Tampereen yliopisto

Ville Heikkinen

TIETOTURVAN HALLINTAJÄRJESTELMÄN TOTEUTTAMINEN

Onnistumistekijät toteutusprojekteissa

Diplomityö
Informaatioteknologian ja viestinnän tiedekunta
Tarkastajat: Jukka Koskinen
Helmikuu 2023

TIIVISTELMÄ

Ville Heikkinen: Tietoturvan hallintajärjestelmän toteuttaminen
Diplomityö
Tampereen yliopisto
Tietotekniikan DI-ohjelma
Helmikuu 2023

Työn tavoitteena on syventää ymmärrystä tietoturvan hallintajärjestelmän toteutusprojekteista sekä lisätä ymmärrystä tietoturvan hallintajärjestelmästä kohdeyrityksessä. Työssä tehtävän tutkimuksen tarkoituksena on tunnistaa integroivan kirjallisuuskatsauksen avulla tekijöitä, jotka edesauttavat toteutusprojektien onnistumista sekä ymmärtää syitä, joiden takia hallintajärjestelmän toteutusprojekti onnistui kohdeyrityksessä. Lisäksi työssä tehtävän kirjallisuuskatsauksen löydösten ja toteutusprojektista tunnistettujen onnistumistekijöiden perusteella luodaan malli, jota muut tietoturvan hallintajärjestelmän toteutusta harkitsevat organisaatiot voivat hyödyntää.

Työ aloitetaan esittelemällä tietoturvan ja tietoturvan hallintajärjestelmän teoriaa, kuten ISO/IEC 27000 -standardiperhettä sekä riskienhallintaan liittyviä menetelmiä. Työtä jatketaan tekemällä integroiva kirjallisuuskatsaus, jossa tutkitaan tietoturvaan ja IT:n hallintaan liittyvien projektien onnistumistekijöitä. Työn empiirisessä osuudessa toteutetaan tietoturvan hallintajärjestelmä kohdeyritykselle tapaustutkimuksena, minkä jälkeen esitellään malli, joka sisältää kirjallisuuskatsauksen ja tapaustutkimuksen perusteella tunnistettuja onnistumistekijöitä.

Kirjallisuuskatsauksen tuloksissa korostuivat johdon rooli sekä tietoturvakoulutusten merkitys. Erityisesti johdon tuki, taloudellinen tuki sekä tietoturvan tärkeyden ymmärtäminen että sen strateginen yhdenmukaisuus liiketoiminnan välillä vaikuttavat toteutusprojektien onnistumiseen. Kohdeyrityksessä tehty toteutusprojekti onnistui ja tärkeimmiksi onnistumistekijöiksi todettiin johdon tuki, tietoturvamyönteinen organisaatiokulttuuri ja aiemmat panostukset tietoturvaan. Lisäksi henkilöstö on kiinnostunut tietoturva-asioista ja henkilöstöä osallistettiin projektiin. Työssä kehitetyn mallin tärkeimmiksi onnistumistekijöiksi todettiin johdon rooli, valmistelutyö, projektinhallinta sekä motiivit hallintajärjestelmän toteuttamiselle.

Avainsanat: tietoturva, tietoturvan hallintajärjestelmä, ISO 27001, onnistumistekijä, riskienhallinta

ABSTRACT

Ville Heikkinen: Implementing an information security management system
Master's Thesis
Tampere University
Master's Programme in Information Technology
February 2023

The aim of the work is to deepen the understanding of the implementation projects of the information security management system and to increase the understanding of the information security management system in the target company. The purpose of the research carried out in the work is to identify factors that contribute to the success of implementation projects and to understand the reasons why the implementation project of the management system was successful in the target company with the help of an integrated literature review. In addition, based on the findings of the literature review and the success factors identified from the implementation project, a model is be created that can be used by other organizations considering the implementation of an information security management system.

The work begins by introducing the theory of information security and the information security management system, such as the ISO/IEC 27000 family of standards and methods related to risk management. The work is continued by conducting an integrative literature review, which examines the success factors of projects related to information security and IT governance. In the empirical part of the work, an information security management system is implemented for the target company as a case study, after which a model is presented that includes the success factors identified based on the literature review and the case study.

The results of the literature review highlighted the role of management and the importance of information security training. In particular, management support, financial support as well as understanding the importance of information security and its strategic alignment between businesses affect the success of implementation projects. The implementation project at the target company was successful and the most important success factors were found to be management support, an information security-friendly organizational culture and previous investments in information security. In addition, the personnel is interested in information security issues and the personnel was involved in the project. The most important success factors of the model developed in the work were found to be the role of management, preparatory work, project management and motives for implementing the management system.

Keywords: information security, information security management system, ISO 27001, success factor, risk management

ALKUSANAT

Onpahan ollut melkoinen matka. Opiskelut alkoivat Tampereen teknillisessä yliopistossa vuonna 2012 ja loppuivat heti perään vuonna 2023 Tampereen yliopistossa. Yliopisto on opettanut ja antanut paljon, yliopistoyhteisö sitäkin enemmän. Kiitos Spinni ja spinniläiset kaikesta. Paljon on tehty ja koettu. Kerhohuoneen sohvilla ei ole koskaan yövytty, siellä on vain on kerätty voimia kotiin siirtymiseen.

