Opinnäytetyö YAMK

Teknologiaosaamisen johtamisen koulutusohjelma

2019

Mika Lindroos

TIETOTURVALLISUUDEN KEHITTÄMINEN ISO/IEC 27001 -STANDARDIN VAATIMUSTEN MUKAISESTI

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ YAMK | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Teknologiaosaamisen johtamisen koulutus

Marraskuu 2019 | 41 sivua

Mika Lindroos

TIETOTURVALLISUUDEN KEHITTÄMINEN ISO/IEC 27001 -STANDARDIN VAATIMUSTEN MUKAISESTI

Tässä opinnäytetyössä kuvataan ISO/IEC 27001 -standardin mukaisen tietoturvallisuuden hallintajärjestelmän vaatimukset Erillisverkot Oy:n tytäryhtiölle sekä selvitetään miten nämä vaatimukset pystytään täyttämään. Opinnäytetyön teoriaosuudessa käsitellään standardin vaatimukset ja kehityshankeosuudessa kuvataan millaisilla menetelmillä tavotteiden täyttymistä on analysoitu.

Opinnäytetyö on luonteeltaan kehitystehtävä ja sen tärkein tavoite oli tuottaa dokumentti, jossa verrataan yrityksen nykytilaa suhteessa ISO/IEC 27001 -standardin vaatimuksiin.

Riskien tunnistamiseksi tehtiin laadullinen kyselytutkimus, jonka tavoitteena oli tuottaa tietoa mahdollisista riskitekijöistä.

Opinnäytetyön tuotoksena saavutettiin kattava dokumentti yhtiön nykytilasta ja toimenpiteistä, joita standardin vaatimusten täyttäminen edellyttää. Kyselytutkimuksen avulla tunnistettiin useita mahdollisia riskitekijöitä, joita hyödynnettiin riskienhallinnassa.

Tuotetun dokumentin avulla yritys sai selkeän kuvan puutteista, jotka vielä pitäisi täyttää. Lisäksi tämän kehitystehtävän avulla hankittujen tietojen avulla yritys kykenee laajentamaan ISO/IEC 27001 -standardin mukaista tietoturvallisuuden hallintajärjestelmää muihinkin organisaationsa osiin.

ASIASANAT:

ISO/IEC 27001, tietoturvallisuuden hallintajärjestelmä, tietoturvallisuus, riskianalyysi, VAHTI-ohje

MASTER'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme in Technology Competence Management

November 2019 | 41 pages

Mika Lindroos

DEVELOPMENT OF INFORMATION SECURITY ACCORDING TO THE REQUIREMENTS OF ISO/IEC 27001

The purpose of the present Master's thesis was to describe information security management system requirements according to the ISO/IEC 27001 -standard for the subsidiary of Erillisverkot Oy and to study how these requirements can be achieved. The theoretical part of the thesis discusses the requirements of the standard and the development part addresses the methods used to analyze the achievement goals.

The thesis is a development project and its main goal was to produce a document that compares the current state of the business with the requirements of the ISO/IEC 27001 -standard.

In order to identify the risks, a qualitative survey was conducted with the aim of providing information about potential risk factors.

The result of this thesis is a comprehensive document on the company's current status and the measures required to meet the requirements of the standard. The survey also identified potential risk factors which were utilized in risk management.

The document provides the company with a clear picture of the shortcomings which need to be rectified. The information, which was gathered during this development project, can help the company to extend its ISO/IEC 27001 based information security management system to other parts of the organization.

KEYWORDS:

ISO/IEC 27001, information security management system, information security, risk analysis, ISMS

SISÄLTÖ

KUVIOT

TAULUKOT

1 JOHDANTO

Tämä opinnäytetyö tehtiin Suomen Erillisverkot Oy:n tytäryhtiön toimeksiannosta. Erillisverkot turvaavat yhteiskunnalle kriittistä johtamista ja tietoyhteiskunnan palveluja kaikissa olosuhteissa. Palveluja käyttävät Hätäkeskuslaitos, Rajavartiolaitos, pelastustoimi, sosiaali- ja terveyssektori, Puolustusvoimat, Poliisi, valtion ja kuntien toimijat sekä huoltovarmuuskriittiset yritykset. Erillisverkot on kokonaan valtion omistama erityistehtäväyhtiö.

Tietoturvallisuuden hallintajärjestelmän käyttöönotto ja sen mukaisen toiminnan edut ovat kiistattomia. Hallintajärjestelmän tärkeitä osia ovat prosessit ja dokumentoidut toimintatavat. Toimeksiantajayrityksen tavoitteena on varmistaa tietoturvallisuuden jatkuvuus kaikissa olosuhteissa. Hallintajärjestelmän käyttöönoton avulla pyritään huomioimaan kaikki tietoturvan osa-alueet.

Opinnäytetyön lähtötilanteessa toimeksiantajayrityksen tietoturvallisuus oli hyvällä tasolla ja sen tietoturvaa oli kehitetty ISO/IEC 27001 -standardin ja muiden ohjeistuksien kuten VAHTI ja KATAKRI mukaisesti. Opinnäytetyöltä toimeksiantaja tavoitteli tietoturvallisuuden jatkokehityssuunnitelmaa ja puutteellisten kohtien havainnollistamista.

Opinnäytetyön tavoitteena on tuottaa toimeksiantajayritykselle selkeä dokumentti siitä, millaisilla toimenpiteillä voidaan saavuttaa ISO/IEC 27001 -standardin vaatimukset täyttävä tietoturvallisuuden hallintajärjestelmä ja millaisia riskitekijöitä työn soveltamisalaan liittyy.

Opinnäytetyössä perehdytään ISO/IEC 27001 –standardin mukaiseen tietoturvallisuuden hallintajärjestelmään ja sen vaatimuksiin. Työn teoriaosuudessa kuvataan standardin asettamat vaatimukset kokonaisuudessaan. Kehittämishankeosuudessa kuvataan toimeksiantajalle tehtyjä toimenpiteitä yleisellä tasolla. Varsinainen suunnitelma on ei-julkisena liitteenä, koska se on luokiteltu viranomaisasiakirjaksi.

Opinnäytetyön kehityshanke käynnistyi soveltamisalan määrittämisellä, jossa pyrittiin kuvaamaan hankkeen sisältöä mahdollisimman tarkasti. Soveltamisala rajattiin koskemaan tiettyä organisaation osaa, jotta työn laajuus pysyisi sopivana. Rajausten jälkeen aloitettiin riskienhallinnan suunnittelu. Työssä kuvataan riskienhallintaprosessi ja sen toimenpiteet. Tehokkaan riskientunnistamisen varmistamiseksi suoritettiin organisaatiosta valituille asiantuntijoille sähköpostikysely, jonka avulla pyrittiin saavuttamaan laajempi kuva

työn soveltamisalaan kohdistuvista riskitekijöistä. Viimeisessä osuudessa kuvataan puuteanalyysin menetelmät, joiden avulla saavutettiin kuva toimeksiantajayrityksen tilasta suhteutettuna ISO/IEC 27001 -standardin vaatimuksiin.

2 ISO/IEC 27001

ISO/IEC 27001 on kansainvälinen standardi, jossa määritellään vaatimukset koskien tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitoa ja jatkuvaa parantamista. Tietoturvallisuuden hallintajärjestelmän avulla suojataan tiedon luottamuksellisuutta, saatavuutta ja eheyttä riskienhallintaprosessin avulla sekä vahvistetaan sidosryhmien luottamusta siihen, että riskienhallinta suoritetaan asianmukaisesti. (SFS ry. 2017a, 5.)

2.1 Toimintaympäristö

Organisaation tulee määrittää ulkoiset ja sisäiset asiat, joilla on vaikutusta tietoturvallisuuden hallintajärjestelmältä vaadittuihin tuloksiin ja jotka vaikuttavat olennaisesti organisaation tarkoitukseen. Olennaisena toimintona tietoturvallisuuden hallintajärjestelmää organisaation tulee analysoida itseään ja ympäristöään jatkuvasti. Tarkoituksena on tietoturvallisuuden hallintajärjestelmän mukautuminen sisäisten tai ulkoisten muutosten mukaisesti, riskien ja mahdollisuuksien määrittäminen sekä oman toimintaympäristön ymmärtäminen . Ulkoiset asiat ovat esimerkiksi poliittisia, taloudellisia, kilpailuun tai teknologioihin liittyviä ja näitä asioita organisaatio ei voi itse hallita. Organisaation sisäisiä asioita, joita se pystyy itse hallitsemaan, ovat esimerkiksi prosessit, fyysinen infrastruktuuri sekä organisaation kulttuuri. (SFS ry. 2017d, 7-8.)

Tietoturvallisuuden hallintajärjestelmän kannalta tulee määrittää olennaisten sidosryhmien tietoturva. Sidosryhmä voi olla organisaatio tai henkilö, jolla on vaikutusta päätöksentekoon tai se on itse päätöksenteon kohteena. Sidosryhmällä voi olla sisäiseen tai ulkoiseen tietoturvaan kohdistuvia odotuksia, vaatimuksia tai tarpeita. Sidosryhmien odotusten, vaatimusten ja tarpeiden muuttumisen vuoksi näitä tarpeita tulisi katselmoida säännöllisesti. Toimintaympäristönsä tiedot organisaatio voi dokumentoida siinä laajuudessa, kun katsoo hallintajärjestelmänsä vaikuttavuuden kannalta tarpeelliseksi. (SFS ry. 2017d, 9-10.)

Organisaation tulee määrittää tietoturvallisuuden hallintajärjestelmän soveltamisala, jossa määritellään hallintajärjestelmän soveltaminen ja sen rajaukset. Tällä luodaan pohja hallintajärjestelmän muille toiminnoille. Esimerkiksi riskien käsittelyn ja arvioinnin

ohajuskeinojen määritys ei tuota kelvollista tulosta ilman tarkkaa ymmärrystä hallintajärjestelmän sovellettavuudesta. Tekijöitä, jotka vaikuttavat soveltamisalan määritykseen ovat esimerkiksi organisaation ulkoiset ja sisäiset asiat, sidosryhmät, liiketoiminnot ja liiketoimintojen tukemiseen tarvittavat toiminnot. (SFS ry. 2017d, 10-11.)

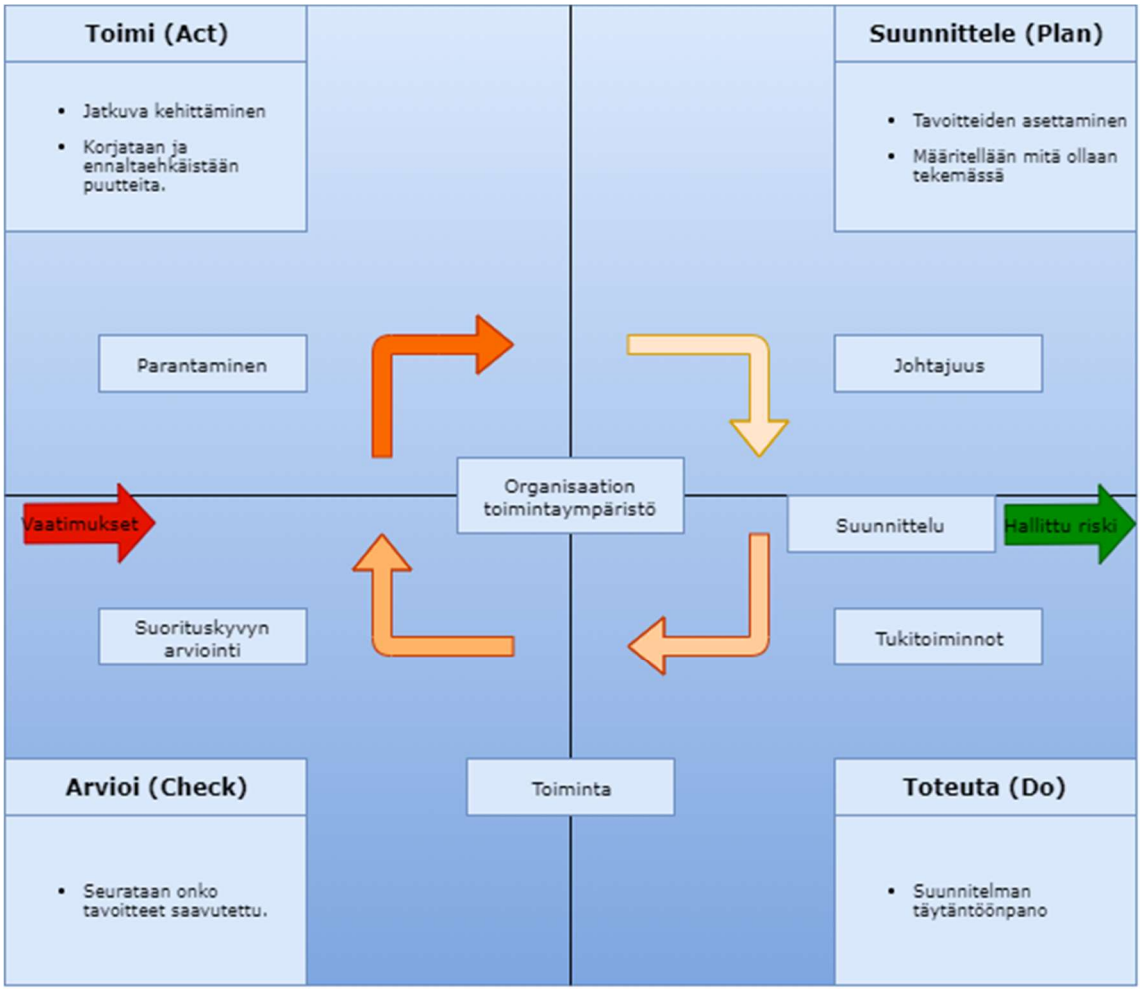
2.2 Prosessimainen toimintamalli

Organisaation tehokkaan toiminnan mahdollistamiseksi organisaation tulee hallita ja määrittää useita toisiinsa liittyviä toimintoja. Kaikki toiminnot, jotka hyödyntävät resursseja tarvitsevat hallintaa. Tämä mahdollistaa sen, että toiminnan panoksista saadaan toisiinsa liittyvien toimintojen sarjojen avulla luotua tuotoksia. Prosessin tuotos voi toimia myös toisen prosessin panoksena. Prosessimaiseksi toimintamalliksi voidaan kutsua sitä, kun organisaatio soveltaa prosessijärjestelmää, tunnistaa prosesseja ja niiden vuorovaikutusta sekä johtaa näitä prosesseja. (SFS ry. 2017a, 21-22.)

