuva 8. Malli tietoturvallisuuden hallintajärjestelmästä. (Vahti 9/2009).

Tietoturvallisuuden hallintajärjestelmän tärkeimmät (Kuva 8) osat ovat säännöllinen riskienhallinta, johon liittyy nykyisen toiminnan lisäksi suunnitellut muutokset sekä ajantasainen tietoturvapolitiikka, johon kuuluu siihen liittyvät asiakirjat. Tietoturvastrategia ja suunnitelmat laaditaan niiden pohjalta ja tietoturvaratkaisut toteutetaan tietoturvavaatimusten mukaan. Hallintajärjestelmään sisältyy myös tarkoituksenmukaisuuden säännöllinen arviointi ja mittaaminen sekä tietoturvatoiminnan tehokkuus. (Vahti 9/2009.)

2.3.2 Tietoturvan CIA-malli

Tietoturvan analysointimalleista CIA on yleisimmin käytetty ja yksinkertaisin. CIA tulee sanoista confidentiality (luottamuksellisuus), integrity (eheys) ja availability (saatavuus). (Jarva 2009, 3.)



Kuva 9. CIA-malli.

Yllä olevassa kuvassa (Kuva 9) on CIA-malli, sitä voi soveltaa ajattelemalla kolmiota, johon tieto sijoitetaan. Confidentiality (luottamuksellisuus) osiossa tietoa pääsevät näkemään siihen oikeutetut henkilöt. Integrity (eheys) osiossa tietoa voivat muokata vain siihen oikeutetut henkilöt. Availability (saatavuus) osiossa tietoon päästään käsiksi silloin kun siihen on tarvetta. Tämä kolminaisuus muodostaa tietoturvassa laajalti käytetyn CIA-mallin. Esimerkki CIA-mallista on pankkitili, jonka tärkein ominaisuus on eheys, eli tilille ei tule hyväksymättömiä tapahtumia. (Suvilehto 2011, 7-9.)

2.4 Organisaation sisäinen valvonta

Sisäisen valvonnan käsitteellä tarkoitetaan yleisesti organisaation eri tasoille rakennettuja toimenpiteitä ja -tapoja. Ne muodostuvat useista osa-alueista, esimerkiksi työtehtävien jaosta, hyväksymisvaltuuksista ja laskenta- ja ohjausjärjestelmien sisältämistä kontrolleista. Näillä toimenpiteillä on tarkoitus varmistaa, että organisaatiossa toimitaan toimintaohjeiden ja tavoitteiden mukaisesti. Sisäisen valvonnan avulla pyritään paljastamaan ja ehkäisemään virheitä, väärinkäytöksiä ja erehdyksiä. Sisäisen valvonnan perimmäinen tavoite on saada riittävä varmuus siitä, että yritystä koskevien säädösten ja lakien mukaisesti on raportoitu taloudellista informaatiota ja se on luotettavaa. Kaikissa organisaatioissa on erilainen sisäinen valvonta, johon vaikuttaa yrityksen toimiala, koko, rakenne, omistussuhteet ja toiminnot. Sisäisen valvonnan tarpeeseen vaikuttaa myös organisaation muutostila, kuten omistuspohjan vaihto tai kasvu. Tärkeintä sisäisessä valvonnassa on se, että se toimii, eikä se millä tavalla se on järjestetty. (Ahokas 2012, 10-11.)

Raudasojan ym. mukaan sisäinen valvonta on yrityksen itse järjestämää ja toteuttamaa toiminnan hallintaa ja ohjausta, joiden avulla yritys pyrkii poistamaan tehottomuutta ja epätoivottavien tapahtumien mahdollisuutta, edistää tavoitteiden saavuttamista ja paljastamaan väärinkäytöksiä. (Raudasoja & Johansson 2009, 199.) Sisäisen valvonnan määritelmän tarjoaa yleisesti tunnettu COSO-malli. COSO on lyhenne sanoista The Committee of Sponsoring Organizations of the Treadway Commission. COSO on sisäisen valvonnan malli, joka rakentuu viidestä osa-alueesta, jotka ovat yhteyksissä toisiinsa: riskien arviointi, valvontaympäristö, valvontatoimenpiteet, kommunikaatio ja informaatio sekä seuranta. (Ahokas. 2012, 145). Organisaation valvonta on sen johdon, hallituksen sekä muun henkilökunnan toteuttama prosessi, jonka tarkoitus on tuottaa kohtuullinen varmuus siitä, että tavoitteet toteutuvat seuraavanlaisissa asioissa:

- lakien ja säädösten noudattaminen,
- toimintojen tarkoituksenmukaisuus ja tehokkuus, sekä
- taloudellisen raportoinnin luotettavuus.

Sisäiseen valvontaan COSO:n mukaan kuuluu riskien arviointi, organisaation valvontaympäristö, informaatio ja kommunikaatio, valvontatoiminnot sekä seuranta. (Ahokas 2012, 10-11.)

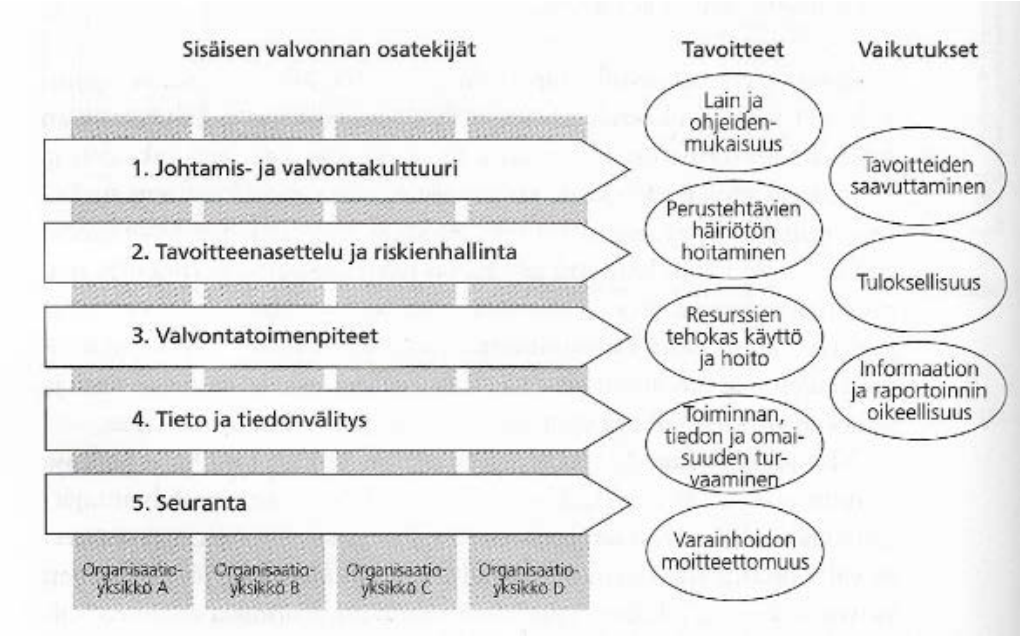
Ihmiset saavat aikaan prosessin, joka on sisäistä valvontaa. Parhaiten sisäinen valvonta saadaan toimimaan silloin, kun se on rakennettu liiketoimintaprosessin osaksi ja siihen kuuluvat komponentit ovat läsnä organisaation kaikilla tasoilla. Mikäli olemassa olevien prosessien päälle rakennetaan uusi valvontajärjestelmä, jää se usein irtonaiseksi. Tällöin siihen kuuluvat toiminnot eivät sulaudu osaksi yksilöiden vastuita ja tehtäviä. (Ahokas 2012, 14.)

Organisaatioiden sisäinen valvonta on viimeisen viidentoista vuoden aikana saanut huomattavasti huomiota niin yrityksiltä itseltään kuin niiden sidosryhmiltä. Sisäisen valvonnan kehittämisen ja arvioimisen tarve voi tulla suositusten tai lainsäädännön pakottamana tilanteissa, esimerkiksi mikäli yritys on listautumassa pörssiin tai olemassa olevassa valvontajärjestelmässä havaitaan väärinkäytöksiä tai merkittäviä puutteita. Sisäisen valvonnan järjestämiseen on kiinnitetty yrityksissä merkittävästi enemmän huomiota viime vuosina. Sen voi havaita lisääntyneenä kouluttautumisena ja valveutuneisuutena aihepiirissä sekä sisäisen valvonnan ja tarkastuksen yksiköiden määränä organisaatioissa. Joissakin yrityksissä sisäisen valvonnan kehittämishankkeita on käytetty avuksi liiketoiminnan kehittämisessä. Onnistuneesti järjestetty sisäinen valvonta tukee liiketoimintaa ja tuottaa lisäarvoa organisaation prosesseille. (Ahokas 2012, 63.)

Yrityksen sisäistä valvontaa kohtaan on kiinnostus lisääntynyt heikon sisäisen valvonnan aiheuttamien konkurssien ja yritysskandaalien myötä. Ulkoisilta tahoilta on tullut vaatimuksia paremmalle hallinto- ja johtamistavalle. Yritysten suhtautuminen on muuttunut merkittävästi sisäistä valvontaa kohtaan ja se saa paljon enemmän huomiota yrityksen ylimmältä johdolta nykyisin. Tietoisuus sisäisestä valvonnasta saa yrityksiä kehittämään sitä ja panostamaan siihen taloudellisesti. Sisäinen valvonta katsotaan osaksi yrityksen kokonaisvaltaista ohjausjärjestelmää, ei enää pelkästään kirjanpitoon liittyvänä toimintana. Tämän kehityssuunnan oletetaan jatkuvan. Tämä näkyy tällä hetkellä siinä, että organisaatioissa sisäisestä valvonnasta puhutaan organisatorisena yksikkönä tai erillisenä käsitteenä. Sisäisen valvonnan kehittäminen ja korostaminen tuovat organisaatiolle merkittäviä hyötyjä. (Ahokas 2012, 143.)

Yrityksen liiketoimintaa voidaan ymmärtää selkeämmin arvioimalla kontrolleja ja riskejä sekä dokumentoimalla taloudellisten ja operationaalisten prosessien kuvauksia. Hyväksyttämisrajojen tarkemmalla määrittämisellä, tarkentuneilla työnkuvauksilla ja tehostuneella käyttöoikeuksien hallinnalla selkeytetään eri henkilöiden ja funktioiden välillä olevia vastuusuhteita. Formalisoimalla olemassa olevia prosesseja ja kontrolleja dokumentoimalla saadaan varmuutta siitä, että yrityksessä tehdään oikeita asioita oikeiden henkilöiden toimesta. Tällöin virheiden ja väärinkäytöksien riskien mahdollisuus pienenee. Sisäistä valvontaa arvioitaessa saadaan merkittävää tietoa organisaation valvontajärjestelmän tilasta. Tiedosta on hyötyä, kun kehitetään toimintatapoja ja prosesseja. (Ahokas 2012, 144.)

Organisaation ylin johto vastaa sisäisen valvonnan järjestämisestä. Raportoinnin ohella, sisäisen valvonnan avulla johto saa arvokasta tietoa yrityksen aikaansaannoksista ja tilasta. Seuraava kuva (Kuva 10) kuvaa sisäisen valvonnan kokonaisuutta. (Raudasoja, ym. 2009, 141, 143-144.)



Kuva 10. Sisäisen valvonnan osatekijät, tavoitteet ja vaikutukset. (Raudasoja, ym. 2009, 144).

Johtamis- ja valvontakulttuuri muodostuu organisaation eettisistä arvoista ja periaatteista, yksilöistä ja heidän henkilökohtaisista ominaisuuksistaan, kuten rehellisyydestä, pätevyydestä ja organisaation toimintaperiaatteista. Tämä muodostaa perustan, johon kuvassa mainittujen muiden osatekijöiden avulla voidaan rakentaa systemaattinen valvontarakenne. *Tavoitteenasettelu* tulee tehdä selkeästi yksilö-, tiimi- ja yksikkötasolla ja samalla tulee sopia seurantakäytännöistä. Erilaiset ulkoiset auditoinnit ja itsearvioinnit nähdään yleensä osana laadunhallintaa, mutta ne ovat osa myös valvontajärjestelmää. *Valvontatoimenpiteisiin* kuuluu esimiehen suorittama jatkuva seuranta ja erikseen rakennetut laskentatoimen ja muiden kontrolleista. *Tiedonvälityksen* tavoite organisaatiossa on varmistaa tarkoituksenmukaisen, oikea-aikaisen ja luotettavan informaation tuottaminen päätöksenteon tueksi. *Seurannassa* keskeistä on asettaa raportointivelvoitteet ja raporttien tuloksien vertailu asetettuihin tavoitteisiin. (Raudasoja, ym. 2009, 145-146.)

Seuraavassa taulukossa (Taulukko 2) on esitetty käytännön esimerkkejä organisaation sisäisessä valvonnassa yksittäisen esimiehen tehtävistä. (Raudasoja, ym. 2009, 146).

	Tavoite	Esimiehen tehtäviä
1.	Tavoitteiden saavuttamisen varmistaminen	Yksilöiden ja ryhmien tavoitteiden saavuttamisen seuranta ja poikkeamiin puuttuminen.
2.	Perustehtävien häiriötön hoitaminen	Vahinkotapahtumien, keskeytysten ja ongelmien syiden analysointi ja estäminen jatkossa.
3.	Lainsäädännön, sääntöjen, ohjeiden, päätösten ja sopimusten mukainen menettely	Ohjeiden ja toimivaltuuksien noudattamisen seuranta, yksittäisten viranhaltijapäätösten tarkastaminen pistokokein (esim. hankintapäätökset, avustuspäätökset).
4.	Hankintojen asianmukainen hoito	Hankinta- ja sopimusvaltuuksien käytön valvonta, hankintojen taloudellisuuden ja tarkoituksenmukaisuuden valvonta.
5.	Varainhoidon moitteettomuus	Tehtävien eriyttäminen, hyväksymiskäytäntöjen noudattamisen valvonta, väärinkäytösten ehkäisy.
6.	Tietojen ja omaisuuden turvaaminen	Tietojärjestelmien suojaus- ja varmistuskäytäntöjen tarkistus, rekisterien ylläpidon valvonta, käyttäjätietojen rekisteröinti, omaisuuden merkitseminen.
7.	Toimintaa ja taloutta koskevan tiedon oikea-aikaisuus, oikeellisuus ja riittävyys	Kirjanpito-ohjeiden sekä laskutus- ja muiden kirjanpidon aikataulujen noudattamisen valvonta.

Taulukko 2. Esimiehen tehtävistä esimerkkejä. (Raudasoja, ym 2009, 146).

Sisäisen valvonnan katsotaan olevan johdon, hallituksen ja muiden osapuolten niitä toimenpiteitä, joilla hallitaan riskejä ja täten lisätään tavoitteiden ja päämäärien saavuttamisen todennäköisyyttä. Johdon tehtävä on suunnitella, ohjata ja organisoida toimintaa niin, että tavoitteiden ja päämäärien saavuttamisesta saataisiin kohtuullinen varmuus. (Holopainen, ym. 2010, 47.)

Sisäinen valvonta koostuu viidestä osatekijästä, jotka liittyvät toisiinsa. Osatekijät on johdettu tavasta, jolla perus liiketoimintaa johdetaan ja ne ovat johtamisprosessin osa. Osatekijöitä ovat:

1. johtamistapa ja organisaatiokulttuuri (control environment)
2. riskien arviointi (risk assesment)
3. päivittäisvalvonta ja tehtävien eriyttäminen (control activities)
4. raportointi ja tiedonvälitys (information and communication)
5. seuranta ja tarkastus (monitoring).

Sisäinen valvonta ei ole pelkästään prosessien sarja, vaan monensuuntainen kertautuva prosessi, jossa mitkä tahansa osatekijät voivat vaikuttaa toisiinsa (Kuva 11). Millään organisaatiolla ei voi olla samanlaista sisällön valvontajärjestelmää keskenään. (Holopainen, ym. 2010, 55.)

Kuva 11. Järjestelmien hierarkia (Holopainen, ym. 2010, 85).

2.4.1 Käyttöoikeuksien hallinta

Tietojärjestelmien hallinnassa on otettava aina huomioon se, kenellä on järjestelmiin oikeus. Henkilöllä tulisi olla oikeudet sellaisiin järjestelmiin, joita edellytetään hänen työtehtävissään. Liian laajat käyttöoikeudet voivat johtaa epähuomiossa tehtyihin virheisiin tai tahallisiin väärinkäytöksiin. Huomiota tulee kiinnittää myös siihen, salliiko käyttöoikeudet järjestelmien tietojen katselemisen, muokkaamisen tai jopa ylläpidon. Käyttöoikeudet, jotka sallivat ylläpidon, tulisi olla vain hyvin rajatulla määrällä henkilöstöä. Varamiestilanteita varten tulisi myös määritellä käyttöoikeuksien hallinta. Valvonnan avulla tulisi ehkäistä tilanteet, joissa useat eri henkilöt käyttävät samoja tunnuksia tai käyttäjätunnuksia lainataan. Yritysten tulisi pitää järjestelmien käyttäjistä ja heidän käyttöoikeuksien laajuudesta dokumentaatiota, jota tulisi tarkistaa säännöllisesti. Työtehtävien vaihtuessa tai ihmisten lähtiessä yrityksestä on pidettävä huoli, että heille ei jää oikeuksia järjestelmiin, joita he eivät enää tarvitse. (Ahokas 2012, 122.)

Seuraavassa taulukossa (Taulukko 3) on esimerkki käyttöoikeuksien hallintaan liittyvistä kontrolleista. Pystysarakkeissa on eritelty kohdat: kontrolli, tavoite, kontrollitoiminto, evidenssi. Kontrolleina on Käyttäjien hallinta, Käyttäjien tunnistaminen ja Käyttäjien todennus. Taulukossa käydään läpi näiden kontrollien tavoitteet, kontrollitoiminnot ja evidenssit.

Kontrolli	Tavoite	Kontrollitoiminto	Evidenssi
Käyttäjätilien hallinta	Käyttäjätilien hallinta-prosessi on olemassa, ja sitä noudatetaan.	Käyttäjätilien anomiselle, perustamiselle, hyllyttämiselle ja sulkemiselle on olemassa prosessi. Prosessi on dokumentoitu ja viestitty asianomaisille työntekijöille. Prosessi tarkastetaan vuosittain.	Prosessin dokumentaatiossa kuvataan roolit, vastuut ja menettelytavat. Vuotuisesta prosessin tarkastamisesta tulee olla muistiinpanot ja prosessin muutoksista historiatiedot. Käyttäjätilien ylläpitäjiksi valtuutetuista henkilöistä on oltava listat.
Käyttäjien tunnistaminen	Käyttäjät tunnistetaan yksilöllisellä tunnisteella.	Jokaiselle käyttäjälle annetaan yksilöllinen tunnus ja salasana henkilökohtaiseen käyttöön.	Käyttäjätietokannassa on lista kaikista käyttäjätileistä ja tilin omistajista.
Käyttäjien todennus	Käyttäjät todennetaan ennen pääsyn sallimista järjestelmään.	Anonyymi järjestelmien käyttö evätään. Järjestelmän asetukset vaativat, että käyttäjä tulee todentaa.	Järjestelmä on konfiguroitu niin, että käyttäjä todennetaan ennen pääsyä järjestelmään.

Taulukko 3. Esimerkkejä käyttöoikeuksien hallintaan liittyvistä kontrolleista. (Ahokas 2012, 123).

Sisäisen valvonnan lainsäädäntö

Sisäiseen valvontaan ei ole Suomessa erillistä lakia, mutta pörssiyhtiöiltä saa tiettyjä määräyksiä ja ohjeistuksia. Yhdysvalloissa lainsäädäntö sisäisessä valvonnassa on kehittynyt pidemmälle ja merkittävin laki on Sarbanes-Oxley. Sisäisen valvonnan järjestämisestä ei ole Suomen laissa suoraan määräyksiä. Suomen osakeyhtiölaissa säädetään, että yrityksen hallituksen tulee huolehtia, että yrityksen varainhoidon valvonta ja kirjanpito on lainvoimainen ja varainhoidon tulee olla luotettavasti järjestetty. Yrityksen johto päättää, miten organisaation sisäinen valvonta käytännössä järjestetään. (Ahokas 2012, 126.)

Suomessa sisäisen valvonnan menetelmistä on määräyksiä ja ohjeita, jotka koskevat tiettyjä aloja. Listayhtiöiden hallinnointikoodissa ohjeistetaan sisäisen valvonnan, sisäisen tarkistamisen ja riskienhallinnan järjestämisestä. Koodin mukaan riskienhallinnan ja sisäisen tarkastuksen tavoitteena on varmistaa, että yhtiön informaatio on luotettavaa, toiminta on tuloksellista ja tehokasta sekä toimintaperiaatteita ja säännöksiä noudatetaan. Tavoitteisiin kuuluu myös liiketoimintaan kuuluvien riskien tunnistaminen, arvioiminen ja seuraaminen. Suositus sisäisestä valvonnasta on, että organisaatio määrittelee toimintaperiaatteet sisäiselle valvonnalle. Tuloksellinen liiketoiminta edellyttää, että toimintaa valvotaan jatkuvasti. Hallituksen vastuulla on huolehtia, että sisäistä valvontaa koskevat toimintaperiaatteet on määritelty ja valvonnan toimivuutta seurataan. (Ahokas 2012, 126-129.)

2.5 Riskienhallinta

Riskienhallinta on yksi perustehtävistä organisaatioiden johtamisessa. Miksi yrityksissä on johtajia? Miksi kapteenia tarvitaan laivassa? Tietysti siksi, että he ohjaisivat tilanteita niin, että turhilta riskeiltä vältyttäisiin, saavutettaisiin tavoitteet ja mahdollisuudet käytetään hyväksi. Organisaatioiden hallitus huolehtii siitä, että heillä on riskienhallintajärjestelmä. Riskienhallinnassa on aina tarve päästä sellaiseen tilanteeseen, että halutun tavoitteen saavuttamisriski on hallinnassa tai tietyn riskin sisältämä mahdollisuus käytetään hyväksi. (Holopainen, ym. 2010, 39, 41.) Riskienhallinta on seurauksiltaan merkittävien negatiivisten tapahtumien eli riskien systemaattista määrittelyä ja varautumista niihin. Merkittäviin riskeihin kuuluu ne, jotka vaikuttaisivat johdon tekemiin päätöksiin. Riskienhallinta on prosessi, joka liittyy toimintoihin, joiden riskejä käsitellään. (Raudasoja & Johansson 2009, 198.)

Sisäiset ja ulkoiset riskit kohdistuvat jokaisen organisaation toimintaan, joita ei voida koskaan täysin eliminoida. Riskien todennäköisyyttä ja vaikutusta voidaan vähentää sisäisen valvontajärjestelmän avulla. Arvioidessa organisaation riskejä COSO-mallin mukaan, tarkoittaa se yrityksen sisäisten ja ulkoisten riskien tunnistamista ja analysointia, jotka ovat uhkana tavoitteiden saavuttamisessa. Aluksi organisaation toiminnalle tulee asettaa tavoitteet, jonka jälkeen on mahdollista tunnistaa riskit, jotka liittyvät tavoitteiden saavuttamiseen. Tämän jälkeen riskejä voidaan arvioida. Hyväksyttävä riskitaso tulee määritellä johdon toimesta ja tavoitetason pitääkseen toimia sen mukaisesti. Tehokkaan sisäisen valvonnan keskeisenä osatekijänä on riskien tunnistaminen ja analysointi. Yleensä riskit tunnistetaan suunnitteluprosessien yhteydessä. Riskien tunnistaminen

on jatkuva prosessi, sillä lainsäädännölliset, taloudelliset, teknologiset ja toiminnalliset olosuhteet muuttuvat koko ajan, jonka vuoksi muutoksiin liittyy uusia riskejä. (Ahokas 2012, 31.)

Riskit voidaan jakaa toimintatason ja yritystason riskeihin. Yritystason ulkoisia riskejä aiheuttavia tekijöitä ovat esimerkiksi vaihtuvat asiakastarpeet, uusiutuva lainsäädäntö, teknologinen kehitys, kilpailu ja taloudelliset muutokset. Riskien tunnistamisessa on tärkeintä selvittää riskiä aiheuttavat tekijät ja riskiä lisäävät tekijät. Kun riskeistä suurimmat on tunnistettu, ne linkitetään toimintatasolle. Toimintatason riskejä sen sijaan on riskit, jotka johtuvat henkilöstön epäpätevyydestä, sisäisistä tekijöistä kuten tiedonkulun katkeamisesta, epävarmasta tai tehottomasta hallituksesta, toiminnan muutoksesta tai tarkastusvaliokunnasta. Toimintatason riskit tulisi tunnistaa kattavasti. (Ahokas 2012, 31-32.)

Kun riskit on tunnistettu, voidaan niitä ryhtyä analysoimaan. Metodien vaihtelevuus voi vaihdella suuresti, sillä useita riskejä on haasteellista ilmaista määrällisesti. Riskien analysointiprosessissa etsitään vastaus seuraaviin kysymyksiin:

- Miten merkittävä riski on?
- Mitä toimenpiteitä täytyy tehdä riskien hallitsemiseksi?
- Millä todennäköisyydellä riski toteutuu?

Todennäköisimmät ja merkittävät riskit tulee analysoida perusteellisemmin. Riskejä voidaan ilmaista kokoluokassa, onko kyse pienestä, kohtuullisesta vai suuresta riskistä. (Ahokas 2012, 32.)

Riskeille on useita hallitsemiskeinoja. Niitä voidaan hallita niiden luonteen mukaisesti. Yritys voi tehdä esimerkiksi toimintasuunnitelmia jokaisen riskin realisoitumisen varalle tai hinnoittelee hinnan korkeaksi riskisen tuotteen kohdalla. Riskeihin vastaamisessa voidaan päätyä seuraavanlaisiin vaihtoehtoihin:

- Riski jätetään ottamatta.
- Riskin ollessa hyvin alhainen, se voidaan hyväksyä ilman erillisiä toimenpiteitä.
- Riskin todennäköisyys ja/tai sen aiheuttaman vahingon määrä yritetään alentaa hyväksyttävälle tasolle.
- Hyväksyttävälle tasolle riski saadaan siirtämällä se muiden kannettavaksi suojaustoimenpiteiden tai vakuutusten avulla.

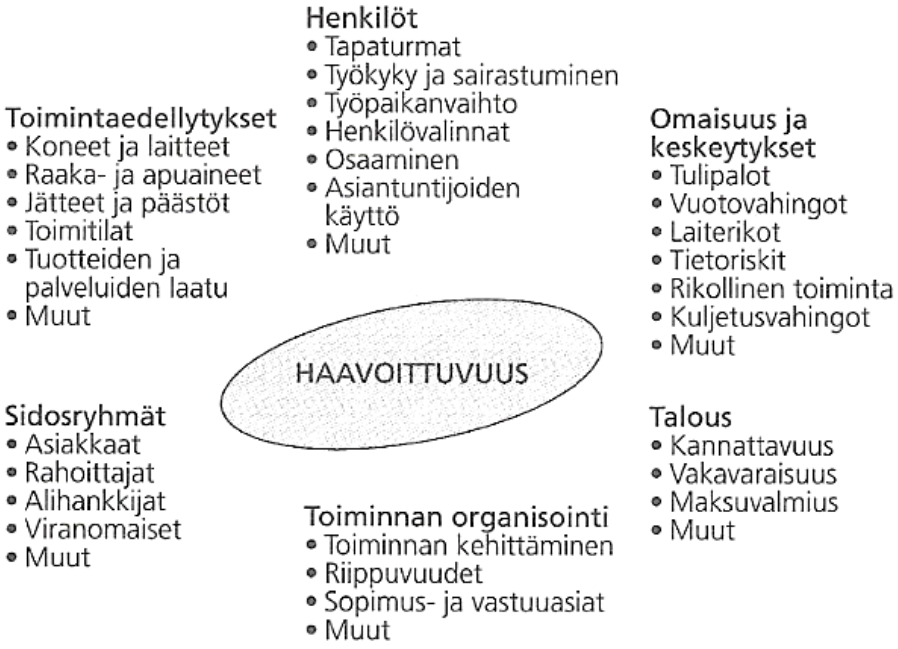
- Riski otetaan, mikäli katsotaan, että se ei vaaranna liiketoimintaa liikaa.

Organisaation riskinottohalukkuudesta ja sietokyvystä riippuu, mikä vaihtoehto valitaan. Riskinhallintakeinoja valitessa päätetään uhkaavien riskien ja niiden hallinnan tasapainosta huomioiden muun muassa tehokkuus, kustannukset ja hallintavaihtoehtojen hyöty. (Ahokas 2012, 32-33.)

Sisäinen valvonta linkittyy oleellisesti riskienhallintaan, jonka tavoitteena on tukea liiketoiminnan tavoitteiden saavuttamista ja yhtiön strategian toteuttamista sekä taata liiketoimintaan menestyksellinen jatkuvuus. Riskienhallinnan ja sisäisen valvonnan suhdetta voidaan luonnehtia niin, että sisäisen valvonnan avulla toteutetaan suurin osa käytännön riskienhallintatoimista. Sen avulla varmistetaan toiminnan tehokkuutta, tuloksellisuutta ja jatkuvuutta, omaisuuden ja resurssien turvaamista, tiedon ja raportoinnin luotettavuutta sekä ohjeiden ja lainsäädännön noudattamista. Sisäinen valvonta ja riskienhallinta ovat siis osia samasta prosessista. Riskien arviointi ja kartoitus ylläpitää sisäisen valvontajärjestelmän ajanmukaisuutta. Riskienhallinta arvioi toimintaympäristössä ja toiminnassa tapahtuvien muutosten vaikutusta yrityksen toimintaan ja sen riskeihin sekä auttaa sopeuttamaan muuttuneita olosuhteita sisäisen valvonnan menettelyihin. Ensisijaisessa vastuussa riskienhallinnan johtamisesta ja järjestämisestä on organisaation ylin johto. (Ahokas 2012, 59.)