Kiitos perheelle kaikesta tuesta ja kannustuksesta opintojen suhteen. Haluan kiittää yliopistonlehtori Jukka Koskista ohjauksesta ja avusta tämän työn kirjoitusprosessin aikana. Kiitos Veikko Lindbergille työn ohjauksesta sekä painostuksesta opintojen eteenpäin viemisessä. Kiitos eräs tamperelainen huonekaluvalmistaja ja työkaverit, kohti ääretöntä ja sen yli!

Kiitos ystävät ja kaverit aiheellisista muistutuksista valmistumisen suhteen. Oli itseltä päässyt unohtumaan. Erityiskiitos Jennille sparrailusta, syväluotaavista ja säkenöivistä keskusteluista akatemian saloista tämän työn kirjoittamisen aikana. Olet kylpytakin ansainnut. Erityiskiitos Ullalle sekoilevasta, mutta inspiroivasta koutsaamisesta tämän työn parissa, tough love method works! Kiitos Ippe-koiralle viihdyttämisestä työn kirjoittamisen aikana. Luulen, että olet maailman hauskin koira. Kiitos Bistro Vilja – eli BV – täällä olen saanut viettää aikaa itseäni älykkäämpien ihmisten seurassa. Kiitos Gastropub Nordic & yhteisö myötäelämisestä. Paras henkinen lähikuppila, joka ihmisellä voi olla.

Tampereella, 23. helmikuuta 2023

Ville Heikkinen

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

CIA	Confidentiality, Integrity, Availability, Luottamuksellisuus, Eheys, Saatavuus
CSF	Critical success factors, kriittiset onnistumistekijät
ISMS	Information Security Management System, tietoturvan hallintajärjestelmä
ISO	International Organization for Standardization, kansainvälinen standardointiorganisaatio
NIST CSF	NIST Cybersecurity Framework, National Institute of Standards and Technologyn kehittämä tietoturvakehikko
NIST	National Institute of Standards, Yhdysvaltojen standardisoimisvirasto
OCTAVE	OCTAVE, Operationally Critical Threat, Asset, and Vulnerability Evaluation, riskienhallintamenetelmä
PIMS	Privacy Information Management System, henkilötietojen hallintajärjestelmä

1. JOHDANTO

Kaikkien organisaatioiden toiminnan perusluonteeseen kuuluu 2020-luvulla datan tallennus, käsittely ja siirto eri tietojärjestelmien avulla sekä niiden välillä. Sen myötä tietoturvan merkitys toiminnalle on huomattava. Mikäli tieto, data tai tietojärjestelmät eivät ole käytettävissä, yrityksen tai organisaation voi olla mahdotonta toimia ja tuottaa palveluita tai tuotteita kohderyhmilleen. Näin ollen yritykset ja organisaatiot ovat tulleet riippuvaisiksi tietojärjestelmistä ja niillä on tarve suojata tietoa ja tietojärjestelmiä siten, ettei niiden toiminnalle aiheudu häiriötä. Organisaatiot voivat kehittää tietoturvaansa monin tavoin ja yksi niistä on sen kehittäminen systemaattisesti tietoturvan hallintajärjestelmän avulla.

Työssä käydään läpi tietoturvan ja tietoturvan hallintajärjestelmän teoriaa, minkä lisäksi työssä tehdään kirjallisuustutkimus, jossa tutkitaan integroivan kirjallisuuskatsauksen avulla tietoturvan ja IT:n hallintaan liittyvien toteutus- ja käyttöönottoprojektien onnistumistekijöitä. Työn empiirisen osan muodostaa tapaustutkimus, jossa analysoidaan tutkimuksen kohteena olleen yrityksen tietoturvan hallintajärjestelmän toteutusprojektin onnistumisen syitä ja kehitetään kokemuksiin ja kirjallisuuteen perustuen malli tulevia toteutusprojekteja varten. Työn kirjoittaja vastasi hallintajärjestelmän toteutusprojektista.

1.1 Tutkimuksen tavoitteet

Tämän työn tavoitteena on syventää ymmärrystä tietoturvan hallintajärjestelmien toteutusprojekteista. Lisäksi työn tavoitteena on lisätä ymmärrystä tietoturvan hallintajärjestelmästä kohdeyrityksessä sekä tuoda hallintajärjestelmän oppeja ja käytäntöjä myös muualle organisaatioon. Näitä ovat mm. riskienhallintaprosessi, poikkeamanhallinta sekä haavoittuvuuksien seuraaminen ja hallinta. Tutkimus keskittyy seuraavien kysymysten selvittämiseen:

1. Mitkä tekijät edesauttavat tietoturvan hallintajärjestelmän toteutusprojektien onnistumisessa?
2. Mitkä syyt johtivat tutkimuksen kohdeyrityksen tietoturvan hallintajärjestelmän toteutusprojektin onnistumiseen?
3. Mitä onnistumiseen liittyvää ymmärrystä työssä syvällisesti tarkastellusta yksittäistapauksesta olisi mahdollisesti siirrettävissä muihin konteksteihin?