ISO/IEC 27001 -standardin mukaisen PDCA- prosessimallin (Kuvio 1) tehtävät jaetaan neljään osaan.

- **(Plan)** Suunnitteluvaihe, jossa suunnittelu käynnistetään tekemällä liiketoimintavaikutusanalyysi ja riskianalyysi, joiden pohjalta muodostetaan jatkuvuusstrategia.
- **(Do)** Toteutusvaihe, jossa suunnitelma toteutetaan.
- **(Check)** Tarkistusvaihe, jossa prosessin tilasta hankitaan tietoa testauksen, valvonnan, auditoinnin, katselmoinnin ja raportoinnin avulla.
- **(Act)** Kehitysvaihe, jossa korjataan ja ennaltaehkäistään havaittuja puutteita.

(Vahti 2007, 38-39.)



Kuvio 1. PDCA-cycle (Mataracioglu 2017.)

2.3 Tietoturvallisuuden hallintajärjestelmä (ISMS)

ISO/IEC 27001 -standardissa kuvataan standardin vaatimusten mukaisen tietoturvallisuuden hallintajärjestelmän luominen, toteuttaminen ja ylläpito. Hallintajärjestelmän tarkoitus on tiedon luottamuksellisuuden, eheyden ja saatavuuden suojaaminen riskienhallinnan, riskienhallintakeinojen, ohjeiden, sekä prosessien keinoin. (Vetikko 2019.)

Tietoturvallisuuden hallintajärjestelmä on viitekehysluonteinen ja ISO/IEC 27001 -standardissa vaaditaan ainakin seuraavat dokumentit:

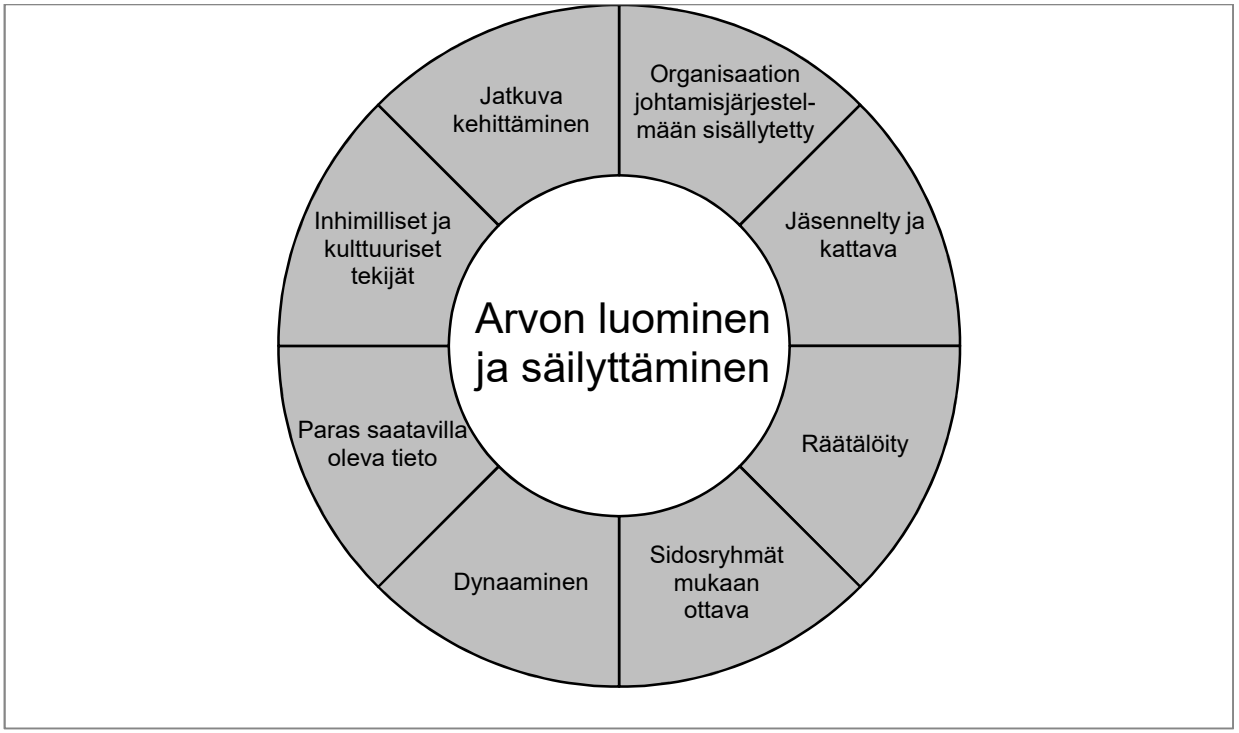
- tietoturvallisuuden hallintajärjestelmän soveltamisala
- tietoturvapolitiikka, joka sisältää tavoitteet, toteutustavan, vastuut, sanktiot ja seurannan
- tietoturvariskien arviointi

- tietoturvariskien käsittely, jossa on perusteltu liitteen A hallintakeinojen käyttäminen tai käyttämättä jättäminen.
- tietoturvatavoitteet ja niiden saavuttamiseksi vaadittavat toimet
- henkilöstön pätevyys ja sen ylläpito
- toiminnan suunnittelu ja ohjaus
- suorituskyvyn seuranta, mittaus, analysointi ja arviointi
- sisäinen auditointi
- johdon katselmus
- poikkeamat ja korjaavat toimenpiteet

(Hinson ym. 2018, 7-11)

2.4 Riskienhallinta

Riskienhallinnan tavoitteena on arvon luominen ja säilyttäminen, jonka avulla se auttaa parantamaan suorituskykyä, tukee innovointia ja auttaa tavoitteiden saavuttamisessa.



Kuvio 2. Riskienhallinnan periaatteet (SFS ry. 2018, 8-9.)

Kuviossa 2 (SFS ry. 2018, 8-9.) on esitetty periaatteita, jotka kuvaavat tehokkaan riskienhallinnan ominaisuuksia. Organisaation riskienhallintaa ja sen prosesseja määriteltäessä nämä ominaisuudet tulisi ottaa huomioon.

Riskienhallinnan tulee olla organisaation johtamisjärjestelmään sisällytetty ja siten olennainen osa kaikkia organisaation toimintoja. Tavoitteena on tehdä jäsennelty ja kattava toimintamalli, jonka avulla tuloksista saadaan yhdenmukaisempia ja vertailukelpoisempia. Riskienhallinnan prosessit ja puitteet räätälöidään toimintaympäristöön sopiviksi

Sopivien sidosryhmien sitominen riskienhallintaan mahdollistaa sidosryhmien näkemysten, tietämyksen sekä havaintojen huomioimisen riskienhallinnassa. Tällä varmistetaan parhaaseen tietoon perustuva riskienhallinta sekä lisätään sidosryhmien tietoisuutta riskienhallinnasta.

Riskit voivat muuttua tai uudistua toimintaympäristön muuttuessa. Muutoksia ennakoidaan, havaitaan ja niihin reagoidaan dynaamisella toiminnalla sopivalla tavalla ja oikeaan aikaan.

Lähtötiedot perustuvat historiaan, nykyisiin tietoihin sekä tulevaisuuden odotuksiin. Riskienhallinnassa tulisi myös huomioida lähtötietoihin liittyvät rajoitukset ja epävarmuudet, ja tietojen tulisi olla saatavissa olennaisilla sidosryhmillä.

Inhimilliset ja kulttuurilliset tekijät täytyy myös ottaa huomioon, sillä ne ovat merkittäviä asioita riskienhallinnan näkökohdissa. Riskienhallintaa tulee myös kehittää jatkuvasti kokemuksen ja oppimisen myötä. (SFS ry. 2018, 8-9.)

2.5 Johtaminen

Organisaation määrittämällä tietoturvallisuuden ylimmällä johdolla tulee olla vastuullaan ainakin seuraavat asiat:

- tietoturvapolitiikka on laadittu ja sille on asetettu tavoitteet, jotka ovat linjassa organisaation strategian kanssa
- tietoturvallisuuden hallintajärjestelmän vaatimukset on sidottu organisaation prosesseihin
- tarvittavat resurssit tietoturvallisuuden hallintajärjestelmää varten (taloudelliset, toimitilat, henkilöstö ja tekninen infrastruktuuri) on varattu

- viestiä tietoturvan ja sen hallintajärjestelmälle asetettujen vaatimusten noudattamisen tärkeydestä
- varmistaa, että hallintajärjestelmälle asetetut tavoitteet täyttyvät
- kannustaa ja tukea henkilökuntaa hallintajärjestelmän vaikuttavuuden kehittämiseen
- edistää hallintajärjestelmän jatkuvaa parantamista
- tukea muita johtoon kuuluvia omilla vastuualueillaan (SFS ry. 2017a, 7.)

Kosutic on todennut kokemukseensa pohjautuen, että ilman riittävää budjettia ja työntekijöiden resursointia ISO/IEC 27001 -projekti tulee epäonnistumaan. Kirjassan hän painottaa ylimmän johdon vastuun lisäksi konkreettisia tekoja budjetin ja resurssien suhteen, ja toteaa johdon monesti epäonnistuvan tässä. (Kosutic 2016, 114-115.)

Tietoturvapolitiikka kuvaa tietoturvallisuuden hallintajärjestelmän strategisen merkityksen organisaatiolle ja ohjaa sen tietoturvatoimintoja. (SFS ry. 2017a, 7.)

Ylin johto vastaa, että tietoturvallisuuden roolit, vastuut ja valtuudet on jaettu ja niistä on viestitetty koko organisaatiolle. Ylin johto myös hyväksyy tietoturvallisuuden hallintajärjestelmän roolit, vastuut ja valtuudet. Tietoturvatoimintoihin sisältyvät: (SFS ry. 2017a, 7.)

- tietoturvallisuuden hallintajärjestelmän perustus, toteutus, ylläpito, parantaminen ja järjestelmän tason raportointi
- tietoturvariskien arviointi ja käsittelyn ohjeistaminen
- tietoturvaprosessien ja -järjestelmien suunnittelu
- tietoturvallisuuden hallinnan määrittäminen, kokoonpano ja toimintaa ohjaavien standardien asettaminen
- tietoturvahäiriöiden hallinta
- tietoturvallisuuden hallintajärjestelmän auditointi ja katselmointi (SFS ry. 2017d, 15.)

Esimerkiksi seuraaviin rooleihin voidaan sisällyttää tietoturvavastuita:

- tietojen omistajat
- prosessien omistajat
- suojattavien omaisuuksien omistajat
- riskin omistajat

- tietoturvallisuutta koordinoivat roolit
- projektipäälliköt
- linjaesimiehet (SFS ry. 2017d, 15-16.)

Edellä luetellut asiat organisaatio voi dokumentoida siinä laajuudessa, kuin katsoo hallintajärjestelmänsä vaikuttavuuden kannalta tarpeelliseksi.

2.6 Suorituskyvyn arviointi, sisäinen auditointi ja katselmointi sekä jatkuva parantaminen

Organisaation tulee määritellä mittarit ja arviointikeinot, joiden avulla arvioidaan tietoturvan tasoa, sekä tietoturvallisuuden hallintajärjestelmän vaikuttavuutta. Määrittelyssä tulee huomioida, mitä mitataan ja millaisilla mittaus-, seuranta-, arvionti- ja analysointimenetelmillä varmistetaan tulosten kelvollisuus ja tulosten vertailukelpoisuus. Lisäksi tulee määritellä milloin ja keiden toimesta seurantaa ja mittausta toteutetaan sekä vastuut tulosten analysoinnista ja arvioinnista. (SFS ry. 2017a, 12.)

Sisäisten auditointien tarkoituksena on varmistaa, että tietoturvallisuuden hallintajärjestelmä on saavuttanut sille asetetut vaatimukset. Organisaation tulee suunnitella ja toteuttaa auditointiohjelma, joka määrittää auditointien menetelmät, vastuut, vaatimukset, aikataulun sekä raportoinnin. Lisäksi organisaation tulee määrittää auditoinnin kriteerit ja soveltamisalan, sekä suorittaa auditoinnit tavalla, jolla objektiivisuus ja puolueettomuus pystytään varmistamaan. (SFS ry. 2017a, 13.)

Organisaation ylimmän johdon tulee katselmoida tietoturvallisuuden hallintajärjestelmä säännöllisesti. Tällä tavalla varmistetaan järjestelmän soveltuvuus ja huomioidaan ulkoisten sekä sisäisten asioiden muutoksien vaikutus järjestelmään. Muita huomioitavia asioita ovat järjestelmästä saatu ja mitattu palaute, auditointien tulokset, riskiarvio, sekä jatkuvan parantamisen mahdollistaminen. (SFS ry. 2017a, 13.)