Raudasojan & Johanssonin (2009, 147.) määritelmä riskienhallinnasta on seuraavanlainen: sillä tarkoitetaan systemaattista menettelyä, jonka avulla voidaan tunnistaa ja arvioida riskejä, jotka uhkaavat toimintaa, sekä määritellään keinot ja toimintatavat riskien hallitsemiseksi ja raportoimiseksi. Yleensä vain menetyksiä on pidetty riskeinä ja riskienhallintaa on lähestytty omaisuusriskien näkökulmasta pelkästään. Riskienhallinta on kuitenkin paljon laajempaa. Riski on epävarma ja ei-toivottu tapahtuma. Riskien toteutuessa aiheuttavat ne muun muassa merkittäviä taloudellisia vahinkoja ja häiritsevät tuntuvasti liiketoimintaa.

Ihmiset aiheuttavat useimmat riskit, joten niihin kannattaa varautua ja suojautua. Mikäli riskeihin ei ole osattu varautua, pääsevät ne yllättämään. Liikeriskien hyvällä hallinnalla on mahdollisuus parantaa onnistumista ja selviytyminen turvataan mahdollisen riskin toteutuessa. Menestyvään yritykseen usein yhdistetään terve riskinottokyky. On olennaista sisäisen valvonnan kannalta, että toimintaan liittyvät riskit on ymmärretty ja arvioitu. Riskejä voidaan luokitella monin eri tavoin, ne voivat olla operatiivisia tai strategisia, ulkoisia tai sisäisiä, taloudellisia tai toiminnallisia, omaisuus- tai henkilöriskejä tai tietoriskejä. Alla olevassa kuvassa (Kuva 12) on eräänlainen luokitus erilaisista riskeistä. (Raudasoja, ym. 2009, 147-148.)



Kuva 12. Riskilajeja. (Raudasoja, ym. 2009, 148).

Riskienhallinta on tilanteiden suunnittelua, arviointia ja käytännön tekoja, johon koko henkilöstö osallistuu omassa roolissaan. Parhaimmillaan riskienhallinta on suunnitelmallista, ennakoivaa, järjestelmällistä ja tietoista. Organisaatioissa esimiesten tulisi tunnistaa oman vastuualueensa merkittävimmät riskit ja soveltaa niihin riskienhallintakeinoja. Sisäisen valvonnan ja riskienhallinnan menettelyjen täytyy olla järkevät ja asianmukaiset suhteessa toiminnan sisältöön ja laajuuteen sekä niihin liittyviin riskeihin. Hyvin toteutettu sisäinen valvonta ei ole tae yrityksen menestykselle, pysyvyydelle tai toiminnan virheettömyydelle. (Raudasoja, ym. 2009, 150, 152.)

2.6 Muutoksen johtaminen

Aktiivinen viestintä sekä koko yrityksen mukaan ottaminen hankkeeseen on muutoksen johtamisessa hyvin tärkeää varmistaa. (Collin, ym. 2016, 292). Suurimmalle osalle organisaatioita muutosmatka alkaa vasta, kun käynnistetään muutosohjelma. On tärkeää pitää mielessä henkilöstön sitouttaminen muutokseen koko transformaation ajan. Matkan varrella ilmenee ongelmia ja haasteita, jotka tulee hoitaa henkilöstön kanssa tavalla tai toisella. Seuraava ohjelista auttaa välttämään pahimmat karikot: Johda ja viestitä muutoksista asiakaslähtöisesti; käyttäjiä kuunnellaan

ja virheistä opitaan; tulee muistaa, että mennään prosessit edellä ja tietotyökalut tulevat perässä; datan jakamisen pelisäännöistä tulee sopia; datan laatuun ja tietoturvaan tulee panostaa; luo, jaa ja etsi parhaat käytänteet. (Collin, ym. 2016, 303.) Muutosta kannattaa johtaa asiakaslähtöisesti ja organisaatio tulee pitää mukana viestimällä avoimesti muutoksesta. Organisaation tulee ymmärtää ja sisäistää niin sanottu 'big picture', eli iso kuva.

Ylimmän johdon lähestymistavalla ja persoonallisuudella on muutoksissa suuri merkitys. Johtajan on oltava mukana muutoksissa. Naiset tuntuvat Hirvikorven mukaan menevän muutosprosessiin mukaan kyynärpäitään myöten. Kun koko organisaatio on laajasti mukana muutoksen suunnittelussa ja läpiviennissä, lisää se sitoutumista. Muutoksen suunnittelu alkaa jo varaisessa vaiheessa, jota seuraavat avoin viestintä, prosessimainen toteutus, aktiivinen osallistuminen ja sitoutuminen muutoshankkeisiin. Naisjohtajat pitävät tärkeänä henkilöstön osallistamista. (Hirvikorpi 2005, 159-160.)

Muutoksessa on tarpeen avoin ja selkeä viestintä ennakkoon, asioiden pelkistäminen ja toistaminen. Yksilön kannalta muutos tarkoittaa yleensä jotakin negatiivista, YT-neuvotteluja, aseman menetystä, työpaikan menetystä. Muutos voi olla myös positiivista, saa uusia työtehtäviä ja kollegoita. Haastatellut johtajat totesivat, että joskus muutokseen tarvitaan kriisi, joskus unelma. Muutosjohtaminen lähtee usein siitä, että yhtiön luvut kertovat missä mennään. On analysoitava, missä on parannettavaa ja mistä johtuu heikko kannattavuus, strategia on tarkistettava ja tehtävä toimenpidesuunnitelmia. Yhdessä muutoksesta päättämällä ei synny muutoksia. Kriisejä syntyy automaattisesti tai niitä on jo yrityksessä valmiina, pelkästään omistajien vaatima parempi tulos voi olla kriisin aihe. (Hirvikorpi 2005, 161-162.)

2.6.1 Digitalisaatio muutoksen johtamisessa

Yleisesti ottaen toiminnan digitalisoiminen tarkoittaa palveluiden kehittämistä käyttäjän ja toiminnan tarpeiden näkökulmasta, hyödyntäen alati kehittyvää teknologiaa. Toimintoja ja palveluita digitalisoimalla painopiste siirretään teknologiasta toiminnan kehittämiseen. Käyttäjää ei saa eristää täysin digitaaliseen maailmaan, vaan hänelle tulee tarjota kriittisimmillä osa-alueilla vaihtoehtoinen tapa käyttää palvelua, myös häiriötilanteissa. (Järvinen & Rousku 2017, luku 1.)

Vuosituhannen vaihteessa digitaalisen ja fyysisen maailman välinen ero oli selvä. Nyt elämme maailmassa, jossa fyysinen ja virtuaalinen maailma lyövät kättä ja kulkevat yhä lähempänä toisiaan. Näiden maailmojen väliset raja-aidat ovat katoamassa. Digitalisaatio vaikuttaa kaikkiin yrityksiin, paikallisiin ja kansainvälisiin, pieniin ja suuriin. Yritysjohdolla on kaksi vaihtoehtoa suhtautua muutokseen. Ensimmäinen on tarttua digitalisaation tarjoamiin mahdollisuuksiin ja rakentaa siitä kilpailuetu. Toinen on olla tekemättä mitään, jolloin digitalisaatiosta tulee kilpailukyvyn este. Menestyville yrityksille on olemassa täten vai yksi vaihtoehto. (Ilmarinen & Koskela 2015, alkusanat.)

Digitalisaatiossa ollaan astumassa seuraavaan vaiheeseen. Edeltävän vuosikymmenen ajan puhtaasti online-toimijat kuten Google, Facebook ja Twitter ovat olleet digitalisaation ikoneja. Seuraavan vuosikymmenen aikana tulemme mitä luultavimmin näkemään kuinka perinteiset toimialat ottavat digitaalisuuden omakseen. Digitalisaatio muuttaa yrityskulttuuria myös. Digitalisaatio pakottaa yritykset hajauttamaan päätöksenteon ja valtuuttaa tiimit ottamaan omistajuutta. Menestyvä organisaatio reagoi nopeasti, ei pelkää epäonnistumisia ja ottaa opiksi virheistään. Digitaalinen transformaatio ei tapahdu itsestään, vaan sitä pitää johtaa aktiivisesti. Johtaminen on muutoksen johtamista organisaation kaikilla tasoilla. Organisaation elinehto on nopeuden ja ketteryyden rakentaminen. (Ilmarinen, ym. 2015, alkusanat.)

Digitalisaatio on aikakautemme suurin muutosvoima. Se muuttaa radikaalisti ihmisten tapaa hankkia informaatiota, kuluttaa palveluja, ostaa tuotteita, hoitaa asioitaan, jakaa kokemuksiaan ja olla vuorovaikutuksessa muiden kanssa. Se murtaa perinteisiä toimialarajoja, sekoittaa yrityksen kilpailuympäristöä, pakottaa yrityksiä uudistamaan toimintatapojaan ja osaamistaan. Se synnyttää uusia voittajia ja häviäjiä. Digitalisaatio koskettaa jokaista yritystä toimialasta riippumatta. Digitalisaatiosta on tullut kansantalouden kilpailukyvyn ja julkisen talouden tehostamisen taikasana. Uhat saavat usein yksipuolisesti päähuomion, kun media uutisoi sen vähentävän työpaikkoja, kadottavan ammatteja tai aiheuttavan vähittäiskaupoille ongelmia. Digitalisaatio on kuitenkin valtava mahdollisuus kaikille suomalaisyrityksille. (Ilmarinen, ym. 2015, johdanto.)

Digitalisaatio näyttäytyy usein verkkokauppoina, verkkosivustoina, asiointipalveluina ja mobiilisovelluksina. Kyse on kuitenkin yritysten toiminnan paljon syvemmästä ja laajemmasta murroksesta. Digitalisaatio synnyttää uudenlaisia liiketoimintamalleja, palveluja, tuotteita ja prosesseja, jotka tuovat hyötyä sekä yritykselle että sen asiakkaille. Samaan aikaan se edellyttää yrityksiltä uudenlaista johtamista, tehtävien organisointia, osaamista, toimintamalleja ja yrityskulttuuria. Digitalisaation ytimessä on muutos ja uudistuminen. Nykyinen toiminta on syytä kyseenalaistaa.

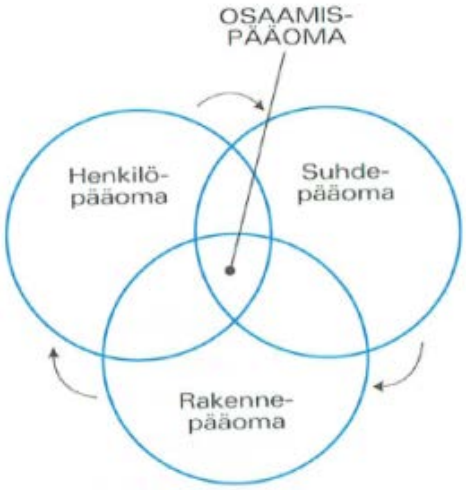
Monista aikaisemman menestyksen peruskivistä tulee luopua, uusiin mahdollisuuksiin tulee suhtautua uteliaasti. Vaikka yritys olisi ottanut merkittäviä askelia digitalisaatiossa, olisi hyvin vaarallista tyytyä nykytasoon, sillä vauhti on kiihtyvä. Kyky uudistua ja ajoittaa isot uudistukset oikein ovat menestyksen kannalta ratkaisevia. (Ilmarinen, ym. 2015, johdanto.)

2.6.2 Osaamisen johtaminen

Osaamisen ja osaamispääoman johtamisen rinnalla on puhuttu paljon tietämyksen ja tiedon johtamisesta. Vaikka lähtökohta termeille osaaminen ja tieto on erilainen, ovat tiedon johtaminen ja osaamisen johtaminen käytännössä aika lähellä toisiaan. Tieto-oppi on filosofian ala, joka tutkii tietämistä koskevia yleisiä käsitteellisiä kysymyksiä, esimerkiksi kysymyksiä tiedon luonteesta, alkuperästä ja varmuudesta. Filosofit ovat kautta aikojen tutkineet, mikä erottaa tietämisen ja tiedon pelkästä mielipiteestä ja luulosta. Osaaminen puolestaan liittyy tekemiseen ja toimintaan. Osaaminen syntyy tiedon soveltamisen kautta ja näkyy toiminnassa. Oppiminen tarkoittaa tiedon hankkimista, omaksumista ja soveltamista. (Otala 2008, 48.)

Osaamispääoman kannalta tärkeintä on henkilöstön määrä, osaamistaso, koulutus ja oppimishalu. Organisaation oppimisen kannalta on hyvä tarkastella henkilöstön diversiteettiä, esimerkiksi ikärakennetta, koulutustaustoja tai muuta erilaistavaa tekijää. Mikäli kaikki ovat samaa sukupuolta, saman ikäisiä ja kaikilla on sama koulutustausta, on organisaatiossa vaikea nähdä asioita useammasta näkökulmasta, joka taas on innovatiivisuuden kannalta välttämätöntä. (Otala 2008, 59.)

Osaaminen tarkoittaa yksilön kykyä suoriutua tehtävistään, kehittää ja parantaa työtään ja ratkaista ongelmia. Yksilö ei useinkaan suoriudu yksin tehtävästä, vaan työ on yhä enemmän tiimin, ryhmän ja organisaation aikaansaannos, on osaaminenkin yhä enemmän organisaation osaamista, sen osaamispääomaa. Osaamispääoma muodostuu henkilöpääomasta, suhdepääomasta ja rakennepääomasta (Kuva 13). Henkilöpääoma koostuu ihmisistä ja heidän osaamisestaan, sekä halustaan käyttää osaamistaan yhteisen tavoitteen saavuttamiseksi. Yksilön osaaminen muodostuu hänen taidoistaan, tiedoistaan, kokemuksestaan, verkostoistaan ja kyvyistään toimia toisten osaajien kanssa yhteistyössä, sekä hänen asenteistaan ja halustaan oppia jatkuvasti uutta. (Otala 2008, 47.)



Kuva 13. Osaamispääoman rakenne. (Otala 2008, 58).

Osaamispääomaan kuuluvat ihmiset, heidän osaamisensa ja osaamisen edellytyksenä oleva sitoutuminen, innostus ja motivaatio. Osaamispääomasta tätä ihmisten myötä syntyvää osaa kutsutaan henkilöpääomaksi. Osaamispääomaan kuuluvat ne rakenteet, jotka mahdollistavat ihmisten osaamisen muuttamisen organisaation osaamiseksi ja toiminnaksi, osaamisen kehittämisen, ylläpidon ja hankkimisen. Tätä osaa osaamispääomasta kutsutaan suhdepääomaksi. (Otala 2008, 57.)

Suhdepääomaan kuuluvat ne osaamiskumppanit, jotka täydentävät omaa osaamista tai joiden kanssa voidaan kehittää tarvittavaa osaamista paremmin ja tehokkaammin kuin yksin. Rakennepääoman muodostavat kaikki yrityksen henkiset ja fyysiset rakenteet, järjestelmät, teknologia ja toimintatavat sekä kulttuuri. Nämä mahdollistavat jokaisen henkilön osaamisen kehittämisen vastaamaan yrityksen tarpeita, sekä muuttamisen organisaation yhteiseksi toiminnaksi ja osaamiseksi. Osaamispääoman johtaminen tarkoittaa henkilöpääoman, suhdepääoman ja rakennepääoman johtamista. Tärkein alue on rakennepääoman johtaminen, koska rakenteet määräävät toiminnan. Oppiva organisaatio kuvaa sellaisia organisaatiorakenteita, jotka mahdollistavat ja tukevat organisaation oppimisen. Organisaation oppiminen on prosessi, joka kuvaa, miten henkilöpääomaan sidottu osaaminen muutetaan organisaation osaamispääomaksi. Tämän prosessin johtaminen on esimiesten keskeisin vastuualue. (Otala 2008, 47.)

Osaamispääoma on aina dynaamista. Mikäli osaamispääoman eri osien välissä ei ole jatkuva virtaus, se jämähtää paikalleen ja menettää arvonsa nopeasti. Jatkuva oppiminen turvaa osaamispääoman lisääntymisen ja kehittymisen. Osaamispääoman dynaamisuus takaa, että oppiva organisaatio toteutuu. Organisaation osaamisen kehittyminen edellyttää sellaista johtamiskulttuuria

ja ilmapiiriä, henkisiä rakenteita, jotka tukevat monen tasoista yhteistyötä ja yhdessä oppimista. (Otala 2008, 58 – 60.)

Haasteelliseksi organisaatiotason osaamisen hallinnan tekee se, että osaaminen on luonteeltaan alati uudistuva ja muotoutuva resurssi. Toimialat muuttuvat usein ennakoimattomasti ja nopeasti erityisesti teknologisen kehityksen, globaalien kulutus- ja tuotantomarkkinoiden kehityksen sekä erilaisten säätelymekanismien myötä. Osaaminen tulisi näin ollen olla sekä joustavaa että vahvaa. (Viitala & Uotila 2014, 100.)

Kuva 14. Henkilön osaaminen. (Otala 2008, 51.)

Osaamisesta puhutaan yksilöiden, ryhmien, tiimien ja organisaatioiden resurssina. Osaamiselle käytetään usein synonyymina kompetenssi-termiä. Yksilön osaaminen (Kuva 14) muodostuu tiedoista, taidoista, kokemuksesta, kontakteista ja verkostoista, asenteesta, sekä henkilökohtaisista ominaisuuksista, jotka auttavat selviytymään kulloisestakin työtilanteesta ja joiden seurauksena on hyvä työsuoritus. Tiedot ja taidot on hankittu opiskelun, koulutuksen, lukemisen ja tekemisen kautta. Kokemus liittyy myös tekemiseen ja hiljaiseen tietoon. Henkilökohtaiset ominaisuudet vaikuttavat siihen, miten samakin koulutus ja osaaminen painottuvat ja ilmenevät eri henkilöillä. Henkilökohtaisiin ominaisuuksiin kuuluvat persoonallisuus ja asenteet, jotka ovat hyvin tärkeitä tekijöitä, kun jokaiselta odotetaan jatkuvaa sopeutumista uusiin tilanteisiin. Henkilökohtaisiin ominaisuuksiin kuuluu myös tunneäly. Se sisältää joukon sosiaalisia ja henkilökohtaisia taitoja, jotka vaikuttavat siihen, miten hyvin tulemme toimeen itsemme ja toisten kanssa. Siihen kuuluu myös kyky tuottaa ja luoda mielikuvia, ymmärtää ja nähdä mahdollisuuksia, miten ne voi hyödyntää. Motiivit sisältyvät henkilökohtaisiin ominaisuuksiin. (Otala 2008, 50-51.)

Organisaation osaaminen on organisaation yhteinen käsitys tai näkemys toiminnan kannalta tärkeästä asiasta ja yhteisesti omaksuttu toimintatapa. Yksilöiden osaaminen muuttuu yhteisön tai organisaation osaamiseksi, kun ihmiset jakavat, kehittävät ja yhdistävät osaamistaan yhdessä ja kun osaaminen muunnetaan yhteiseksi näkemykseksi ja yhteiseksi toiminnaksi. Tämä edellyttää organisaatiolta rakenteita, jotka mahdollistavat kehittämisen, yhdistämisen, käyttämisen ja jakamisen. Organisaation osaaminen on se resurssi, jota yrityksessä pitää vaalia ja jonka syntymistä pitää ohjata ja tukea. (Otala 2008, 53.)

Ihmiset voivat olla eri puolilla organisaatiota hajallaan. Organisaation osaaminen muodostuu tällöin hajautuneesta asiantuntijuudesta, joka pitää rakenteilla, eritoten johtamisella saada yhteen. Rakenteet ovat organisaation osaamisen kannalta jopa tärkeämpiä kuin yksittäisen ihmisen osaaminen. (Otala 2008, 53.) Kohdeorganisaatio on hajallaan ympäri Suomea. Tiivis yhteydenpito, avoin keskustelu ja hyvä tiedonkulku edesauttavat asioiden hoitamista.

Employer branding eli työnantajamielikuvan kehittäminen on tullut mukaan strategisen johtamisen yhteyteen, koska on huomattu, että yrityksen arvo riippuu nykyisin yhä enemmän työntekijöistä. Rekrytointi on tämän vuoksi yksi yrityksen merkittävimmistä investoinneista. Työnantajamielikuva on yksi keskeisimmistä resursseista parhaiden työntekijöiden rekrytoinnissa, sekä työntekijän motivoinnissa ja sitouttamisessa. Täten se on varsin olennainen teema pitkän aikavälin menestyksen saavuttamisessa. Erityisesti nopeasti muuttuvilla, eli innovatiivisuutta ja oppimista edellyttävillä toimialoilla se, että organisaatio saa rekrytoitua parhaat työntekijät, sekä pidettyä heidät sitoutuneina ja motivoituneina, saattaa olla kilpailukyvyn kannalta paljon ratkaisevampaa kuin perinteiset toiminnan suunnitteluun, suorituskyvyn ennustamiseen ja mittaamiseen perustuvat lähestymistavat. (Vuorinen 2013, 189.)

3 Tutkimusstrategia, tutkimus- ja kehittämismenetelmät

Konstruktiivisella tutkimusotteella pyritään ratkaisemaan ongelmia reaalimaailmasta. Tässä tutkimusotteessa ydinkäsite, uusi konstruktio, on abstrakti käsite, jolla on suuri määrä mahdollisia toteutumia. Jokainen ihmisen tekemä artefakti, kuten suunnitelmat, mallit, kaupalliset tuotteet, organisaatiorakenteen, tietojärjestelmämallit ja diagrammit ovat konstruktioita. Tunnusomaista niille on, että niitä ei löydetä, vaan ne kehitetään ja keksitään. (Lukka 2001.) Tässä kehittämistyössä tutkimusstrategiana käytetään konstruktiivista tutkimusotetta. Tehdään järjestelmämigraatio, jota varten tehdään ryhmäjako henkilöstöstä, uusi kansiojärjestys dataa varten, kansioihin luodaan käyttöoikeudet ryhmäkohtaisesti ja lopulta tutkija siirtää tiedot. Tässä tutkimuksessa muutos on pysyvä, pilvipalvelun tiedot tullaan siirtämään uuteen järjestelmään ja ryhmät luomaan tämän hetkisten työntekijöiden mukaan. Tässä kehittämistyössä tutkija kerää aineiston, tekee tiedonsiirtotestauksia uuteen pilvipohjaiseen järjestelmään, on mukana työryhmässä, joka suunnittelee kerätyn aineiston perusteella ryhmäjaon.

3.1 Tutkimusmenetelmät

Tutkimusmenetelmäksi on otettu monimenetelmä triangulaatio. Siinä käytetään useita tutkimusmenetelmiä. Tässä tutkimuksessa käytetään kvalitatiivista sekä kvantitatiivista tutkimusmenetelmää aineistonkeruu menetelmien vuoksi. Tutkimusmetodeina käytetään teemahaastattelua pienelle otokselle, kahdelle henkilölle. Haastattelut tehdään verkon välityksellä Adobe Connectin kautta. Puolistrukturoitu kysely tehdään verkossa Google Forms:lla ja osoitetaan muulle henkilökunnalle. Kysely tapahtuu poikittaistutkimuksena, eli kerätään aineistoa samaan aikaan useilta vastaajilta. Haastattelu aineistonkeruu menetelmänä on osa kvalitatiivisen tutkimuksen tiedonkeruumenetelmää. Kysely on kvantitatiivisen tutkimuksen aineistonkeruumenetelmä. Haastattelun avulla kerätty aineisto litteroidaan. Tämän jälkeen tutkimusaineistolle tehdään sisällönanalyysi.

Kvalitatiivista ja kvantitatiivista tutkimusta voidaan käyttää rinnakkain. Useampaa näkökulmaa käyttämällä saadaan luotettavampaa tietoa. Tutkimusotteet eroavat tutkimusmetodien osalta myös toisistaan. Kvalitatiivisessa tutkimuksessa käytetään haastatteluja, havainnointia ja tekstianalyysiä, joiden avulla ilmiötä pyritään ymmärtämään. Kvantitatiivisessa tutkimuksessa laske-

taan määriä ja tiedonkeruumenetelmänä käytetään haastattelua, joka koostuu valmiista avoimista tai strukturoiduista kysymyksistä. Niiden avulla yritetään selvittää ilmiöön liittyviä yhteyksien esiintymistiheyksiä eli frekvenssejä tai ominaisuuksia. Laadullisen (qualitative) tutkimuksen aineisto on laadullista ja se perustuu puheisiin eli ei-numeraaliseen aineistoon ja kirjoitettuun tekstiin. (Kananen 2008, 10-11.)

Mixed methods, eli triangulaatio eli kolmiomittaus soveltuu tutkimusstrategiaksi laajoihin tutkimushankkeisiin, esimerkiksi jos tarkastellaan ilmiötä taloudelliselta, sosiaaliselta, yhteiskunnalliselta ja lääketieteelliseltä kannalta. Tutkimusongelmat ja -kohteet ovat usein niin monisyisiä ja laajoja, joten yhdellä tutkimusmenetelmällä ei saada riittävää tietoa tutkittavasta ilmiöstä. Triangulaatio ei ole oma tutkimusmenetelmä, vaan yhdistelmä kvantitatiivista ja kvalitatiivista tutkimusta. Triangulaatio on rinnastettavissa case-tutkimukseen ja monimenetelmäiseen (blended) tutkimukseen. (Kananen 2013, 33-34.) Triangulaatio on monimenetelmä tutkimus, jota käytetään tässä kehittämistyössä tutkimusmenetelmänä, sillä aineistonkeruumenetelmänä käytetään määrällistä ja laadullista menetelmää.

Haastattelun ideana on saada vastaus suoraan kysyttyyn kysymykseen. Kyse on eräänlaisesta keskustelusta, joka tapahtuu tutkijan ehdoilla ja aloitteesta, jossa tutkijan tavoite on saada haastateltavilta selville häntä kiinnostavat asiat, jotka kuuluvat tutkimuksen aihepiiriin. Teemahaastattelun ominaispiirteitä ovat ne, että haastattelun teema-alueet ja aihepiirit on etukäteen määrätty. Strukturoidulle haastattelulle on tyypillistä kysymysten tarkka järjestys ja muoto, jotka teemahaastattelusta puuttuvat. Strukturoidussa haastattelussa kysymysten järjestys ja muotoilu on kaikille sama. Puolistrukturoidussa haastattelussa haastateltaville esitetään samat kysymykset, mutta valmiita vastausvaihtoehtoja ei ole, vaan omin sanoin voi vastata. Avoin haastattelu on keskustelun kaltainen. Haastattelussa keskustellaan tietystä aiheesta, mutta kaikkien kanssa ei käydä läpi kaikkia teema-alueita. (Valli, ym. 2015, 27-30.)

Haastattelun etuna on joustavuus, siinä voidaan oikaista väärinkäsityksiä, toistaa kysymyksiä, käydä keskustelua tiedonantajan kanssa ja selventää ilmausten sanamuotoa. Haastattelun tarkoitus on saada haastateltavalta mahdollisimman paljon tietoa tutkittavasta aiheesta. Tällöin on perusteltua antaa haastattelukysymykset tai ainakin haastattelun aihe ennakkoon haastateltaville. Teemahaastattelussa, eli puolistrukturoidussa haastattelussa edetään etukäteen valittujen teemojen mukaan. (Tuomi & Sarajärvi 2013, 73, 75). Tässä tutkimuksessa käytetään aineistonkeruumenetelmänä teemahaastattelua. Haastattelija kysyy samat kysymykset kaikilta haastateltavilta yhdenmukaisuutta varten. Haastattelut toteutetaan yksilöhaastatteluna kahdelle henkilölle.

Kyselylomaketutkimuksessa voidaan erottaa kaksi erilaista tutkimusasetelmaa: pitkittäis- eli seurantatutkimus sekä poikittaistutkimus eli poikkileikkausaineistolla tehty tutkimus. Seurantatutkimuksessa aineistoa on kerätty ainakin kahdessa eri ajanjaksossa samoilta vastaajilta. Poikittaistutkimuksessa aineisto kerätään useilta vastaajilta yhdessä ajankohdassa. Poikkileikkausaineistolla tehtävillä analyyseilla eri ilmiöitä voidaan kuvailla ja pitkittäistutkimuksen avulla niitä voidaan myös selittää. Onnistuneen tutkimuksen kannalta on tärkeää, että kyselylomake on laadittu hyvin. (Valli, ym. 2015, 121, 127). Tässä kehittämistehtävässä kyselylomakkeella kerätään aineistoa poikittaistutkimuksella, eli useilta vastaajilta samaan aikaan. Kyselyn avulla saadaan suurelta otokselta mielipiteitä.

Kyselytutkimus on tärkeä tapa kerätä ja tarkastaa tietoa erilaisista ihmisten toiminnasta, yhteiskunnan ilmiöistä, arvoista, asenteista ja mielipiteistä. Tutkija esittää kyselytutkimuksessa kysymyksiä vastaajalle kyselylomakkeen välityksellä. Kyselylomake on mittausväline kyselytutkimuksessa. Haastattelututkimuksessa tutkija esittää kysymykset suoraan vastaajalle. Haastattelulomake muistuttaa kyselylomaketta, erona näissä on se, että kyselylomakkeen on toimittava itsenäisesti ilman haastattelijan apua. (Vehkalahti 2008, 11.)

Sähköisten kyselyiden suosio on kasvanut tutkimuskäytössä. Sähköisten kyselyiden vahvuutena pidetään niiden visuaalisuutta. Verkkokyselyiden etuna pidetään myös nopeutta, kyselyä jaettaessa sekä vastauslomaketta palauttaessa. Kolmantena etuna on taloudellisuus. Kyselylle ei ole maantieteellisiä rajoitteita. Kyselylomakkeen tulee toimia niin tietokoneella, tabletilla kuin älypuhelimessa. Hyvänä puolena on myös se, että aineiston syöttö- ja litterointivaiheessa tehdyt kirjoitusvirheet jäävät pois, tällöin aineisto on vieläkin luotettavampi. (Valli, ym. 2015, 109-110.)

3.2 Analysointi- ja kehittämismenetelmät

Teemahaastatteluaineisto kirjoitetaan sanatarkasti tekstimuotoon. Litteroinnissa on eri tasoja: sanatarkka, yleiskielinen ja propositiotason litterointeja. Sanatarkassa kaikki äänähdyksetkin kirjataan ylös, yleiskielisessä murresanat muutetaan kirjakielelle ja propositiotasossa kirjataan ylös sanoman tai havainnon ydinsisältö. (Kananen 2014, 105.) Mikäli haastattelussa kiinnostus kohdistuu esiin tuleviin asiasisältöihin, ei ole tarpeen tehdä kovin yksityiskohtaista litterointia. Keskusteluanalyysissä vaaditaan litteroinnilta tarkkuutta. Tarkkuustaso litteroinnissa määräytyy tutkittavan ilmiön mukaan. Litterointi nähdään osana laadullisen tutkimuksen validiteettia. Tulkintojen ankkuroiminen aineistoon ja analyyttinen läpinäkyvyys ovat kurinalaisen laadullisen tutkimuksen

validiteettia parantava piirre. (Ruusuvuori & Nikander & Hyvärinen 2010, 425, 432-433.) Tässä tutkimuksessa tullaan käyttämään yleiskielistä litterointia.