1.2 Tutkimuksen rajaus

Työn tutkimus toteutettiin laadullisena tutkimuksena. Työn tavoitteena oli aluksi toteuttaa tietoturvan hallintajärjestelmä ja sen toteutuksen myötä tutkimusta päätettiin painottaa onnistumistekijöihin, koska ne ilmenivät empiirisesti yllättäväksi ja kiinnostavaksi osa-alueeksi. Näitä tekijöitä analysoimalla luodaan abstraktimpi konstruktio, eräänlainen luokittelu onnistumista edesauttavista tekijöistä tämänkaltaisissa projekteissa. Työ keskittyy vain onnistumistekijöihin ja siitä rajataan pois mm. yksityiskohtaiset projektinhallintakäytännöt toteutusprojekteissa sekä organisaatiokulttuuriin liittyvät arvot ja perusoletukset.

Tutkimus keskittyy kohdeyritykseen ja erityisesti sen yhteen funktioon ja sen tuottamaan verkkopalveluun. Tutkimuksen aikana toteutettu tietoturvan hallintajärjestelmän toteutusprojekti on kertaluontoinen tapahtuma.

1.3 Tutkimuksen rakenne

Työn toisessa luvussa perehdytään tietoturvaan, sen johtamiseen ja hallintaan, ISO/IEC 27000 -standardiperheeseen, NIST Cybersecurity Frameworkiin, tietoturvariskienhallintaan sekä siihen liittyviin menetelmiin. Kolmannessa luvussa käydään läpi työssä käytettäviä menetelmiä ja aineistoja, eli laadullista tutkimusta, kirjallisuuskatsausta, hallintajärjestelmän toteutuksen taustoja kohdeyrityksessä sekä tutustutaan konstruktiiviseen tutkimusotteeseen. Neljännessä luvussa käsitellään kirjallisuuskatsauksen löydöksiä.

Luvut 2–4 luovat perustan työn myöhemmille luvuille, joissa esitellään työn empiirinen osuus. Viidennessä luvussa käydään läpi tietoturvan hallintajärjestelmän toteutusprojektia, sen taustoja ja tietoturvan tilaa kohdeyrityksessä sekä hallintajärjestelmään liittyvässä verkkopalvelussa. Kuudennessa luvussa analysoidaan onnistumistekijöitä tietoturvan hallintajärjestelmän toteutusprojekteissa sekä kehitetään konstruktio hallintajärjestelmän toteutusprojekteja varten. Seitsemännessä luvussa esitetään yhteenveto ja johtopäätökset sekä pohditaan aiheeseen liittyviä jatkotutkimusaiheita.

2. TIETOTURVA JA SEN JOHTAMINEN

Tässä luvussa käydään ensimmäisenä läpi oleellisimpia tietoturvan perusperiaatteita ja siihen liittyviä käsitteitä. Seuraavaksi käsitellään tietoturvan hallintajärjestelmää sekä siihen liittyviä tietoturvastandardeja. Lopuksi tässä luvussa käsitellään kahta yleistä riskienarviointimenetelmää sekä vertaillaan niiden soveltuvuutta eri organisaatioille.

2.1 Tietoturva

Tietoturva tai tietoturvallisuus voidaan nähdä turvallisuuden tai kokonaisturvallisuuden yhtenä alakäsitteenä. Turvallisuudesta (engl. *security*) puhuttaessa tarkoitetaan toimintaa tai toimintoja, joilla pyritään riskien ja uhkien hallitsemiseen sekä ehkäisemiseen [35]. Yhdysvaltojen standardisoimisvirasto NIST:n (National Institute of Standards) [18] mukaan tietoturvan määritelmä on ”tiedon ja tietojärjestelmien suojaaminen luvattomalta pääsyltä, käytöltä, paljastamiselta, häirinnältä, muokkaukselta tai tuhoamiselta eheyden, luottamuksellisuuden ja saatavuuden takaamiseksi”. Kansainvälinen standardointiorganisaatio ISO:n (International Organization for Standardization) julkaisema ISO/IEC 27000 -standardi [26, s. 9] puolestaan määrittelee tietoturvallisuuden tarkoittavan ”tiedon luottamuksellisuuden, eheyden ja saatavuuden säilyttämistä”, jonka lisäksi tietoturvallisuuteen voi sisältyä muitakin ominaisuuksia kuten aitous, kiistämättömyys, vastuuvelvollisuus ja luotettavuus. Tietoturvan synonyyminä nähdään usein kyberturvallisuus. Turvallisuuskomitean vuonna 2018 tekemän määritelmän mukaan kyberturvallisuudella tarkoitetaan digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta, jonka häiriytyminen usein aiheutuu toteutuneesta tietoturvauhasta [16, s. 31].

Eräs yleisesti käytettävä määritelmä, johon myös ISO:n määritelmä nojautuu, on nk. CIA-kolmikko tai -malli, joka koostuu sanoista *confidentiality* (luottamuksellisuus), *integrity* (eheys) ja *availability* (saatavuus). CIA-kolmikon avulla tietoturva voidaan jakaa kolmeen osa-alueeseen ja sitä kautta kolmeen kysymykseen. Esimerkiksi kuinka tiedon tai tietojärjestelmän luottamuksellisuus varmistetaan, kuinka varmistutaan tiedon eheydestä ja kuinka varmistetaan tietojärjestelmän saatavuus?