Organisaation havaitessa poikkeaman tietoturvallisuuden hallintajärjestelmässä on sen ryhdyttävä toimiin ongelman hallitsemiseksi ja korjaamiseksi sekä käsiteltävä ongelmasta aiheutuneita seurauksia. Toimenpiteiden avulla pyritään poistamaan ongelman syyt sekä estämään ongelman esiintyminen uudestaan. Korjaavia toimenpiteitä ja niiden vaikuttavuutta tulee seurata ja tehdä muutoksia hallintajärjestelmään mikäli se on tarkoituksenmukaista. (SFS ry. 2017a, 14.)

3 HALLINTATAVOTTEIDEN JA -KEINOJEN VIITELUETTELO

Organisaation tulee parhaan mahdollisen tietoturvallisuuden tason saavuttamiseksi toteuttaa soveltuvin hallintakeinoin järjestelmä, joka koostuu menettelyistä, prosesseista, politiikoista, organisaatiorakenteista sekä ohjelmisto- ja laitteistotoiminnoista. Teknisten keinojen avulla saavutetulla tietoturvallisuudella on rajansa, jonka vuoksi sitä tulee tukea asianmukaisella hallinnalla ja menttelyillä. Organisaation turvallisuus- ja liiketoimintatavoitteiden saavuttamiseksi nämä hallintakeinot tulee ottaa käyttöön, katselmoida säännöllisesti ja parantaa tarvittaessa. (SFS ry. 2017b, 6.)

3.1 Tietoturvapolitiikat

Tietoturvalle tulee määrittää johdon hyväksymät politiikat, jotka tiedotetaan henkilöstölle ja asiaankuuluville sidosryhmille. Ylemmän tason tietoturvapolitiikan tulee määrittää tapa organisaation tietoturvatavoitteiden hallintaan sekä kattaa liiketoimintastrategiasta, laeista, sopimuksista sekä nykyisistä ja ennustetuista tietoturvauhista peräisin olevat vaatimukset. Lisäksi tietoturvapolitiikassa tulee määritellä tietoturvaperiaatteet ja -tavoitteet, roolien vastuut sekä prosessit, joilla käsitellään tietoturvapoikkeamia. (SFS ry. 2017b, 10.)

Alemman tason tietoturvapolitiikkojen tulisi tukea hallintakeinojen toteuttamista ja olla rakenteellisesti suunnattuja tiettyihin organisaation osiin tai tietyille kohderyhmille. Näiden politiikoiden tulee olla niitä tarvitsevien henkilöiden tiedossa ja saatavilla organisaation sisällä sekä niitä tarvitseville ulkopuolisille sidosryhmille. Lisäksi politiikoiden tulee olla lukijalle ymmärrettävässä muodossa. (SFS ry. 2017b, 10.)

Tietoturvapolitiikkojen katselmointi tulee toteuttaa suunnitelluin aikavälein tai jos merkittäviä muutoksia ilmenee. Politiikoilla on oltava hyväksytyt omistajat, jotka vastaavat kyseisten politiikkojen kehittämisestä, arvioinnista ja katselmoinnista. (SFS ry. 2017b, 11.)

3.2 Tietoturvallisuuden organisointi

Tietoturvavastuut tulee jakaa politiikkojen mukaisesti. Suojattavan omaisuuden suojaus- ja tietoturvallisuusprosesseja koskevat velvollisuudet tulee yksilöidä selkeästi. Tietoturvavastuullisiksi nimetyt henkilöt voivat delegoida tehtäviä muille, mutta vastuun kantaa silti nimetty henkilö. (SFS ry. 2017b, 11.)

Ristiriidassa olevat tehtävät ja vastuut tulee eriyttää, jolloin vähennetään suojattavan omaisuuden luvatonta tai tahatonta muuntelua tai väärinkäytön riskiä. Tavoitetilana tulee olla, ettei yksittäinen käyttäjä pääse käsiksi suojattavaan omaisuuteen ilman paljastumista tai valtuutusta. (SFS ry. 2017b, 12.)

Viranomaisyhteyksissä tulee määritellä menettely, jonka avulla tietoturvahäiriöstä raportoidaan ajallaan esimerkiksi, kun epäillään sen rikkovan lakia. Menettelyn tulee myös nimetä ketkä saavat olla yhteydessä viranomaisiin ja milloin näin tulee toimia. Turvallisuusasioissa tulisi myös tehdä yhteistyötä muiden osaamisyhteisöjen kanssa. Tämä mahdollistaa ennakkovaroitusten saannin ja lisää tietoa tietoturvallisuudesta ja parhaista käytännöistä. (SFS ry. 2017b, 12.)

Tietoturvallisuus tulee integroida projektinhallinnan prosesseihin, jotta voidaan tunnistaa ja vastata projekteissa mahdollisesti ilmeneviin tietoturvariskeihin. Projektin luonteesta riippumatta tietoturvatavoitteet tulee sisällyttää projektitavoitteisiin ja arvioida riskejä jo projektin varhaisessa vaiheessa tietoturvariskien hallintakeinojen tunnistamiseksi. (SFS ry. 2017b, 13.)

Mobiililaitteille ja etätyölle tulee määritellä politiikka, jossa kuvataan laitteiden sekä käyttöympäristöön ja käyttäjän vastuuseen liittyvät vaatimukset. Poliikassa tulee huomioida riskit, jotka liittyvät mobiililaitteilla työskentelyyn suojaamattomissa toimintaympäristöissä. Mobiililaitteiden turvallisuus tulee olla ajantasalla ja käyttäjille tulee ohjeistaa miten ja millaisessa ympäristössä etätyötä voi tehdä. (SFS ry. 2017b, 13-16.)

3.3 Henkilöstöturvallisuus

Rekrytoitavan henkilön taustatarkastus tulee toteuttaa lakien sekä määräysten mukaisesti ja siinä tulee huomioida tietosuoja, henkilötietojen suojaus ja työsuhteisiin liittyvä

lainsäädäntö. Taustatarkastuksen tarkoituksena on varmistua henkilön taustoista, luottamuksellisuudesta ja hänen esittämästään pätevyydestä. (SFS ry. 2017b, 16.)

Työsopimuksen yhteydessä tulee sopia vastuista ja allekirjoittaa salassapito- ja vaitiolositoumus, jos työntekijällä on pääsy luottamukselliseen tietoon. Lisäksi työntekijän tulee olla tietoinen ja sitoutunut organisaation tietoturvapolitiikkaan. Johdon vastuulla on edellyttää, että kaikki työntekijät toimivat tietoturvallisesti politiikkojen ja menettelyjen mukaisesti. (SFS ry. 2017b, 17-18.)

Kaikkien organisaatiossa työskentelevien on saatava ajantasalla oleva asiallinen tietoturvatietoisuuskoulutus ja -valmennus. Lisäksi organisaatiolla on oltava muodollinen ja työntekijöille tiedotettu kurinpitoprosessi, jonka perusteella toimitaan, mikäli työntekijä syyllistyy tietoturvarikkomukseen. (SFS ry. 2017b, 18-20.)

Työsuhteen päättyessä tai muuttuessa tulee organisaation määrittää tietoturvavastuut ja -velvollisuudet, jotka jäävät voimaan työsuhteen muuttumisen tai päättymisen jälkeen. Työntekijää tulee tiedottaa näistä vastuista, jotta niiden noudattamisesta voidaan varmistua. (SFS ry. 2017b, 20.)

3.4 Suojattavan omaisuuden hallinta

Organisaation tulee yksilöidä tiedon elinkaaren kannalta tärkeä suojattava omaisuus luetteloksi ja ylläpitää tätä. Suojattavalle omaisuudelle tulee määritellä tärkeysaste ja omistajat, joilla on omaisuuden hallintavastuu. Omaisuuden hyväksyttävälle käytölle tulee määritellä politiikka, joka sisältää esimerkiksi työntekijöiden oikeudet omaisuuden käyttöön. Työsuhteen päättyessä työntekijän tulee palauttaa kaikki suojattava omaisuus ja luovuttaa jatkuvuuden kannalta tärkeät tietonsa organisaatiolle dokumentoitavaksi. Työsuhteen irtisanomisaikana organisaation tulee varmistua, ettei työntekijä kopioi luvattomasti tärkeää aineetonta omaisuutta. (SFS ry. 2017b, 21-22.)

Tieto tulee luokitella sen kriittisyyden, arvon ja luvattoman paljastumisen aiheuttaman haitan perusteella. Tiedon merkitsemistapa tulee määritellä fyysiseen sekä sähköisessä muodossa olevaan suojattavaan tietoon. (SFS ry. 2017b, 23-24.)

Tietovälineiden siirtäminen tulee määritellä luokitteluperusteisesti ja siihen tulee olla ohjeistus. Tietovälineiden hävittämiseen on laadittava menettely, jonka avulla riski luottamuksellisen tiedon paljastumiseen saadaan minimoitua. (SFS ry. 2017b, 25-26.)

3.5 Pääsynhallinta

Organisaation tulee määritellä pääsynhallintapolitiikka, jossa eri käyttäjärooleille määritellään pääsyoikeudet ja -rajoitukset suojattavaan omaisuuteen. Käyttäjille tulee sallia pääsy vain verkkoihin ja -palveluihin, joita he tarvitsevat tehtävänsä hoitamiseen ja joihin heille on myönnetty pääsy. Ylläpito-oikeuksien käyttöä ja jakamista tulee valvoa ja rajoittaa. Henkilökunnan tulee sitoutua tunnistautumistietojen luottamuksellisuuteen ja noudattaa niille asetettuja ehtoja. Pääsyoikeudet tulee arvioida uudelleen säännöllisin aikavälein ja poistaa heti työsuhteen päättyessä tai käytön luonteen muuttuessa. Salasanojen hallintajärjestelmän tulee olla vuorovaikutteinen ja sen tulee edellyttää vahvojen salasanojen käyttöä. (SFS ry. 2017b, 27-36.)

3.6 Salaus

Salauksen hallintaan tulee laatia politiikka, jota noudatetaan suojattavan tiedon salauksessa koko salausavainten käyttöiän ajan. Laitteiden käyttöympäristöön ja tiedon arkaluonteisuuteen perustuvan riskiarvion avulla määritetään tarvittava suojaustaso salausalgoritmin tyyppi, laatu ja voimakkuus huomioiden. Politiikan tulee sisältää vaatimukset salausavainten hallintaan koko elinkaaren ajan. Sopimattoman käytön todennäköisyyden pienentämiseksi avaimille tulisi määrittää alku- ja vanhenemispäivät. (SFS ry. 2017b, 36-38.)

3.7 Ympäristön turvallisuus ja fyysinen turvallisuus

Fyysiset turva-alueet tulee määrittää paikkoihin, joissa käsitellään arkaluontoista materiaalia tai tietojenkäsittelypalveluita. Turva-alueen suojaus pystytään saavuttamaan luomalla fyysisiä esteitä alueelle pääsyn estämiseksi. Tämän lisäksi turva-alueet tulee varustaa kulunvalvonnalla, jolla varmistetaan vain sallittujen henkilöiden pääsy alueelle. Turva-alueiden suunnittelussa tulee huomioida myös ulkoiset ja ympäristön aiheuttamat uhat. Tällaisia ovat esimerkiksi luonnonkatastrofit, onnettomuudet tai vihamieliset hyökkäykset. (SFS ry. 2017b, 39-41.)

Laitteistot tulee sijoittaa siten, että pääsy työskentelyalueille pystytään rajaamaan vain laitteistojen kanssa työskenteleville luvitetuille henkilöille. Sijoituksessa tulee suunnitella

hallintakeinot esimerkiksi varkauksien, tulipalon, vesivahingon, sähkön saannin, häirinnän, sähkömagneettisen säteilyn tai vandalismin estämiseksi. Laitetilan olosuhteita tulee myös tarkkailla. Peruspalvelut kuten sähkönsaanti tulee varmistaa ja testata säännöllisesti. Sähkö- sekä tietoliikennekaapelointi tulee suojata häirinnältä, salakuuntelulta, ja vahingoittumiselta. Laitteet tulee huoltaa asianmukaisesti käytettävyyden ja eheyden varmistamiseksi. Laitteiden poiston tulee tapahtua asianmukaisesti, jotta voidaan varmistua kaiken suojattavan tiedon hallitusta hävittämisestä ennen laitteen poistoa. Toimitilojen ulkopuolelle kuljetettavien ja ilman valvontaa jäävien laitteiden turvallisuudesta tulee varmistua. (SFS ry. 2017b, 41-45.)

3.8 Käyttöturvallisuus

Organisaation tulee suunnitella toimintaohjeet tietojenkäsittelyn ja tietoliikenneverkon hallintaa varten. Toimintaohjeissa tulee huomioida tietokoneiden käynnistys- ja sammutusmenettelyt, tiedonvarmistus, huolto, tietovälineiden käsittely ja tietokonehuoneen turvallisuus ja hallinta. (SFS ry. 2017b, 46.)

Organisaatioon, liiketoimintaprosesseihin, tietojenkäsittelyjärjestelmiin ja -palveluiden tietoturvallisuuteen vaikuttavia muutoksia tulee hallita muutoksenhallinnan avulla. Muutoksenhallinnan prosessin avulla tunnistetaan ja arvioidaan epätoivottuja vaikutuksia ja ennaltaehkäistään tai minimoidaan niiden vaikutukset. Muutosten hallintavastuut ja menettelyt tulee määrittää ja tehdyistä muutoksista tulee säilyttää yksityiskohtaista lokia. (SFS ry. 2017b, 47.)