Konkreettiset päätökset tehdään aineistonkeruumenetelmässä siitä, missä muodossa aiemmat määrittelyt näytetään. Sitä kutsutaan kvantitatiivisessa tutkimuksessa operationalisoinniksi eli käsite saadaan mitattavaan muotoon. Kvalitatiivisessa tutkimuksessa sen sijaan käsite on saatava tutkittavaan muotoon. (Kyrö 2003, 107-108.) Aineiston analyysiä aloittaessa siitä poistetaan tunnistetiedot, eli aineisto anonymisoidaan. Suoria tunnistetietoja ovat haastateltavan nimi, syntymäaika ja tarkat yhteystiedot. Epäsuoriin tunnistetietoihin kuuluu sukupuoli, asuinpaikkakunta, koulutustausta ja työpaikka. (Ruusuvuori, ym. 2010, 452.)

Kerätystä aineistosta kysytään tutkimusongelman mukaisia kysymyksiä. Aineistosta tunnistetaan asiat, joista ollaan kiinnostuneita tutkimuksessa. Asioita ilmaisevat lauseet pelkistetään yksittäisiksi ilmaisuiksi, jotka ryhmitellään yhtenäisten ilmaisujen joukoiksi. Saman sisältöiset ilmaisut yhdistetään samaan kategoriaan eli luokkaan ja nimetään uudelleen. Analyysin kriittisin vaihe on kategorioiden muodostaminen, jota jatketaan yhdistämällä alakategorioita ja muodostamalla niistä yläkategorioita. Lopulta yläkategoriat yhdistellään ja muodostetaan kategorioita, joiden avulla tutkimusongelmiin saadaan vastaus. (Tuomi, ym. 2013, 101.) Kerätty aineisto luokitellaan, analysoidaan ja tulkitaan. Luokittelussa aineisto käydään järjestelmällisesti läpi.

Sisällönanalyysillä pyritään saamaan tutkittavasta ilmiöstä kuvaus yleisessä ja tiivistetyssä muodossa. Tutkimusta varten kerätty aineisto on tarkoitus saada järjesteltyä johtopäätöksien tekoa varten. Hyvin järjestellyn aineiston tulokset eivät ole tutkimuksen tuloksia. Sisällönanalyysi on tekstianalyysia, jossa etsitään tekstin merkityksiä. (Tuomi, ym. 2013, 103-104.) Sisällönanalyysin tavoitteena on tuottaa selkeä ja sanallinen kuvaus siitä, mitä aineisto tarkoittaa. (Kananen 2014, 111-112.) Aineistolähtöisen laadullisen eli induktiivisen aineiston analyysin voi jakaa kolmeen vaiheeseen: 1) aineisto redusoidaan eli pelkistetään, 2) aineisto klusterioidaan eli ryhmitellään ja 3) abstrahointi eli luodaan teoreettisia käsitteitä. (Tuomi, ym. 2013, 108-109.)

Kehittämismenetelmänä käytetään työryhmää. Siihen kuuluu kolme henkilöä, tutkijan lisäksi kaksi asiantuntijaa kohdeorganisaatiosta. Asiantuntijat olivat alun perin ensimmäisessä palaverissa olleet, joka koski muutostarvetta. Kehittämistyössä on tarkoitus siirtää nykyisestä pilvipalvelusta tiedot uuteen järjestelmään. Työtehtäväkyselyn avulla työryhmä voi tehdä ryhmäjaottelun työtehtävien mukaan kohdeorganisaation henkilökunnalle. Tietoturva kyselyn avulla voidaan tehdä uusi kansiojärjestys uuden Jaetun Driven puolelle. Työryhmä saa tehtyä teorian, kyselyn ja haastatteluiden materiaalien perusteella uuden järjestelmän kansioiden käytönjakamisoikeudet.

Tietoturva kyselyiden tuloksista saadaan selville millä mallilla on tämän hetken tietoturva-asiat henkilöstön mielestä yrityksessä. Haastatteluiden tulosten perusteella tehdään tarvittavia muutoksia sisäiseen valvontaan ja riskinhallintaan. Nämä kaikki tehdään työryhmässä yhdessä.

4 Pilvipalvelun järjestelmämigraatio

Muistamme, kun 2000-luvun taitteessa kännykät alkoivat muuttua älypuhelimiksi. Niihin tuli tiheään uusia ominaisuuksia, mutta käytettävyys ei pysynyt kehityksen matkassa. Valikkopolut käyttöliittymässä mutkistuivat ja valtaosa uutuuksista jäi käyttäjille tuntemattomiksi. Tämä on hyvä muistaa, että toiminnallisuuksia ei kannata kehittää vain siksi, että ne on mahdollista toteuttaa. Kehittämisessä kannattaa kuunnella käyttäjiä ja heidän antamaa palautetta kannattaa analysoida systemaattisesti. (Collin, ym. 2016, 305.) Haastatteluiden ja kyselyn avulla tullaan kysymään myös käytettävyyteen liittyvistä asioista. Tarkoitus on saada käyttäjäystävällinen kansiojärjestys uuteen pilvipohjaiseen tallennusjärjestelmään. Niin kuin Collin kehottaa kuuntelemaan käyttäjiä kehittämisessä, tullaan kysymysten avulla henkilökuntaa kuulemaan muutosta varten.

Kehittämistyön tavoitteena on selvittää mitä kaikkea tulee ottaa huomioon, kun aiotaan tehdä järjestelmämigraatio. Kohdeorganisaatio tallentaa tiedot pilvipalveluun. Tavoite on parantaa tietosuojaa ja tietoturvaa rajaamalla henkilöiden pääsyä tiedostoihin samalla kun pilvipohjainen tallennusjärjestelmä vaihdetaan. Tällä hetkellä työntekijän työnkuvan kannalta tietoa on saatavilla liian laajoina asiakokonaisuuksina, mikä on tarpeetonta työnkuvaan nähden. Tarvitaan uudenlainen tallennusratkaisu. Sen tulee olla uuden GDPR:n, tietosuoja-asetuksen mukainen. Kehittämistyössä etsitään vastauksia seuraaviin kysymyksiin: Millaisiin ryhmiin työntekijät jaetaan uutta tallennusjärjestelmää varten? Miten tietosuoja ja tietoturva tulisi ottaa huomioon yrityksen pilvipalvelussa? Miten organisaation sisäinen valvonta toteutetaan ja riskejä hallitaan esimiehen näkökulmasta? Tavoitteena on uudistaa pilvipohjainen tallennusratkaisu tietosuoja ja tietoturva huomioiden sekä rajata tarpeettomien tietosuojaluokitusten alaisten tietojen leviäminen oikeudettomille tahoille. *Kehittämistehtävän tarkoituksena* on rakentaa uusi pilvipohjainen tallennusratkaisu jo olemassa olevan rinnalle, eli tehdä järjestelmämigraatio. Sisäinen valvonta ja riskienhallinta ajanmukaistetaan.

Aineistonkeruumenetelmänä tässä kehittämistehtävässä käytetään kyselyä ja haastattelua. Tarkoitus on selvittää kyselyn avulla henkilöstöltä työtehtävät, joiden mukaan ryhmittely tehdään uuden järjestelmän puolelle. Toisella kyselyllä, johon vastataan anonyymisti, selvitetään millainen olisi toimiva kansiojärjestys tiedon etsintää ajatellen, mikä toimii ja mikä ei nykyisessä järjestelmässä, tietoturva sekä pilvipalvelu asioista kysellään. Tietohallinnon tasolla tulee miettiä, kenellä on oikeus katsella ja muuttaa olemassa olevia tiedostoja. Työntekoon tarvittava tieto tulisi saada helposti löydettäväksi ja pääsy tiedostoihin tulisi olla työtehtävien mukaan.

Tässä tutkimuksessa analysoitavana on haastattelu- ja kyselyaineisto. Aineistosta karsitaan tutkimuksen kannalta epäolennainen pois joko tiivistämällä tai osiin pilkkomalla. Aineisto litteroidaan ensin. Sen jälkeen aineisoa analysoidaan aina vain tiiviimpään muotoon luokkien avulla: Alkuperäisilmaukset, Pelkistetty ilmaus, Alaluokka, Yläluokka, Yhdistävä luokka.

Kun aineisto on luokiteltu, voidaan se esittää taulukkona. Teemoittelussa painotetaan sitä, mitä on sanottu kustakin teemasta. Laadullinen aineisto siis ryhmitellään ja pilkotaan erilaisten aihepiirien mukaan. Tyypittelyssä aineisto jaetaan tietyiksi tyypeiksi. Viimeisen, neljännen vaiheen kohdalla tulee miettiä, hakeeko aineistolta erilaisuutta vai samanlaisuutta. (Tuomi, ym 2013, 93.) Tässä kehittämistehtävässä käytetään sisällönanalyysia, koska sen avulla saadaan parhaiten tietää eri teemoihin kuuluvista asioista. Teemoja ovat muun muassa tietoturva, riskienhallinta, sisällön valvonta ja pilvipalvelut.

Kehittäminen mielletään yleensä konkreettiseksi toiminnaksi, joka tähtää selkeästi asetellun tavoitteen saavuttamiseen. Kehittäminen voi olla yksikkökohtaista, siinä tavoitellaan yhtä aikaa rakenteellisia ja toimintatavallisia uudistuksia. Kehittäminen on luonteeltaan käytännöllistä asioiden korjaamista, edistämistä ja parantamista. Kehittämisellä tähdätään muutokseen, jolla tavoitellaan tehokkaampaa ja parempaa toimintatapaa- ja rakennetta. Lähtökohtana kehittämistoiminnalle voi olla tämän hetkisen tilanteen ongelmat. (Toikko & Rantanen 2009, 14, 16.) Kehittämismenetelmänä haastatteluista ja kyselyistä saatu aineisto käydään kehittämisryhmän työpajassa läpi. Työtehtävien sisältö vaikuttaa oleellisesti ryhmien muodostamiseen, joiden pohjalle uuden järjestelmän tiedonjakamisoikeudet tiedostoihin annetaan. Materiaalien avulla voidaan suunnitella ryhmäjakoa järjestelmämigraatiota varten, sekä päivittää tietoturva ja tietosuoja ohjeistuksia. Sisäisen valvonnan ja riskienhallinnan ohjeistus päivitetään myös uusien tuloksien myötä.

4.1 Kohdeorganisaatio

Kohdeorganisaatio on yksityinen koulutusalan yritys. Yritys järjestää työvoimakoulutusta ja asiantuntijapalveluita. Organisaation hankkija-asiakkaina toimii Elinkeino-, liikenne- ja ympäristökeskukset eli ELY sekä Työ- ja elinkeinotoimistot eli TE-toimistot ympäri Suomen. Koulutuksissa opiskelevat työttömät tai työttömyysuhanalaiset henkilöt. Suurimmat päätoimialat ovat tällä hetkellä työnhaku- ja uravalmennukset sekä maahanmuuttajien kieli- ja kotoutumiskoulutukset. Yritys järjestää myös maahanmuuttajien kielitaidon kartoituksia, YKI-testejä.

Yritys työllistää noin sataviisikymmentä osaamisen kehittämisen ammattilaista erilaisissa asiantuntijatehtävissä, suurin osa heistä on kouluttajia ja valmentajia. Asiakkaita kohdataan päivittäin yli 2000, 180:llä paikkakunnalla, 100:ssa eri palvelussa ja toiminnan kivijalkana on asiakaslähtöisyys. Palvelujen laadukas toteutus perustuu jatkuvaan kehittämiseen ja kehittymiseen, sekä annettujen lupausten pitämiseen. Palveluihin kuuluu valmennukset työnhakijoille, ammattitutkinnot, maahanmuuttajakoulutukset, koulutukset yrityksille, yleiset kielitutkinnot ja tilavuokraukset.

Yritys on oppiva organisaatio. Virtasen mukaan organisaatiosta tulee oppiva, kun se tulee tietoisesti siitä, että oppivaksi organisaatioksi tulo edellyttää ennakkoluulotonta kyseenalaistamista ja kun se oppii kriittisiä tapoja arvioida toimintaansa. Oppivan organisaation tunnuspiirteitä on myös poisoppiminen, eli se osaa luopua aiemmista toimintamalleistaan ja -tavoistaan. (Virtanen 2007, 177-178.) Organisaatio ei opi samalla tavalla kuin ihminen, vaan organisaation toimintaa on muutettava, kuten muokattava strategiaa ja yksiköitä sekä käyttöönottaa uusia menetelmiä ja ohjeita.

Muutoksen johtaminen on ajankohtainen kohdeorganisaatiossa, sillä kuluneen vuoden aikana monien työnkuvissa on tapahtunut muutoksia. Työntekijöiden tulee päästä erinäisiin tiedostoihin työtehtäviä hoitaakseen, mutta toisaalta tietoa on myös liian laajoina asiakokonaisuuksia saatavilla tällä hetkellä. Tämänhetkisen tallennusjärjestelmän rakenne pilvessä on toisinaan varsin työläs ja kankea tiedon etsimiseen. Tarvitaan ketterämpi pilvipohjainen tallennusjärjestelmä, jolloin työtehoa saadaan kehityksen myötä samalla parannettua, kun tiedon löydettävyys helpottuu. GDPR:n myötä myös tietosuoja ja tietoturva-asiat tulee ottaa entistä paremmin huomioon tietoja käsiteltäessä. Organisaation osaaminen on myös olennainen osa toimivaa työyhteisöä. Työtehtävien sisältö vaikuttaa ryhmittelyperusteisiin, joita tarvitaan uudessa järjestelmässä. Kohdeorganisaatiossa kehittämistä tapahtuu koko ajan digitalisoitumisen saralla. Muutoksia kuluneen vuoden aikana on tullut paljon, joten on syytä ottaa huomioon muutoksen ja osaamisen johtaminen tässä kokonaisuudessa. Niillä on tärkeä merkitys muutoksen hyväksymisessä ja käyttöönotossa työyhteisössä.

4.1.1 GAPPS

GAPPS on Googlen kumppani Suomessa ja kohdeorganisaatio ostaa G Suite palvelun heidän kautta, eli GAPPS on Googlen jälleenmyyjä. GAPPS antaa kohdeorganisaatiolle Helpdesk tukea G Suiten Google asioissa. Yritys hankkii tukea GAPPS:lta pilvipalvelun muokkaamiseen. GAPPS on

esittänyt ratkaisun, miten yrityksen tulisi päivittää Basic versio Business versioksi ja rakentaa tallennusjärjestelmä sen mukaan tulevan Team Drivesin puolelle. Kesällä 2019 Google muutti Team Driven nimen Shared Driveksi eli Jaetuksi Driveksi.

Gapps on Suomen johtava Google Cloud -asiantuntijatalo ja he ovat erikoistuneet työyhteisöjen muutosjohtamiseen. Gapps Oy on perustettu vuonna 2010. Tietojenkäsittely, palvelintilan vuokraus ja niihin liittyvät palvelut ovat sen toimialana. Yrityksen kotipaikkana toimii Helsinki. (Kauppalehti. 2019.) Gappsin visioon kuuluu auttaa suomalaisia yrityksiä pysymään kilpailukykyisinä nopeasti muuttuvassa kansainvälisessä kilpailussa sekä tarjota työntekijöille joustavuutta ja vapautta työskentelytapoihin. Gapps etsii asiakkailleen heidän tarpeisiinsa sopivat ja toimivat ratkaisut. (Gapps 2019.)

Tekniikka & Talous uutisoivat vuonna 2014, että julkisen palvelun mediayhtiö Yleisradio on siirtänyt toimintojaan pilvipalveluun, muun muassa sähköposti- ja kalenterisovelluksensa sekä toimisto-ohjelmistonsa osittain. Kilpailutuksen oli voittanut pieni it-palveluyritys, suomalainen Gapps, Google Apps -pohjaisella palvelullaan. Ylen työntekijät siirtyivät 1980-luvulta nykyaikaan uuden palvelun käyttöönoton myötä. (Tekniikka & Talous 2014.)

Syitä Business -lisenssiin siirtymiseen

Seuraavassa GAPPSin suunnitelma kohdeorganisaatiolle. G Suite Business versio tuo mukanaan huomion arvoisia lisämahdollisuuksia.

- Ketterämpää yhteistyötä projektien ja tiimien sisällä. Team Driven avulla pystytään hallitsemaan projekteihin liittyvää dataa ja niiden jako-oikeuksia keskitetysti. Team Drive mahdollistaa hyvän rakenteen esimerkiksi osastojen tai projektien sisäiseen kollaboratioon lokeroimalla tiedonjaon tarkemmin.

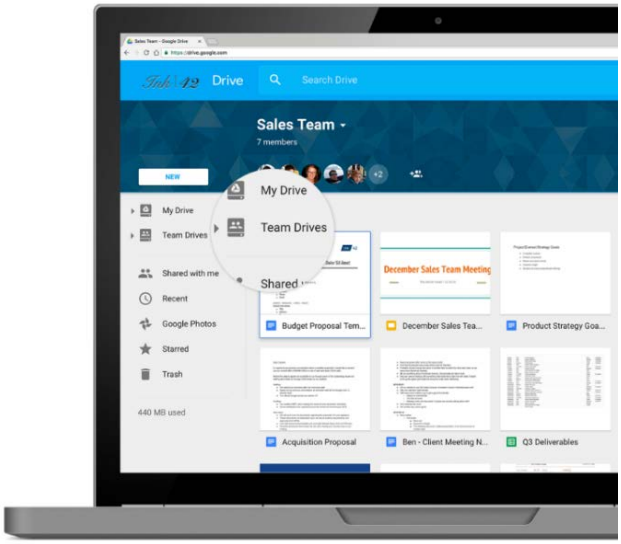
- Datan sitominen Eurooppaan. Datan kiinnittäminen Eurooppaan, jolloin se ei matkusta käyttäjien mukana Euroopan ulkopuolelle. Tämän myötä yhteistyökumppanien mahdollinen arkuus datan liikkumiseen liittyen saadaan hallittua.

- Mahdollisuus omaan sisäiseen sovelluskehitykseen. App Maker on Googlen oma low-code -sovellus, jolla voi rakentaa kevyitä sovelluksia talon sisäiseen käyttöön. Tämä antaa mahdollisuuden esimerkiksi datan ja tehtävien keruun automatisointiin.

- Rajaton tallennustila. Rajaton Drive-tallennustila luo mahdollisuuden kaiken datan viemiseen Driveen. Basicissa tallennustila on rajattu 30 Gb per käyttäjä ja lisätilasta saa maksaa extraa.

- Tietoturvallisuuteen liittyvät lisätoiminnot. Google Data Vault (eDiscovery & retention) vastaa tehokkaasti sekä GDPR:n mukana tuomiin sekä tiedostojenhallintaan liittyviin tarpeisiin. Data Vaultin avulla voidaan esimerkiksi palauttaa poistettuja tiedostoja, nähdä tiedostojen muutoslokeja, määrittää kuinka kauan tiedostoja tallennetaan henkilön poistuttua yrityksen palveluksesta, datan vienti ulos esimerkiksi virkavallan pyynnöstä sekä sisällön etsimisen tiedostojen sisältä.

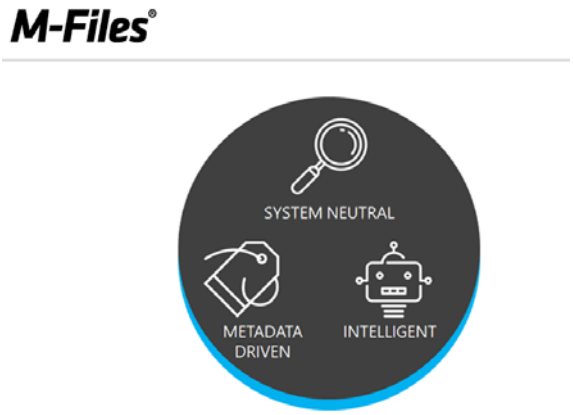
Business versio tuo mukanaan laajemman admin paneelin, jonka avulla Driven hallinnointi on mahdollista keskitetymmin. Tähän yhdistyy myös laajemman käytön auditoinnin mahdollisuudet, jonka avulla pystytään tarkemmin näkemään esimerkiksi mitä Drivessä on luotu ja mihin sitä on jaettu. (GAPPS 2019, Power Point esittelymateriaali kohdeorganisaatiolle.)



Kuva 15. Gappsin kuvakaappaus My Drive ja Team Driven näkymästä. (Gapps 2019.)

4.1.2 M-Files

Kohdeorganisaatiossa kaikki tieto tallennetaan Google Driven pilvipalveluun. Tiedon hakemistojärjestelmänä on puumainen kansiorakenne, jonka sisältöä ja rakennetta voidaan muokata tarpeiden mukaan, pääkansioista alikansioihin, aihealueittain. M-Files tarjoaa markkinoille toisenlainen tiedonhallintaratkaisun kuin Google.



Kuva 16. M-Files. (M-Files 2019.)

M-Files on tiedonhallintaratkaisu (Kuva 16), sillä sen järjestelmä on rakennettu kolmen pilarin varaan: se perustuu metatietojen käyttöön, se on älykäs ja se ei ole riippuvainen yksittäisistä järjestelmistä tai tietovarannoista. Tietojen etsiminen ja niiden hyödyntäminen perustuu sisältöön, ei sijaintiin. Tiedot näkyvät automaattisesti oikeassa kontekstissa, riippumatta alkuperäisestä järjestelmästä. Tietoja ei tarvitse siirtää, sillä niitä voi säilyttää nykyisessä sijainnissaan ja ne ovat heti käytettävissä. (M-Files, Tutustu M-Filesiin.) M-files tarjoaa tehokkaan, tuottavan ja kilpailukykyisen tiedonhallinnanratkaisun liiketoiminnan päätöksenteon tueksi. (M-Files, Tiedonhallinta).

M-Files hallinnoi ja järjestää tietoa sisällön perusteella, riippumatta sijaitseeko tieto M-Filesissa vai muissa järjestelmissä. Hallinnointi tapahtuu yhden näkymän kautta. M-Filesin avulla liiketoiminnan kasvua voi nopeuttaa erillisten järjestelmien, tietovarastojen ja sovellusten puuttuessa. Ratkaisu parantaa asiakaskokemusta, sillä se tukee kokonaisvaltaista automaatiota.

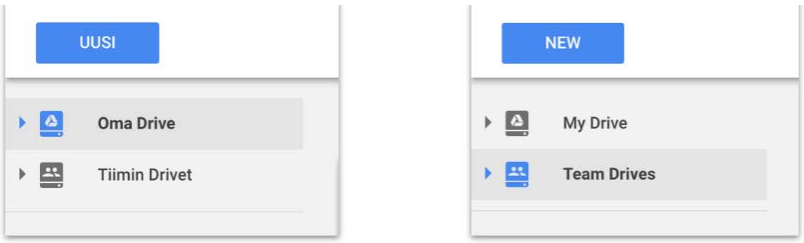
M-Filesin tärkeimmät ominaisuudet ovat: 1.) Tiedon etsiminen sisällön perusteella sijainnin asemesta. 2.) Voi etsiä, hallinnoida ja käyttää kaikkia tietoja, jotka ovat yrityksen verkossa. 3.) Sisällön

ja tiedostojen tehokkaaseen hallintaan voi hyödyntää tekoälyä. 4.) Alusta vaihtoehtoja on konesaliasennus, pilvi tai hybridi. 5.) Tietoja voi muokata, käyttää ja etsiä millä tahansa laitteella. (M-Files, Älykäs tiedonhallinta.)

Tiedonhallinnan palvelualustana M-Files on ensimmäinen, jossa on samanlainen helppo käyttöliittymä niin pilvessä kuin omassa konesalissa sijaitsevalla sisällöllä. Ohjelmisto päivitetään automaattisesti ja pilvipalvelu on ajan tasalla aina. Käytössä on aina uusin ja turvallisin versio, joten huoltotoimenpiteitä on harvoin. Tukitiimi on sertifioitu ISO 27001:2013 -standardin mukaisesti. Laatujärjestelmä noudattaa ISO 9001:2015 -standardia. Tiedot on aina salattu siirron aikana ja tallennettaessa myös aktiivisten infrastruktuurin turvatoimien lisäksi. Käyttöön voi ottaa myös muita lisäturvatoimia verkkoyhteyksien ja tunnistautumisen osalta. M-Files toimii Microsoftin Azure -pilvialustalla ja hyödyntää luotettavaa ja hyvin skaalautuvaa maantieteellisesti laajaa datakeskusverkkoa. Sen avulla on mahdollistettu nopea palvelu kaikkialla maailmassa. (M-Files, Pilvipalvelu.)

4.2 Googlen Drivet

Kohdeorganisaatiossa käytetään tällä hetkellä Oma Driveä (My Driveä). Yhteiset tiedostot piti opinnäytetyön alkumetreillä keväällä siirtää Tiimin Driven (Team Drives) puolelle (Kuva 17). Kesällä 2019 Google teki muutoksia kesken kehittämistyön ja Tiimin Driven muuttui Jaetuksi Driveksi (Shared Drive). Yhteiset tiedostot tullaan siirtämään siis Jaettuun Driveen. Ominaisuudet Jaetussa Drivessä pysyivät kuitenkin lähes ennallaan. Googlella on työ vielä kesken ja uudet ominaisuudet ovatkin valmiina alkuvuodesta 2020.



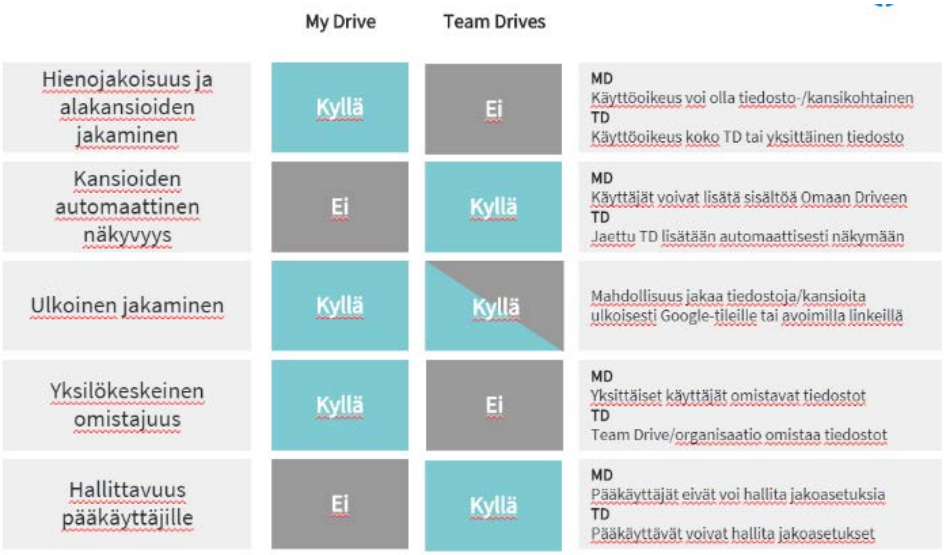
Kuva 17. Päävalikko pilvipalvelun kansionäkymästä Google Drivessä. (Gapps:n esitysmateriaali.)

Oma Drive (My Drive)

My Drive puolella tiedostot ovat yksilökohtaisessa omistuksessa. Käyttäjästä, joka luo tai lataa uuden tiedoston/kansion tulee omistaja. Hienojakoiset asetukset jakamiseen, eli käyttöoikeudet ja näkymät voivat vaihdella käyttäjien välillä. Käyttäjät kontrolloivat omaa sisältöään, eli voivat halutessaan lisätä jaettua sisältöä Omaan Driveen.

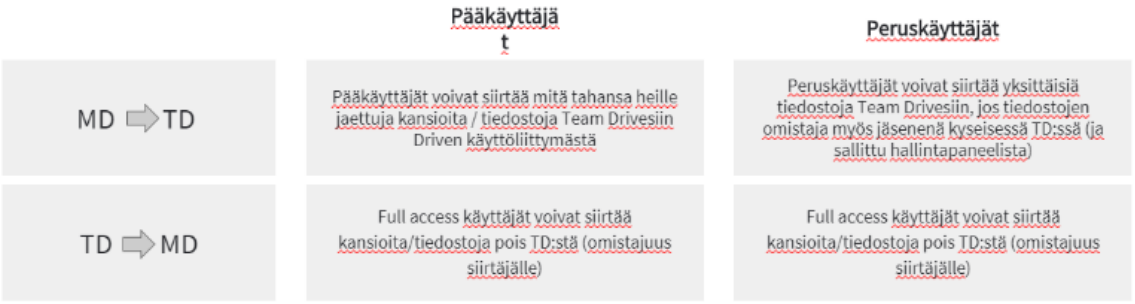
Tiimin Drive (Team Drives)

Tiimin Drivessä tiedostot ovat kollektiivisessa omistuksessa. Tiimi/organisaatio omistaa datan, eivät yksittäiset käyttäjät. Yksinkertaiset asetukset jakamiseen, eli kaikki näkevät saman näkymän ja sisällön, mutta käyttöoikeudet voivat vaihdella (täydet (full)/muokkaus (edit)/katselu (view)). Uusille työntekijöille helppo onboarding. Tiimin Drivet tulevat näkyville automaattisesti käyttäjille, kun ne jaetaan heille (Kuva 18).



Kuva 18. Kuvassa on Oma Driven ja Tiimin Driven ominaisuudet eritelty. (Gapps:n esitysmateriaali.)

Tiedostoja voidaan siirtää Oma Driven ja Team Driven välillä seuraavanlaisesti Pääkäyttäjien ja Peruskäyttäjien toimesta (Kuva 19):



Kuva 19. Pääkäyttäjän ja peruskäyttäjän tiedonsiirto mahdollisuuksia. (Gapps:n esitysmateriaali.)