Luottamuksellisuudella tarkoitetaan tiedon tai tietojärjestelmän ominaisuutta, mikä tarkoittaa ettei luvattomilla henkilöillä tai tahoilla ole pääsyä tietoihin eikä tietoja luovuteta sellaisille [28, s. 7]. Andress mainitsee esimerkkeinä luottamuksellisuuden vaarantumisesta

mm. dataa sisältävän kannettavan tietokoneen katoamisen ja sähköpostin liitteen lähettämisen väärälle henkilölle [3, s. 6]. Myös yrityksen tai organisaation asiakastietojen vuotaminen luvattomille tahoille tarkoittaa luottamuksellisuuden vaarantumista. Esimerkiksi vuonna 2020 julkisuuteen tulleessa tietomurrossa psykoterapiakeskus Vastaamon potilaiden tietojen luottamuksellisuus vaarantui tietojen jouduttua luvattoman henkilön haltuun [20].

CIA-kolmikon keskimmäisellä termillä eheydellä tarkoitetaan tiedon ominaisuutta, johon sisältyy tiedon oikeellisuus, virheettömyys ja kattavuus [28, s. 10]. Tiedon eheyden turvaamisella pyritään estämään tiedon muokkaaminen tai poisto ilman lupaa tai sen tahaton muuttuminen esimerkiksi tietojärjestelmässä tapahtuneen häiriön seurauksena. Andressin mukaan eräs esimerkki tiedon eheyden vaarantumisesta on lääketieteellisten testien tulosten muokkaaminen, jonka seurauksena potilas voi saada väärää hoitoa mikä voi johtaa potilaan kuolemaan [3, s. 6].

Saatavuudella puolestaan tarkoitetaan, että tieto tai tietojärjestelmä on hyödynnettävissä oikeutetuille käyttäjille määriteltynä tai haluttuna aikana [22, s. 20] [35][28, s. 7] . Saatavuus voi vaarantua, mikäli esimerkiksi pilvipalveluna toimitettava sähköpostijärjestelmä ei ole käytettävissä järjestelmään vaikuttavan teknisen vian, kiristyshyökkäyksen tai sähkönsyöttöongelmien takia. Toisin sanoen, jos palvelu ei ole käytettävissä silloin kuin käyttäjä odottaa ja haluaa, saatavuus on vaarantunut. Esimerkiksi Suomen Tietotoimisto STT joutui kiristyshyökkäyksen (*ransomware attack*) kohteeksi heinäkuussa 2022, minkä myötä heidän tuottamansa ja tarjoamansa uutis- ja kuvapalvelut eivät toimineet normaalisti [39].

Tietoturva voidaan rinnastaa myös laatuun. Yleisen käsityksen mukaan laadulla tarkoitetaan asiakkaiden toiveiden, odotusten ja vaatimusten täyttämistä tai jopa niiden ylittämistä. Lisäksi laatuun liittyy myös virheettömyys, esimerkiksi yrityksen toiselta hankkiman palvelun tai tuotteen virheettömyys. Myös asioiden tekeminen ensimmäisellä kerralla oikein nähdään yhtenä laadun käsitteenä. [33, s. 5-7] Yleisesti ottaen organisaatiot pyrkivät saamaan tietoturvan tason eli laadun sellaiselle tasolle, jotta tietoon ja tietojärjestelmiin liittyvät riskit eivät toteudu. Organisaation asiakkaille ja muille sidosryhmille tämä näkyy luottamuksellisuuden, eheyden ja saatavuuden säilymisenä, eli hyvänä laatuna.

2.2 Tietoturvan hallintajärjestelmä

Tietoturvan hyvä taso ei rakennu organisaatioihin itsestään eikä tietoturvaa voi ostaa kaupasta. Jotta organisaatiot voivat varmistua tietoturvan riittävästä tasosta, siihen liittyviä teknisiä ja hallinnollisia toimenpiteitä täytyy ottaa käyttöön, parantaa jatkuvasti, seurata, mitata ja ylläpitää – toisin sanoen johtaa ja hallita. Klassisen sanonnan mukaan ”mitä et mittaa, sitä et voi johtaa” [14, s. 21] mukaan tietoturvan johtaminen ja hallitseminen on vaikeaa tai jopa mahdotonta, mikäli sen tasoa ei mitata säännöllisesti. Tietoturvan kokonaisvaltaista hallitsemista varten on kehitetty malleja, tietoturvan hallintajärjestelmiä.