Resurssien käyttöä tulee seurata, säätää ja kapasiteetinvaatimuksista tulee tehdä ennusteita, joiden avulla säilytetään järjestelmien riittävä suorituskyky. Kapasiteettivaatimukset tulee yksilöidä järjestelmän kriittisyyden mukaan. Testaus-, kehitys- ja tuotantoympäristöt tulee erottaa toisistaan, jolloin tuotantoympäristön muuttumisen tai luvattoman käytön riski pienenee. (SFS ry. 2017b, 48-49.)

Haittaohjelmilta suojautumisen tulee perustua haittaohjelmien havaitsemis- ja korjausohjelmistoihin, järjestelmien pääsynvalvontaan, tehokkaaseen muutoksenhallintaan, sekä tietoturvatietoisuuteen. Tuotantokäytössä olevien järjestelmien ohjelmistojen asentamista tulee valvoa. Ympäristöt, joissa haittojen seuraukset voivat olla erittäin suuria, tulee eristää muusta infrastruktuurista. (SFS ry. 2017b, 49-50.)

Organisaation tulee suunnitella varmuuskopiointipolitiikka, jossa määritetään tietojen, ohjelmien ja järjestelmien varmuuskopioinnin vaatimukset. Politiikan tulee sisältää säilyttämistä, suojaamista ja säännöllisyyttä koskevat vaatimukset. Käyttäjien suorittamat toiminnot sekä havaitut poikkeamat, virheet ja tietoturvatapahtumat tulee tallentaa tapahtumalokeihin. Lokit tulee suojata luvattomilta muutoksilta ja pääsyltä, sekä säilyttää ja katselmoida säännöllisesti. Organisaation tietojenkäsittelyjärjestelmien kellot tulee asettaa ja synkronoida saman viiteaikalähteen mukaisesti. (SFS ry. 2017b, 51-53.)

3.9 Viestintäturvallisuus

Verkkoja tulee hallita ja valvoa, jotta pystytään suojaamaan järjestelmissä ja sovelluksissa oleva tieto. Verkkopalveluiden turvamekanismit, hallintavaatimukset ja palvelutasot tulee yksilöidä ja sisällyttää sopimuksiin huolimatta siitä tuotetaanko palvelut itse vai ulkoisesti. Verkossa olevat tietojenkäsittelypalvelut, ryhmät tai käyttäjät tulee eriyttää toisistaan. Tiedonsiirto tulee suojata sen kriittisyyden mukaan ja ohjeistaa hyväksyttävä käyttötapa henkilöstölle. Tiedon suojauksen salassapito- ja vaitiolositoumusta koskevat vaatimukset tulee yksilöidä, dokumentoida ja katselmoida säännöllisesti. (SFS ry. 2017b, 57-62.)

3.10 Järjestelmien hankinta, ylläpito ja kehitys

Tietojärjestelmien vaatimuksilla tulee varmistaa hankittavien tai parannettavien järjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Soveltuvia menetelmiä ovat esimerkiksi johtaminen, vaatimustenmukaisuusvaatimukset politiikoista, säännöksistä, häiriökatselmuksista, uhkamallinnuksista ja haavoittuvuuskynnyksien käytöstä. Tuotteita hankittaessa tulee noudattaa määriteltyä hankinta- ja testausprosessia, jonka hyväksymiskriteerit varmistavat tuotteelta vaadittavien yksilöityjen turvallisuusvaatimusten täyttymisen. Järjestelmiin tehtävät muutokset elinkaaren aikana tulee suorittaa muutoksenhallinnanprosessin mukaisesti. Sovellukset, joilla on kriittinen merkitys liiketoimintaan tulee testata ja tarkastaa, jos niiden käyttöalusta muuttuu. Lisäksi ohjelmistopaketteihin tehtäviä tarkoituksenmukaisettomia muutoksia tulisi välttää. (SFS ry. 2017b, 62-69.)

3.11 Suhteet toimittajiin

Organisaation tulee määrittää tietoturvavaatimukset, joilla pyritään ehkäisemään toimittajan pääsyoikeuksista suojattavaan omaisuuteen aiheutuvia riskejä. Toimittajan kanssa tulee laatia sopimus, jossa kuvataan vaatimukset tieto- ja viestintätekniikkapalveluihin ja tuotteen toimitusketjuun liittyvien tietoturvariskien ennaltaehkäisemiseksi. Toimittajan palveluiden toimittamista tulee seurata, katselmoida ja auditoida säännöllisesti, jotta varmistutaan sopimuksen tietoturvaehtojen noudattamisesta. (SFS ry. 2017b, 71-74.)

3.12 Tietoturvahäiriöiden hallinta

Organisaation tulee määrittää hallintavastuut ja menettelyt, jotka takaavat nopean, tehokkaan ja järjestelmällisen reagoinnin tietoturvahäiriöihin. Menettelyjen avulla pyritään varmistamaan tietoturvahäiriöitä käsittelevien henkilöiden pätevyys ja että havaitsemiselle ja raportoinnille on asianmukainen yhteydenottopiste. (SFS ry. 2017b, 75-76.)

Tietoturvatapahtumista tulee raportoida mahdollisimman nopeasti sovittua hallintokanavaa pitkin. Koko henkilökunnan tulee olla tietoinen tietoturvatapahtumien raportointikanavasta ja velvollisuudestaan raportoida asiasta mahdollisimman nopeasti. (SFS ry. 2017b, 76.)

Yhteydenottopisteen tulee arvioida tietoturvatapahtumat sovitun luokitteluasteikon mukaisesti ja päättää luokitellaanko tapahtuma tietoturvahäiriöksi. Jos organisaatiolla on tietoturvahäiriöistä vastaava erityisryhmä, voidaan arviointi siirtää ryhmän vahvistettavaksi tai uudelleenarvioitavaksi. (SFS ry. 2017b, 77.)

Tietoturvahäiriöön tulee reagoida keräämällä todistusaineistoa ja kirjaamalla tiedot tarkasti myöhempää analyysia varten. Tärkein tavoite tietoturvahäiriöön vastaamisessa on normaalin turvallisuustason palauttaminen. Analysoinnista ja ratkaisusta kerättyä tietoa tulee hyödyntää tulevien häiriöiden todennäköisyyden vähentämisessä ja vaikutusten pienentämisessä. Menettelyt todistusaineistoksi kelpaavan tiedon keräämiseen, hankkimiseen, yksilöimiseen ja säilyttämiseen tulee määrittää ja kehittää menettelyt kurinpitotoimenpiteitä tai juridisia toimenpiteitä varten. (SFS ry. 2017b, 78-79.)

3.13 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia

Organisaation tulee määrittää vaatimukset tietoturvallisuuden hallinnan jatkuvuuden varmistamiseksi epäsuotuisissa tilanteissa, esimerkiksi kriisin tai katastrofin aikana. Mikäli liiketoiminnan jatkuvuussuunnittelua tai katastrofeista toipumisen suunnittelua ei ole, tulisi olettaa, että tietoturvavaatimukset ovat samanlaiset kuin normaaleissa toimintaolosuhteissa. Tietoturvallisuuden vaadittu taso tulisi kuitenkin säilyttää myös poikkeusolosuhteissa. Tietoturvallisuuden jatkuvuuden hallintamekanismit tulee todentaa säännöllisin aikavälein, jotta ne ovat vaikuttavia ja päteviä kaikissa tilanteissa. Tietojenkäsittelypalvelut tulee toteuttaa niin vikasietoisina, että saatavuusvaatimukset täyttyvät kaikissa olosuhteissa. (SFS ry. 2017b, 79-81.)

3.14 Vaatimustenmukaisuus

Kaikkia tietoturvallisuuteen liittyviä lakeja, sopimuksia, säännöksiä, asetuksia ja mahdollisia turvallisuusvaatimuksia tulee noudattaa. Immateriaalioikeuksien sekä omistajan oikeuksilla suojattujen ohjelmistojen käyttöön liittyvien vaatimuksien tai lakien noudattamisesta tulee varmistua. Tallenteiden suojaus katoamisen, väärentämisen, tuhoutumisen, sekä luvattoman leviämisen varalta tulee hoitaa lakien, liiketoiminnan, sopimusten ja viranomaisten vaatimusten mukaisesti. Tietosuoja ja henkilötiedot tulee suojata lakien ja viranomaisvaatimusten mukaisesti. (SFS ry. 2017b, 82-84.)

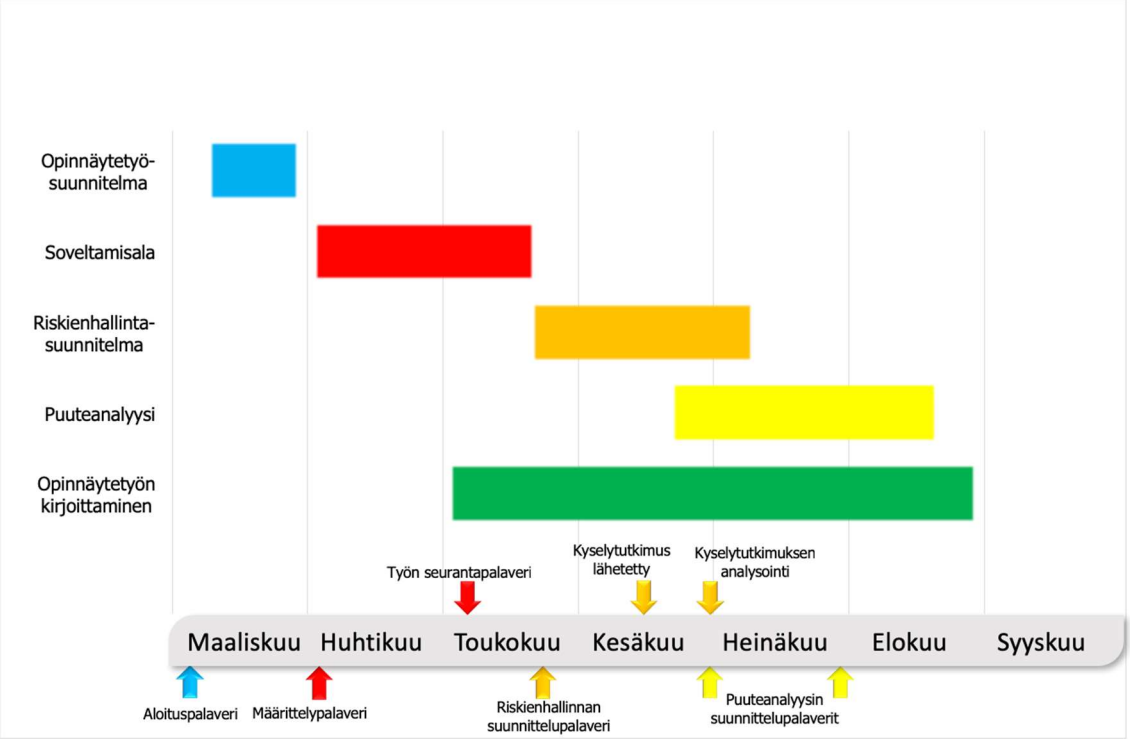
Organisaation tietoturvallisuuden toimintamallia tulee katselmoida säännöllisesti tai kun tapahtuu merkittäviä muutoksia. Näin varmistutaan tietoturvallisuuden hallintajärjestelmän sopivuudesta, riittävyydestä ja tehokkuudesta. Katselmoinnin tulee sisältää tietoturvallisuuden toimintamallin arviointi, johon sisältyvät politiikat, valvontatavoitteet, muutostarpeet ja parannusmahdollisuudet. (SFS ry. 2017b, 85.)

4 KEHITYSHANKE

4.1 Alustavat valmistelut

Hanke aloitettiin etsimällä materiaalia ISO/IEC 27001 -standardista. ISO/IEC 27001 -standardi oli lähtökohta, jonka lukemisen jälkeen alkoi hahmottua, mitä standardin vaatimukset pitävät sisällään. Tarkennuksia standardin eri kohtiin löytyi muista ISO -standardeista. Aiheen hahmottuminen kuitenkin vaati melko paljon perehtymistä ja aiheeseen liittyvästä kirjallisuudesta sain lisää konkreettisempaa tietoa, joka helpotti aihealueen ymmärtämistä. Organisaation toimintaympäristö ja -tavat olivat jo entuudestaan tuttuja, minkä vuoksi pääsin helposti alkuun sisäistettyäni standardin perusajatuksen. Kävimme aloituspalavereissa läpi standardin vaatimuksia omaan organisaatioomme peilaten ja pikkuhiljaa alkoi muodostua käsitys siitä, mistä lähdemme liikkeelle.

4.2 Kehittämishankkeen aikajana



Kuvio 3. Kehittämishankkeen Gantt-kaavio.

Kuviossa 3 on esitetty kehittämisankkeen aikajana, jossa kuvataan milloin ja missä järjestyksessä projekti eteni. Työvaiheiden tarkemmat kuvaukset esitellään työssä myöhemmin.