Oma Drivestä Tiimin Driveen

- Pääkäyttäjät voivat siirtää mitä tahansa heille jaettuja kansioita/tiedostoja Tiimin Driveen, Driven käyttöliittymästä.
- Peruskäyttäjät voivat siirtää yksittäisiä tiedostoja Team Drivesiin, jos tiedostojen omistaja on myös jäsenenä kyseisessä Tiimin Drivessä (ja on sallittuna hallintapaneelista).

Tiimin Drivestä Omaan Driveen

- Pääkäyttäjät, joka on Full access käyttäjät voivat siirtää kansioita/tiedostoja pois Tiimin Drivestä (omistajuus siirtäjälle).
- Peruskäyttäjät, joka on Full access käyttäjä voi siirtää kansioita/tiedostoja pois Tiimin Drivestä (omistajuus siirtäjälle).

Yhteiset kansiorakenteet ja jakaminen

Seuraavassa kuvassa (Kuva 20) malli yhteisten kansiorakenteiden suunnittelusta:

Kuva 20. Yhteisten kansiorakenteiden suunnittelu. (Gapps:n esitysmateriaali.)

Seuraavassa kuvassa (Kuva 21) malli yhteisten kansiorakenteiden jakamisesta:

Kuva 21. Yhteisten kansiorakenteiden jakaminen. (Gapps:n esitysmateriaali.)

Jaettu Drive (Shared Drive)

Kesällä 2019 Google teki muutoksen ja päivitti Tiimin Driven nimen Jaettuun Driveen (Shared Drive). Jaettuun Driveen on tulossa uusia ominaisuuksia, joka mahdollistaa kaikkien tiedostojen siirron uudelle puolelle. Marraskuun lopulla pidetyssä palaverissa vahvistui tieto, että ensi vuoden alussa kaiken datan siirtoon mahdollistava ominaisuus tulee valmiiksi. Myös alikansioiden jakaminen tulee käyttöön, kun Google saa uudet ominaisuudet valmiiksi. Tällä hetkellä Google testaa beta versiolla toimintoja. Kehittämistehtävälle on tyypillistä, että muutoksia tulee kesken työn.

Jaetun Driven ja Oma Driven vertailua (Taulukko 4)

	Jaettu Drive	**Oma Drive**
Minkä tyyppisiä tiedostoja voi lisätä?	Kaikenlaisia paitsi Google Mapseja	Kaikki tiedosto tyypit
Kuka omistaa tiedostot ja kansiot?	Organisaatiosi	Henkilö, joka on luonut tiedoston tai kansion.
Voinko siirtää tiedostoja ja kansioita?	Käyttäjät voivat siirtää vain tiedostoja. Ylläpitäjä voi siirtää tiedostoja ja kansioita.	Kyllä
Voinko synkronoida tiedostoja tietokoneeseeni?	Drive File Stream sovelluksella: Kyllä Varmuuskopioinnin ja synkronoinnin avulla: Ei	Kyllä
Kuinka jakaminen toimii?	Kaikki tiimin jäsenet näkevät saman tiedostojoukon.	Eri käyttäjät voivat nähdä kansioissa erilaisia tiedostoja riippuen heidän pääsystä yksittäisiin tiedostoihin.
Kuinka kauan poistetut tiedostot pysyvät roskakorissa?	• Jokaisella jaetulla asemalla on oma roskakori. • 30 päivän jälkeen roskakorissa olevat tiedostot ja kansiot poistetaan lopullisesti. • Jäsenet voivat poistaa tietyt tiedostot nopeammin.	Roskakorissa olevat tiedostot ja kansiot pysyvät siellä, kunnes käyttäjä valitsee Poista lopullisesti.
Voinko palauttaa tiedostoja?	Kyllä, jos sinulla on Päällikön, Sisällönhallinnan tai Avustajan käyttöoikeudet.	Kyllä, jos olet luonut ne.

Taulukko 4. Jaetun Driven ja Oma Driven ominaisuuksien vertailua. (Google 2019, What are shared drives).

Uuteen järjestelmään tiedot tallennetaan eri tavalla, jolloin tiedonsaantioikeuksia voi säätää eri tavalla. Oma Driveen tallennetaan tiedostoja siten, että lopulta vain tietty henkilö näkee tietyt kansiot. Jaetun Driven puolelle kansiorakenne rakentuu siten, että tietyille ryhmille annetaan oikeus päästä kansioihin. Oma Driven puolella yksilö omistaa tiedon, kun taas Jaetun Driven puolella yritys omistaa tiedon. Käyttäjän tasoja voi muokata viiteen eri tasoon. Käyttäjän pääsytasot

Jaetun Driven käyttötasot

Tämä ominaisuus on saatavana G Suite Business -julkaisussa. G Suite Basic -käyttäjillä on joissakin tilanteissa rajoitettu pääsy.

Käyttäjän pääsytasot

Hallitakseen Jaettua Driveä ja niiden sisältöä, käyttäjä tarvitsee sopivat pääsytasot (Taulukko 5).

Tehtävä	Johtaja	Sisältö päällikkö*	Avustaja**	Kommentoija	Katsoja
Tarkastele jaettuja asemia ja tiedostoja	✔	✔	✔	✔	✔
Kommentoi jaettujen asemien tiedostoja	✔	✔	✔	✔	✗
Tee, hyväksy ja hylkää tiedostojen muokkaukset	✔	✔	✔	✗	✗
Luo ja lähetä tiedostoja ja luo kansioita jaettuihin asemiin	✔	✔	✔	✗	✗
Lisää ihmisiä tiettyihin tiedostoihin jaetuissa asemissa	✔	✔	✔	✗	✗
Siirrä tiedostoja ja kansioita jaetussa asemassa	✔	✔	✗	✗	✗
Siirrä tiedostot yhdestä jaetusta asemasta toiseen jaettuun asemaan	✔	✗	✗	✗	✗
Siirrä jaetut asematiedostot roskakoriin	✔	✔	✗	✗	✗
Poista pysyvästi roskakorissa olevat tiedostot	✔	✗	✗	✗	✗
Palauta tiedostot roskakorista (enintään 30 päivää)	✔	✔	✔	✗	✗

Lisää tai poista ihmisiä jaettuihin levyihin tai niistä	✔	✗	✗	✗	✗
Muokkaa jaetun aseman asetuksia	✔	✗	✗	✗	✗
Poista jaettu asema	✔	✗	✗	✗	✗

Taulukko 5. Jaetun Driven käyttötasot. (Google 2019, Shared drives access levels).

* Uusien jäsenten oletusrooli

** Avustajan käyttöoikeudella vain lukuoikeus Drive File Streamiin -tiedostoihin.

Jaetun Driven tiedostojen käyttöoikeuspyynnöt menevät tiedoston tekijälle. Mikäli tiedoston luoja ei ole enää jäsenenä, niin pyyntö menee Jaetun Driven Johtajalle. (Google 2019, Shared drives access levels).

4.3 Kehittämistehtävän tutkimustulokset

Tässä tutkimuksessa tutkija käytti aineistonkeruumenetelmänä haastatteluja ja kyselyitä. Tutkittavana kohteena oli kohdeorganisaation työntekijöitä. Haastatteluun valittiin kaksi henkilöä, joka tehtiin verkossa. Kokonaisuudessaan haastattelut nauhoitettiin ja myöhemmin litteroitiin. Kysely lähetettiin henkilökunnalle, johon he vastasivat verkossa. Vastausaikaa annettiinn viikko. Kysymykset tehtiinn osaksi likertin asteikkoa käyttäen. Siinä valintavaihtoehtoja oli yhdestä viiteen, eli ’Ei samaa mieltä’ ja toisena ääripäänä ’Täysin samaa mieltä’. Useaan kohtaan tuli vapaan sanan osio. Ennen kyselyä lähetettiin sähköpostilla saatekirje tulevasta kyselystä ja kerrottiin tutkimuksen aiheesta ja tarkoituksesta. Kyselyyn vastaaminen oli suostumus osallistua tutkimukseen, ellei vastannut, hän ei silloin antanut suostumusta. Myös haastateltaville lähetettiin sähköpostilla saatekirje asiasta, jossa ehdotettiin aikaa, milloin haastattelun voi toteuttaa. Haastattelut tehtiin työajan puitteissa viikon 45 aikana. Samaan aikaan oli kysely käynnissä.

Kyselyn avulla kartoitettiin käyttäjien toiveita uutta pilvipohjaista tallennusjärjestelmää kohtaan. Millaisia toiveita heillä on uudelle kansiorakenteelle? Mikä nykyisessä mallissa toimii ja mikä ei?

Minkä tulisi ehdottomasti muuttua? Mitä työtehtäviä kenelläkin on? Miten tiedon käytettävyyttä voidaan parantaa? ja niin edelleen. Haastattelu tehtiin puolistrukturoituna. Kyselyssä oli tarkoitus kartoittaa myös organisaatiomuutoksen myötä muuttuneita työtehtäviä, jotka vaikuttavat tiedon saantiin ja käytettävyyteen. Kysely luotiin Google Forms -ohjelmalla ja se kohdistettiin 70:lle henkilölle. Tutkija mietti etukäteen, mikäli vastausprosentti jää pieneksi, saadaan tuosta määrästä jo jonkinlainen otos, joka on riittävä. Haastattelussa selvitettiin, miten tämän hetkinen yrityksen sisäinen valvonta ja riskienhallinta on järjestetty sekä tietoturva ja tietosuoja asioiden hoidosta halutaan saada lisätietoa.

Kyselyn ja haastattelun jälkeen aineisto järjestettiin, kumpikin omiin osioihin. Aineisto tarkistettiin, oliko virheellisyyksiä tai puuttuiko vastauksia. Kyselylomake luotiin siten, että likertin asteikolla oleviin kysymyksiin oli vastattava, ennen kuin pääsi etenemään kyselyssä. Kysymyksiä oli vain yksi sivua kohden, jolloin keskittyminen kyseiseen kohtaan oli paras mahdollinen. Aineiston analyysi kannatti aloittaa madollisimman pian aineiston keräämisen jälkeen. Analyysin myötä tutkijalle selvisi, millaisia vastauksia saatiin tutkimusongelmiin. Tutkimuksen tulokset esitettiin kuvina ja taulukoina, joita tulkittiin ja selvitettiin, eli tutkija kertoo omista johtopäätöksistä ja pohdinnoistaan. Kaikki kehittämistyön osapuolet tulkitsevat tutkimusta omalla tavallaan, eli niin tutkimuksen lukija, tutkittava eli haastateltava ja tutkija eli haastattelija. Jokainen tulkitsee tutkimusta ja asioita eri tavalla.

Tässä kehittämistyössä etsitään vastauksia seuraaviin tutkimuskysymyksiin:

- Millaisiin ryhmiin työntekijät jaetaan uutta tallennusjärjestelmää varten?
- Miten tietosuoja ja tietoturva tulisi ottaa huomioon yrityksen pilvipalvelussa?
- Miten organisaation sisäinen valvonta toteutetaan ja riskejä hallitaan esimiehen näkökulmasta?

4.3.1 Kyselyn tulokset

Kysely tehtiin Google Forms -ohjelmalla. Kyselystä tehtiin seitsemän versiota. Kysely osoitettiin kohdeorganisaation henkilökunnalle. Otokseen valittiin 70 vastaajaa, 120 henkilön joukosta. Tämä otos kuvastaa koko populaatiota. Kysely toteutettiin anonyyminä kyselynä, eli vastaajien tietoja ei kerätty. Kyselyyn vastanneita ei voida tunnistaa. Kyselyn aihepiiri koski tietoturvaa ja

pilvipalvelua. Kysely lähetettiin kaikkien ryhmien edustajille, tukitoimien henkilöistä ylemmän johdon henkilöihin ja kaikkiin siltä väliltä. Kysymyksiä oli 27 kappaletta.

Kyselyä varten lähetettiin saatekirje otokseen valituille henkilöille (LIITE 1) 31.10.2019 sähköpostin välityksellä. Viestissä kerrottiin, mitä varten kysely tehdään. Samaan viestiin liitettiin erillisen kyselyn linkki, jonka mukaan ryhmittely tehdään uuden pilvijärjestelmän, Jaetun Driven puolelle. Vastausaikaa kyselyyn oli viikko. Lähes heti, kun saateviesti oli lähetetty, tuli yksi paluuviesti. Siinä eräs vastaanottaja ilmaisi huolensa siirrettävistä tiedostoista. Hänen huolensa oli, että siirrämmekö kaikkien henkilökohtaiset tiedostotkin. Vaikka moni oli lukemassa saateviestin tekstejä ja luotiin monta versiota, kukaan ei huomannut tätä seikkaa. Kaikille kyselyihin valituille henkilöille lähetettiin uusi tarkennusviesti perään. Viestissä kerrottiin, että henkilökohtaisia tiedostoja ei tulla siirtämään, niihin käyttöoikeus pysyy entiseen tapaan.

Kyselyn julkaisemisen alkuvaiheilla tuli myös muutamia yhteydenottoja. Eräs huolehti jo ennakkoon sitä, että sitten kun tiedostojen siirrot tehdään, niin onko kansiot käytettävissä. Toiset työskentelevät myös muulloin kuin niin sanottuun virka-aikaan. Tiedostojen siirroista tiedotetaan etukäteen henkilökuntaa ja siirrot pyritään tekemään hiljaisempaan aikaan. Kyselyyn valituille henkilöille lähetettiin muistutusviesti sähköpostitse edellisenä päivänä ennen kyselyn sulkeutumista. Anonyymiin kyselyyn osallistui 25 henkilöä. Kysely lähetettiin 70 henkilölle. Vastausprosentti oli 35 %. Kysely rakennettiin Google Formsiin siten, että kaikkiin kohtiin oli pakko vastata. Kysymyksiä ei voinut ohittaa. Yleisesti ottaen näkymät oli säädetty niin, että vain yksi kysymys kerrallaan oli näkyvissä. Vastauksia tuli 24 sivun verran ja liikesalaisuuden vuoksi niitä ei voida lisätä tähän työhön liitteeksi.

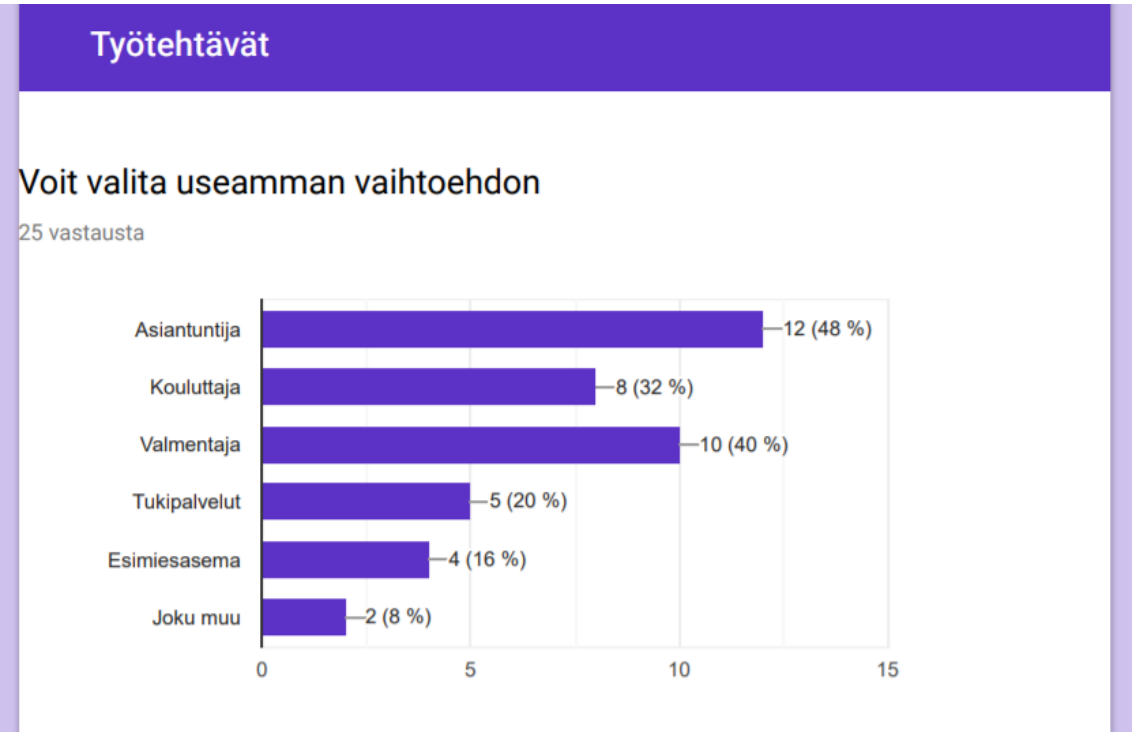
Kyselyn teemat

Taustatiedot

Vastauksia tuli 25 kappaletta. Vastaajista naisia oli 68 %ja miehiä 32 %. Ikähaarukka oli aseteltu 20 vuoden jaksoihin: 20-39, 40-59 ja 60-79. Vastaajista 24 % oli 20-39 vuotiaita, 72 % oli 40-59 vuotiaita ja 4 % oli 60-79 vuotiaita. Tutkinnon tasoa kysyttäessä toisen asteen koulutustausta oli 4 % vastaajista, korkea-aste 28 % vastaajista, ylempi korkea-aste 64 % ja jokin muu oli 4 % vastaajista.

Työtehtävät

Työtehtävä (Kuva 22) osiossa sai valita useamman vaihtoehdon, sillä moni kuuluu useampaan ryhmään. Vaihtoehtoja oli Asiantuntija, Kouluttaja, Valmentaja, Tukipalvelut, Esimiesasema, Joku muu. Alla olevassa kuvassa näkyy jakaumat, kuinka moni 25 henkilöstä kuuluu erilaisiin ryhmiin.



Kuva 22. Työtehtävät.

Oma Drive

Oma Drive osiossa oli kolme kysymystä. Ensimmäisessä kysymyksessä pyydettiin kertomaan **mikä toimii nykyisessä kansiorakenteessa**. Vastaajat kertoivat, että kansioiden nimeäminen hankenumerolla on hyvä malli ja niissä selkeät otsikoinnit alakansioissa. Kehuja sai projektien omat kansiot, jotka on jäsennelty hyvin. Osa kertoi hyvästä toimivuudesta ja olleensa itsekin rakentamassa kansiorakennetta. Jaettujen kansioiden määrä on hallittavissa vielä, kansioiden nimet ja projektikoodit näkyvät selkeästi.

”Mielestäni tämä nykyinen systeemi on ollut ihan ok.”

Helppokäyttöisyys, kokonaisuutena toimii hyvin. Osa kertoi siellä olevan liikaa rönsyjä. Omat tarvittavat kansiot ovat löytyneet. Tieto oikeiden henkilöiden saatavilla. Kunhan muistaa minne on tallentanut materiaalin, on silloin hyvä. Yksilöllistä tietoa voi hukkua, jaottelun puuttuessa. Kansiorakenne on looginen ja hakupalvelu toimii hyvin. Vastausten perusteella suurin osa on tyytyväisiä nykyiseen järjestelmään, kansioiden nimeämistapaan ja tarvittavan tiedon löytymiseen. Osa koki, että löytää tarvittavan tiedon ja kokonaisuus toimii hyvin. Palvelukohtaisia kansiota pidettiin toimivana ratkaisuna.

Toisena kysymyksenä kysyttiin **mikä vastaavasti ei toimi nykyisessä kansiorakenteessa**. Kokonaisuuden hahmottaminen on ollut toisinaan hankalaa. Alakansiot paisuvat melkoisesti, kun jokainen rakentaa omia tiedostoja alakansioihin. Erilaiset tavat nimetä kansioita aiheuttaa epäselvyyttä ja etsintähetkiä tuottaa välillä. Toisen valmentajan materiaaliin ei ole pääsyä. Usein vaikeudet liittyvät kansiorakenteen monimutkaisuuteen ja siihen, että dokumentaatiota on paljon. Korjausehdotuksena oli vuosittain tehtävä arkistointi ja driven siivous. Hankaluutena koettiin, jos kansioita ei nimetä projektinumeron mukaan.

”Toimii, mutta häiritsee saman tiedoston/kansion monenlaiset kopiot. On myös tyhjiä kansioita.”

Tiedon löytämisessä oli vastaajien mielestä vaikeuksia, polut olivat kateissa. Liian pitkistä koulutusten nimistä tuli palautetta. Asiasanalla haettaessa ei välttämättä löydetä oikeita dokumentteja. Siivousta pitäisi tehdä Driveen, osa on vanhentunutta tietoa ja rönsyjä on liikaa. Arkaluonteiselle tiedolle olisi toive saada tallennuspaikka, jos oikeus tulisi olla käyttäjäryhmän ulkopuoliselle henkilölle. Tiedostojen poiston tai siirron voi tehdä kuka tahansa, mutta palautusta ei voi tehdä kukaan muu. Päivitystä, eli tarpeettomien ja vanhentuneiden kansioiden poistamista toivottiin. Oman alueen yhteisiä asioita toivottiin olevan samoissa kansioissa. Osan mielestä tietoa on liian laajan joukon saatavilla. Loogista jaottelua toivottiin eri aihealueisiin. Kansiorakenteeseen toivottiin parannusta, tiedon etsimiseen voi mennä kauankin aikaa.

Kolmantena kysyttiin **millainen kansiojärjestys olisi hyvä uudessa Jaetussa Drivessä**. Vastaajista eräs kertoi, että ylätason järjestys voisi olla esimerkiksi valmennukset, kotoutumiskoulutus ja niin edelleen. Hankekoodia toivottiin jokaisen pääkansion ja alakansion aloitukseen ennen varsinaista tekstiä. Toivottiin yhteisiä käsitteitä kansioiden nimeämiseen. Alakansioiden nimeämiseen toivottiin loogisuutta ja selkeyttä. Olemassa oleva materiaali erikseen, jonka jälkeen projektikansio toimii hyvin. Toivottiin mahdollisimman yksinkertaista ja selkeää kansiorakennetta.

”Toive on, että tarvittavan tiedon voi löytää helposti, mutta ei pääse katsomaan tietoja, jotka eivät ole itselle tarkoitettuja.”

Toiveita oli, että kansiojärjestys menisi aiheiden mukaan, esimerkiksi koulutukset, valmennukset, eri järjestelmien ohjeet ja niin edelleen. Kaikkia koulutuksen asioita toivottiin samaan paikkaan. Kansioiden nimeämistä helposti löydettäväksi toivottiin. Selkeää jakoa kansioihin, eli mitä näkyy kouluttajille ja mitä hallinnolle, sen avulla saisi jaettua kokonaisia kansioita yksittäisien tiedostojen sijaan. Kansiojärjestys ehdotus: palvelut, tarjoukset, henkilöstö, opiskelijat. Työtehtävien mukaista jaottelua toivottiin.

Tietoturva

Tietoturva osiossa kysyttiin 15 kysymystä. Seuraavassa ensimmäinen kysymys, **onko sinulla selvillä yrityksemme tietoturvalinjaukset ja toimintaohjeet?** Vastaajista 92 % eli 23 henkilöä vastasi kyllä ja 8 % eli 2 henkilöä vastasi, että ei ole selvillä. Eli vastaajista lähes kaikki kahta lukuunottamatta tiesivät yrityksen tietoturvalinjaukset ja toimintaohjeet.

Toisessa kohdassa **pyydettiin kuvailemaan tarkemmin**. Kansioiden jakoa saa tehdä vain tarvekohtaisesti, kaikki materiaalit ovat yrityksen omaisuutta. Nimilistoja ei saa olla esillä paperisena tai sähköisessä muodossa tietoturvasyistä. Zoho kirjauksiin on annettu hyvät ohjeet. Eräs kertoo olleensa hyväksymässä ohjeistusta. Tietosuojapolitiikan voi tarkistaa laatusivustolta. Laatusivustoa nostetaan useammassa vastauksessa esille.

”Ohjeet ovat pääasiassa selvät. Aikoinaan niistä pidettiin koulutus, joskin samansisältöisen koulutuspäivän voisi pitää uudestaankin.”

Osa toivoo, että näitä asioita tulisi kerrata sopivin väliajoin tiivistetysti. Vastaajien keskuudessa on tiedossa, keneen otetaan yhteyttä, jos ongelmia ilmenee, perehdytyksessä on asioista kerrottu. Osa vastaavasti kertoi, ettei tiedä asioista ja ettei ole perehdytetty. Osa kertoi, että tietoturva asioita käydään läpi säännöllisesti, kvartaaleittain.

Johtopäätöksenä vastauksista voisi päätellä, että esimiestiimille sekä johtoryhmän henkilöille tietoturva-asiat ovat selkeämmin tiedossa kuin muille. Moni toivoo saavansa säännöllisin väliajoinpienen koulutuksen tai muistutuksen tietoturva asioista. Ohjeistuksen todetaan olevan kunnossa Laatusivustolla, kaikki eivät tosin näytä löytävän sinne. Kerran tai pari vuoteen sellainen tiivis tietoisku työntekijöille voisi olla paikallaan. Ajankohtaisia nostoja voisi tehdä aina tarpeen mukaan.

Kolmantena kysyttiin, **pystyykö ohjeita noudattamaan**. Vastaajista 96 % eli 24 henkilöä vastasi ’kyllä ja yksi henkilö eli 4 % vastasi ’ei’. Seuraavassa osiossa pyydettiin kuvailemaan mikä on ohjeiden noudattamisen onnistumisen esteenä. Aika moni vastaajista kertoi, ettei osaa sanoa tai vastasi pelkällä viivalla tai kysymysmerkillä. Moni vastasi, ettei ole kohdannut ohjeiden noudattamisessa esteitä. Perehdytyksen puutetta oli vastauksissa myös. Eräs vastasi, että ”Jos ei tiedä, niin se on jo esteenä toimiiko oikein vai ei”. Toisille tietoturvan taso näyttäytyy riittävänä.

Ohjeiden noudattamisen esteenä nousi esille seuraavia asioita:

- Nimilistojen kerääminen on pakollista, koska olemme hajautetussa organisaatiossa, on niiden tietoturvallinen hävittäminen toisinaan haasteellista.

- Arkaluontoisten asioiden kirjaamisesta toivotaan, että sovittaisiin etukäteen, miten ne tehdään.

- Uudet työntekijät eivät omaksu näitä tietoturva asioita alkuvaiheessa, eikä ne nousekaan heti esille. Kokeneilla vastaavasti on tilanne, että uusien toimintatapojen oppiminen pelkkien kirjallisten ohjeiden perusteella ei ole todennäköistä.

- Drivessä toivotaan pääsyä vain niihin kansioihin, joita työssään tarvitsee, ettei tarvitse päästä niin sanottuun ylimääräiseen tietoon. Tärkeänä pidetään, että asiakkaasta ei kerätä turhaa tietoa. Kirjauksia kannattaisi tehdä muulloin kuin asiakkaan aikana, jolloin 100 % tietosuoja saavutettaisiin. Onnistumisen takaa tarkkuus ja huolellisuus.

- Kiireessä ei aina muisteta millaisia asioita pitäisi tallentaa järjestelmiin.

- Laatusivustolla olevia ohjeita ei pidetä samana asiana kuin perehdyttäminen. Itse perehdyttäjäkin voi olla tietämätön ohjeistuksista.

Edellä mainitut kohdat ovat hyviä nostoja, joihin tulee puuttua. Tietoturvasta pitää jatkossa puhua useammin tiimeissä. Perehdytyksessä näihin tietoturva asioihin tulisi ottaa entistä paremmin kantaa. Perehdyttäjän tulisi muistaa kertoa käytänteistä ja kertoa mistä lisää ohjeita löytyy, eli yrityksen Laatusivustolta.

Seuraavissa osioissa kysyttiin, **onko tietoturvan ohjeet helposti saatavilla**. Vastaajista 76 % eli 19 henkilöä vastasi ’kyllä’ ja 24 % eli 6 henkilöä vastasi ’ei’. Kysymykseen onko tietoturva ohjeet **riittävän selkeät**, vastaajista 80 % eli 20 henkilöä vastasi ’kyllä’ ja 20 % eli 5 henkilöä vastasi ’ei’.

Kysyttäessä onko tietoturva ohjeet **ajan tasalla**, ’kyllä’ vastasi 84 % eli 21 henkilöä ja ’ei’ vastasi 16 % eli 4 henkilöä.

Edellä mainituista kohdista **pyydettiin kuvailemaan tarkemmin, eli tietoturva ohjeistuksen saatavuudesta, selkeydestä ja ajan tasaisuudesta**. Yleisesti koettiin, että tietoa löytyy hyvin yrityksen laatusivustolta, G+ -sivustolta ja it-puolen ihmisiltä saa apua. Koettiin, että ICT-ryhmä pitää huolen tietojen ajantasaisuudesta.

”Mielestäni ohjeet ovat helposti saatavilla, selkeät ja ajantasaiset.”

Eräs vastaajista muistaa lukeneensa tietoturva asioista, mutta ei enää muista mistä ohjeet löytyvät. Toivottiin linkkiä Tietosuojaselosteesta Laatusivustolle, seloste löytyy yrityksen kotisivuilta. Eräs ei tiennyt onko ohjeet ajan tasalla, luottaa kuitenkin, että ne ovat. Tietoturvakäytännöt ovat selkeät, tietosuojapolitiikka ei ole, joten sitä ei tule luettua. Jotkut eivät ole löytäneet ohjeita. Näiden tietojen hakuun joku käyttää laatusivustoa. Mietintää aiheuttaa sähköisitä rekistereistä tuhoamisen tapa ja käytön rajaaminen oikeutetuille henkilöille.

Tästä johtopäätöksenä voidaan sanoa, että osalle ohjeistuksen sisältö ja niiden sijainti on hyvinkin selvillä, osa taas on hieman epävarma mistä tietoa saa ja onko se ajan tasalla. Tähän epäselvyyteen auttaisi pienet tietoturva koulutukset ja käytäntöjen kertaamiset. Ohjeistuksen koetaan olevan ajan tasalla, joten ohjaus niiden äärelle on paikallaan. Henkilökunnalle pienimuotoinen perehdytys asiaan korjaa epäselvyytenä olevat asiat.

Seuraavassa kysymyksessä kysyttiin, **millaisia ohjeita kaipaa tietoturvasta**. Vastaajista eräs toivoi yhteistä koulutuspäivää, jotkut pitivät hyvänä nykyisiä IT-vinkkejä, joka on hyvä kanava saada hyviä arjen ohjeita. Vastaajat toivoivat todella ytimekkäitä, kannustavia, selkeitä ja helppoja ohjeita. Moni oli jättänyt vastaamatta tai ei osannut sanoa. Nykyisiä ohjeita pidettiin hyvänä joidenkin mielestä. Vastaamatta jättäminen tapahtui (-) viiva- tai (?) kysymys -merkillä.