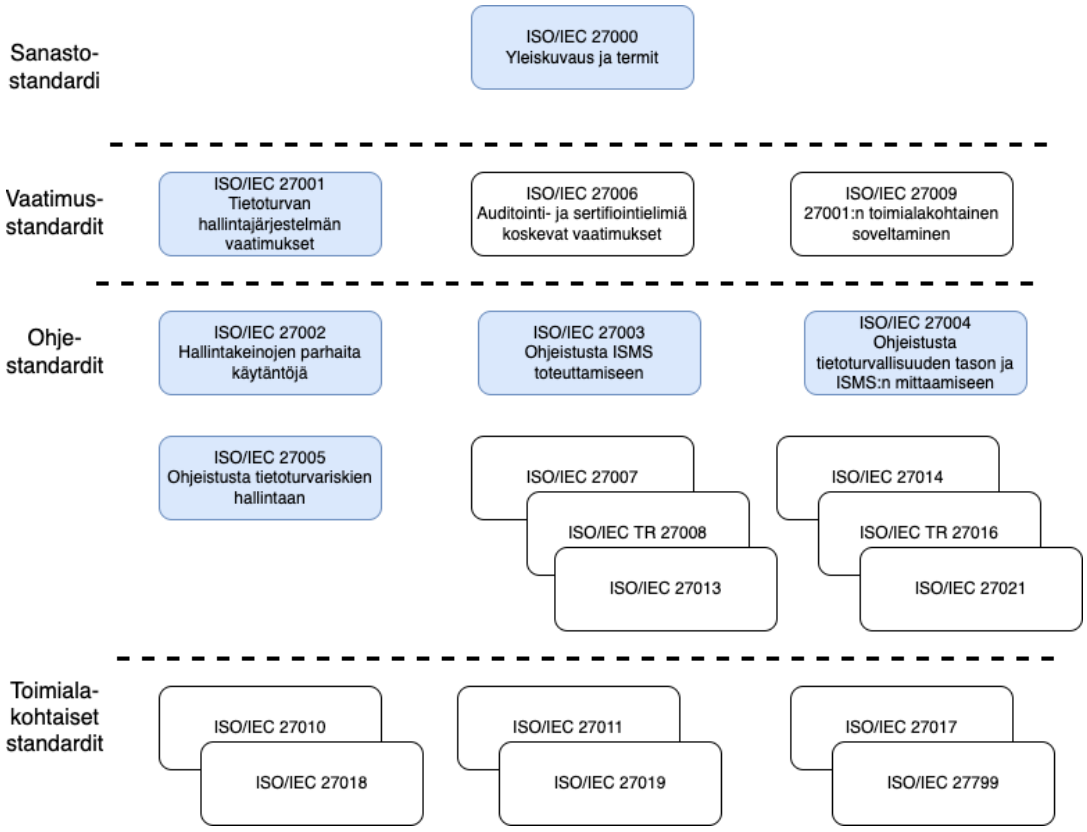
Tietoturvan hallintajärjestelmästä käytetään englanniksi yleensä termiä ISMS (Information Security Management System). ISO/IEC 27000 -standardin määritelmän mukaan hallintajärjestelmän avulla asetetaan tietoturvaan liittyvät politiikat, tavoitteet, prosessit, menettelytavat ja ohjeet sekä resurssit ja toiminnot, joita organisaatio hallinnoi kootusti suojatakseen tietoa ja tietojärjestelmiään sekä saavuttaakseen tavoitteet. [28, s. 10, 17]. Raggad puolestaan määrittelee tietoturvan hallintajärjestelmän prosessiksi, joka kykenee tunnistamaan organisaation IT-ympäristön, hallitsemaan siihen liittyviä riskejä sekä mahdollistaa jatkuvan parantamisen [22, s. 25]. Hallintajärjestelmän avulla organisaatio voi järjestelmällisesti johtaa ja hallita sen tietoturvaa tarkastellen sitä useista eri näkökulmista, millä tähdätään organisaation kaikkia toimintoja koskevien riskien arviointiin.

Organisaatiot ovat erilaisia niin kokonsa kuin luonteensa puolesta, joten tietoturvan hallintaan ei ole olemassa yhtä kaikille sopivaa mallia. Käytettävät tietojärjestelmät, tieto ja sen luonne, organisaation toimintaympäristö sekä näihin liittyvät riskit ovat avaintekijöitä tietoturvan hallintajärjestelmän kannalta. Tässä työssä keskitytään kahteen yleiseen hallintamalliin, joista ensimmäinen on ISO:n julkaisema ISO/IEC 27000 -standardiperhe. Se määrittelee vaatimukset ja tarjoaa ohjeita sekä käytännön opastusta tietoturvan hallintajärjestelmän toteuttamiseen. Toinen yleinen hallintamalli on NIST CSF (Cybersecurity Framework), joka on NIST:n kehittämä kyberturvallisuuden viitekehys, joka keskittyy kyberturvallisuuden kehittämiseen sekä riskitietoisuuden kasvattamiseen.

2.2.1 ISO/IEC 27000

ISO/IEC 27000 -standardiperhe on sarja tietoturvastandardeja, johon kuuluu yhteensä 12 eri standardia. Tässä työssä käsitellään ISO/IEC standardeja 27000, 27001, 27002, 27003, 27004, 27005 sekä 27701. Työn ulkopuolelle jäävät standardit keskittyvät mm. tietoturvan hallintajärjestelmän auditointiin ja sertifiointiin. Standardiperhe jakautuu sanastostandardiin, vaatimusstandardeihin, ohjestandardeihin ja toimialakohtaisiin standardeihin. Standardiperheen rakenne on esitetty kuvassa 2.1 ja tässä työssä käsiteltävät standardit on korostettu sinisellä.