4.3 Soveltamisala

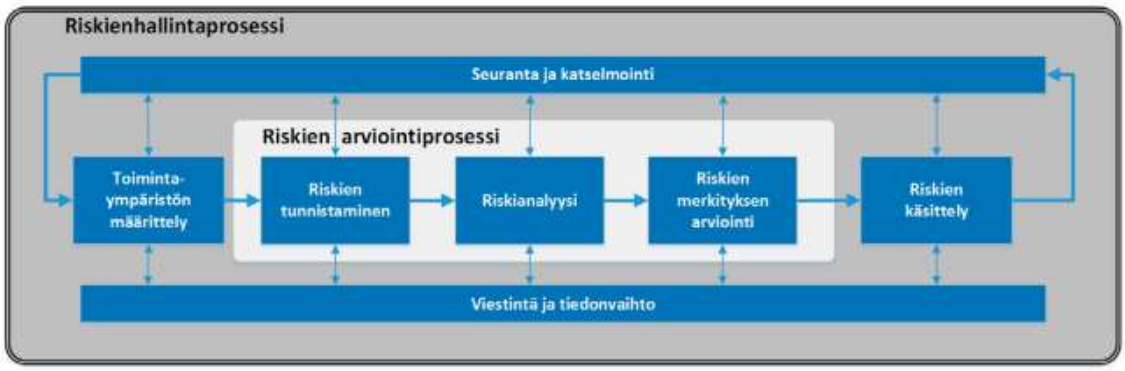
Hankkeen alussa määriteltiin soveltamisala (scope), jonka tärkeimpänä tavoitteena on määritellä, mitä tietoa halutaan suojata. Tämän työn kehityshankkeessa rajasimme soveltamisalan käsittämään valitulle asiakkaalle tuotettavan palvelun tietojen käsittelyä tietyssä toimipisteessä. Rajauksen tarkoituksena oli lähteä liikkeelle pienestä osasta organisaatiota ja saada käsitys millainen työ on suunnitella ISO/IEC 27001 -standardin mukainen tietoturvallisuuden hallintajärjestelmä. Tämän jälkeen olisi helpompi lähteä laajentamaan hallintajärjestelmää muihinkin organisaation osiin, kun on tiedossa miten projekti etenee ja mitä se vaatii. Lisäksi tämän opinnäytetyön kannalta koko organisaation kattava tietoturvallisuuden hallintajärjestelmä olisi ollut liian laaja projekti suhteutettuna käytettävissä oleviin resursseihin.

Kokonaisuuden rajauksen jälkeen lähdimme määrittelemään ulkoisia ja sisäisiä asioita, jotka ovat olennaisia oman organisaation, sekä asiakkaan kannalta ja joilla on vaikutusta tietoturvallisuuden hallintajärjestelmältä vaadittuihin tuloksiin. Tietoturvallisuuden hallintajärjestelmään vaikuttavat sisäiset ja ulkoiset sidosryhmät ja niiden turvallisuusvaatimukset määriteltiin. Organisaation suorittamien toimintojen rajapinnat ja riippuvuudet jaoteltiin kolmeen pääryhmään, jotka olivat ihmiset, prosessit ja teknologiat. Ihmisiin kuuluvat kaikki henkilöt ja ryhmät, jotka osallistuvat millä tahansa tavalla soveltamisalassa määritellyn alueen tehtäviin tai joilla on vaikutusta päätöksiin. Prosesseihin listattiin kaikki prosessit, jotka vaikuttavat hallintajärjestelmään, kuten esimerkiksi tapahtumanhallinnanprosessi. Teknologioihin kuuluvat ohjelmistot sekä muut teknologiat sekä kaikki fyysiset laitteet. Selvennykseksi teimme myös listat asioista, jotka kuuluvat tai eivät kuulu soveltamisalaan.

4.4 Riskienhallinta

Riskienhallintaan käytimme VAHTI-ohjeen riskienhallintaprosessin mukaista riskiarviointityökalua. Kuviossa 4 esitetty VAHTI- ohjeen riskienhallintaprosessi perustuu ISO

31000- standardiin, joka on siten yhteensopiva ISO/IEC 27001 -standardin kanssa. Riskienhallintaprosessissa kuvataan riskeille tehtävät toimenpiteet, joissa noudatetaan johdon hyväksymiä toimintamalleja, -ohjeita ja riskienhallintapolitiikkaa.



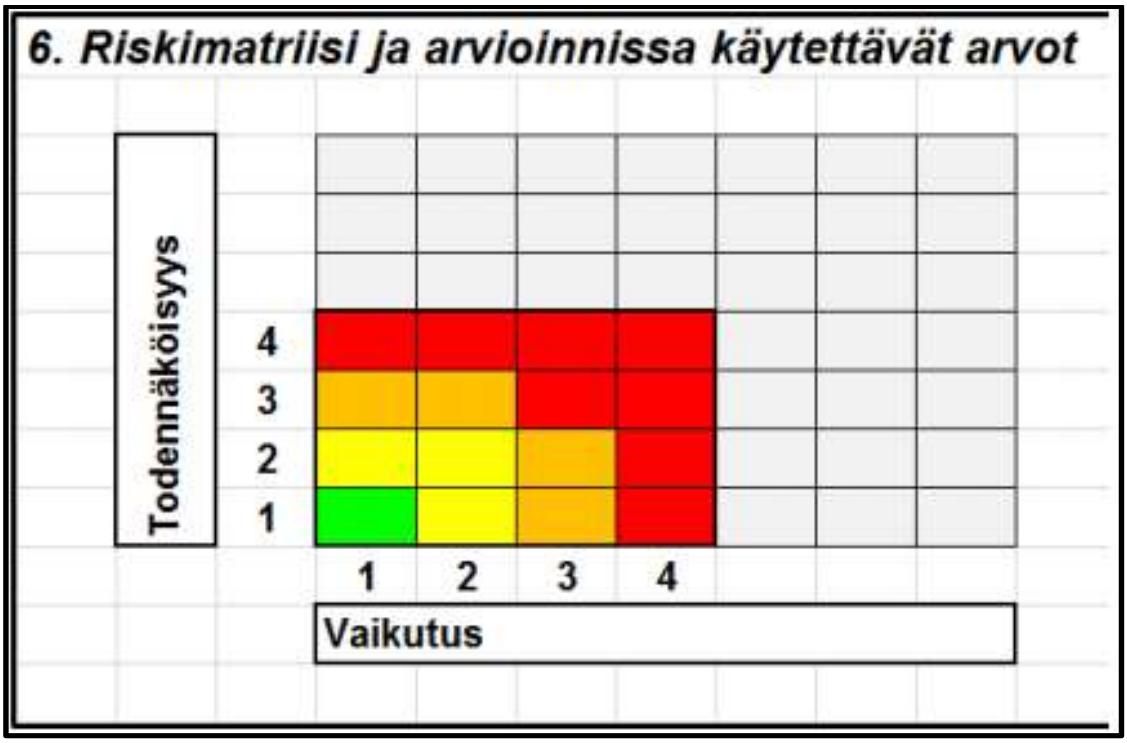
Kuvio 4. Riskienhallintaprosessi (Kangas 2017, 2.)

Toimintaympäristön määrittely tehtiin osittain jo soveltamisalaa määriteltäessä. Rajasimme kuitenkin tarkemmin ulkoista ja sisäistä toimintaympäristöä, jotta saimme kokonaisvaltaisen kuvan siitä, mihin riskejä kohdistuu. Tavoitteena oli hahmottaa organisaation toiminnot, palvelut, prosessit, tietojärjestelmät ja tietovarannot, sekä näiden keskinäiset riippuvuudet ja kriittisyys. Suljimme pois muutamia kohtia, jotka esiintyvät ISO/IEC 27001 -standardin hallintatavoitteiden ja -keinojen viiteluettelossa. Poissuljetut kohdat eivät suoranaisesti liittyneet soveltamisalan toimintaympäristöön ja sen vuoksi niiden hallintakeinoja ei tässä työssä otettu käyttöön. Tulevaisuudessa organisaation laajentaessa tietoturvallisuuden hallintajärjestelmäänsä tulee nämä kuitenkin ottaa käyttöön. Riskienhallinnan avulla kuitenkin määriteltiin poissuljettujen kohtien tietoturvan taso riittäväksi, jotta niistä ei aiheudu vaikutusta soveltamisalan toimintaympäristöön.

Riskien tunnistamisella pyrittiin havaitsemaan merkittävät riskitekijät, niiden lähteet, vaikutusalueet sekä mahdolliset olosuhteiden muutokset. Tunnistamisen kattavuuden varmistamiseksi valittiin henkilöitä, joiden asiantuntemus toiminnasta on riittävä ja heille lähetettiin sähköpostikysely. Kyselyn tarkoituksena oli saada laaja-alainen kuva riskitekijöistä. Aiemmin tunnistettujen riskien lisäksi kyselyllä saatiin esiin huomioitavia asioita, jotka olivat vielä tunnistamatta.

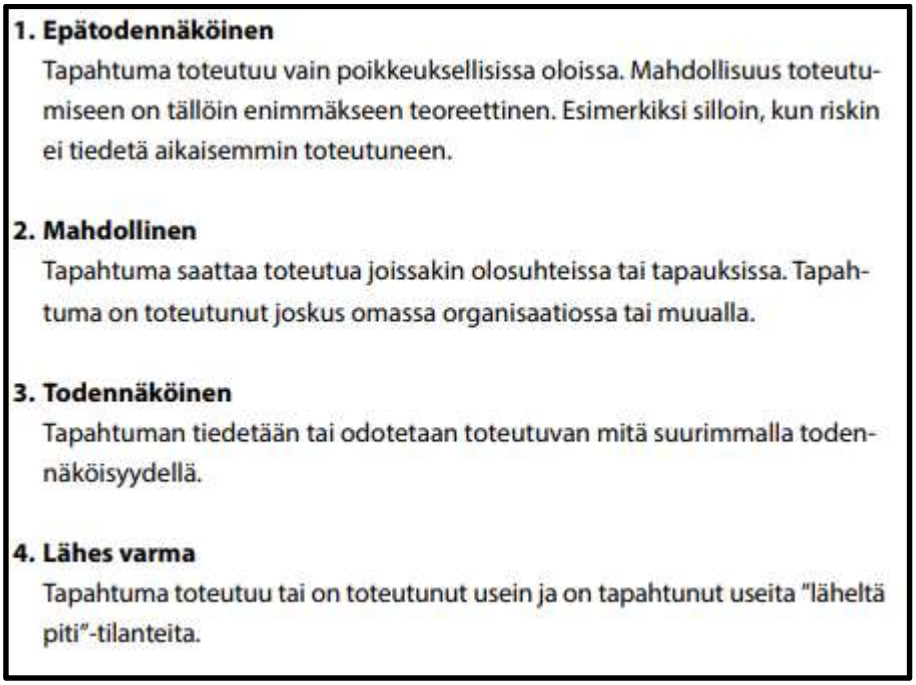
Riskianalyysissä arvioitiin riskin toteutumisen todennäköisyyttä ja vaikutusta riskimatriisin avulla. Riskimatriisi havainnollistaa riskin merkittävyyttä ja sitä, miten riski sijoittuu

suhteessa muihin riskeihin. Esimerkki riskimatriisista on esitetty kuviossa 5. Riskimatriisia tukevana riskianalyysimenetelmänä käytettiin kvalitatiivista menetelmää, jossa riskejä pyrittiin kuvailemaan mahdollisimman tarkasti. Riskianalyysin avulla luotiin selkeä perusta päätöksille, miten riskejä käsitellään.

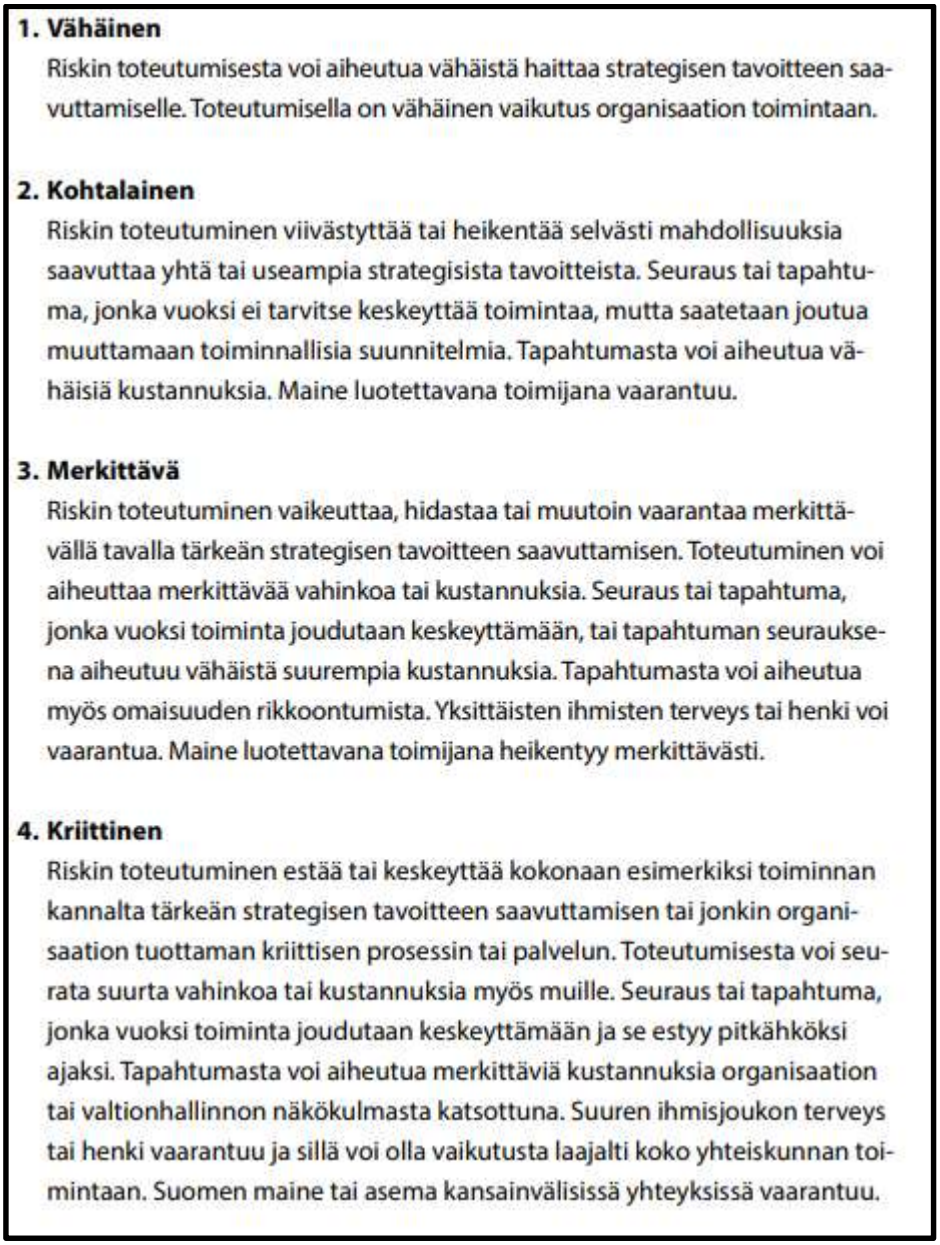


Kuvio 5. Riskimatriisi (Kangas 2017, 6.)