Vastaajilla nousi esille seuraavanlaisia kysymyksiä:

- Miten toimitaan, jos asiakas pyytää nähtäväksi, mitä tietoja hänestä on kirjattu?
- Jos joku toinen taho tiedustelee opiskelijan tietoja, mitä tietoja saa antaa?
- Kuinka lähetetään salaista postia?

Yksi vastaajista oli käynyt lukemassa muistin virkistämiseksi ohjeistuksen juuri, hän ei tarvitse enää mitään tietoa. Moni vastaajista toivoi lyhyttä käyttökoulutusta ja tai perehdytystä aina silloin tällöin. Kansiorakenteen pohdintaa täytyy erään vastaaja mielestä käydä säännöllisin väliajoin, kuka näkee mitä ja kenelle tieto on olennaista.

Yrityksessä lähetetään viikon IT-vinkkejä henkilökunnalle henkilöstökanavalle. Vinkeissä kerrotaan pieniä ohjeita arjen työskentelyä helpottamaan. Niistä on pidetty ja niiden toimittamista kannattaa jatkaa jatkossakin. Ohjeistusta koetaan olevan, mutta pienimuotinen koulutuksen tarve nousee tässäkin osiossa esille. Vastaajien heräämiin kysymyksiin tulee etsiä vastaukset ja tiedottaa niistä vaikka juuri IT-vinkkien muodossa.

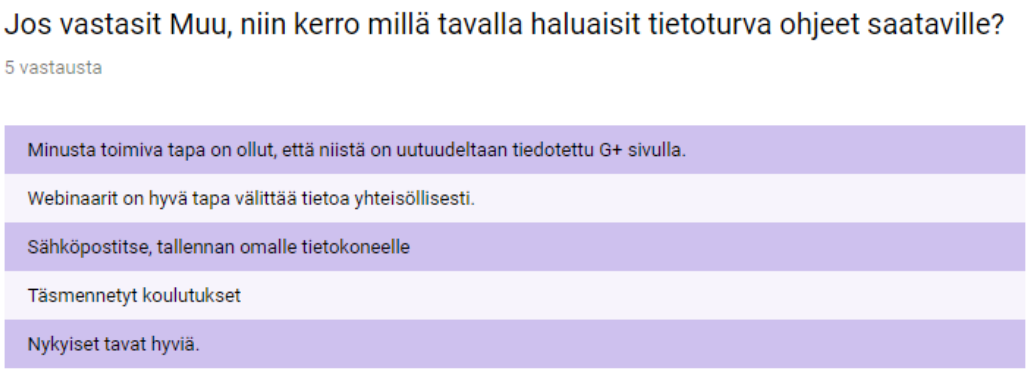
Seuraavassa kysymyksessä kysyttiin, **mistä saa tietoa tietoturva asioissa**. Useampi vastaaja vastasi, että Laatusivustolta, esimiehiltä ja tietohallinnolta. Tietohallinto johtajan kerrotaan pitäneen hyviä webinaareja asiasta. ”Yrityksen osalta tietohallinto, joskus myös toimisto ja esimiehet sekä kollegat. Yleisen tason asioissa internet.” Tässä osiossa oltiin aika yksimielisiä. Tietoa osataan kysyä, kun sitä tarvitaan.

Seuraavaksi kysyttiin, **miten haluaisi tietoturva -ohjeita saada** (Kuva 23). Alla olevassa kuvassa näkyy valittavana olleet kohdat. Tässä osiossa sai valita useamman vaihtoehdon. Valmiit vaihtoehdot olivat: Intrasta, Palavereista, Esimieheltä, Videotallenteina, Viikon IT-vinkkinä, Kysymällä toimistolta sähköpostitse, Kysymällä toimistolta soittamalla, Muu.

Kuva 23. Tietoturva -ohjeiden saatavuus toiveet.

Vastaajat saivat valita useamman vaihtoehdon. Tietoa halutaan vastausten mukaan saada ensisijaisesti Intrasta. Palavereiden ja esimiesten kautta tietoa haluttiin saada jaetun toisen sijan verran ja kolmanneksi toivotuin vaihtoehto oli viikon IT-vinkkinä. Neljännelle sijalle tuli videotallenne, viidennelle toimistolta kysymällä sähköpostilla. Loppujen järjestys meni kysymällä toimistolta soittamalla, G+, webinaarit, todella lyhyt opas, täsmennetyt koulutukset voisivat toimia, Googlaamalla.

Alla olevassa kuvassa (Kuva 24) on toiveet, miten muuten toivoisi ohjeita tietoturvasta saavan. Tähän tuli viisi vastausta ja vastaaminen tähän oli vapaaehtoista.



Kuva 24. Toiveet muusta ohjeiden saantitavasta.

Kysyttäessä **miten tärkeänä tietoturvallisuutta pidetään yrityksessä**, käytettiin likertin asteikkoa. Vastausvaihtoehdot olivat: 1 = ei lainkaan, 2 = vähän tärkeänä, 3 = en osaa sanoa, 4 = melko tärkeänä, 5 = tärkeänä. Vastaajista 52 % eli 13 henkilöä kertoi pitävänsä tärkeänä. Melko tärkeänä piti vastaajista 40 % eli 10 henkilöä ja 8 % eli 2 vastaajaa ei osannut sanoa. Yleisesti ottaen vastaajat olivat sitä mieltä, että tietoturva-asiat ovat yritykselle tärkeitä.

Seuraavassa kohdassa kysyttiin **auttaako tietoturvavaatimukset päivittäisessä työssäsi** (Kuva 25). Likertin asteikolla vastausvaihtoehdot olivat: 1 = ei lainkaan, 2 = vähän, 3 = en osaa sanoa, 4 = melko paljon, 5 = paljon. Vastaajista 2 eli 8 % oli sitä mieltä, että ei lainkaan auta. Yksi vastaaja eli 4 % oli valinnut, että vähän auttaa. Vastaajista 8 eli 32 % ei osannut sanoa. Vastaajista 9 henkilöä eli 36 % kertoi, että melko paljon on apua. Vastaajista 5 henkilöä, eli 20 % vastasi, että on paljon apua. Yllättävän moni vastasi, ettei osaa sanoa onko apua tietoturvasta päivittäisessä

työssä, lähes joka kolmas (32 %). Suurin osa kuitenkin vastasi, että on tietoturvavaatimuksista melko paljon hyötyä.

Kuva 25. Tietoturvasta apua päivittäisessä työssä. (1 = ei lainkaan – 5 = paljon)

Vastaavasti kysyttäessä **haittaako tietoturvavaatimukset päivittäisessä työssä**, 7 vastaajista eli 28 % vastasi, että ei haittaa. Tässä osiossa käytettiin myös likertin asteikkoa: 1 = ei lainkaan, 2 = vähän, 3 = en osaa sanoa, 4 = melko paljon, 5 = paljon. Vastaajista 11 eli 44 % vastasi, että haittaa vähän. Vastaajista 5 eli 20 % vastasi, ettei osaa sanoa. 2 vastaajaa eli 8 % kertoi tietoturvavaatimusten haittaavan melko paljon. Kukaan ei valinnut vaihtoehtoa paljon. Yhteenvetona voidaan sanoa, että vastaajia tietoturvavaatimukset haittaavat päivittäisessä työssä vähän.

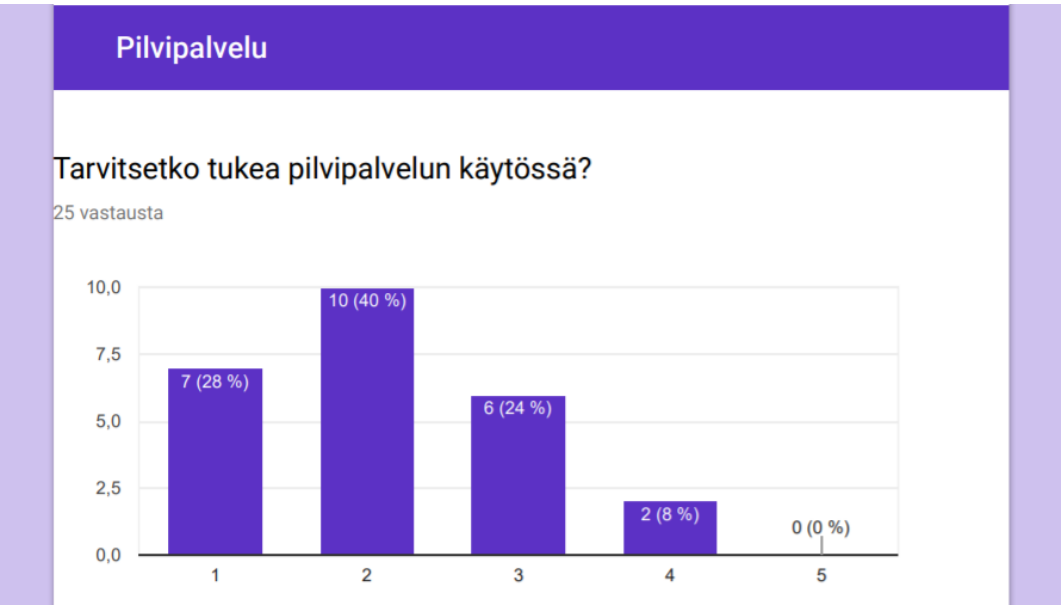
Seuraavana kyselyssä kysyttiin, **mitä pitää vakavimpana tietoturvaongelmana työssään**. 25 vastaajan joukossa oli kaksi tyhjää vastausta. Vakavimpina tietoturvaongelmina pidettiin seuraavanlaisia asioita; mahdolliset tietoturvamurrot, Driven kansiorakenteen käyttöoikeuksista, sähköpostin lähettämistä väärälle vastaanottajalle osoitteiden automaattitäytön johdosta, henkilötietojen antamista puhelimitse, henkilötietolistausten poistaminen käytön jälkeen, koneen katoaminen, tunnusten hakkeroiminen, huolimattomuudesta tapahtuvia vahinkoja.

”En osaa sanoa. Ehkä tässä olisi koulutuksen paikka! Henkilöstöä voisi olla hyvä kouluttaa aktiivisesti havaitsemaan tietoturvaongelmia eikä vain opettelemaan sääntöjä.”

Osa ei tiedä onko Jump Cloud toiminnassa koneella, joku ei tiedä saako Exceliä käyttää, Googlen Driveä ei pidetty turvallisena ympäristönä. Vakavana pidettiin myös sitä, jos pomo kopioi työsi ja ottaa kunnian. Eräs vastasi, että vakavimpana tietoturvaongelmana pitää työssään enemmänkin tapaa tehdä työtä kuin järjestelmiä, kuten vaitiolovelvollisuuden rikkomista, asiakkaan henkilökohtaisien asioiden ja yrityssalaisuuksien vuotamista. Yrityksen kriittisiin tietoihin murtautumista pidettiin myös vakavana. Edellä kuvaillut huolet ovat todellisia. Työryhmässä mietimme vastauksia myös näihin, mitä tietoturva koulutus pitää sisällän. Selkäesti tilausta ja tarvetta on tietoturvaan liittyvään koulutukseen. Sellaisen henkilökunta tulee saamaan.

Pilvipalvelu

Pilvipalveluosion ensimmäinen kysymys oli, **tarvitseeko tukea pilvipalvelun käytössä** (Kuva 26). Likertin asteikkoa käytettiin tässäkin kysymyksessä seuraavasti: 1 = en lainkaan, 2 = vähän, 3 = jonkin verran, 4 = melko paljon, 5 = paljon. Vastaajista 7 eli 28 % ei tarvitse tukea, 10 vastaajaa eli 40 % kertoi tarvitsevansa vähän tukea. Vastaajista 6 eli 24 % kertoi tarvitsevansa jonkin verran tukea ja 2 vastaajaa eli 8 % kertoi tarvitsevansa melko paljon tukea. Kukaan ei vastannut, että tarvitsisi paljon tukea pilvipalvelun käytössä. Pilvipalvelun käyttöön ei tukea paljon tarvita vastaajien mukaan. Seuraavassa kuva auttaa havainnollistamaan vastauksia.



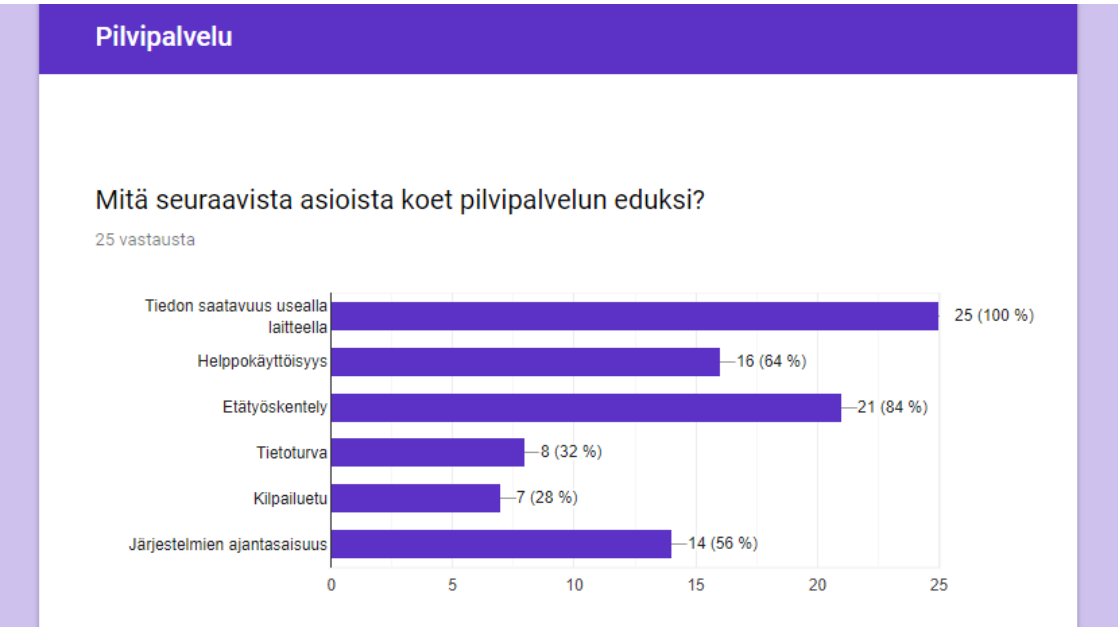
Kuva 26. Tuen tarve pilvipalveluiden käytössä (1 = en lainkaan – 5 = paljon).

Seuraavassa kysymyksessä kysyttiin, **millaista tukea tarvitsee**. Kaksi vastausta oli tyhjää. Vastaajista viisi tiesi sanoa, ettei tarvitse tukea. Joku kertoi tarvinneensa alussa tukea ja oli myös sitä saanut. Eräs vastaajista toivoi vinkkejä nopeaan käyttöön, joku toivoi perehdytystä, uusista toiminnoista toivottiin tukea saavan, osa tietää kenen puoleen kääntyä tukea tarvitessaan.

”Esim googlen palvelut ovat niin laajat ja ne kehittyy koko ajan, oma aika ei riitä perehtymään omaaloitteisesti kaikkiin mahdollisuuksiin, jotka todennäköisesti helpottaisivat työtäni. Työntekijöille toivoisin että meillä olisi säännöllinen verkkotuki tyyliin kerran kuussa jonne työntekijät voivat tulla tuomaan it pulmiaan ja oppimaan. Näihin haasteisiin törmää viikoittain, missä tapauksessa tiedoston oikeasti voi siirtää toiseen paikkaan drivessä, milloin siitä pitää tehdä kopio, jonka voi siirtää, miten tehdään kysely, miten siihen lisätään kuva, miten tehdään ilmoitustaulu, miten annat käyttöoikeuksia jne... Aiheita riittää. Voin tehdä sisällöt puoleksi vuodeksi :)”

Tämänkin osion päätoive on, että saadaan koulutusta säännöllisin väliajoin tietoturvasta. Koulutuksen ei tarvitse olla massiivista, eikä pitkäkestoista yhdellä kerralla. Vaan pieniä tärkeitä nostoja keskeisistä asioista.

Seuraavaksi kysyttiin, **mitä seuraavista asioista kokee pilvipalvelun eduksi** (Kuva 27). Vastaajalla oli mahdollista valita useampi vaihtoehto. Jokainen vastaaja oli valinnut pilvipalvelun tärkeimmäksi eduksi tiedon saatavuuden usealla laitteella. Seuraavaksi tärkeimmäksi nousi etätyöskentely, helppokäyttöisyys, järjestelmien ajantasaisuus, tietoturva ja viimeiseksi valittiin kilpailuetu.



Kuva 27. Pilvipalvelun etuja.

Seuraavassa osiossa kysyttiin, **onko ollut huolissaan pilvipalvelun tietoturvasta** (Kuva 28). Likertin asteikolla: 1 = en lainkaan, 2 = vähän, 3 = jonkin verran, 4 = melko paljon, 5 = paljon. Vastaajista 9 eli 36 % ei ole lainkaan huolissaan ollut pilvipalvelun tietoturvasta. Vastaajista 7 eli 28 % sen sijaan on vähän huolissaan ollut. Vastaajista 4 eli 16 % on ollut jonkin verran huolissaan ja 5 henkilöä eli 20 % on melko paljon huolissaan ollut. Eli viidennes on ollut huolissaan melko paljon yrityksen pilvipalvelun tietoturvasta. Alla olevassa kuvassa on vastauksien määrä.

Kuva 28. Pilvipalvelun tietoturva (1 = en lainkaan – 5 = paljon).

Seuraavaksi kysyttiin, **millaisissa tilanteissa olet ollut huolissaan pilvipalvelun tietoturvasta**. Eli aiempaan kohtaan viitaten vastaajat saivat avata hieman tilanteita, joissa huolta on esiintynyt.

”Joskus mietin, että onko jaettujen kansioiden lukuoikeudet kohdillaan.”

”Tänään viimeksi kaivoin tiedostoja roskakorista drivessä kun työntekijä oli poistanut kaikki....”

Suurin osa vastaajista oli kuitenkin kirjallisessa kommentoinnissa sitä mieltä, että ei ole huolissaan pilvipalveluiden tietoturvasta. Muutama vastaaja nosti esille huolen, että aina on pieni riski tietomurtoon, joku voi poistaa vahingossa tietoja, henkilötietojen osalta oltiin huolissaan, poistuvien työntekijöiden, kansioiden jakojen ja tiedostojen oikeuksista oltiin huolissaan. Tässä nousee esille

se, että tiedostoja voi poistaa kuka tahansa, kun tiedostot omistaa henkilö nykyisen pilvipalvelujärjestelmän puolella. Tämän vuoksi myös muutosta tehdään, että yksittäinen henkilö ei voi tietoja poistaa uuden järjestelmän puolella.

Seuraavassa kysyttiin, **onko pilvipalvelun käytön turvallisuutta lisätty seuraavilla asioilla**: Työntekijöiden koulutuksella, Teknologialla, Prosesseilla, Muu? Kaksi ensimmäistä vaihtoehtoa saivat saman verran vastauksia, eli 12 kummassakin. Prossin oli valinnut 10 vastaajaa ja muun vaihtoehdon 4 henkilöä. Tässä osiossa pystyi valitsemaan useamman vaihtoehdon. Kysyttäessä **millä muulla tavoin pilvipalvelun käytön turvallisuutta on lisätty**, moni vastasi, ettei tiedä. Tyhjiäkin vastauksia oli. Henkilökunnan koulutus nousi jälleen esille vastauksissa. Vastaukseksi tuli, että tietoturvallisuuden lisäystä on tehty kaksivaiheisella kirjautumisella, sopimuksilla, esimies on käynyt asioita läpi, koneet on vahvasti suojatut ja tiedon rajaamista on tehty.

Viimeisenä kysymyksenä kysyttiin, onko **muuta kommentoitavaa pilvipalvelun käytöstä**. Monilla ei ollut enää kommentoitavaa. Pilvipalvelu koettiin tärkeäksi osaksi työskentelyä ja se mahdollistaa joustavan työskentelyn useammalla laitteella eri paikoissa. Joltakin vastaajalta oli evätty pääsy joihinkin kansioihin. Tiedonkeruukäytänteitä toivottiin yhteneistettävän. Joku halusi lomakalenterin selkeälle paikalle. Pilvipalvelua kehuttiin nykyaikaiseksi ja käteväksi systeemiksi. ”Hienoa että asian kehittämistä pohditaan, mielestäni meillä on jo nyt varsin toimivalla tasolla olevia ominaisuuksia pilvipalveluissa.” Lopuksi vielä tutkijan mieltä piristävä kommentti ” Kiitos Taina kun teet tätä!”

Otos, eli nämä kyselyyn vastaajat edustavat vastauksillaan koko populaatiota, eli kohdeorganisaatiota. Tutkimuskysymykseen *Miten tietosuoja ja tietoturva tulisi ottaa huomioon yrityksen pilvipalvelussa?* saatiin vastaus. Vastauksista nousi hyvin esille teoriaviitekehyksessä läpikäytyjä asioita. Johtopäätöksenä voi vetää, että yleisesti ottaen yrityksessä tietoturvaan liittyvä ohjeistus on olemassa, ajan tasalla ja seurantaa tehdään muun muassa tietoturvapoikkeamista. Asia, joka vaatii muutosta, on tiedon jalkauttaminen ja tietoon saattaminen henkilökunnalle. Esimies ja johtoryhmä tasolla oltiin hyvin valveutuneita tietoturvallisuuteen liittyvissä asioissa. He käyvätkin niitä kokouksissaan läpi useasti vuodessa. Muut työntekijät sen sijaan tunsivat epävarmuutta järjestelmien käytössä ja tiedon löytämisessä. Koettiin, että on tiedossa, että tietoa on jossain olemassa, mutta sitä ei löydetty.

Tilanteen parantamiseksi tulisi pitää pieniä koulutustuokioita tietoturvasta useamman kerran vuodessa. Työntekijät tarvitsevat muistutusta mistä ohjeita ja toimintoja löytyy. Työtapojen ker-

taus on myös paikallaan. Moni tiimi kokoontuu viikoittain. Niissä voisi esimerkiksi kerran kuukaudessa tehdä muutamia nostoja tärkeistä asioista. Ottaa palaveriin pienen hetken aikaa ja kysyy, onko jotain epäselviä asioita, joihin kaipaa apua. Pienillä muutoksilla saisi työntekijöiden osaamista lisättyä ja työn sujuvuutta parannettua. Uudelta järjestelmältä odotetaan sitä, ettei tietoa ole saatavilla niin laajoina asiakokonaisuuksina, kuin sitä tällä hetkellä on.

4.3.2 Haastattelun tulokset

Kehittämistyötä varten tehtiin teemahaastattelu kahdelle henkilölle. Opinnäytetyön suunnittelun alkuvaiheessa haastateltavia oli tarkoitus ottaa enemmänkin. Kysymykset muotoutuivat niin, että haastateltaville lähetettiin ennen haastattelua pienimuotoinen taustakysely Google Formsin kautta ja erikseen tehtiin teemahaastattelu Adobe Connection -ohjelmalla. Kysymyspatteriston valmistuttua sen pohjalta, mitä tietoa haluttiin haastatteluiden avulla saada selvitettyä, karsiutui haastateltavien joukko varsin pieneen määrään, kahteen henkilöön. Haastattelun kysymykset olivat sen luonteisia, ettei niihin olisi kaikilta haastatteluun aiotuilta henkilöiltä saatu vastausta, jotka olisi hyödyntäneet tätä kehittämistyötä. Haastateltavien valinta tapahtui sen mukaan, mikä oli tehtävänkuva organisaatiossa. Heiltä odotettiin saatavan eniten vastauksia haastattelukysymyksiin.

Taustakysely haastateltaville

Ennen haastattelua, haastateltaville lähetettiin pienimuotoinen taustakysely koskien riskienhallintaa. Kysely toteutettiin Google Forms -ohjelmalla. Riskienhallintaosiota oli neljä, kysymyksiä oli yhteensä 14 kappaletta ja lisäksi 4 avointa kohtaa jokaisen osion perässä. Kysymyksissä oli kolme vastausvaihtoehtoa; Kyllä/Ei/En tiedä. Korjausehdotuksena taustakyselyyn tuli lisätä vaihtoehto ’en tiedä’. Taustakysymykset riskienhallinnasta haastateltaville (LIITE 6). Avoimiin kommentti -kenttiin ei tullut vastauksia. Vaihtoehtokysymyksissä oli pääosin yhteneväisiä vastauksia.

Ensimmäisessä osiossa kysyttiin, onko yrityksessä tehty riskikartoitusta, jossa on tunnistettu ja arvioitu tietojärjestelmien riskitekijöitä. Vastaajien mukaan on tehty. Toiminnan riskitekijöistä, kuten ostopalvelujen vaikuttavuutta uhkaavista tekijöistä, kuten laadusta, asiakastyytyväisyydestä ja saatavuudesta, vastaajat olivat eri mieltä, toisen mukaan on tehty ja toinen ei tiennyt. Toiminnan tuottavuutta sekä taloudellisuutta uhkaavista tekijöistä vastaajat olivat samaa mieltä,

että riskikartoitus on tehty. Lain- ja hyvä hallintotavat mukaisuutta uhkaavista tekijöistä toiminnassa vastaajilla ei ollut tietoa. Sen sijaan eri mieltä vastaajat olivat toiminnan edellyttämien koneiden, laitteiden ja tilojen toimivuutta uhkaavista tekijöistä, toinen vastasi ’kyllä’ ja toinen ’ei’.

Henkilöstöön liittyvistä riskitekijöistä kysyttiin, onko avainasemassa oleville henkilöille nimetty varahenkilöt, vastaajista toinen vastasi ’kyllä’ ja toinen ’ei’. Tässä kohtaa olisi syytä käydä johtoryhmässä läpi käytänteitä ja kirjata poissaolojen varalle toimintaohjeet ja avainasemassa oleville varahenkilöiden nimet. Henkilöstön poissaolo seurannasta vastaajat olivat samaa mieltä, eli he vastasivat ’kyllä’.

Investointeihin liittyvissä riskitekijöissä kysyttiin, onko investointihankkeiden suunnittelulla riittävä kytkentä taloudelliseen liikkumavaraan eri aikajänteillä. Vastaajista toinen ei tiennyt ja toinen vastasi kyllä. Ilmeisesti toinen vastaajista ei ole tekemässä investointeihin liittyviä suunnitelmia, kun vastasi ’en tiedä’. Myöntävästi vastattiin kysymykseen, onko sopimusten ja kustannusarvioiden toteutumisen seuranta, toiminnallisen etenemisen, muutoksiin reagointi ja niiden hyväksyminen systemaattista. Tämä osio investointien riskitekijöistä on toimivaa.

Viimeinen osio taustakysymyksissä oli tietojärjestelmiin ja tietoturvaan liittyvistä riskitekijöistä. Ensimmäinen kysymys oli, että onko varmistettu tietojärjestelmien käytettävyys, tiedon oikeellisuus ja häiriöttömyys. Toinen kysymys oli, onko toiminnan julkisuuden ja hyvän tiedonhallintatavan toteutuminen, kuten rekisteriselosteiden laadinta ohjeistettu. Kolmantena kysyttiin, onko salasana- ja käyttöoikeushallinnan menettelyt ohjeistettu. Viimeisenä kysymyksenä kysyttiin, onko tietosuojaan ja tietoturvaan liittyvät riskit arvioitu. Kaikkiin tämän osion kysymyksiin vastaajat vastasivat kyllä. Eli nämä riskitekijät oli otettu huomioon, ohjeistus on kunnossa ja riskit on arvioitu vastaajien mielestä.

Teemahaastattelu

Haastattelut tehtiin viikolla 45 Adobe Connection -ohjelman avulla, jolla saatiin tallennettua haastattelut. Yhteen haastatteluun oli varattu aikaa noin 30 minuuttia. Haastattelukysymykset toimitettiin haastateltaville ennakkoon edellisenä päivänä. Tallennus onnistui ensimmäisillä kerroilla, uusintoja ei tarvinnut tehdä. Huomionarvoista oli se, jos opinnäytetyö olisi luettu ennen haastatteluita, olisi vastaukset olleet toisenlaisia. Haastattelun teemojen osilta teoriaviitekehys oli lähestulkoon valmis kuukautta ennen haastatteluita. Opinnäytetyö oli ollut luettavissa haastateltavilla. Kysymyksiä esitettiin kummallekin haastateltavalle 13 kappaletta. Ensimmäisen haastattelun

kesto oli 15.27 minuuttia ja toisen haastattelun kesto oli 18.32 minuuttia. Arvioitu ja varattu aika riittivät hyvin haastatteluiden pitoon. Haastattelun kysymykset ovat liitteenä (LIITE 7). Kysymyspatteristoa hiottiin useaan otteeseen, luultavasti 7. versio sai hyväksynnän ohjaavalta opettajalta. Haastateltavilta sai kiitettävästi tietoa kehittämistyötä varten.

Haastatteluiden tallenteet litteroitiin, joka vei yllättävän paljon aikaa. Litterointiin käytettiin yleislitteroinnin mallia, johon ei kirjattu ylös äänähdyksiä. Joka kerta, kun klikkasi tauko -nappia Adobe Connectiossa, pysäytys vei kolme sanaa pois, eli joka kerta joutui kelaamaan äänitettä taaksepäin jatkaakseen. Litterointi eteni hitaasti, mutta varmasti. Litteroidut tekstit, eli alkuperäis ilmaukset, sisälsivät loppujen lopuksi niin paljon liikesalaisuuksia, ettei niitä voitu lisätä liitteeksi opinnäytetyöhön. Ohjaava opettaja sai työt luettavaksi. Kummankin litteroinnin pituus oli neljä sivua Word tekstiä, eli kahdeksan sivua vastauksia yhteensä (sisältäen kysymykset). Tietoa tuli erittäin hyvin, joten kysymysten asettelu onnistui ja vastauksia saatiin varsin kattavasti.