ISO/IEC 27000 sisältää yleiskuvauksen standardiperheestä ja esittelee standardeissa käytettävät termit sekä niiden määritelmät. Vaatimukset hallintajärjestelmän luomiseen, toteuttamiseen, käyttämiseen, seurantaan, katselmointiin, ylläpitoon sekä jatkuvaan parantamiseen määritellään ISO/IEC 27001 -standardissa. Lisäksi ISO/IEC 27001 -standardin liitteessä A määritellään hallintakeinojen toteuttamista koskevat vaatimukset. Organisaatiot, joilla on käytössään tietoturvan hallintajärjestelmä, voivat auditoida hallintajärjestelmänsä ja hakea sertifikaattia ISO/IEC 27001 -standardia vasten. [28, s. 24]. ISO/IEC 27001 -standardissa – kuten muissakin vaatimusstandardeissa – käytetään vaatimuksia koskevissa lauseissa rakennetta ”on tehtävä” (*shall*), kun taas ohjestandardeissa suosituksia koskevissa lauseissa käytetään rakennetta ”olisi tehtävä” (*should*).



Kuva 2.1. *ISO/IEC 27000 -standardiperhe, perustuu lähteeseen 27000:2020 [28]*

Ohjeistusta esittelevistä standardeista ISO/IEC 27002 keskittyy ISO/IEC 27001:n liitteen A hallintakeinojen parhaisiin käytäntöihin, joita voi käyttää ohjeina toteuttamisen yhteydessä [28, s. 25]. Hallintakeinoilla tarkoitetaan teknisiä sekä hallinnollisia keinoja, joiden tavoitteena on pienentää riskien toteutumisen todennäköisyyttä. ISO/IEC 27003 esittelee ISO/IEC 27001 -standardissa esitettyjä vaatimuksia ja tarjoaa ohjeistusta niiden täyttämiseen. Tietoturvan hallintajärjestelmän vaikuttavuuden arviointia sekä tietoturvan tason mittaamista käsitellään ISO/IEC 27004 -standardissa. Sen esittämien mittareiden tai niistä sovellettujen mittareiden avulla organisaatiot voivat täyttää ISO/IEC 27001:n kohdan 9.1 vaatimukset. Standardi ISO/IEC 27005 esittelee ohjeistusta tietoturvariskien hallintaan. Sen avulla organisaatiot voivat toteuttaa prosessin riskienhallintaan, sisältäen riskien arvioinnin, käsittelyn ja hyväksymisen. [28, s. 25-26] Standardia ISO/IEC 27005 käsitellään tarkemmin alaluvussa 2.3.

Yksityisyyden suojaan liittyvät kysymykset ovat nousseet uutisotsikoihin 2010-luvun lopussa ja 2020-luvun alussa ja tietosuojaan liittyvää lainsäädäntöä sekä sääntelyä on tiukennettu, esimerkiksi vuonna 2018 voimaan tulleen EU:n yleisen tietosuoja-asetuksen (GDPR) myötä [8]. Vuonna 2019 julkaistu ISO/IEC 27701 on ISO/IEC 27001 mukaisen tietoturvan hallintajärjestelmän yhteydessä käytettäväksi tarkoitettu tietosuojalaajennus, jonka avulla organisaatiot voivat toteuttaa henkilötietojen hallintajärjestelmän, josta käytetään englanniksi yleensä termiä PIMS (Privacy Information Management System) [30].

ISO/IEC 27701 ei ole pelkästään GDPR:ää koskeva standardi, mutta se voi auttaa organisaatioita noudattamaan GDPR:n sekä muiden tietosuojavaatimusten noudattamista. Organisaatiot voivat sertifioida henkilötietojen hallintajärjestelmän joko ISO/IEC 27001 -sertifioinnin yhteydessä tai erikseen.

ISO/IEC 27001 -standardi julkaistiin virallisesti vuonna 2005, mutta sen historia ulottuu 1990-luvun alkuun, jolloin julkaistiin brittistandardi BS 7799. Vuonna 2005 BS 7799 uudistettiin ja nimettiin uudelleen ja se sai nimeksi ISO/IEC 27001. Standardiperhe laajeni vuonna 2007, jolloin ISO/IEC 27002 lisättiin mukaan sekä vuonna 2010 ISO/IEC 27003:n myötä. [11, s. 20-25] ISO/IEC 27001 sekä 27002 -standardit on uudistettu vuosina 2013 sekä 2022 vastaamaan paremmin organisaatioiden kohtaamiin haasteisiin. [12]

2.2.2 NIST Cybersecurity Framework

NIST CSF on viitekehys, joka on alun perin tarkoitettu kriittisen infrastruktuurin kyberturvallisuuden hallitsemiselle ja kehittämiselle. Viitekehyksen ensimmäinen versio julkaistiin vuonna 2014, versio 1.1 huhtikuussa 2018 ja tämän työn kirjoitushetkellä NIST on kehittämässä viitekehyksestä versiota 2.0. Vaikka viitekehys olikin alun perin tarkoitettu kriittistä infrastruktuuria varten, sitä voi käyttää mikä tahansa organisaatio toimialasta riippumatta. Viitekehyksen tarkoitus on auttaa organisaatioita tunnistamaan ja hallitsemaan riskejä. Näin organisaatiot voivat parantaa kyberturvallisuuden tasoaan ja resilienssiä. NIST kehottaa organisaatioita soveltamaan viitekehystä niiden omien tarpeiden mukaan, jotta ne saavat siitä suurimman hyödyn. NIST CSF poikkeaa ISO 27001:stä siten, ettei sitä vasten ole mahdollista sertifioitua. [17, s. ii-vi]