Todennäköisyyden ja vaikutuksen arvioinnissa käytettiin molemmissa neliportaista asteikkoa, joiden perusteet on esitetty kuvioissa 6 ja 7.



Kuvio 6. Todennäköisyyden arvioinnin asteikko (Rousku 2017, 23.)



1. Vähäinen

Riskin toteutumisesta voi aiheutua vähäistä haittaa strategisen tavoitteen saavuttamiselle. Toteutumisella on vähäinen vaikutus organisaation toimintaan.

2. Kohtalainen

Riskin toteutuminen viivästyttää tai heikentää selvästi mahdollisuuksia saavuttaa yhtä tai useampia strategisista tavoitteista. Seuraus tai tapahtuma, jonka vuoksi ei tarvitse keskeyttää toimintaa, mutta saatetaan joutua muuttamaan toiminnallisia suunnitelmia. Tapahtumasta voi aiheutua vähäisiä kustannuksia. Maine luotettavana toimijana vaarantuu.

3. Merkittävä

Riskin toteutuminen vaikeuttaa, hidastaa tai muutoin vaarantaa merkittävällä tavalla tärkeän strategisen tavoitteen saavuttamisen. Toteutuminen voi aiheuttaa merkittävää vahinkoa tai kustannuksia. Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään, tai tapahtuman seurauksena aiheutuu vähäistä suurempia kustannuksia. Tapahtumasta voi aiheutua myös omaisuuden rikkoontumista. Yksittäisten ihmisten terveys tai henki voi vaarantua. Maine luotettavana toimijana heikentyy merkittävästi.

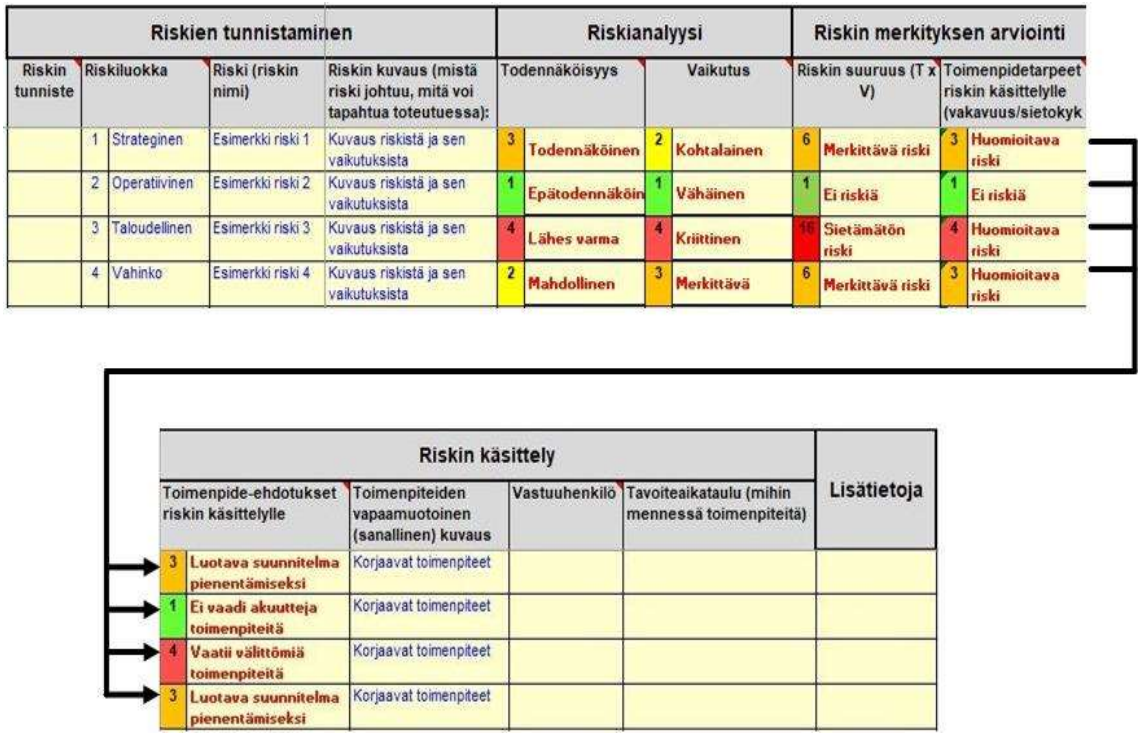
4. Kriittinen

Riskin toteutuminen estää tai keskeyttää kokonaan esimerkiksi toiminnan kannalta tärkeän strategisen tavoitteen saavuttamisen tai jonkin organisaation tuottaman kriittisen prosessin tai palvelun. Toteutumisesta voi seurata suurta vahinkoa tai kustannuksia myös muille. Seuraus tai tapahtuma, jonka vuoksi toiminta joudutaan keskeyttämään ja se estyy pitkähköksi ajaksi. Tapahtumasta voi aiheutua merkittäviä kustannuksia organisaation tai valtionhallinnon näkökulmasta katsottuna. Suuren ihmisjoukon terveys tai henki vaarantuu ja sillä voi olla vaikutusta laajalti koko yhteiskunnan toimintaan. Suomen maine tai asema kansainvälisissä yhteyksissä vaarantuu.

Kuvio 7. Vaikutuksen arvioinnin asteikko (Rousku 2017, 24.)

Riskien merkityksen arvioinnin avulla hahmottuvat selkeästi riskien käsittelytarpeet ja ne pystytään helposti järjestämään tärkeyden mukaan. Riskin suuruus syntyy vaikutuksen ja todennäköisyyden tulosta. Riskien merkityksen arvioinnissa käytimme apuna VAHTI-ohjeen riskiarviontityökalua, joka määrittää riskin suuruuden perusteella tarvitseeko riski jatkotoimenpiteitä. (Kangas 2017, 10.)

Taulukko 1. Esimerkki riskien merkityksen arvioinnista.



Riskien tunnistaminen				Riskianalyysi				Riskin merkityksen arviointi			
Riskin tunniste	Riskiluokka		Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys		Vaikutus		Riskin suuruus (T x V)		Toimenpidetarpeet riskin käsittelylle (vakavuus/sietokyk
	1	Strateginen	Esimerkki riski 1	Kuvaus riskistä ja sen vaikutuksista	3	Todennäköinen	2	Kohtalainen	6	Merkittävä riski	3 Huomioitava riski
	2	Operatiivinen	Esimerkki riski 2	Kuvaus riskistä ja sen vaikutuksista	1	Epätodennäköin	1	Vähäinen	1	Ei riskiä	1 Ei riskiä
	3	Taloudellinen	Esimerkki riski 3	Kuvaus riskistä ja sen vaikutuksista	4	Lähes varma	4	Kriittinen	16	Sietämätön riski	4 Huomioitava riski
	4	Vahinko	Esimerkki riski 4	Kuvaus riskistä ja sen vaikutuksista	2	Mahdollinen	3	Merkittävä	6	Merkittävä riski	3 Huomioitava riski

Riskin käsittely				Lisätietoja
Toimenpide-ehdotukset riskin käsittelylle	Toimenpiteiden vapaamuotoinen (sanallinen) kuvaus	Vastuuhenkilö	Tavoiteaikataulu (mihin mennessä toimenpiteitä)	
3 Luotava suunnitelma pienentämiseksi	Korjaavat toimenpiteet			
1 Ei vaadi akuutteja toimenpiteitä	Korjaavat toimenpiteet			
4 Vaatii välittömiä toimenpiteitä	Korjaavat toimenpiteet			
3 Luotava suunnitelma pienentämiseksi	Korjaavat toimenpiteet			

Riskien merkityksen arvioinnin yhteydessä riskeille määritellään tarvittavat jatkotoimenpiteet, sekä vastuuhenkilöt ja tavoiteaikataulu korjaaville toimenpiteille. Jatkotoimenpiteiden avulla riskejä pyritään poistamaan, hallitsemaan tai tehdään päätös ettei jatkotoimenpiteitä tarvita. Jatkotoimenpiteiden keinoja ovat esimerkiksi riskin aiheuttaman toiminnan päättäminen, riskin lähteeseen tai sen todennäköisyyteen vaikuttaminen, seurauksiin varautuminen tai riskin jakaminen osiin. Tietynlaisiin riskeihin voidaan varautua myös hankkimalla vakuutus ja joissain tapauksissa riskinotto saattaa kannattaa jonkin mahdollisuuden saavuttamiseksi. (Kangas 2017, 10-12.) Riskien jatkuva seuranta ja katselmointi ovat osa riskienhallintaprosessia, joita toteutetaan säännöllisesti.

4.4.1 Kyselytutkimus

Kattavan ja vaikuttavan riskienhallinnan saavuttamiseksi tehtiin laadullinen kyselytutkimus, jonka tavoitteena oli selvittää työn soveltamisalaan kohdistuvia riskitekijöitä. Tutkimus suoritettiin sähköpostikyselynä kesäkuussa ja vastauksille annettiin aikaa kaksi viikkoa. Kysely lähetettiin kolmelletoista aiheen parissa työskentelevälle henkilölle sekä kolmelle heitä johtavalle esimiehelle. Tutkimustavaksi valittiin teemahaastattelun sijasta

sähköpostikysely henkilöstön ajan säästämiseksi ja korkeamman vastausprosentin saavuttamiseksi. Kysely rajattiin käsittelemään ainoastaan riskitekijöitä, joilla on vaikutusta tiedon luottamuksellisuuteen, eheyteen tai saatavuuteen. Kysymyslomakkeessa oli vain yksi kysymys, jonka vastaukset tuli laittaa kriittisyysjärjestykseen. Kysymys oli, millaisia riskitekijöitä liittyy valitun asiakkaan tapahtumanhallinnan tietojen käsittelyyn valitussa toimipisteessä. Pohjustuksen avulla tavoitteena oli saada esitettyyn kysymykseen keskustelua herättäviä vastauksia. Saatujen vastauksien avulla oli tarkoituksena saavuttaa laajamittaisempi näkemys mahdollisesti huomioimattomista riskitekijöistä. Kyselyllä saatuja vastauksia hyödynnetään riskianalyysissä ja ne sijoitetaan riskimatriisin vaikutukseksi analysoinnin jälkeen.

Kyselyyn vastasi seitsemän työntekijää sekä yksi heidän esimiehensä. Vastausprosentiksi saatiin 50%, koska kuudestatoista henkilöstä kahdeksan vastasi määrä-ajassa kyselyyn. Vastausten määrä oli kohtalaisen hyvä, koska kysely järjestettiin kesälomakauden aikana ja kyselyyn annettu aika oli suhteellisen lyhyt. Kysely tuotti hyvän lopputuloksen ja vastauksena saatiin paljon toiminnassa mahdollisesti ilmeneviä riskejä. Mikäli olosuhteet olisivat sen sallineet, kysely olisi ollut parempi toteuttaa teemahaastatteluna. Usean henkilön kohdalla kyselyn tarkoitus ei aluksi selvinnyt ja siksi he joutuivat kysymään tarkennusta henkilökohtaisesti. Tarkennusten jälkeen henkilöt ymmärsivät paremmin kyselyn tarkoituksen ja tämän vuoksi osasivat tuottaa parempia ja konkreettisempia vastauksia.

Kyselyn tuloksia analysoitiin Excel-ohjelmistolla ja vastauksien perusteella muodostettiin tarvittavat kategoriat, joiden avulla vastaukset saatiin luokiteltuun muotoon syvällisempää analyysiä varten.