Litteroinnin valmistuttua aineisto siirrettiin Exceliin, jonne rakennettiin taulukko sisällönanalyysiä varten (Taulukko 6). Sisällönanalyysissä ensimmäiseen sarakkeeseen kerättiin raakateksti, eli perus ilmaukset. Toiseen sarakkeeseen muodostettiin pelkistetty ilmaus raakatekstistä. Alaluokkaan laitettiin typistettynä pelkistetyn ilmauksen sisältö ja yläluokkaan laitettiin asiasana tai -sanoja kuvaamaan alaluokka tiivistetysti. Yleistys sarakkeeseen kerättiin teeman mukaiseen jaotteluun Yläluokassa eniten toistuva sana. Haastattelussa oli kysymyksiä neljästä teemasta: tietoturvasta, pilvipalvelusta, sisäisestä valvonnasta ja riskienhallinnasta. Alla olevassa taulukossa on näkymä sisällönanalyysistä. Tällä tyylillä litteroitu aineisto käytiin läpi. Kaikista kohdista ei Yleistys -sarakkeeseen asia -sanaa tullut. Havainnollistavaa kuvaa varten taulukosta on poistettu raakateksti anonymisoinnin vuoksi ja ettei liikesalaisuuden piiriin kuuluvia asioita tule ilmi. Litteroidusta tekstistä tulisi hyvin ilmi haastateltavan henkilöllisyys, jos sanatarkka vastaus olisi nähtävillä. Haastatteluiden vastauksista on tunnistettavissa henkilöllisyys, joten myös sen vuoksi litteroituja tekstejä ei voida liittää työhön.

	A	B	C	D	E	F
1	SISÄLLÖNANALYYSI x			Haastattelu x		13.11.2019
2						
3		RAAKATEKSTI	PELKISTETTY ILMAUS	ALALUOKKA	YLÄLUOKKA	YLEISTYS
4	**Tietoturva**					
5		Litteroitu teksti, perus ilmaus.	Tietosuojaan liittyvä uudistus tehtiin osana GDPR projektia keväällä 2018. Tietoturvan nykytilanne on kohtalaisen hyvässä mallissa.	Tietosuojan GDPR projekti keväällä 2018. Tietoturva hyvällä mallilla.	Tietosuoja. Tietoturva.	Tietoturva.
6						

Taulukko 6. Sisällönanalyysi.

Yleistetyt ilmaukset olivat ensimmäisessä sisällönanalyysissä: Tietoturva, Perehdytys, Palvelukatkos, Pilvipalvelu, Työssäjaksaminen, Työtyytyväisyyskyselyn tulokset ja Riskienhallinta. Toisessa sisällönanalyysissä ilmaukset olivat: Tietoturva, Pilvipalvelu, Työtyytyväisyys, Riskit ja Toimintamalli. Yhteneväiset ilmaukset toistuivat kummassakin aineistossa. Yleistetyt ilmaukset peilautuvat teoriaan erittäin hyvin. Teoriassa on käsitelty tietoturvaa, riskienhallintaa, johon toimintamallit liittyvät. Pilvipalvelua, sekä siihen liittyvää palvelukatkosta. Sisäisen valvonnan teoriaan kuuluu työtyytyväisyys ja työssäjaksaminen. Abstrahointi eli pelkistäminen sujui luontevasti, eli tietoturva, riskienhallinta, pilvipalvelu ja sisäinen valvonta tulivat tulokseksi, joista kaikista on teoria avattu teoriaviitekehyksessä. Samaa tarkoittavat asiat on koottu saman asian alle.

Yksi tutkimuskysymyksistä tässä kehittämistyössä oli: *Miten organisaation sisäinen valvonta toteutetaan ja riskejä hallitaan esimiehen näkökulmasta?*

Sisäiseen valvontaan löytyy ohjeistusta toisen haastateltavan mukaan olemassa olevalta Laatusivustolta, eli intrasta. Sisäisen valvonnan käsite ei ole kaikille selvä, joka selvisi haastattelussa. Teoriaviitekehyksessä aihetta on avattu, joten on syytä tuoda tietoa esille. Ei voi olettaa, että kaikki lukisivat tämän opinnäytetyön näin kiireisenä aikakautena, joten täytyy tehdä tiivistetty tietopaketti asian tiimoilta ja toimittaa se johtoryhmälle ja esimiehille.

Riskienhallintaan sen sijaan oli olemassa jo jonkinlaista seurantaa ja ohjeistusta yrityksen Laatusivustolla. Laatusivustolla on Laatujohtamiseen liittyviä toimintakaavioita, jotka todettiin toimiviksi toimintamalleiksi riskejä vastaan. Toimintakaaviot ovat: Riskien hallinta, Riskien tunnistaminen ja Riskitapahtuman hallinta. Kaaviot on päivätty viimeksi helmikuussa 2017. Toimintakaaviot

ovat yleismaallisia toimintaohjeita riskin kohdatessa. Haastattelussa tuli esille, että riskienhallintaan liittyviä asioita käydään läpi auditoinneissa, niin sisäisessä, kuin ulkoisessa auditoinnissa kerran vuodessa. Valmis opinnäytetyö toimitetaan sisäisen auditoinnin pitäjälle. Opinnäytetyöntekijä ja auditoinnin pitäjä voivat yhdessä katsoa, olisiko auditoinnissa syytä käydä läpi sisäiseen valvontaan ja riskienhallintaan kuuluvia asioita. Voi olla, että tämän vuotiseen sisäiseen auditointiin, joka järjestetään kuukauden päästä, tämän työn asiat ehtivät mukaan, mikäli esiin nostettavia asioita on. Huomionarvoista oli myös kahvipöytäkeskustelu, jossa uusi työntekijä kysyi, mikä on auditointi.

Yhteenveto haastatteluiden vastauksista

Tietoturva

Haastatteluissa käytiin läpi yrityksen tietoturva asioita. Ensimmäisenä kysyttiin miten kuvailisi yrityksen tietoturvan nykytilanteen. GDPR:n myötä tietosuojaan oli tehty iso projekti keväällä 2018 ja siihen liittyviä tietoturva asioita oli parannettu. Yrityksen data tallennetaan täysin Google pilvipalveluun, joka tuo enemmän tietoturvaa kuin fyysiset palvelimet. Yrityksessä on pari tuhatta laitetta ympäri Suomen, joten fyysisten palvelimien ylläpito olisi aika raskasta. Tietoturvan nykytilannetta pidetään erinomaisena.

Toisena kysymyksenä käsiteltiin vakavimpia tietoturvauhkia. Palvelukatkos koettiin uhkana liiketoiminnan kannalta. Tietoturvauhkana nähtiin myös tiedon joutuminen vääriin käsiin, esimerkiksi lukitsemattoman tietokoneen kautta. Koettiin, että moni laiminlyö salasanakäytänteitä. Koneet tulisi lukita poistuessa koneelta. Henkilötietojen kalastelu koettiin myös uhkana. Sitä on sattunut muutamaan otteeseen. Laitteiden katoamista ei niin ikään pidetty suurena uhkana, sillä laitteet itsessään eivät sisällä mitään dataa. Mainehaitaksi koettiin, jos henkilötietoja pääsisi vääriin käsiin.

Kolmantena kysymyksenä käsiteltiin aihetta, saako haastateltavat tarpeeksi palautetta työntekijöiltä palveluiden tietoturvallisuudesta ja että tuleeko ilmoituksia poikkeamista. Todettiin, että yrityksessä on olemassa tietoturva ja tietosuoja poikkeamia varten taulukko, johon kerätään tiedot poikkeamista systemaattisesti. Laatusivustolta löytyy tietoturva asioista kuusi pykäläinen kohta, jossa yhtenä kohtana on että ’Ilmoita aina, jos edes epäilet’. Haastateltavien mielestä ilmoituksia oli tullut hyvin, kaikki oli kirjattu ja kun tilannetta katsoo puolitoista vuotta taaksepäin, ei ole tullut ainuttakaan tapausta ilmi jälkeenpäin, että miksi ei ilmoitusta tehty. Tämä asia on

hyvällä mallilla yrityksessä. Työntekijät ilmoittavat tietoturvapoikkeamista valppaasti. Tietoturvasta tulee kuitenkin pitää säännöllisin väliajoin muistutus ja tai päivitys vartteja. Niiden avulla saadaan ylläpidettyä hyvää tietoturvan tasoa.

Neljäntenä kysymyksenä käsiteltiin, onko yritys joutunut tietoturvahyökkäyksen kohteeksi kuluneen vuoden aikana. Haastateltavat kertoivat, että tietokone varkaus oli sattunut hiljattain. Koneet olivat olleet sellaisia, joissa ei ole ollut mitään dataa sisällä ja ne olivat olleet vanhimmasta päästä, joten haitta ei ole hirveän suuri. Jos koneet olisivat pitäneet tietoa sisällään, olisi se ollut kriittistä. Tähän nostettiin esille myös tietojen kalasteluyritykset käyttäjätunnuksia ja salasanoja kohtaan. Tämä ei ollut kohdennettu ainoastaan meihin, vaan moniin muihinkin yrityksiin. Suoranaisia tietoturvahyökkäyksiä ei todettu muita olleen.

Pilvipalvelu

Pilvipalvelu teeman ensimmäisenä kysymyksenä oli, miten suureksi uhkaksi palvelukatkos pilvipalvelussa koetaan. Uhka koettiin suurena, jos palvelukatkos tulisi. Todettiin, että pilvipalvelu on kriittinen järjestelmä ja sen toimivuus on yrityksen toiminnan kannalta elintärkeää. Hallinnon toiminta seisahtuisi palvelukatkoksen aikana, koulutukset toki jatkuisivat. Samaan hengenvetoon kuitenkin todettiin, että palvelukatkos on aika epätodennäköistä, sillä yrityksen pilvipalvelu on Googlen Drivessä. Googlella on valtavat resurssit selvittää palvelukatkoksen syytä, jos niin kävisi. Palvelukatkos pilvipalvelussa todettiin sisältyvän myös tietoturvauhkaan. Näin ollen luokat limittyvät ja nivoutuvat osaksi toisiaan.

Toisena kysymyksenä selvitettiin, onko ollut syytä olla huolissaan pilvipalvelun tietoturvasta ja jos on, niin millaisissa tilanteissa. Haastateltavat kertoivat, etteivät he ole huolissaan pilvipalvelun tietoturvasta. Enemmän huolta aiheuttaisi fyysiset palvelimet, koska niihin murtautuminen, tai jopa niiden varastaminen on paljon helpompaa. Huolta pilvipalveluiden turvallisuudesta ei koettu olevan, vaan päinvastoin, pilvipalvelut koettiin pelastuksena.

Sisäinen valvonta

Sisäisen valvonnan ensimmäisenä kysymyksenä oli, onko yrityksessä käytettävissä riittävä ohjeistus sisäisestä valvonnasta ja riskienhallinnasta. Haastateltavilla kaikilla ei ollut selvillä mitä kaikkea

sisällön valvonnan käsite pitää sisällään. Riskienhallinnasta yrityksellä on ISO9001 laatujärjestelmä. Ulkoisissa auditoinneissa riskienhallinta on noussut tärkeäksi aiheeksi. Ohjeistusta riskienhallinnasta löytyy jonkin verran. Toisen haastateltavan mukaan sisäinen valvonta on hyvällä mallilla. Laatusivustolta, sisäisestä intrasta, löytyy kattavasti tietoa moniin aiheisiin. Hieman huolta aiheutti se, että löytävätkö työntekijät sivustolle. Tämä on asia, josta tulisi aika ajoin tehdä nostoja ja muistuttaa sen olemassaolosta.

Toisena kysymyksenä sisäisessä valvonnassa oli henkilöstön jaksaminen, seurataanko sairaus poissaoloja ja työtyytyväisyyttä työtyytyväisyyskyselyjen avulla. Haastateltavat vastasivat, että sairauspoissaoloja seurataan. Työtyytyväisyyttä seurataan kyselyllä, joka järjestetään kolme tai neljä kertaa vuodessa. Kumpikin vastaajista vastasi eri tavalla. Kysely sisältää pääosin esimiestyöhön liittyviä asioita, mutta myös työssä jaksamiseen liittyviä kysymyksiä on. Kohdennetumpiakin kyselyitä on, esimerkiksi tasa-arvon toteutumiseen liittyvä.

Kolmantena kysyttiin, otetaanko työtyytyväisyyskyselyn tulokset huomioon toiminnan kehittämisessä ja jos otetaan, niin millä tavalla. Kyselyt käydään läpi kahdella tasolla, esimiestasolla, sekä koko yrityksen tasolla esimiestiimissä. Jokainen esimies käy tulokset läpi oman tiiminsä kanssa. Asiat ovat hyvällä tasolla yleisesti ottaen, mitään kriisejä ei ole päällä.

Neljäntenä asiana käytiin läpi, jos toteutuneet tavoitteet poikkeavat huomattavasti asetetuista tavoitteista, selvitetäänkö syyt poikkeamiin. Haastateltavat kertoivat, että systemaattisia tavoitteita ei ole. Tavoitteiden asettelu ei ole hirveän kirkasta. henkilöstökyselyssä on tietyt tavoitteet, jotka pyritään saavuttamaan. Työtyytyväisyyspuolella ei ole selviä tavoitteita asetettu. Koulutuksissa on laatupalautteissa tietyt tavoitteet ja ne pyritään täyttämään.

Riskienhallinta

Riskienhallinta osiossa kysyttiin, onko yrityksellä johtoryhmän hyväksymä riskienhallinnan politiikka ja jos on, niin millainen se on. Haastateltava kertoi, että Laatukäsikirjaan sisältyy riskienhallintaosio. Laatukäsikirja on johtoryhmän hyväksymä. Riskienhallintapolitiikkaa ei erillisenä dokumenttina ole, vaan se on osana Laatukäsikirjaa. Sertifioidussa laatujärjestelmässä riskit on luokiteltu eri riskiluokkiin. Siellä on valmiita toimintamalleja, kuinka toimia, jos riski kohdataan.

Toisena kysymyksenä riskienhallinnan osiossa kysyttiin, onko riskit määritelty esimerkiksi taloudellisiin, operatiivisiin ja vahinkoriskeihin. Haastateltavat kertoivat, että suoranaisesti ei näihin

kategorioihin ole riskejä luokiteltu. Riskiluokittelu on tehty pikemminkin asiakkuuksiin ja toimintaympäristöön liittyviksi. Asiakkuuksiin liittyvä riski on luokiteltu vakavimpiin seurauksiin.

Riskienhallinnan osion kolmantena kysymyksenä käsiteltiin, että onko merkittäville riskeille määritelty hallintatoimenpiteitä ja valvotaanko niiden toteutumista. Vastaukseksi tuli, että hallintatoimenpiteitä ei ole määritelty riskienhallintaa varten. Auditoinneissa keskustellaan riskienhallintaan liittyvistä asioista. Vuosikymmenien kokemuksella on tunnistettu todennäköisimmät riskitekijät, joita varten on toimintamalleja muodostettu. Toimintamallit on todettu toimiviksi ratkaisuiksi, joten tämä osio on yrityksessä kunnossa.

Seuraavassa yhteenveto toimintaohjeista haastatteluiden tuloksista. Näitä asioita otetaan huomioon, kun suunnitellaan koulutuksia henkilöstölle.

- Työntekijöitä tulisi muistuttaa, että tietokoneet tulisi lukita poistuessa koneen ääreltä.
- Tietoturvasta tulee pitää säännöllisin väliajoin muistutus/päivitys vartteja. Niiden avulla saadaan ylläpidettyä hyvää tietoturvatasoa.
- Laatusivuston olemassaoloa kannattaa muistutella myös säännöllisin väliajoin. Kaikki työntekijät eivät välttämättä muista sen olemassaoloa ja mitä se pitää sisällään.
- Tämän työn myötä sisäisen valvonnan käsite aukeaa varmasti paremmin lukijalle.
- Tietohallintojohtaja päivittää olemassa olevaa Tietosuojapolitiikkaa.
- Johtoryhmässä tulisi käydä läpi käytänteitä ja kirjata avainhenkilöiden poissaolojen varalle toimintaohjeet ja varahenkilöiden nimet.

4.3.3 Työryhmä

Kehittämistehtävää varten perustettiin työryhmä kohdeorganisaatiossa. Työryhmä aloitti toimintansa huhtikuussa 2019. Työryhmään kuului tutkijan lisäksi kaksi tietohallinnon asiantuntijaa, joiden kanssa järjestelmän vaihtoa suunniteltiin. Työryhmän asiantuntijat olivat tutkijan tukena kehittämistehtävän ajan. Tämän kehittämistyön ensimmäisessä vaiheessa käytiin keväällä muutostarve läpi. Työryhmän toinen asiantuntija oli yhteydessä pilvipalvelun help deskiin. Sieltä saatiin

ehdotus siirtymisestä Basic -versiosta Business -versioon. GAPPSin ehdotuksen perusteella tiedettiin, että henkilöstö tulee jakaa ryhmiin. Pohdittiin miten jaottelut voisi tehdä. Todettiin, että tarvitaan lisää tietoa, että mitä tulee ottaa huomioon, kun ryhdytään tekemään järjestelmämigraatiota. Nykyiseen tallennusjärjestelmään ei voi tehdä tarvittavia muutoksia. Tietoja on liian paljon saatavilla työntekijöille tällä hetkellä. Tarvitaan uusi järjestelmä, johon voi säätää asetuksia, pääsyoikeuksia eri tavalla.

Helatorstaina tehtiin tiedostojen koesiirtoja. Tutkittiin, paljonko menee aikaa kokonaisen kansion siirtoon uudelle puolelle. Aikaa meni joidenkin kansioiden siirrossa lähes vuorokausi. Nämä olivat hyviä testejä, jonka avulla pystytään suunnittelemaan tulevien siirtojen aikataulua ja ennakoimaan ajan käyttöä. Pohdittiin mihin teoriaviitekehyksen aihepiirien aiheista tutkimukselle on tutkimuksellista arvoa ja mistä saa lisätietoa muutoksen tekemiseen.

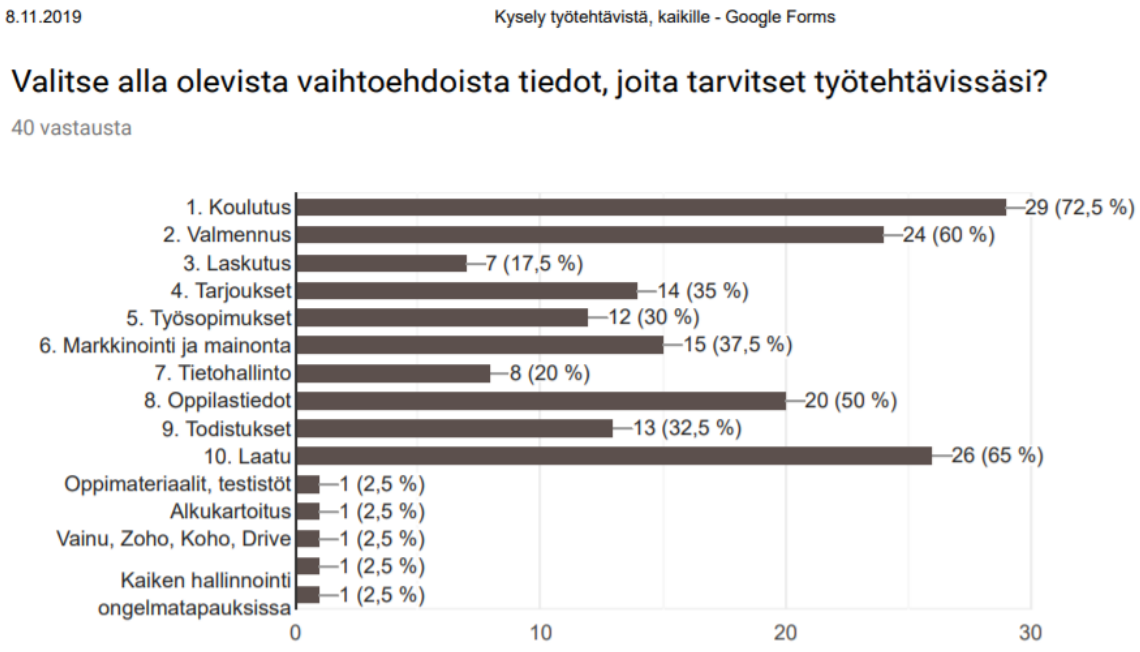
Kesätauon jälkeen kokoonnuttiin verkkopalavereissa ja sovittiin aina seuraavien steppien etenemisestä. Syksy oli kiireistä aikaa. Hyvä, että lukijoita työlle oli kaksi, niin aina toinen oli ehtinyt katsoa työtä ja antoi palautetta. Työryhmässä pohdittiin Googlen kesällä tekemää muutosta Team Drivestä Shared Driveen. Alikansioiden jakamisen ominaisuus muuttui. Googlen kehittelemä muutostyö ei tullut valmiiksi vielä vuoden 2019 puolella, joten tiedostojen siirto uuden järjestelmän puolelle viivästyy.

Haastatteluista ja kyselyistä saadut materiaalit käytiin läpi työpajassa. Uusien tutkimustulosten pohjalta suunniteltiin henkilöstön ryhmittely. Sen lisäksi sisäinen valvonta ja riskienhallinnan teoria tuodaan esimiehille ja johtoryhmälle tiedoksi. Tutkimuksen tulokset tuodaan myös edellä mainituille ryhmille tietoon. Tutkija teki muistion joka palaverista ja kirjasi asiat ylös. Ne toimivat samalla muistin tukena ja tehtävälistana. Palavereita pidettiin toistakymmentä ja ne tallennettiin yrityksen Drivelle.

Erillinen kysely työtehtävistä (Kuva 29) lähetettiin lähes koko henkilöstölle, eli noin 120:lle työntekijälle. Kysely tehtiin Google Formsilla. Pienimuotoisessa kyselyssä kysyttiin työtehtävistä ryhmäjaottelua varten, jota tarvitaan uudessa Jaetussa Drivessä. Kyselyyn oli viikko aikaa vastata. Vastauksia saatiin 40, eli 33 %, eli yksi kolmasosa henkilöstöstä vastasi tähän kyselyyn. Tarkoitus oli selvittää kyselyn avulla, että mitä osioita henkilökunta tarvitsee työnsä tekemisessä. Osiot on jaettu päätehtävien mukaan. Vastaajalla oli mahdollisuus valita niin monta vaihtoehtoa kuin oli tarvetta.

Vaihtoehdot työtehtäville oli seuraavanlaiset; Koulutus, Valmennus, Laskutus, Tarjoukset, Työsopimukset, Markkinointi ja mainonta, Tietohallinto, Oppilastiedot, Todistukset, Laatu, Muu. Alla

olevassa kuvassa (Kuva 29) on vastauksien määrät. Tulokset sai ulos Google Formsista nimen perusteella. Tämän mukaan nähtiin mitä henkilöt olivat vastanneet. Työtehtävä osioissa on pääkohdat, joiden mukaan tullaan uusi kansiorakenne rakentamaan Jaetun Driven puolelle. Pääsyoikeudet kansioihin tulee ryhmäjaon mukaan.

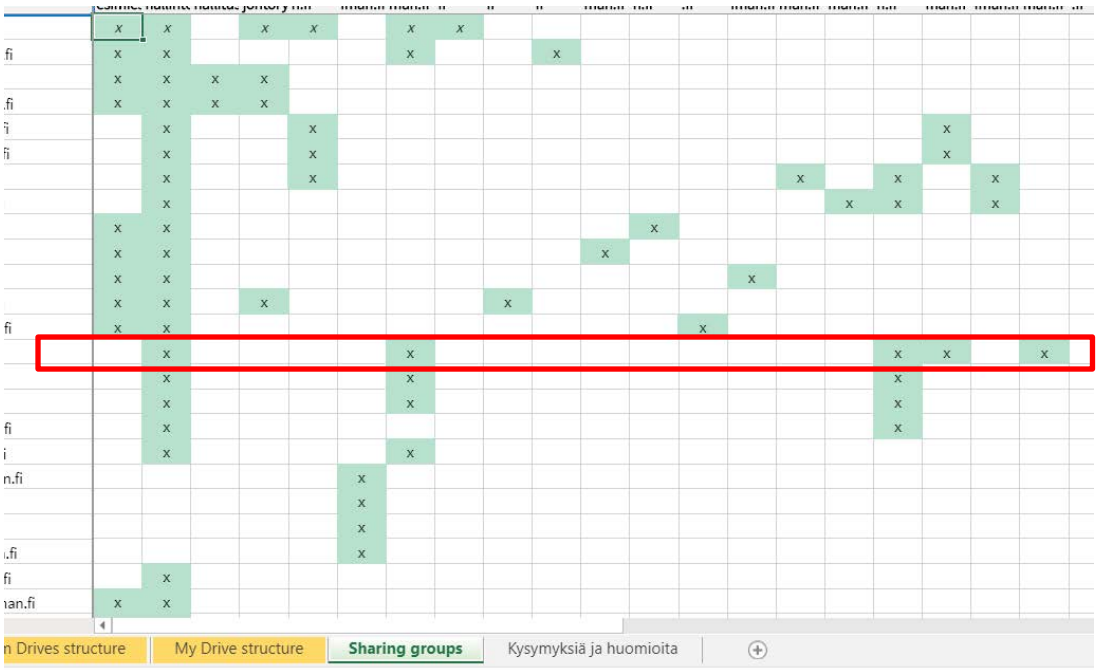


Kuva 29. Kyselyn tulokset työtehtävistä.

Koulutus, Laatu ja Valmennus valinnat olivat kärkikolmikossa tässä järjestyksessä. Työsopimusten valinnan suhteellisen suuresta määrästä kertoo se, että kysymysasettelu ei ole tässä kohtaa onnistunut. Tutkija on tarkoittanut henkilökunnan työsopimuksia, kun taas vastaajat ovat mitä ilmeisemmin tarkoittaneet asiakkaiden työsopimuksia. Sanamuotojen asettelulla on merkitystä. Tässä on konkreettinen esimerkki. Tässä kohtaa työryhmä tekee linjauksen ja työsopimuksiin pääsee vain muutama henkilö, ei edelleenkään kyselyn osoittama määrä. Kyselyn päättymistä edeltävänä päivänä tutkija lähetti muistutusviestin kyselyn päättymisestä. Tämä ryhmäjakoa varten tehty erillinen kysely ei ollut anonyymi. Työryhmässä katsottiin tuloksia ja tehtiin ryhmäjako henkilöstölle. Puuttuvien henkilöiden tiedot ryhmittelyä varten saatiin esimiehiltä.

Seuraavana olevassa taulukossa (Taulukko 7) näkyy millä tavalla ryhmäjakoja on suunniteltu. Tietosuojan vuoksi sähköpostiosoitteet eivät tule nähtäville. Vasemmassa laidassa pystysarakkeella

on henkilökunnan sähköpostiosoitteet. Ylärivillä on erinäisten ryhmien sekä esimiesten sähköpostiosoitteet. Ryhmästä esimerkkinä on tietyn maantieteellisen alueen ryhmä ja siihen voi kuulua tietyn alueen työntekijät. Hallintoa varten on oma ryhmä ja niin edelleen. Ryhmien nimiä ei voi avata enempää, nämä voivat olla esimerkkinä hahmottamaan tilannetta tarkemmin. Tutkija on rivillä 14, jota on punaisilla reunoilla korostettu. Tutkija kuuluu työtehtäviensä perusteella viiteen eri ryhmään.



Taulukko 7. Henkilöstön ryhmittely Jaettua Driveä varten.

Henkilökunta jaoteltiin työtehtävine mukaisiin ryhmiin. Jaetun Driven puolella annetaan tiedostoihin pääsyoikeus tietylle ryhmälle. Ryhmälle voi antaa tietyntason käyttöoikeuden. Tällä tavalla tieto on paremmin hallittavissa ja rajattuna vain tietylle ryhmälle. Kaikkien ei tarvitse päästä kaikkiin tiedostoihin kiinni edes lukuoikeuksilla. Kaikkia tietoja ei tulla siirtämään uuden Jaetun Driven puolelle.

Kehittämistehtävän tuloksena saatiin tehtyä ryhmäjaottelu henkilöstöstä uutta järjestelmää varten. Järjestelmän vaihto onnistuu vuoden 2020 alussa alkuperäisestä suunnitelmasta poiketen. Työryhmässä saimme valmiiksi suunnitelman myös jaottelun käyttöoikeuksista eri ryhmille. Kansiorakenne suunnitelmat tehtiin myös. Googlen ominaisuus alikansioiden jaosta ei ole valmis. Ky-

selyiden ja haastatteluiden aineistossa nousi esille tietoturva koulutusten tarve työntekijöille. Aineiston perusteella voi sanoa, että tietoturva ohjeistus on ajan tasalla organisaatiossa. Loppukiireiden vuoksi emme työryhmän kanssa ehtineet tehdä yhteenvetoa mitä kaikkea koulutukset voisivat pitää sisällään. Uusia tietoja voi verrata jo aiemmin käytettyihin. Tietohallintojohtaja pitää koulutuksia tietoturvasta kohdeorganisaation henkilöstölle. Hyviä aiheita nousi aineistosta esille koulutuksia varten. Riskienhallinta todettiin olevan haastatteluiden vastausten perusteella hyvällä tasolla. Sen sijaan sisäisestä valvonnasta tehdään pienimuotoinen tietopaketti esimiehiä ja johtoryhmää varten. Kyselyiden ja haastatteluiden vastauksia ei voi kertoa liikesalaisuuden vuoksi kokonaisuudessaan, joten niitä tiedostoja ei tule tämän opinnäytetyön liitteiksi. Ohjaavat opettajat ovat saaneet materiaalit luettavakseen.

5 Johtopäätökset ja pohdinta

Elämme parhaillaan uuden teollisen vallankumouksen keskellä, jonka uusista mahdollisuuksista ja vaikutuksista olemme nähneet vasta pienen osan. Älykkäät verkkoon kytketyt palvelut ja tuotteet tulevat muuttamaan ihmisten arkea samalla tavalla, kuin 20-30 vuotta sitten matkapuhelimet. Tällä hetkellä olemme uuden teollisen paradigman alkuvaiheessa, joten muutokset näkyvät vasta tulevina vuosina asteittain. Turvatakseen olemassaolonsa yritys ei voi sivuuttaa teollista digitalisaatiota. Hinta ei ole merkittävä ryhtymällä tekoihin, mutta ellei tee mitään siitä seuraa iso hinta. (Collin, ym. 2016, 317-318.) Ketterästi kehittyvät ja muutoksiin nopeasti reagoivat yritykset pysyvät muutoksessa ja kilpailussa mukana. Tällaisella alalla, jossa muutos on jatkuvaa, on pysyttävä ajanhermolla. Tulevia muutoksia on osattava ennakoida ja on rohkeasti kokeiltava uusia ratkaisuja.