Viitekehyksessä on kolme keskeistä osaa: ydin (*Framework Core*), implementointitasot (*Implementation Tiers*) ja profiili (*Framework Profile*). Ydin koostuu kyberturvallisuuteen liittyvistä aktiviteeteista, toivotuista lopputuloksista sekä sovellettavista standardeista, ohjeistuksista ja käytännöistä, jotka ovat yleisiä kriittisen infrastruktuurin aloilla. Implementointitasot tarjoaa kontekstin ja työkaluja organisaatioille kyberturvallisuusriskien katselmointiin ja prosessien hallintaan. Kolmas taso eli profiilit kuvaa organisaation kyberturvallisuuden nykytilaa ja tulevaisuuteen asetettua tavoitetilaa.

Ydin esittelee alan standardeja, ohjeistuksia ja käytäntöjä tavalla, joka mahdollistaa kyberturvallisuuteen liittyvien aktiviteettien ja lopputulosten kommunikoimisen organisaation operationaaliselta tasolta johtoon asti. Ytimessä on viisi toiminnallisuutta: tunnistus (*Identify*), suojautuminen (*Protect*), havaitseminen (*Detect*), vastaaminen (*Respond*) ja palautuminen (*Recover*). Tarkastellessaan näitä toiminnallisuuksia yhdessä organisaatiot voivat muodostaa strategisen näkymän kyberturvallisuuden riskienhallinnasta.

Implementointitasot esittelevät työkaluja kyberturvallisuusriskien katselmointiin sekä prosessien hallintaan. Tasoja on neljä. Niiden avulla organisaatiot voivat arvioida oman tieto-

turvan tilan ja kehittyneisyyden sekä auttaa kyberturvallisuusriskeihin liittyvässä päätöksenteossa. Niiden avulla organisaatiot voivat myös määritellä, missä määrin kyberturvallisuusriskien hallinta perustuu liiketoiminnan tarpeisiin sekä miten se on integroitu organisaation yleisiin riskienhallintakäytäntöihin. Implementointitasot on esitelty taulukoissa 2.1 ja 2.2.

Taulukko 2.1. *Implementointitasot 1 ja 2 [17, s. 9-11]*

Taso 1 - Osittainen	
Riskienhallintaprosessi	Organisaation riskienhallintamenetelmiä ei ole sovittu, riskejä hallitaan tapauskohtaisesti ja reaktiivisesti. Kyberturvallisuuteen liittyvien toimien priorisointi ei perustu organisaation riskitavoitteisiin, uhkaympäristöön tai liiketoimintatavoitteisiin.
Integroitu riskienhallintaohjelma	Organisaation tietoisuus kyberturvallisuusriskeistä on rajallinen, riskienhallinta on epäsäännöllistä ja kyberturvallisuuteen liittyvään tiedonjakoon ei ole prosesseja.
Ulkoinen osallistuminen	Organisaatio ei ymmärrä sen roolia isommassa ekosysteemissä riippuvuuksien ja huollettavien suhteen, eikä se tee yhteistyötä vaihtaakseen tai jakaakseen tietoja esimerkiksi uhkatiedustelun tai parhaiden käytäntöjen suhteen. Organisaatio ei ole myöskään tietoinen IT-toimitusketjuun liittyvistä riskeistä.
Taso 2 - Riskitietoinen	
Riskienhallintaprosessi	Johto on hyväksynyt riskienhallintakäytännöt, mutta niitä ei ole vakiinnutettu organisaatiotasoisen politiikan avulla. Kyberturvallisuustoimintojen priorisointi- ja suojaustarpeet riippuvat suoraan organisaation uhkaympäristöstä, riskitavoitteista ja liiketoimintavaatimuksista.
Integroitu riskienhallintaohjelma	Organisaati on tietoinen kyberturvallisuusriskeistä, mutta koko organisaation kattavaa lähestymistapaa kyberturvallisuusriskien hallintaan ei ole luotu. Kyberturvallisuuteen liittyvää tietoa jaetaan organisaation sisällä epävirallisesti ja kyberturvallisuuteen liittyviä tavoitteita ja ohjelmia esiintyy joillain organisaation tasoilla, mutta ei kaikilla. Riskienarviointia tehdään, mutta se ei ole toistuvaa ja toistettavaa.
Ulkoinen osallistuminen	Organisaatio ymmärtää roolinsa osana isompaa ekosysteemiään joko sen omien riippuvuuksien tai huollettavien suhteen, mutta ei molempien. Se tekee yhteistyötä sekä saa tietoa muilta organisaatioilta, mutta ei jaa tietoa muille. Organisaatio on osittain tietoinen käyttämiinsä ja tarjoamiinsa tuotteisiin ja palveluihin liittyvistä riskeistä, mutta ei toimi johdonmukaisesti näiden suhteen.