Taulukko 2. Riskikategoriat

Kategorian väri	Kategorian selitys
5	Henkilöstön tietovuotoon, irtisanoutumiseen, sairastumiseen, kuolemaan tai muun hiljaisen tieton menettämiseen liittyvä riski
4	Henkilökunnan osaamiseen, tarkkuuteen tai motivaatioon liittyvä riski
6	Dokumentoinnin luottamuksellisuuteen, eheyteen tai saatavuuteen liittyvä riski
9	Ohjelmistoon, konfigurointivirheeseen tai hallintajärjestelmän käytettävyyteen liittyvä riski
6	Laiterikkoon tai laitteiden korjaukseen liittyvä riski
4	Prosessiin tai päätöksentekoon liittyvä riski

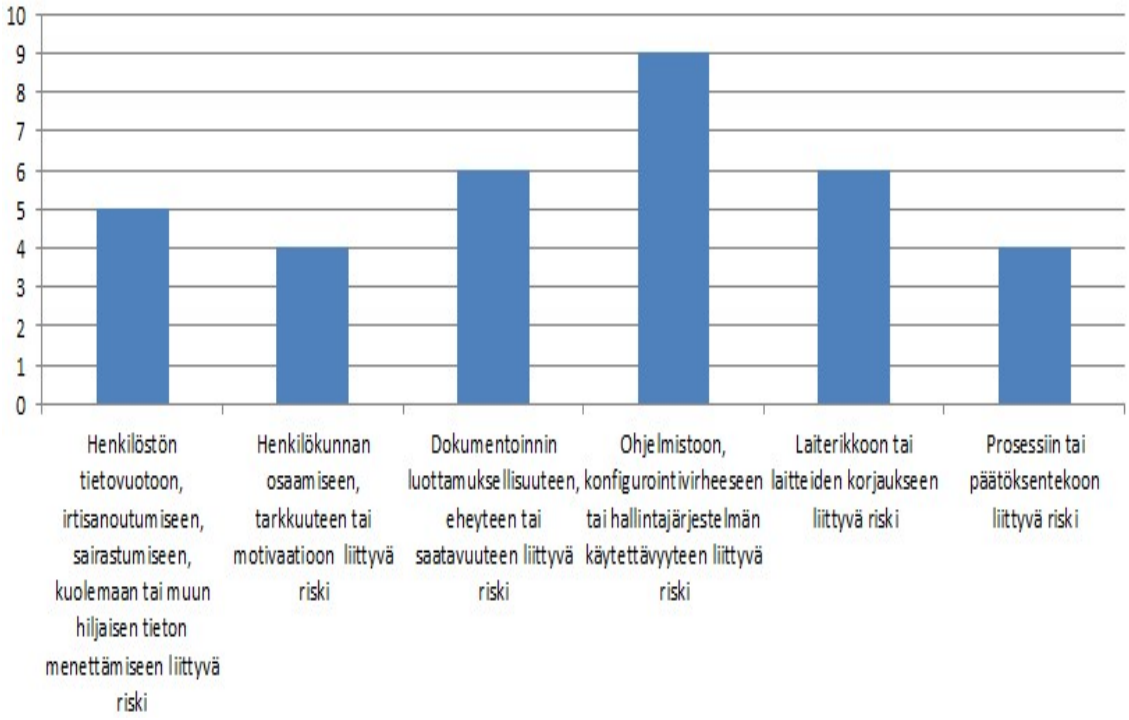
Taulukossa 2 on esitetty riskikategoriat, analysoinnissa käytetyt värit sekä kaikissa kategorioissa esiintyneiden riskien määrä.

Kyselyn riskikategoriat määriteltiin vastausten perusteella. Kategorisoinnin tarkoituksena oli tarkkojen tietojen suodattaminen, sekä saada vastaukset helpommin analysoitavaan ja esitettävään muotoon. Kategorisoinnin perustana käytettiin organisaation suorittamien toimintojen rajapintojen ja riippuvuuksien kolmea pääryhmää, ihmisiä, prosesseja, sekä teknologioita.

Taulukko 3. Kyselyn tulokset taulukoituna.

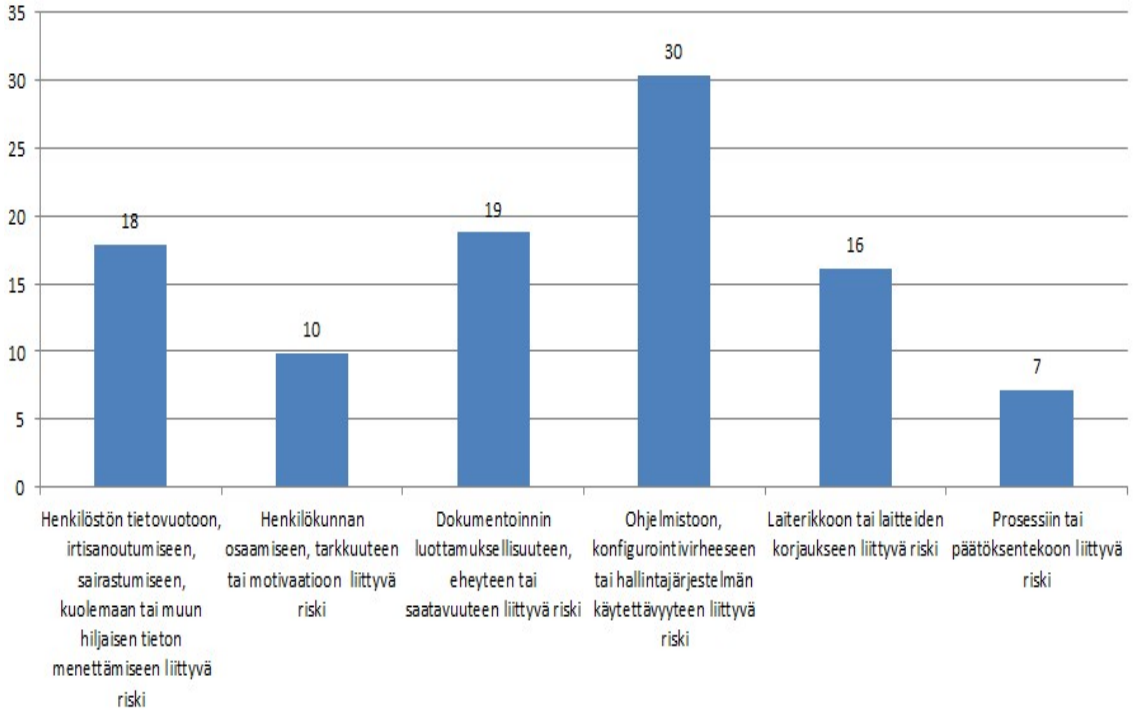
Kriittisyys järjestys	Vastaus 1	Vastaus 2	Vastaus 3	Vastaus 4	Vastaus 5	Vastaus 6	Vastaus 7	Vastaus 8	Pisteytys
1									5
2								4	4
3									3
4							2		2
5		1				1			1

Taulukossa 3 on esitetty kyselyn tulokset taulukoituna kategorioiden värien mukaisesti. Varsinaiset vastaukset on tietoturvallisuussyistä poistettu julkisesta työstä. Taulukon ensimmäinen sarake kuvaa kriittisyysjärjestystä, jossa yksi on kriittisin ja viisi vähiten kriittinen. Taulukon viimeisissä sarakkeessa on vastaavasti kriittisyyden pisteytys myöhempää analyysia varten. Tumman harmaat ruudut eivät sisältäneet vastausta. Tulokset on merkitty taulukossa 2 esitettyjen kategorioiden värien mukaisesti. Jokainen taulukon kategorisoitu solu ja sen pisteytys laskettiin kategorioittain yhteen, josta muodostui kategorian kokonaiskriittisyys pisteytys. Esimerkiksi prosessiin tai päätöksentekoon liittyvän riskin jokaisen solun pisteytys on esitetty taulukossa 3. Solujen pisteiden yhteenlaskulla muodostuu kategorian kokonaiskriittisyys pisteytys, josta myöhemmässä vaiheessa lasketaan prosentuaalinen osuus kokonaispisteisiin suhteutettuna.



Kuvio 8. Vastausten lukumäärä kategorioittain (vastauksia yhteensä 34 kpl).

Kyselyn vastausten tuloksena saatiin yhteensä 34 riskiä, jotka ovat esitettynä kuviossa 8 kategorioittain.



Kuvio 9. Vastaukset analysoituna ja pisteytettynä. Pystyakselilla kuvataan pisteytyksen jälkeistä prosenttiosuutta kokonaismäärästä.

Taulukon 3 kohdat pisteytettiin kriittisyyden mukaan siten, että kriittisyysluokka yksi oli viiden pisteen arvoinen, kun taas kriittisyysluokka viisi oli yhden pisteen arvoinen. Tämän jälkeen kunkin kategorian pisteet laskettiin yhteen. Kaikkien kategorioiden pisteiden summasta laskettiin prosenttiosuudet kullekin kategorialle. Kuviossa 8 on esitettynä tulosten pisteytetyt prosenttiosuudet.

Kyselyn perusteella suurin riski toiminnan jatkumiselle aiheutuu ohjelmistojen toimimattomuudesta, konfigurointivirheestä tai hallintajärjestelmän käytettävyyden menettämisestä. Tämä kategoria sai kolmekymmentä prosenttia kaikista yhteenlasketuista pisteistä.

Keskitason riskeistä yhdeksäntoista prosenttia pisteistä liittyi dokumentoinnin luottamuksellisuuteen, eheyteen tai saatavuuteen liittyvään riskiin. Henkilöstön tietovuotoon, irtisanoutumiseen, sairastumiseen, kuolemaan tai hiljaisen tiedon menettämiseen liittyvä riski sai kahdeksantoista prosenttia pisteistä. Laitteiden hajoamiseen ja korjaukseen liittyvät riskit saivat kuusitoista prosenttia pisteistä.

Pienimmät riskitekijät olivat henkilökunnan osaamiseen, tarkkuuteen tai motivaatioon liittyvät riskit kymmenellä prosentilla pisteistä ja prosessiin tai päätöksentekoon liittyvät riskit, jotka saivat seitsemän prosenttia kaikista pisteistä.

4.5 Puuteanalyysi (GAP-analyysi)

Puuteanalyysin (GAP-analyysi) tavoitteena oli selvittää organisaation nykytilaa suhteessa ISO/IEC 27001 -standardin vaatimuksiin. Analyysiin sisällytimme liitteen A hallintakeinoja, jotka sisältyivät työn soveltamisalaan. Muutamia hallintakeinoja rajasimme pois, koska niille ei ollut riskianalyysin perusteella tarvetta. Tavoitteena oli, että analyysi tuottaa selkeän kuvan organisaation nykytilasta ja suoritettavista toimenpiteistä, joita vaaditaan vaatimusten täyttämiseksi.

Puuteanalyysin vaatimukset on esitelty tämän opinnäytetyön teoriaosuudessa ja niiden pohjalta lähdimme suunnittelemaan analyysiä. Analysointityökaluksi valitsimme internetistä löytyvän Excel- pohjaisen työkalun. (Ramge 2015) Työkalu oli yksinkertainen käyttää ja sen avulla työn etenemisen seuraaminen helpottui. Työkalu sisälsi kaikki hallintakeinot sekä kysymyksiä niiden täyttymisestä. Työkaluun täytetään prosentuaalisesti kunkin kohdan valmiusaste ja sen vuoksi suunnittelimme yhtenevät vaatimukset kullekin valmiusasteelle. Valmiusasteet ja niiden selitykset on esitettynä taulukossa 4.

Taulukko 4. Puuteanalyysin työkalun valmiusasteet ja niiden selitys.

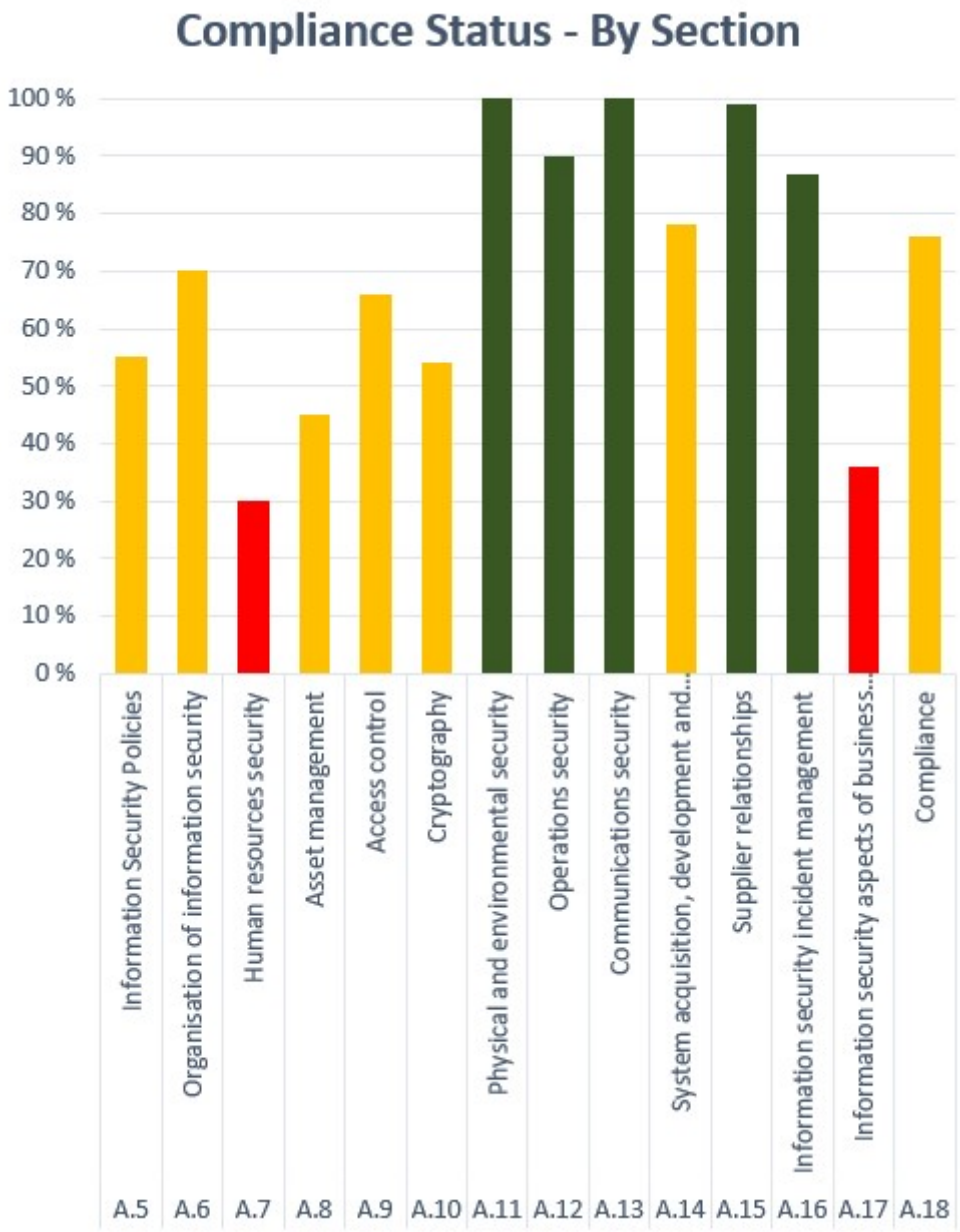
Valmiusaste (%)	Valmiusasteen selitys
0 %	Ei aloitettu
20 %	Suunnitelma toteuttamiseksi valmis
40 %	Suunnitelman toteutus käynnissä
60 %	Suunnitelma toteutettu
80 %	Jalkautettu tuotantoon
100 %	Ohjeistus ja dokumentointi valmis

Valmiusasteen seuranta eteni kahdenkymmenen prosentin portain. Ennen seuraavaan portaaseen siirtymistä kaikkien edellisten vaiheiden tuli olla valmiina.