Toimintatutkimuksessa toteutuu yhtä aikaa tutkimus ja työelämän kehittäminen. Työelämässä tapahtuu luonnostaan toiminnan parantamista ja kehittämistä, mutta kun siihen liitetään tutkimus, saadaan siitä toimiva työkalu työelämän ja tutkimustoiminnan kehittämiseen. Toimintatutkimus tarjoaa uuden ja demokraattisen, työelämässä työskentelevistä ja työelämän tarpeista lähtevän lähestymistavan. (Kananen 2014, 9.) Toimintatutkimuksen avulla on pyrkimys löytää tietoa, joka auttaa kehittämään käytänteitä. Toimintatutkimuksessa ei tutkita toimintaa, vaan toiminnan sisällä toiminnankehittämistä. Tutkimuksen aikana tutkija ei ole ulkopuolinen, vaan hän on aktiivinen osallistuja tehden muutosinterventioita eli muutokseen tähtääviä väliintuloja. Toimintatutkimuksessa käytäntöä ja teoriaa ei käsitellä erillisinä asioina, vaan saman asian eri puolina. (Valli & Aaltola 2015, 204-205.) Alun perin tutkimusstrategiana käytettiin toimintatutkimusta. Kehittämistyölle on ominaista, että muutoksia tapahtuu kesken projektin. Tämän opinnäytetyön tutkimusstrategia muutettiin opinnäytetyön esityksen jälkeen. Tutkimusstrategiaksi käy paremmin konstruktiivinen tutkimusote.

5.1 Johtopäätökset

Kyselyiden ja haastatteluiden tuloksia analysoidessa johtopäätöksiä tuli hyvin kirjoitettua ylös aina kyseisen kysymyksen yhteydessä. Seuraavassa muutamia tärkeimpiä nostoja yleisiin johtopäätöksiin. Kyselyyn vastanneista henkilökunta tiedostaa ja tietää, että ohjeistusta tietoturva asioista on olemassa, mutta aina ei löydetä tietojen lähteelle. Moni kaipaa pieniä koulutushetkiä

tietoturva asioiden parissa. Esimiehet ja johtoryhmä ovat valveutuneita ja ajan tasalla tietoturva asioissa. He käyvät tietoturva asioita läpi useaan kertaan vuoden aikana. Toivottavaa olisi, että myös henkilökunnalle tulisi toistoja ja kertauksia. Perehdyttäjien tulisi ottaa tietoturva-asiat huomioon perehdytyksissään. Työryhmä ottaa koulutus asian huomioon ja koulutuskertoja lisätään henkilökunnalle, joko tiimien viikoittaisissa palavereissa tai erikseen järjestettävissä webinaareissa.

Anonyymiin kyselyyn tietoturvasta vastanneet kaipasivat uutta järjestelmää tietojen tallennukseen. Nykyisessä järjestelmässä vaarana on, että yksittäiset henkilöt poistavat tärkeitä tiedostoja. Uuden pilvijärjestelmän puolella yritys omistaa tiedon, ei yksittäinen henkilö, joten tietoja ei voi poistaa. Tutkimuskysymykseen *Miten tietosuoja ja tietoturva tulisi ottaa huomioon yrityksen pilvipalvelussa?* saatiin kyselyn avulla vastaus. Työntekijät tulevat saamaan koulutuksia tietoturva-asioista, joihin sisältyy muun muassa toimintaohjeita tietoturvallisista käytänteistä työnteossa sekä neuvoja käytettyjen ohjelmien käyttöön ja niin edelleen. Koulutuksien sisällöstä tehdään kooste opinnäytetyön julkaisemisen jälkeen. Kehittämistyön työryhmän toinen asiantuntija vertaa opinnäytetyön tietoja (teoriaa ja kyselyiden ja haastatteluiden tuloksia) jo olemassa oleviin koulutus materiaaleihinsa ja nostaa tärkeimmät kohdat koulutuksiin mukaan.

Haastatteluiden avulla etsittiin vastausta tutkimuskysymykseen: *Miten organisaation sisäinen valvonta toteutetaan ja riskejä hallitaan esimiehen näkökulmasta?* Haastateltavien vastauksista voi todeta, että riskitekijät on otettu huomioon, ohjeistus on kunnossa ja riskejä on arvioitu. Tämän osion voi todeta olevan kunnossa. Vastauksista nousi esille myös se seikka, että sisäisestä valvonnasta ei välttämättä tiedetä niin hyvin mitä siihen kuuluu. Tutkijan ominaisuudessa voi todeta, että teoriaviitekehyksestä tehdään pieni tietopaketti sisäisestä valvonnasta. Se toimitetaan esimiehille ja johtoryhmälle muistin virkistämiseksi. Haastatteluidenkin johtopäätöksenä voisi pitää, että henkilökunta tarvitsee käytännön tietoturva asioista pieniä koulutustuokioita useamman kerran vuodessa. Niiden avulla voidaan ylläpitää hyvää tietoturvatasoa. Laatusivustolla on todettu olevan ajantasainen ohjeistus, mutta työntekijöitä tulisi muistuttaa sen olemassa olosta ja ohjata heitä sivustolle.

Kolmanteen tutkimuskysymykseen *Millaisiin ryhmiin työntekijät jaetaan uutta tallennusjärjestelmää varten?* saatiin myös vastaus. Erillisen työtehtäväkyselyn avulla työryhmä sai tehtyä henkilökunnan ryhmittelyn työtehtävien mukaan. Kansioiden käyttöoikeuksientaso -suunnitelmat on valmiina ja niitä muutetaan tarpeen mukaan. Suunnitelma kansiorakenteesta on ja tiedostojen

siirrot tehdään, kun Googlelta tulee varmistus tiedostojen alikansioiden jakamis asiaan. Kokonaisten kansioiden siirto vie aikaa. Siirroista tiedotetaan henkilökuntaa etukäteen monissa kanavissa; Google+:ssa (henkilöstökanavalla), sähköpostilla sekä viikoittain pidettävissä viikkopalavereissa.

Kohdeorganisaatio käyttää tiedon tallennukseen Google Driven pilvipohjaista tallennusjärjestelmää. Tutkimusongelmana oli se, että pilvipohjainen tallennusjärjestelmä tuli vaihtaa. Perimmäisenä syynä vaihtoon olivat henkilökunnan työtehtävissä tapahtuneet muutokset, sekä nykyisen kansiorakenteen epäkäytännöllisyys ja tieturva. Henkilötietojen säilytys ja käsittely tuli saada turvalliseksi ja asianmukaiseksi. Työnkuvien muuttuessa tietoa on saatavilla liian laajoina asiakokonaisuuksina. Nykyiseen järjestelmään ei voida tehdä tarvittavia muutoksia, joten oli saatava uusi järjestelmä.

Kehittämistyön tutkimuksellisen osuuden myötä saatiin ratkaisu tutkimusongelmaan. Tietoturva asioissa henkilökuntaa koulutetaan useammin, lyhyesti ja systemaattisemmin. Henkilökunta saatiin jaettua ryhmiin uutta pilvipalvelu järjestelmää varten. Suunnitelma kansiorakenteesta on olemassa. Sisäinen valvonta ja riskienhallinnan nykytilanne saatiin kartoitettua. Kaikki tavoitteet saavutettiin opinnäytetyöprosessin aikana.

Tutkimusetiikka ja hyvä tieteellinen käytäntö

Eettisten normien ja lakien tuntemus auttaa konkreettisten ratkaisujen tekemisessä. Jokainen kantaa itse vastuun tutkimustyössä tehtävistä valinnoista ja ratkaisuista. Tutkijan tulee noudattaa omassa tutkimustyössään parhaansa mukaan yhteisesti sovittuja periaatteita. Eettisesti hyvä tutkimus edellyttää tieteellisiä hyviä toimintatapoja, taitoja ja tietoja tutkimuksen teossa. (Kuula 2006, 21, 26, 34.) Tutkimusetiikka on tutkijoiden ammattietiikka, johon kuuluu eettiset periaatteet, arvot, normit ja hyveet, joita tutkijan tulee noudattaa. Tutkimusetiikka sisältää tutkimustyöhön liittyvät moraaliset käsitykset ja päätökset. (Kuula 2006, 264.) Uskottavaa ja luotettavaa työtä ei taata pelkällä rakenteella, vaan tutkijan hankkima aineisto ja tehdyt analyysit on saatava tieteellisen rakenteen kanssa vuoropuheluun. (Kananen 2013, 14).

Tässä opinnäytetyössä on koko prosessin ajan pyritty avoimuuteen ja läpinäkyvyyteen kaikissa vaiheissa, niin tiedonkeruussa, analyysivaiheista johtopäätöksiin. Tutkija käytti monipuolisia lähteitä etsiessään tietoa tutkimusmenetelmistä ja aineistonhankintatavoista. Toisten tutkijoiden aiemmin tekemiä tutkimuksia on kunnioitettu, heiltä ei ole lainattu tietoa, ainoastaan tutkittu tutkimustyylejä, kirjoitusasua ja poimittu käytettyjä lähteitä.

Kyselyn linkit lähetettiin sähköpostilla saateviesteihin liitettynä. Viesti lähetettiin piilokopiona, ettei vastaanottajat näe kenelle viesti on lähetetty. Viestin lähetys anonymisoitiin. Tutkija on ainut, joka tietää ketkä kaikki kuuluvat otokseen, joille viesti lähti. Nimilistat tullaan hävittämään, kun työ on julkaistu.

Vaikka muistutusviestiä kyselyihin vastaamisista lähetettiin, niin siitä huolimatta kaikki eivät vastanneet kyselyihin. Olisi ollut mielenkiintoista kuulla lisää erilaisia mielipiteitä kysytyistä asioista. Työtehtäväkyselyyn osallistui kuitenkin enemmän henkilökuntaa, joka kolmas. Oliko ajankohta kyselyille liian kiireinen? Vai kokivatko työntekijät, että heidän mielipiteillään ei ole väliä? Vastanneiden määrä, eli otos edustaa nyt koko populaatiota. Henkilökunta saa kyselyn tuloksista yhteenvedon opinnäytetyön julkaisemisen jälkeen. Siinä tulee olemaan samaan tapaan kysymysten läpikäyntiä johtopäätöksineen, kuin tässä opinnäytetyössä, mutta tiivistetysti.

Yksi tieteellisen tutkimuksen luotettavuuden, tulosten uskottavuuden ja eettisen hyväksyttävyyden edellytys on, että tutkimus on tehty hyvän tieteellisen käytännön (good scietific practice) edellyttämällä tavalla. (Hallamaa & Launis & Lötjönen & Sorvali 2006, 406). Hyvää tieteelliseen käytäntöön kuuluu noudattaa tiedeyhteisön toimintatapoja, joita ovat yleinen tarkkuus ja huolellisuus, rehellisyys, tulosten tallennus ja esitys sekä tutkimuksen tulosten arviointi. Tutkimus tulee olla yksityiskohtaisesti ja tieteellisesti asetettujen vaatimusten mukaisesti suunniteltu, toteutettu ja raportoitu. (Kuula 2006, 34-35.) Tutkimuksen eettiset ratkaisut ja uskottavuus kulkevat käsi kädessä. Uskottavuuden perustana on, että tutkija noudattaa hyvää tieteellistä käytäntöä. (Tuomi, ym. 2013, 132).

Opinnäytetyön kirjoittamisessa on pyritty koko prosessin ajan huolellisuuteen, tarkkuuteen, rehellisyyteen ja niin edelleen, kuten aiemmassa kappaleessa Kuulan (2006) tekstissä mainittiin. Esimerkiksi anonyymin kyselyn tulokset aukikirjoitettiin tarkasti, myös numeraalisesti. Raportoinnissa on otettu huomioon tulosten esittämisen lisäksi myös teoriakirjallisuutta.

Tieteenalan huolimattomuus ja huono hallinta tutkimuksen suorittamisessa, tulosten kirjaamisessa, raportoinnissa ja säilyttämisessä ovat merkkejä tutkijan huonosta ammattitaidosta. Hyvän tieteellisen käytännön loukkauksia ovat vilppi tieteellisessä toiminnassa ja piittaamattomuus hyvästä tieteellisestä käytännöstä. Esimerkkeinä piittaamattomuudesta ovat aikaisempiin tutkimustuloksiin puutteellinen viittaaminen tai julkaisun muiden tutkijoiden osuuden vähättely. Vilpissä päätöksentekijöitä ja tiedeyhteisöä harhautetaan, eli heille esitetään vääriä tietoja tai tuloksia ja niitä julkaistaan. (Hallamaa, ym. 2006, 408-409.) Huonoon tieteelliseen käytäntöön kuuluu myös havaintojen vääristelyä, sepittämistä, luvatonta lainaamista ja anastamista. (Kuula 2006, 36-38).

Tässä opinnäyteyössä on pyritty tuomaan seikkaperäisesti esille, miten kehittämistyö etenee. Lähtökohta työlle on avattu, sekä käytetyt tutkimusmenetelmät on kerrottu tarkoin. Menetelmien käytöt on perusteltu ja tietoa on etsitty monista lähteistä. Työn tarkoitus ja merkityksellisyys kohdeorganisaation on avattu läpi työn. Merkitys työlle tuli hyvin esille tehdessä analyysia ja johtopäätöksiä kyselyistä ja haastatteluista. Muutoksen tarve on suuri. Tutkijan rooli läpi kehittämistyön on keskeisessä osiossa, aina suunnitteluvaiheista lopulliseen tiedostojen siirtoon. Kaikki vaiheet on avattu lukijalle ja pyritty noudattamaan hyvää tieteellistä käytäntöä.

Kirjoittaessaan työtä tutkija teki päiväkohtaisia kansioita kaikkina kirjoitus päivinä. Kirjoitus päivien mukaan tehdyn tallennuksen etuna oli se, että jos huomasi jossain vaiheessa esimerkiksi jonkin asetuksen muuttuneen, niin työn sain kätevästi palautettua. Päiväkohtainen tallenne tallennettiin myös muistitikulle. Usean kerran viikossa tiedosto vietiin päivän päätteeksi myös sähköpostin liitetiedostoksi. Omaa pilvipohjaista tallennusjärjestelmää tutkijalla ei ollut käytössä ja koulun drivelle tallentaessa asetukset muuttuivat Word -muotoisessa työssä. Alkuvaiheen jälkeen siitä tallennusmuodosta luovuttiin. Eli työ oli kolmessa paikassa tallessa koko prosessin ajan, kannettavan kovalevyllä, muistitikulla ja sähköpostin liitetiedostona internetissä. Tutkija halusi varmistaa, että työ on tallessa myös internetissä, jos fyysisille laitteille tulisi vahinkoa.

5.2 Pohdinta

Niin kuin kaikissa kehittämistöissä, muutoksia voi tapahtua kesken prosessin. Tässä kehittämistyössä huhtikuussa, työryhmässä suunniteltiin, että tutkija tekee siirrot uusiin kansiorakenteisiin syksyllä 2019. Näin ei kuitenkaan tule tapahtumaan. Google ei saanut järjestelmäänsä vielä valmiiksi vuodelle 2019. Google etenee beta testauksilla ja on luvannut, että uudet ominaisuudet ovat valmiita ensimmäisellä kvartaalilla vuonna 2020. Tämän hetken tilanne on se, että henkilöstön ryhmittely on tehty ja suunnitelma kansiorakenteista on olemassa. Kansiorakenteita ei voida vielä tehdä uuden Jaetun Driven puolelle, ennen kuin Google saa ominaisuuden alikansioiden jakamisesta valmiiksi. Tutkija tekee kansiorakenteen uudelle puolelle ja tekee massiiviset tiedostojen siirrot vuoden 2020 alussa. Siihen mennessä on hyvää aikaa siivota tai arkistoida Oma Driven puolelta tarpeettomia tiedostoja, joita ei tulla tarvitsemaan enää jatkossa, eikä siirtämään turhaan uuden järjestelmän puolelle.

Kyselyiden ja haastatteluiden avulla saatiin merkittävää tietoa yrityksen tietoturva asioista ja kansiojärjestyksistä pilvipalveluissa. Henkilökuntaa on nyt kuultu ja toiveet on otettu huomioon kehittämistyössä. Haastatteluiden avulla organisaation sisäinen valvonta ja riskienhallinta saatiin ajan tasalle. Kansiorakenteiden ja ryhmäjaottelun avulla saadaan tietoturvallisuutta parannettua. Kyselyissä tärkeänä asiana nousi esille tietoturvasta kouluttamiset. Siihen tullaan puuttumaan ja koulutuksia lisätään. Työryhmässä käydään läpi mikä on sopivin tapa hoitaa tietoturvasta tiedottamiset ja kertaukset henkilöstölle. Kyselyistä selvisi myös, että tietoturva-asiat ovat kohdeorganisaatiossa erittäin hyvällä tasolla. Tietoa on olemassa, mutta hektisen arjen keskellä takaisin tiedon äärelle ei enää osata palata, kun ohjeita ei löydetä. Näihin tehdään korjausliike kouluttamalla ja tiedottamalla tietoturva-asioista. Pienillä muutoksilla saadaan kaikille sujuvampia työpäiviä ja onnistumisen kokemuksia työhönsä.

Etsiessäni teoreettiseen viitekehykseen lähteitä luin paljon muiden opinnäytetöitä ja etsin niissä käytettyjä lähteitä. Mielestäni sain koottua kattavasti teoriaa juuri oikeista aihealueista tätä kehittämistyötä varten. Pääsin pureutumaan syvälle teoriaviitekehyksen aiheisiin. Teoriasta oli paljon hyötyä kysymyksiä laadittaessa niin kyselyä kuin haastattelua varten. Oma asiantuntijuus kasvoi valittuja aiheita kohtaan tämän opinnäytetyöprosessin aikana.

Jatkotutkimusaiheet

Halusin nostaa muutoksen johtamisen ja henkilöstön osaamisen osaksi tätä opinnäytetyötä. Mielestäni kaikki muutoksien läpiviennit vaativat hyvää johtamista. Monesti nämä asiat voivat jäädä taka-alalle arjen kiireiden keskellä, kun siirrytään jo seuraaviin tärkeisiin aiheisiin. Muutoksia tapahtuu koko ajan ja olisikin hyvin tärkeää, että esimies asemassa olevat tiedottaisivat asioista niin ennakkoon kuin koko muutosprosessin ajan henkilökuntaa. Myös yhteenveto muutoksen loppuvaiheessa on tärkeää.

Ihmiset omaksuvat tietoa ja muutoksia jokainen omaan tahtiin. Henkilöille on annettava sopeutumisaikaa muutokseen ja parhaiten se onnistuu, kun keskustellaan tiimeissä ja muissa tiedotustilaisuuksissa asioiden kulusta. Kun ihmiset tietävät osansa uusissa muutoksen kuvioissa, he osaavat suhtautua muutoksiin myötämielisemmin ja avarakatseisemmin. Negaatio muutoksia kohtaan ja työssäjaksamisen heikkous johtuvat usein tiedon puutteesta. Asioita ei osata käsitellä, kun ei ole työkaluja niiden hoitamiseen. Henkilöstön osaaminen, vastaan työtehtävien vaativuus voidaan saada kulkemaan käsi kädessä kouluttamalla uusista asioista. Yleensä yhden kerran tiedotettu asia ei jalkaudu heti operatiiviseen toimintaa. Tarvitaan muutamia pieniä toistoja. Tämä on

haasteellista kiireellisissä aikatauluissa, mutta näin tehden saa parempia tuloksia. Tieto omaksutaan paremmin ja työntehokkuus nousee yksilön suoriutuessa työtehtävistään omatoimisesti ja ratkaisukeskeisesti.

Tälle kehittämistyölle jatkoa voisi olla työssäjaksamisen tutkiminen. Tämä kehittämistehtävä ja työssäjaksaminen liittyvät toisiinsa sillä tavalla, kun organisaatiossa tapahtuu muutoksia henkilöstössä, ja työnkuvia yhdistellään, kaikki eivät välttämättä sopeudu muutoksiin. Tässä kehittämistyössä tutkittiin järjestelmän muutosta, seuraavaksi voisi tutkia henkilöstössä tapahtuvaa muutosta. Miten henkilöstö ja yksilö ottaa muutokset vastaan? Mitä työkaluja heillä on muutoksen käsittelemiseen? Mitä voimavaroja heillä on käytettävissä? Onko sopeutumisaikaa muutoksiin riittävästi? Miten työssäjaksamista voidaan edistää? Työssäjaksaminen on ajankohtainen aihe ja varmasti koskettaa kaikkia organisaatioita. Tietoa ja aikaisempia tutkimuksia aiheesta löytyy paljon. Yksilön jaksaminen aina niin hektisessä ympäristössä ei ole itsestäänselvyys. Tämän päivän työtehtävät ovat aivan erilaisia kuin vuosikymmeniä sitten. Paineensietokyky on koetuksella koko ajan. Kaikkiin näihin haasteisiin on olemassa ratkaisuja, joilla työssäjaksamista voidaan edistää. Henkilöstövoimavarojen kehittämisen opinnoista sai alkunsa tämä seuraava tutkimuksen aihe, joka olisi erittäin mielenkiintoinen. Toivottavasti joku tähän aiheeseen tarttuu.

Kehittämistehtävän validiteetti ja reliabiliteetti

Tarkoitus tutkimuksessa on saada mahdollisimman totuudenmukaista ja luotettavaa tietoa. Luotettavuuden arvioinnissa käytetään reliabiliteetti- ja validiteettikäsitteitä, jotka kumpikin merkitsevät luotettavuutta. Reliabiliteetti tarkoittaa tutkimustulosten pysyvyyttä ja validiteetti sitä, että tutkimusongelman kannalta tutkitaan oikeita asioita. (Kananen 2008, 79.) Validiteetti ja reliabiliteetti tarkoittavat luotettavuutta, joista jälkimmäinen viittaa tutkimuksen toistettavuuteen. Jos samaa ilmiötä mitataan samoilla menetelmillä, saataisiinko samanlaisia vastauksia. Ulkoisella validiteetilla tarkoitetaan mittauksen yleistettävyyttä. (Metsämuuronen 2000, 21.)

Kyselytutkimuksessa mittaus ei ole niin suoraviivaista kuin voisi luulla. Mittauksen laatuun ja luotettavuuteen vaikuttavat tilastolliset, sisällölliset, kielelliset, kulttuuriset ja tekniset seikat. Laadukas mittaus edellyttää asiantuntijoiden yhteistyötä. Mittauksen luotettavuudesta voidaan erotella kaksi perustetta: reliabiliteetti ja validiteetti. Reliabiliteettia kutsutaan luotettavuudeksi tai toistettavuudeksi ja validiteettia pätevyydeksi. (Vehkalahti 2008, 40.)

Tiivistettynä validiteetti kertoo, mitataanko sitä mitä piti ja reliabiliteetti, miten tarkasti mitataan. Mittauksen luotettavuuden kannalta validiteetti on ensisijainen peruste, ellei oikeaa asiaa mitata, ei reliabiliteetilla ole merkitystä lainkaan. Validiteetti on tutkittavan ilmiön sisällöllinen kysymys, voi sitä vain osittain lähestyä tilastollisesti. Validiteetin lisäksi tavoittelemisen arvoista on mittauksen reliabiliteetti, joka tulisi saada mahdollisimman hyvälle tasolle. Mitä vähemmän on mittausvirheitä, sitä parempi on mittauksen reliabiliteetti. Tiedonkeruu on mittauksen ohella merkittävä epävarmuuden aiheuttaja tilastollisessa tutkimuksessa. Kokonaisluotettavuus tutkimuksessa edellyttää luotettavuutta tiedonkeruulta ja mittaukselta. (Vehkalahti 2008, 41-42.)

Tutkimuksen reliabiliteetti arvioi tulosten pysyvyyttä mittauksesta toiseen, eli tutkimuksen toistettavuudesta on kyse. Kun joku toinen tutkija tekee saman mittauksen ja saa saman tuloksen, on tutkimus luotettava ja tarkka. Tutkimuksen tarkkuus merkitsee sitä, että siihen ei sisälly satunnaisvirheitä. (Vilkka 2007, 149.) Reliabiliteetti tarkoittaa mittauksen toistettavuutta. Tämän tutkimuksen voi toistaa joku toinen jossain muussa organisaatiossa. Tällä kehittämistyöllä nimenomaan pyrittiin pysyvään muutokseen. Tässä kehittämistyössä itse mittaamisessa ei ollut virheitä. Kyselyt tehtiin Google Forms ohjelmalla ja tulokset saatiin ohjelman kautta selkeästi ulos. Loin lomakkeet siten, että kysymyksiin oli vastattava, jotta pääsi etenemään seuraavaan vaiheeseen, jolloin tyhjiä vastauksia ei tullut. Muutamaan kohtaan jotkut olivat laittaneet viivan (-) tai kysymysmerkin (?) vastaukseksi, jos eivät olleet halunneet tai osanneet vastata.

Tutkimuksen validiudella tarkoitetaan sitä, että tutkimuksen mittauskyvyllä mitataan sitä mitä on aiottukin. Tutkijan tulee muuttaa teoreettiset käsitteet arkikielelle, että ne ovat selkeinä ja helppolukuisina lomakkeella, eli mittarissa. Tutkimuksen validius on silloin hyvä, kun systemaattiset virheet puuttuvat ja tutkija ei ole joutunut harhaan käsitteiden tasolla. (Vilkka 2007, 150.) Validius tarkoittaa sitä, että mittaako tutkimus juuri sitä mitä on tarkoitus mitata, eli onko mittaus tehty pätevästi. Mielestäni kyselyiden ja haastatteluiden avulla saatiin mitattua juuri sitä mitä haluttiinkin ja saatiin vastaukset tutkimuskysymyksiin ja tutkimusongelmaan. Kysymykset olivat selkeitä ja kyselyn julkaisemisesta tiedotettiin saateiestien avulla. Tutkijana olin yhdyshenkilönä ja ilmoitinkin, että jokainen voi olla rohkeasti yhteydessä joko puhelimitse tai sähköpostitse. Muutamia kysymyksiä vastaajilla heräsikin ja yhteydenottoja tuli molempia yhteydenottokanavia pitkin.

Hyöty toimeksiantajalle

Tästä kehittämistyöstä on hyötyä toimeksiantajalle monin tavoin. Saatiin henkilöstön ryhmittely tehtyä ja kansiojärjestyksen suunnitelma ja käyttötaso luotua uuden pilvipalvelujärjestelmän puolelle siirtymiseen. Eli järjestelmämigraatio voidaan tehdä vuoden 2020 alkupuoliskolla. Muutoksessa tuli ottaa huomioon GDPR:n myötä tulleet säädökset henkilötietojen asianmukaista käsittelyä varten. Muutoksia oli kohdeorganisaatiossa tehty jo keväällä 2018, kun tietosuoja-asetus astui voimaan. Tietosuoja ja tietoturva asioista saatiin kattavasti tietoa tässä kehittämistyössä käytetyillä aineistonkeruumenetelmillä. Tuloksien avulla voidaan keskittyä tiheämpään kouluttamiseen ja tiedottamiseen uusista asioista, sekä niiden toistoihin. Henkilökunnan mielipiteitä on kuultu ja ne on otettu huomioon pilvipalvelujärjestelmää vaihdettaessa. Ison muutoksen kannalta on tärkeää, että työntekijät voivat vaikuttaa omilla mielipiteillään muutoksentekoon. Toimeksiantaja saa hyvän tietopaketin sisäisestä valvonnasta ja riskienhallinnasta tämän opinnäytetyön myötä. Tiedoista on apua tulevan suunnittelussa ja kehittämisessä johtamistyössä.

Itsearviointia ja ammatillinen osaaminen

Itsearvioinnin motiiveja on monenlaisia, mutta eniten ne liittyvät oppimiseen. Itseään voi arvioida, vaikka koko organisaatio, työyhteisö tai yksittäinen työntekijä. Arvioinnin tekijä on samaan aikaan arvioinnin kohde. Organisaation, työyhteisön ja yksilön itsearvioinnit eroavat toisistaan erilaisten kriteerien suhteen. Joita ovat muun muassa itsearvioinnin toteutustavat toisin sanoen konkreettiset keinot, itsearvioinnista saatavat hyödyt ja itsearvioinnin motiivit. (Virtanen 2007, 177, 179.) Ammatillinen osaaminen tarkoittaa, että pystyy toimimaan tehtävässä, jossa suoriutuu hyvin ja voi mahdollisimman hyvin toteuttaa itseään. Henkilö, joka on motivoitunut ja jolla on selkeät tavoitteet ja riittävä osaaminen pärjää työssään paremmin. Henkilö, joka saa palautetta työstään, pystyy kehittämään itseään ja kokee työtehtävänsä haasteellisina voi kehittyä ammatillisesti. (Sydänmaanlakka 2004, 152.)

Edellä olevissa lähteissä on muutamia nostoja johtamisopintoihin liittyen. Ammatillinen osaaminen on kehittynyt paljon näiden opintojen aikana. Pitkä opinnäytetyöprosessi kokonaisuudessaan kasvatti itsensä johtamisen taitoja ja ajankäytönhallintaa. Omat opintoni tässä tutkinnossa suoritin siten, että ensin suoritin kaikki kurssit ja sen jälkeen uusien tietojen valossa keskityin opinnäytetyöhön. Koen, että olen saanut todella paljon keinoja hallita omaa jaksamistani ja toimimaan systemaattisemmin. Opintojen avulla tunnen ammatillisen minäni paljon paremmin, tiedän vahvuuteni, heikkouteni ja kehittämispuoleni.

Itsearviointina kokonaisuudessaan huomasin kriittisyyden kasvavan omaa tekstiä kohtaan opinnäytetyön loppua kohden. Keväällä 2019 aloitettu kirjoittaminen ei miellyttänyt enää marraskuussa 2019. Selvää kehittymistä tapahtui kirjoittamisessa ja asioiden auki kirjoittamisessa. Tunne oli loistava huomatessa, että jos nyt lähtisin kirjoittamaan samantien uutta vastaavan laajuista työtä, tulisi siitä selvästi loppuajan kirjoittamisen tyylinen. Syksyn mittaan lähdekritiikki kasvoi ja poistettuja sivuja koko opinnäytetyöstä kertyi reilun 20 sivun verran ainakin.