Taulukko 5. Esimerkki puuteanalyysi työkalusta.

Reference		Compliance Assessment		Results		
Checklist	Standard Section			Status	Details	Documents
	A.13	Communications Security				
	A.13.1	Network security management				
	A.13.1.1	Network controls		80 %		
			Is there a network management process in place?	80 %		
	A.13.1.2	Security of network services		33 %		
			Does the organisation implement a risk management approach which identifies all network services and service agreements?	60 %		
			Is security mandated in agreements and contracts with service providers (in house and outsourced)?	20 %		
			Are security related SLAs mandated?	20 %		
	A.13.1.3	Segregation in networks		100 %		
			Does the network topology enforce segregation of networks for different tasks?	100 %		

Taulukossa 5 on esitetty esimerkki puuteanalyysityökalusta. Taulukossa näkyvät hallintakeinot sekä niiden tarkentavat vaatimukset ja valmiusasteet. Details- kenttään kerättiin tietoa toimenpiteistä, joita vaaditaan tavoitetilan saavuttamiseksi. Documents- kenttään kuvattiin aiheeseen liittyvät valmiit dokumentit ja niiden sijainti. Kun kaikki valitut hallintakeinot oli käyty läpi, muodostui kuviossa 10 esitetty kuvaaja työn valmiusasteesta.



Kuvio 10. Esimerkki puuteanalyysin kokonaisvalmiusasteesta. Värien selitykset ovat kuvattuna taulukossa 4. sivulla 35.

Kuviossa 10 on esimerkki puuteanalyysi työkalun kokonaisvalmiusastetta esittävästä kuvaajasta. Kuvaajan tulokset on esitetty kategorioittain ISO/IEC 27001 -standardin mukaisesti.

5 POHDINTA

Työn tavoitteena oli tutustua ISO/IEC 27001 -standardiin ja tuottaa suunnitelma standardin vaatimukset täyttävän tietoturvallisuuden hallintajärjestelmän käyttöönottamiseksi toimeksiantajayritykseen. Työ aloitettiin rajaamalla tietoturvallisuuden hallintajärjestelmän soveltamisala kohdeyrityksessä.

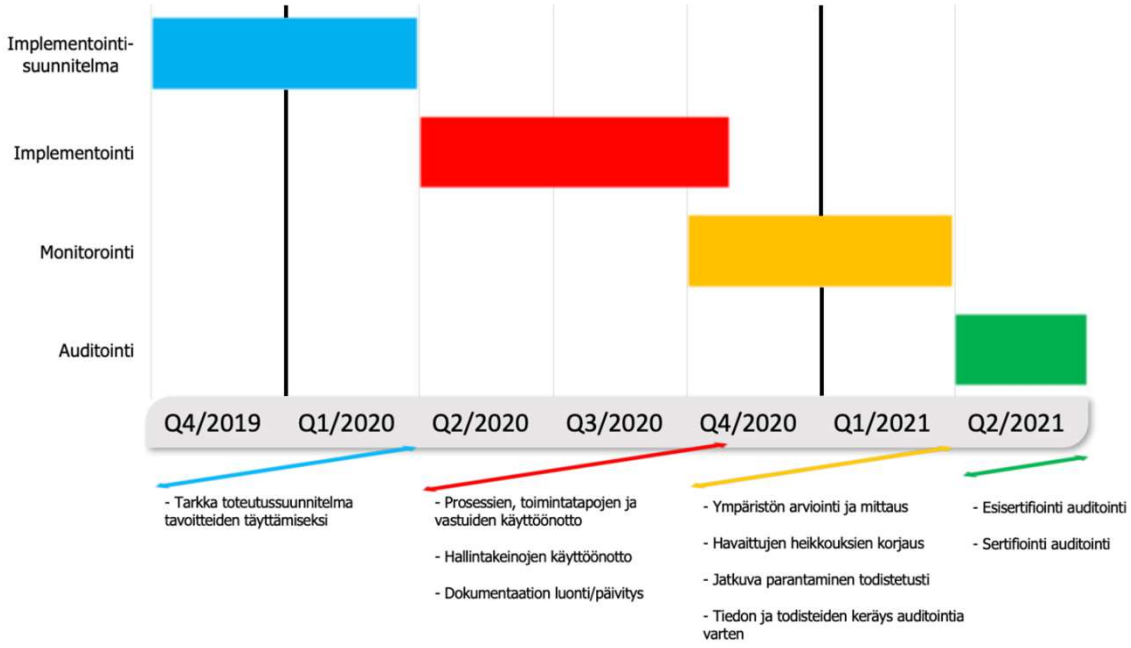
Kuten Kuivalainen opinnäytetyössään toteaa, vaatii ISO/IEC 27001 -standardin mukainen tietoturvallisuuden hallintajärjestelmä organisaation jatkuvaa panostusta ja sitoutumista. Lisäksi käyttöönottovaiheessa projekti muodostuu todella raskaaksi, jos organisaatiossa tietoturvallisuuden perusasiat eivät ole kunnossa. (Kuivalainen 2011, 47.) Toimeksiantajayritykseni tapauksessa tietoturvaa oli kehitetty standardin suuntaisesti ja monissa asioissa pienet korjaukset riittivät täyttämään standardin vaatimukset. Sama johtopäätös tehtiin kuitenkin työn edetessä ja vaatimusten täyttymistä määriteltäessä.

Olennainen osa työtä ja sen etenemisen mahdollistamista oli riskienhallintasuunnitelma. Riskienhallintaprosessi ohjaa riskienhallintaa ja sen ensimmäisessä vaiheessa pitää tunnistaa soveltamisalan riskit. Aiemmin tunnistettujen riskien lisäksi suunniteltiin työntekijöille kysely, jonka avulla saavutettiin kattavampi kuva mahdollisista riskitekijöistä. Riskit analysoitiin niiden tunnistamisen jälkeen ja niiden merkitystä arvioitiin VAHTI-ohjeen riskienarviointityökalulla. Edellä mainittujen toimenpiteiden avulla saavutettiin kattava riskienhallintasuunnitelma.

Riskienhallintasuunnitelman pohjalta käynnistettiin puuteanalyysi, jonka tavoitteena oli saavuttaa tarkka kuva toimeksiantajan nykytilasta suhteutettuna standardin vaatimuksiin. Puuteanalyysiin valittiin ISO/IEC 27001 liitteen A hallintatavoitteiden ja -keinojen viiteluettelosta kohdat, jotka sisältyivät työn soveltamisalaan. Nämä kohdat läpikäymällä tunnistettiin ja kirjattiin ylös toimenpiteet, jotka tulee suorittaa vaatimusten täyttämiseksi. Kuten Niemimaa toteaa blogissaan: ”*Usein yllättävän monet vaatimuksista täyttyvät, vaikka organisaatiolla ei olisikaan aiemmin ollut käytössä ”virallista” tietoturvallisuuden hallintajärjestelmää.”* (Niemimaa 2018) Vastaava havainto tehtiin puuteanalyysin edetessä, monet kohdat täyttivät standardin vaatimukset, mutta varsinaisessa dokumentaatiossa oli puutteita.

Suoritettujen toimenpiteiden jälkeen tuotoksena oli työn soveltamisalan kattava ja kyselytutkimuksen tuloksiin perustuva riskienhallintasuunnitelma. Puuteanalyysi- dokumentissa kuvattiin ISO/IEC 27001 -standardin vaatimusten nykytila, sekä toimenpiteet vaatimusten täyttämiseksi. Dokumentit ovat luokiteltu vain viranomaiskäyttöön, jonka vuoksi ne jätettiin tämän opinnäytetyön ei-julkiseen osaan.

Jatkotoimenpiteinä toimeksiantajayritys voi aloittaa puuteanalyysissä havaittujen puutteiden täyttämisen ja käynnistää projektin, jossa kuvataan tarkemmin vaadittava toteutussuunnitelma. Toinen vaihtoehto olisi laajentaa tässä työssä opituin keinoin puuteanalyysiä muihinkin organisaation osiin ja vasta tämän jälkeen käynnistää projekti puutteiden täyttämiseksi.



Kuvio 11. Jatkotoimenpidesuunnitelma

Kuviossa 11 on kuvattu gantt-kaavion avulla suunnitelma puuteanalyysissä havaittujen puutteiden täyttämiseksi. Suunnitelmassa kuvataan tulevan työn vaiheet ja yleisellä tasolla millaisia toimenpiteitä vaiheet vaativat. Lisäksi kaaviossa kuvataan mahdollinen aikajakso työn suorittamiseksi.

Lopuksi voidaan todeta, että opinnäytetyöltä saavutettiin sille asetetut tavoitteet. Dokumentti, jossa verrataan yrityksen nykytilaa suhteessa ISO/IEC 27001 -standardin vaatimuksiin tuotti hyvän lopputuloksen ja soveltamisalaa koskevat puutteet tulivat selkeästi

esille. Lisäksi dokumentti varmisti jo aiemmin yrityksessä tehtyjen toimenpiteiden oikeellisuuden ja toi esille pienet epäkohdat esimerkiksi puutteellisesta dokumentoinnista. Kyselytutkimuksella saatiin nostettua esille mahdollisia riskitekijöitä, jotka pystytään huomioimaan yrityksen riskienhallinnassa. Näiden toimenpiteiden jälkeen toimeksiantajayrityksen on helppo lähteä jatkamaan varsinaiseen käyttöönoton suunnitteluvaiheeseen ja mahdollisesti toteuttaa sertifiointi auditointi pohjautuen tässä työssä esiteltyyn jatkotoimenpidesuunnitelmaan.

LÄHTEET

Calder, A. 2017. Nine Steps to Success: North American edition: An ISO 27001 Implementation Overview. Cambridgeshire: IT Governance Publishing Ltd.

Hinson, G.; Regalado, R.; Hodgson, E.; Williams, W.; Cort, J. & and Javed, K. 2018. Documentation and records required for ISO/IEC 27001 certification Viitattu 10.7.2019 https://iso27001security.com/ISO27k_ISMS_Mandatory_documentation_checklist_release_1v1.docx.

Kangas, A. 2017. VM 22/2017 Ohje riskienhallintaan Riskiarviointityökalu - käyttö- ja täyttöohje Viitattu 11.7.2019 https://www.vahtiohje.fi/c/document_library/get_file?uuid=40bf6302-b7b8-4afc-88ce-106c40790d88&groupId=10128.

Kosutic, D. 2016. Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own. Zagreb: EPPS Services Ltd.

Kuivalainen, M. 2011. Valmistautuminen ISO/IEC 27001 standardin sertifiointiin. Opinnäytetyö. Teknologiaosaamisen johtamisen koulutusohjelma (YAMK). Pohjois-Karjalan ammattikorkeakoulu. Viitattu 11.11.2019 http://urn.fi/URN:NBN:fi:amk-201201051080

Mataracioglu, T. 2017. Proposal for the Next Version of the ISO/IEC 27001 Standard Viitattu 10.7.2019 https://www.isaca.org/Journal/archives/2017/Volume-4/Pages/proposal-for-the-next-version-of-the-iso-iec-27001-standard.aspx?utm_referrer=.

Niemimaa, E. 2018. ISO27001-puuteanalyysi. Viitattu 16.9.2019 https://www.secrays.com/tietoturvapalvelut/iso27001/iso27001-puuteanalyysi.Ramge, R. 2015. ISO 27001 2013 Compliance audit Checklist. Viitattu 16.9.2019 https://www.scribd.com/doc/314223872/ISO-27001-2013-Compliance-audit-Checklist.

Rousku, K. 2017. Ohje riskienhallintaan Viitattu 11.7.2019 http://urn.fi/URN:ISBN:978-952-251-862-0.

SFS ry. 2017a. SFS-EN ISO/IEC 27001:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen standardisoimisliitto SFS ry.

SFS ry. 2017b. SFS-EN ISO/IEC 27002:2017. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Helsinki: Suomen standardisoimisliitto SFS ry.

SFS ry. 2017c. SFS-EN ISO/IEC 27000:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen standardisoimisliitto SFS ry.

SFS ry. 2017d. SFS-EN ISO/IEC 27003:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Ohjeistusta. Helsinki: Suomen standardisoimisliitto SFS ry.

SFS ry. 2018. SFS-EN ISO/IEC 31000:2018. Riskienhallinta. Ohjeet. Helsinki: Suomen standardisoimisliitto SFS ry.

Vahti3/2017 Viitattu 10.7.2019 https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229.

Vetikko, P. 2019. Mikä on ISO 27001 -standardi? Viitattu 10.7.2019 https://www.secrays.com/tietoturvapalvelut/iso27001/mika-on-iso-27001-standardi/.