Opinnäytetyön tekeminen töiden ohessa vaatii tarkkaa aikatauluttamista koko elämälle. Määränpää näkyi koko prosessin ajan kristallin kirkkaana. Opinnäytetyötä tuli kirjoitettua välillä haastavissakin olosuhteissa. Työn tekeminen vahvisti entisestään keskittymiskykyä, omien aikataulujen laatimista ja niissä pysymistä. Opinnäytetyötä tehdään 97 prosenttisesti täysin yksin (laskettu on). Kukaan ei ole laatimassa aikatauluja ja etenemissuunnitelmaa puolestasi. Kaikesta vastataan yksin. On johdettava itseään läpi pitkän prosessin. Tällainen pitkäkestoinen työ kasvattaa ajanhallinnan käyttöä.

Aikataulusuunnitelma kehittämistehtävälle luotiin alustavasti toukokuussa syksyä varten. Kesä- ja heinäkuu oli kesävapaata. Elokuussa aikataulu suunnitelmaa päivitettiin. Tutkijan oma toive oli valmiille työlle lokakuun alku, mutta ohjaava opettaja jarrutteli kertomalla, että edessä olevat vaiheet vievät aikaa. Oikeassa hän oli. Teoriaviitekehyksen muokkaamiseen ja kirjoittamiseen meni odotettua enemmän aikaa. Oikeiden tutkimusmenetelmien ja analyysimenetelmien löytämiseen meni myös suunniteltua enemmän aikaa. Kaikkein eniten aikaa kuitenkin vei kysely- ja haastattelukysymysten laatiminen. Myös uuden ohjelman, Google Formsin käytön opettelu vei aikaa, jota ei oltu otettu huomioon aikataulua suunniteltaessa. Tulosten analyysien ja auki kirjoittamisen vaiheet veivät odotettua enemmän aikaa, näistä ei aiempaa kokemusta ollut.

Näin jälkeenpäin voi todeta, että kun teoriaviitekehyksen asiat on kirjoitettu, ollaan vasta lähellä puoliväliä. Edessä on iso työ siitä eteenpäin, vaikka sivumäärällisesti työ saattaisi näyttää jo loppusuoralla olevalta. Tämän opinnäytetyön myötä sain syvennettyä asiantuntijuuttani pilvipalveluista, tietosuojasta, tietoturvasta, sisäisestä valvonnasta ja riskienhallinnasta, sekä muutosjohtamisen vaikutuksesta muutosprosessiin. Tällaisen ison projektin kirjoittaisin eri tavalla jatkossa. Nyt se on helppo sanoa, kun puoli vuotta kestäneen prosessin aikana on tullut niin paljon uutta oppia näin laajan työn kirjoittamisesta.

Haasteita riitti tutkimusotteen valinnassa, se vaihtui vielä aivan viimeisinä päivinä. Tutkimussuunnitelman esittämisenkin aikoihin oli painetta vaihtaa strategia. Näiden muutoksien tutkimiseen meni odotettua enemmän aikaa. Tästä projektista opituilla tiedoilla, jos lähtisi tekemään uutta

kehittämistyötä, saisi sen paljon nopeammin valmiiksi. Uskaltaisin jopa väittää, että lähes pari kuukautta säästyisi aikaa. Opinnäytetyön esittämisen jälkeen viimeisimmät palautteet vahvistivat asiaa. Olin ajatellut monissa kohdissa liian monimutkaiseksi asioita, vaikka ne olisi voinut tehdä paljon yksinkertaisemmin ja helpommin. Opinnäytetyön aihe oli mielenkiintoinen ja siihen oli mukava etsiä tietoa. Tällaisen opinnäytetyön tekemistä helpottaa paljon, kun on välineet kunnossa. Kannettava tietokone ja puhelimessa tarpeeksi kaistaa internet yhteyden jakamiselle. Näiden avulla työtä voi tehdä missä vaan, milloin vaan. Aina ei tarvitse olla kotona kiinteän yhteyden äärellä. Odotan innolla järjestelmämigraation loppuun viemistä ensi vuoden alussa. Hyöty kohdeorganisaatiolle ja henkilökunnalle on suuri, saadaan uusi toimiva pilvipohjainen järjestelmä käyttöön.

Lähteet

Ahokas N. (2012). Yrityksen sisäinen valvonta. Edita. Bookwell Oy, Jyväskylä.

Amazon Web Services. (2019). AWS. Types of Cloud Computing. Luettu 2.11.2019 https://aws.amazon.com/types-of-cloud-computing/

Collin J. & Saarelainen A. (2016). Teollinen internet. Talentum pro. Balto print. Liettua.

Finanssiala ry. (2019). Finanssialalle. Pilvipalvelut. Luettu 2.11.2019. http://www.finanssialalle.fi/opintomateriaalit/finanssialan-perusteet/innovaatiot/pilvipalvelut.html

GAPPS. (2017). Luettu 11.8.2019. https://gapps.fi/fi/yritys/visio-ja-arvot/

Euroopan Unioni. (2019). Yleinen tietosuoja-asetus. Luettu 29.9.2019. https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Fandom. (2017). VirtualisointiWiki. Pilvipalvelumallit. Luettu 3.11.2019. https://laovirtualisointi.fandom.com/fi/wiki/Pilvipalvelumallit

Finlex. (2019). Laki naisten ja miesten välisestä tasa-arvosta. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/ajantasa/1986/19860609

Finlex. (2019). Laki sähköisistä allekirjoituksista. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/alkup/2003/20030014

Finlex. (2019). Laki yksityisyyden suojasta työelämässä. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/alkup/2004/20040759

Finlex. (2019). Rikoslaki. 38 luku. Tieto- ja viestintärikoksista. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

Finlex. (2019). Rikoslaki. 40 luku. Virkarikoksista. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L40

Finlex. (2019). Suomen perustuslaki. Yksityiselämän suoja. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Finlex. (2019). Sähköisen viestinnän tietosuojalaki. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/alkup/2004/20040516

Finlex. (2019). Tietosuojalaki. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/alkup/2018/20181050

Finlex. (2019). Yhdenvertaisuuslaki. Luettu 29.9.2019. https://www.finlex.fi/fi/laki/alkup/2014/20141325

Finnish Support Center Oy FSC Oy. Tietojärjestelmien asiantuntija. Migraatio. Luettu 29.9.2019. http://www.fsc.fi/palvelut/migraatio.html

Gartner. (2019). Gartner homepage. Luettu 9.11.2019. https://www.gartner.com/en

G Suite Admin Help. Shared drives access levels. Luettu 16.10.2019. https://support.google.com/a/answer/7337554?hl=en&ref_topic=7337266

G Suite Admin Help. What are shared drives? Luettu 16.10.2019. https://support.google.com/a/answer/7212025?hl=en&ref_topic=7337266

Hallamaa J., Launis V., Lötjönen S. & Sorvali I. (2006). Etiikkaa ihmistieteille. Suomalaisen kirjallisuuden seura. Tietolipas 211. Hakapaino Oy. Helsinki.

Heino P. (2010). Pilvipalvelut. Hämeenlinna. Talentum Media Oy. Kariston Kirjapaino Oy.

Hirvikorpi H. (2005). Valta Jakkupuvussa - naiset ja johtaminen. Vantaa. WSOY

Holopainen A., Koivu E., Kuuluvainen A., Lappalainen K., Leppiniemi J., Mikola M. & Vehmas K. (2010). Sisäinen tarkastus. Tietosanoma Oy. Tallinna Raamatutrukikoda.

Ilmarinen, V. & Koskela, K. (2015). Digitalisaatio, Yritysjohdon käsikirja. Talentum: Alma Talent Oy. Luettu 24.8.2019. https://kamezproxy01.kamit.fi:2335/teos/IACBGXCTEB#kohta:ALKUSANAT((20)

Jarva O. (2009). Pikaviestinnän tietoturva. Ongelmat, vaihtoehdot ja ratkaisut. Kandidaattityö. Teknillinen korkeakoulu. Informaatio- ja luonnontieteiden tiedekunta. Tietotekniikan tutkinto-ohjelma. Tietotekniikan laitos. Espoo. Luettu 23.9.2019 https://olli.jarva.fi/kandi.pdf

Järvinen, P. & Rousku K. (2017). Työpaikan tietoturvaopas. Alma Talent Oy. Luettu 24.8.2019. https://kamezproxy01.kamit.fi:2335/teos/BAFBBXXTBBAED#kohta:1((20)MUUTOSTEKIJ((c4)T((20)JA((20)TIETOTURVALLISUUDEN((20)MERKITYS((20)

Kananen J. (2013). Case-tutkimus opinnäytetyönä. Jyväskylän ammattikorkeakoulu. Suomen Yliopistopaino Oy – Juvenes Print.

Kananen J. (2008). Kvantti. Kvantitatiivinen tutkimus alusta loppuun. Jyväskylän ammattikorkeakoulun julkaisuja -sarja. Jyväskylän yliopistopaino. Jyväskylä.

Kananen J. (2014). Toimintatutkimus kehittämistutkimuksen muotona. Miten kirjoitan toimintatutkimuksen opinnäytetyönä? Suomen Yliopistopaino Oy – Juvenes Print.

Kauppalehti. (2018). Gapps Oy. Luettu 11.8.2019. https://www.kauppalehti.fi/yritykset/yritys/gapps+oy/23482911

Kinnunen M. & Löytty O. (2002). Tieteellinen kirjoittaminen. Vastapaino. Tampere.

Koppinen M. (2014). Pilvipalvelumallien eri muodot. Alfame. Luettu 2.11.2019. https://www.alfame.com/blog/pilvipalvelumallien-eri-muodot

Kuula A. (2006). Tutkimusetiikka. Aineistojen hankinta, käyttö ja säilytys. Gummerus Kirjapaino Oy. Jyväskylä.

Kyrö P. (2003). Tutkimusprosessi valintojen polkuna. Tampereen yliopisto, ammattikasvatuksen tutkimus- ja koulutuskeskus.

Lehto T. (2014). Tekniikka & Talous. Pilviohjelmistot. Yle vei toimistosovellukset pilveen – Google päihitti Microsoftin. Luettu 11.8.2019. https://www.tekniikkatalous.fi/uutiset/yle-vei-toimistosovellukset-pilveen-google-paihitti-microsoftin/86afb856-2938-30f1-a78d-b65ed85caab4

Lehto T. (2014). Pilvipalvelut. Kysely: Google Drive on suosituin pilvipalvelu suomalaisilla työpaikoilla. Luettu 13.10.2019. https://www.tekniikkatalous.fi/uutiset/kysely-google-drive-on-suosituin-pilvipalvelu-suomalaisilla-tyopaikoilla/47fdabb7-9559-379d-bb9e-6205d5dbd210

Liana technologies. (2018). GDPR-muistilista ja peruskäsitteet: näin valmistaudut tulevaan EU:n tietosuoja-asetukseen. Luettu 29.9.2019. https://www.lianatech.fi/blogi/gdpr-muistilista-ja-peruskasitteet-nain-valmistaudut-tulevaan-eun-tietosuoja-asetukseen.html

Lukka K. (2001). Konstruktiivinen tutkimusote. Luettu 8.12.2019. https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Makkonen P. (2017). Sofor. Mistä aineksista syntyy onnistunut migraatio uudelle alustalle? Luettu 3.11.2019 https://www.sofor.fi/blog/mista-aineksista-syntyy-onnistunut-migraatio-uudelle-alustalle/

M-Files (2019). M-Filesin älykäs tiedonhallinta. Luettu 5.10.2019. https://www.m-files.com/fi/intelligent-information-management

M-Files. (2019). Pilvipohjainen älykäs tiedonhallinta. Luettu 5.10.2019. https://www.m-files.com/fi/cloud-vault

M-Files. (2019). Tehokkuutta tiedonhallinnan avulla. Luettu 5.10.2019. https://www.m-files.com/fi/ecm-guide-10-ten-tips-for-selecting-ecm-system

M-Files. (2019). Valmistaudu älykkääseen tiedonhallintaan. Ei enää kaaosta. Luettu 5.10.2019. https://www.m-files.com/fi/explore-m-files

Metsämuuronen J. (2000). Mittarin rakentaminen ja testiteorian perusteet. Metodologia -sarja 6. Jaabes OÜ. Võru, Viro.

Mäkitalo J. (2017). Taloushallinnon digimittari tilitoimiston asiakasyrityksille. Opinnäytetyö 2017. Luettu 24.8.2019. http://urn.fi/URN:NBN:fi:amk-201704225137

Nurmi T. & Rekiaro I. & Rekiaro P. (2001). Uusi suomalainen sivistyssanakirja. Gummerus Kirjapaino Oy. Jyväskylä.

Otala L. (2008). Osaamispääoman johtamisesta kilpailuetu. Porvoo: WS Bookwell Oy.

Raudasoja K. & Johansson M-L. (2009). Esimies talouden johtajana julkishallinnossa. WS Bookwell Oy. Juva.

Ruusuvuori J. & Nikander P. & Hyvärinen M. (2010). Haastattelun analyysi. Vastapaino. Tallinna Raamatutrükikoda. Tallinna.

Salo I. (2014). Big data & pilvipalvelut. Docendo Oy. (Saarijärven Offset Oy).

Salo I. (2010). Cloud computing palvelut verkossa. WSOYpro Oy. Porvoo.

Salo I. (2012). Hyötyä pilvipalveluista. Jyväskylä. Docendo. (Saarijärven Offset Oy).

Saukkonen P. (2003). Tutkielman teon tukisivut. Helsingin yliopiston yleisen valtio-opin laitos. Luettu 8.9.2019. https://www.mv.helsinki.fi/home/psaukkon/tutkielma/Tutkimusasetelma%202.html

Sensoan. (2016). Sensor Architectures and Networks. Pilvipalvelujen perusteet. Luettu 3.11.2019. https://www.sensoan.com/fi/2016/06/21/pilvipalvelujen_perusteet/

Suvilehto J. (2011). Tietoturva. Johdatus tietoliikenteeseen ja multimediatekniikkaan. Aalto-Universitet. Luettu 28.9.2019. http://www.cse.tkk.fi/fi/opinnot/T-110.1100/2011/luennot-files/05.Tietoturva.pdf

Sydänmaanlakka P. (2004). Älykäs johtajuus - Ihmisten johtaminen älykkäissä organisaatioissa. Hämeenlinna: Karisto Oy.

Techopedia. (2019). System Migration. Luettu 3.11.2019. https://www.techopedia.com/definition/16963/system-migration

Tietosuojavaltuutetun toimisto. (2019). Luettu 4.9.2019. https://tietosuoja.fi/gdpr

Tietosuojavaltuutetun toimisto. (2019). Milloin henkilötietoja saa käsitellä? Luettu 28.9.2019. https://tietosuoja.fi/kasittelyperusteet

Tietosuojavaltuutetun toimisto. (2019). Tietosuoja. Luettu 29.9.2019. https://tietosuoja.fi/tietosuoja

Toikko T. & Rantanen T. (2009). Tutkimuksellinen kehittämistoiminta. Tampereen Yliopistopaino Oy. Juvenes Print. Tampere.

Tuomi J. & Sarajärvi A. (2013). Laadullinen tutkimus ja sisällönanalyysi. Kustannusosakeyhtiö Tammi. Hansaprint Oy. Vantaa.

Vahti. (2009). Selvitys valtiohallinnon tietoturvaresurssien jakamisesta. 3.2 Tietoturvallisuuden hallintajärjestelmä. Luettu 25.9.2019. https://www.vahtiohje.fi/web/guest/test?p_p_id=56_INSTANCE_Rx39&p_p_lifecycle=0&p_p_state=exclusive&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_56_INSTANCE_Rx39_struts_action=%2Fjournal_content%2Fview&_56_INSTANCE_Rx39_groupId=10128&_56_INSTANCE_Rx39_articleId=25972&_56_INSTANCE_Rx39_viewMode=print

Valli R. & Aaltola J. (2015). Ikkunoita tutkimusmetodeihin 1. Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. PS-kustannus. Bookwell Oy. Juva.

Vehkalahti K. (2008). Kyselytutkimuksen mittarit ja menetelmät. Kustannusosakeyhtiö Tammi. Vammalan Kirjapaino Oy. Vammala.

Viitala, R. & Uotila, T-P. (2014). Osaamisen uhkana tehokkuusajattelu (sivut 98-113). Teoksessa *Henkilöstöjohtaminen uuden edessä. Henkilöstöbarometrin nostamat kehityshaasteet*. Viitala, R. & Järström, M. Vaasa: Vaasan yliopisto. Luettu 19.8.2019. http://www.uva.fi/materiaali/pdf/isbn_978-952-476-537-4.pdf

Vilkka H. (2007). Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Gummerus Kirjapaino Oy. Tammi. Jyväskylä.

Virtanen P. (2007). Arviointi. Arviointitiedon luonne, tuottaminen ja hyödyntäminen. Edita. Helsinki.

Vuorinen T. (2013). Strategiakirja – 20 työkalua. Talentum. Luettu 23.8.2019 https://kamezproxy01.kamit.fi:2335/teos/CACBEXDTEB#kohta:STRATEGIAKIRJA((20)-((20)20((20)TY((d6)KALUA((20)

Liitteet

LIITE 1

Saatekirje kyselyyn osallistuville 31.10.2019

Kysely pilvipalvelun järjestelmän vaihdosta xxx henkilöstölle

Hyvä xxxlainen!

Nyt on tullut aikasi vaikuttaa! Olemme tekemässä pilvipalvelun järjestelmän vaihtoa. Siirrämme kaikki tiedostot nykyisestä Oma Drivestä Jaettuun Driveen. Tässä kohtaa tarvitsemme juuri sinua! Kutsun sinut vastaamaan pieneen kyselyyn, jossa voit kertoa mitä muutoksia toivoisit nykyiseen kansiojärjestykseen ja käytettävyyteen.

Ensimmäinen kysely pitää sisällään työtehtävien kartoituksen, jonka avulla voimme tehdä ryhmäjaottelun uuden järjestelmän puolelle. Toinen kysely on laajempi ja siihen vastaaminen tapahtuu anonyymisti, eikä vastauksia voi kohdentaa kehenkään. Tutkimustuloksia käytetään selvittämään pilvipalvelun toimivuutta, tietoturvan ohjeistuksen kehittämiseen, sekä kysytään toivomuksia uudesta kansiojärjestyksestä. Ymmärrän, että olet kiireinen, mutta aikaa vastaamiseen ei tarvitse varata kauan, vain noin 10 min. Kaikkien vastaukset ovat tärkeitä tutkimuksen onnistumisen kannalta.

Opiskelen Kajaanin Ammattikorkeakoulussa ylempää tradenomin tutkintoa Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelmassa. Opinnäytetyöhön tulevan tutkimuksen tavoitteena on saada ryhmäjaottelu tehtyä uutta pilvipohjaista järjestelmää varten, sekä kehittää tietoturvan ohjeistusta.

Linkki työtehtävistä ryhmäjaottelua varten

Linkki anonyymiin tutkimuskyselyyn

Vastausaikaa on viikko, eli 7.11.2019 asti. Kiitän jo etukäteen osallistumisestasi ja vaikuttamisesta kehittämistyöhön!

Lisätietoja antaa Taina Säkkinen, email, puh. (työ)

LIITE 2

Saatekirje ryhmäjaottelua varten kaikille 31.10.2019

Hyvä xxxlainen!

Nyt on tullut aikasi vaikuttaa! Olemme tekemässä pilvipalvelun järjestelmän vaihtoa. Tulemme siirtämään kaikki tiedostot nykyisestä Oma Drivestä Jaettuun Driveen. Tässä kohtaa tarvitsemme juuri sinua!

Pieni kysely pitää sisällään työtehtävien kartoituksen, jonka avulla voimme tehdä ryhmäjaottelun uuden järjestelmän puolelle. Ymmärrän, että olet kiireinen, mutta aikaa vastaamiseen ei tarvitse varata kauan, vain pari minuuttia. Kaikkien vastaukset ovat tärkeitä ryhmäjaottelun onnistumisen kannalta.

Opiskelen Kajaanin Ammattikorkeakoulussa ylempää tradenomin tutkintoa Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelmassa. Opinnäytetyöhön tulevan tutkimuksen tavoitteena on saada ryhmäjaottelu tehtyä uutta pilvipohjaista järjestelmää varten.

Linkki työtehtävistä ryhmäjaottelua varten

Vastausaikaa on viikko, eli 7.11.2019 asti. Kiitän jo etukäteen osallistumisestasi ja vaikuttamisesta kehittämistyöhön!

Lisätietoja antaa Taina Säkkinen, email, puh. (työ)

LIITE 3

Saatekirje haastateltaville 4.11.2019

Hyvä vastaanottaja,

Kutsun sinut teemahaastatteluun opinnäytetyötäni varten. Olemme tekemässä pilvipalvelun järjestelmän vaihtoa xxxlla. Siirrämme kaikki jaetut tiedostot nykyisestä Oma Drivestä Jaettuun Driveen.

Haastatteluun valituista henkilöistä ovat tietoisia ohjaava opettajani sekä työyhteisön ohjaajani. Haastattelu nauhoitetaan ja litteroidaan tuloksien analysointia varten. Aineisto käsitellään niin, että haastateltava ei erotu vastauksista. Haastattelu kestää noin puoli tuntia. Haastattelujen avulla kartoitamme tietoturvan, sisäisen valvonnan ja riskienhallinnan nykytilanteen ja teemme tarvittavia päivityksiä haastattelun tuloksista saaduilla tiedoilla.

Haastatteluja varten tehdään pohjakartoitus, tässä linkki kyselyyn

Vastaathan muutamaan kysymykseen ennen haastattelua.

Olisiko sinulla aikaa haastatteluun tällä viikolla (45)?

Ystävällisin terveisin,
Taina

Lisätietoja antaa Taina Säkkinen, email, puh.

LIITE 4

Erillinen kysely työtehtävistä ryhmäjakoa varten

Nimi: _____

Työtehtävät

Minkälaisia tietoja, kansioita tarvitset työtehtäväsi hoitamiseen? Voit valita useamman vaihtoehdon.

- Tarjous -kansiot
- Koulutus -kansiot
- Valmennus
- Laskutus
- Työsopimukset
- CV:t
- Markkinointi ja mainonta
- Tietohallinto
- Oppilastiedot
- Työsopimusasiat
- Muu, mikä? _____

Kerro työnkuvastasi:

_____

_____

LIITE 5

Anonyymi kysely

Kysely tietoturvasta ja pilvipalvelusta.

*Pakollinen

Taustatiedot

1. **Sukupuoli** *
Nainen
Mies

2. **Ikä** *
20-39
40-59
60-79

3. **Valitse tutkintosi korkein aste** *
Toinen aste
Korkea-aste
Ylempi korkea-aste
Muu:

Työtehtävät

Taustatiedot.

4. **Voit valita useamman vaihtoehdon** *
Valitse kaikki sopivat vaihtoehdot.
Asiantuntija
Kouluttaja
Valmentaja
Tukipalvelut
Esimiesasema
Joku muu

Oma Drive

5. **Mikä toimii nykyisessä kansiorakenteessa?** *

6. **Mikä ei toimi nykyisessä kansiorakenteessa?** *

7. **Kuvaile millainen kansiojärjestys olisi hyvä uudessa Jaetussa Drivessä?** *

Tietoturva

8. **1. Onko sinulla selvillä yrityksemme tietoturvalinjaukset ja toimintaohjeet?** *
Kyllä
Ei

9. **2. Jos vastasit ei, kuvaile tarkemmin?**

10. **3. Pystyykö ohjeita noudattamaan?** *
Kyllä
Ei

11. **4. Jos vastasit ei, niin mitkä ovat suurimmat haasteet?**

Onko tietoturva -ohjeet mielestäsi:

12. **Helposti saatavilla?** *
Kyllä
Ei

13. **Riittävän selkeät?** *
Kyllä
Ei

14. **Ajan tasalla?** *
Kyllä
Ei

15. **Millaisia ohjeita kaipaat tietoturvasta?** *

16. **Mistä saat tietoa tietoturva asioissa?** *

17. **Miten haluaisit tietoturva -ohjeita saada?** *
Valitse kaikki sopivat vaihtoehdot.
Intrasta
Palavereista
Esimieheltä
Videotallenteina
Viikon IT-vinkkinä
Kysymällä toimistolta sähköpostilla
Kysymällä toimistolta soittamalla
Muu:

18. **Jos vastasit Muu, niin kerro millä tavalla haluaisit tietoturva ohjeet saataville?**

19. **Miten tärkeänä tietoturvallisuutta pidetään yrityksessämme mielestäsi?** *
(1 = ei lainkaan, 2 = vähän tärkeänä, 3 = en osaa sanoa, 4 = melko tärkeänä, 5 = tärkeänä)

20. **Auttaako tietoturvavaatimukset päivittäisessä työssäsi?** *
(1 = ei lainkaan, 2 = vähän, 3 = en osaa sanoa, 4 = melko paljon, 5 = paljon)

21. **Haittaavatko tietoturvavaatimukset päivittäisessä työssäsi?** *
(1 = ei lainkaan, 2 = vähän, 3 = en osaa sanoa, 4 = melko paljon, 5 = paljon)

22. **Mitä pidät vakavimpana tietoturvaongelmana työssäsi?** *

Pilvipalvelu

23. **Taritsetko tukea pilvipalvelun käytössä?** *
(1 = en lainkaan, 2 = vähän, 3 = jonkin verran, 4 = melko paljon, 5 = paljon)

24. **Mitä seuraavista asioista koet pilvipalvelun eduksi?** *
Valitse kaikki sopivat vaihtoehdot.
Tiedon saatavuus usealla laitteella
Helppokäyttöisyys
Etätyöskentely
Tietoturva
Kilpailuetu
Järjestelmien ajantasaisuus
Muu:

25. **Oletko ollut huolissasi pilvipalvelun tietoturvasta?** *
(1 = en lainkaan, 2 = vähän, 3 = jonkin verran, 4 = melko paljon, 5 = paljon)

26. **Onko pilvipalvelun käytön turvallisuutta lisätty seuraavilla asioilla?** *
Valitse kaikki sopivat vaihtoehdot.
Työntekijöiden koulutuksella
Teknologialla
Prosesseilla
Muu:

27. **Muuta kommentoitavaa pilvipalvelusta?** *

LIITE 6

Haastateltaville taustakysymykset 5.11.2019

(Vastausvaihtoehdot näissä: kyllä/ei)

Riskienhallinta

1) Onko yrityksessä tehty riskikartoitus, jossa on tunnistettu ja arvioitu seuraavia riskitekijöitä:

   a) Tehtävistä, kuten tietojärjestelmien ja prosessien häiriöttömyyteen liittyvistä riskitekijöistä?
   b) Toiminnasta, kuten ostopalvelujen vaikuttavuutta uhkaavista tekijöistä, esimerkiksi laadusta, asiakastyytyväisyydestä ja saatavuudesta?
   c) Toiminnan tuottavuutta uhkaavista tekijöistä?
   d) Toiminnan taloudellisuutta uhkaavista tekijöistä?
   e) Lain- ja hyvän hallintotavan mukaisuutta uhkaavista tekijöistä toiminnassa?
   f) Toiminnan edellyttämien koneiden, laitteiden ja tilojen toimivuutta uhkaavat tekijät?
   Kommentoitavaa? ___

2) Henkilöstöön liittyviä riskitekijöitä:

   a) Onko avainasemassa oleville henkilöille nimetty varahenkilöt?
   b) Seurataanko henkilöstön poissaoloja?
   Kommentoitavaa? ___

3) Investointeihin liittyvät riskitekijät:

   a) Onko investointihankkeiden suunnittelulla riittävä kytkentä taloudelliseen liikkumavaraan eri aikajänteillä?
   b) Onko sopimusten ja kustannusarvioiden toteutumisen seuranta, toiminnallisen etenemisen, muutoksiin reagointi ja niiden hyväksyminen systemaattista?
   Kommentoitavaa? ___

4) Tietojärjestelmiin ja tietoturvaan liittyviä riskitekijöitä:

   a) Onko tietojärjestelmien käytettävyys, tiedon oikeellisuus ja häiriöttömyys varmistettu?
   b) Onko toiminnan julkisuuden ja hyvän tiedonhallintatavan toteutuminen, kuten rekisteriselosteiden laadinta ohjeistettu?
   c) Onko salasana- ja käyttöoikeushallinnan menettelyt ohjeistettu?
   d) Onko tietosuojaan ja tietoturvaan liittyvät riskit arvioitu?
   Kommentoitavaa? ___

LIITE 7

Haastattelukysymykset

5.11.2019

Tietoturva

1) Millaiseksi kuvailisit yrityksen tietoturvan nykytilanteen?
2) Millaiset tietoturvauhkat ovat vakavimpia mielestäsi?
3) Saatko tarpeeksi palautetta työntekijöiltä tietoturvallisuudesta palveluissamme? Ilmoittavatko he poikkeamista tms?
4) Millaisien hyökkäyksien kohteeksi yritys on joutunut kuluneen vuoden aikana?

Pilvipalvelu

1) Kuinka suureksi uhkaksi koet pilvipalvelun palvelukatkoksen?
2) Oletko ollut huolissaan tietoturvasta pilvipalvelun vuoksi? ja jos olet, niin millaisissa tilanteissa?

Sisäinen valvonta

1) Onko mielestäsi yrityksessä käytettävissä riittävä ohjeistus sisäisestä valvonnasta ja riskienhallinnasta?
2) Seurataanko henkilöstön jaksamista, kuten sairaus poissaoloja ja työtyytyväisyyttä työtyytyväisyyskyselyjen avulla?
3) Otetaanko työtyytyväisyyskyselyn tulokset huomioon toiminnan kehittämisessä? Jos otetaan, niin millä tavalla?
4) Jos toteutuneet tavoitteet poikkeavat huomattavasti asetetuista tavoitteista, selvitetäänkö syyt poikkeamiin?

Riskienhallinta

1) Onko yrityksellä johtoryhmän hyväksymä riskienhallinnan politiikka ja jos on, niin millainen se on?
2) Onko yrityksen riskit määritelty esimerkiksi taloudellisiin, operatiivisiin ja vahinkoriskeihin?
3) Onko merkittäville riskeille määritelty hallintatoimenpiteitä ja valvotaanko niiden toteutumista?