Taulukko 2.2. *Implementointitasot 3 ja 4 [17, s. 9-11]*

Taso 3 - Toistettava	
Riskienhallintaprosessi	Riskienhallintakäytännöt on muodollisesti hyväksytty ja julkaistu politiikkoina. Organisaatiotason kyberturvallisuuskäytäntöjä päivitetään jatkuvasti riskienhallintaprosessin, bisnesvaatimusten ja uhka- ja teknologiaympäristössä tapahtuneiden muutosten perusteella.
Integroitu riskienhallintaohjelma	Riskienhallintaohjelma on koko organisaation laajuinen, politiikat, prosessit ja käytännöt on määritelty ja toteutettu kuten on tarkoituskin sekä katselmoitu. Organisaatiolla on johdonmukaiset tavat vastata tehokkaasti muuttuviin riskeihin ja henkilökunnalla on vaadittava osaaminen hoitaa heille nimetyt tehtävät ja vastuut. Organisaatio monitoroi jatkuvasti ja tarkasti riskejä, kokeneet vastuuhenkilöt viestivät toistuvasti kyberturvallisuusriskeistä. Vastuuhenkilöt varmistavat kyberturvallisuuden huomioimisen joka puolella organisaatiota.
Ulkoinen osallistuminen	Organisaatio ymmärtää roolinsa ja riippuvuussuhteensa osana ekosysteemiä ja voi edistää laajempaa ymmärrystä riskeistä. Se tekee yhteistyötä sekä saa muilta tahoilta tietoa, joka täydentää sisäisesti tuotettua tietoa. Lisäksi se jakaa tietoa muiden tahojen kanssa. Organisaatio on tietoinen käyttämiinsä ja tarjoamiinsa tuotteisiin ja palveluihin liittyvistä riskeistä ja lisäksi reagoi yleensä muodollisesti näihin riskeihin.
Taso 4 - Mukautuva	
Riskienhallintaprosessi	Organisaatio sopeuttaa kyberturvallisuuskäytäntöjänsä edellisiin ja nykyisiin kyberturvallisuusaktiviteetteihin, kokemuksiin ja ennakoiviin indikaattoreihin perustuen. Jatkuvaan parantamiseen perustuvan prosessin pohjalta organisaatio mukautuu jatkuvasti muuttuvaan uhka- ja teknologiaympäristöön ja reagoi ajallaan ja tehokkaalla tavalla kehittyviin ja edistyneisiin uhkiin.
Integroitu riskienhallintaohjelma	Riskienhallintaohjelma on koko organisaation laajuinen ja se hyödyntää politiikoita, prosesseja ja käytäntöjä kyberturvallisuustapahtumien käsittelyyn. Yhteys organisaation kyberturvallisuusriskien ja tavoitteiden välillä on selkeästi ymmärretty ja otettu huomioon. Riskejä monitoroidaan samassa yhteydessä taloudellisten ja muiden riskien kanssa. Budjetti perustuu nykyiseen ja ennustettuun riskiympäristöön ja -toleranssiin. Liiketoimintayksiköt toteuttavat johdon visiota ja arvioivat järjestelmätason riskejä organisaation kontekstissa. Riskienhallinta on osa organisaation kulttuuria ja kehittyy aiemmista tapahtumista sekä jatkuvasta tietoisuudesta organisaation järjestelmissä. Organisaatio voi ottaa liiketoiminnan tavoitteiden muutokset nopeasti ja tehokkaasti huomioon riskeihin suhtautumisessa.
Ulkoinen osallistuminen	Organisaatio ymmärtää roolinsa ja riippuvuussuhteensa osana ekosysteemiä ja voi edistää laajempaa ymmärrystä riskeistä. Se vastaanottaa, tuottaa sekä katselmoi tietoa ja jakaa tietoa sekä sisäisesti että ulkoisesti yhteistyötahojen kanssa. Organisaatio käyttää reaaliaikaista tai lähes reaaliaikaista tietoa ymmärtääkseen käyttämiinsä ja tarjoamiinsa tuotteisiin ja palveluihin liittyviä riskejä. Lisäksi se kommunikoi proaktiivisesti kehittääkseen ja ylläpitääkseen suhteita toimitusketjuun.

Viitekehysprofiilit ovat funktioiden, kategorioiden ja alakategorioiden kohdennuksia organisaation liiketoimintavaatimuksiin, riskitoleranssiin ja resursseihin. Niiden avulla organisaatiot voivat laatia tiekartan kyberturvallisuusriskien vähentämiseksi tavalla, joka on myös linjassa organisaation ja toimialan tavoitteiden kanssa, ottaen huomioon myös lakisääteiset vaatimukset, alan parhaat käytännöt ja heijastaen myös riskienhallinnan prioriteetteja. Profiileja voidaan käyttää määrittämään nykytila tai tulevaisuuden tavoitetila yksilöidylle kyberturvallisuusaktiviteetille. Nykytilaprofiili kuvaa kyberturvallisuuden avulla saavutetut tulokset. Tavoiteprofiili kuvaa tarvittavia tuloksia, jotta organisaation kyberturvallisuusriskien hallintatavoitteet saavutetaan. Nykytilaprofiilien ja tavoiteprofiilien vertailu voi paljastaa eroja, joihin pitää tarttua kyberturvallisuusriskien hallintatavoitteiden saavuttamiseksi.

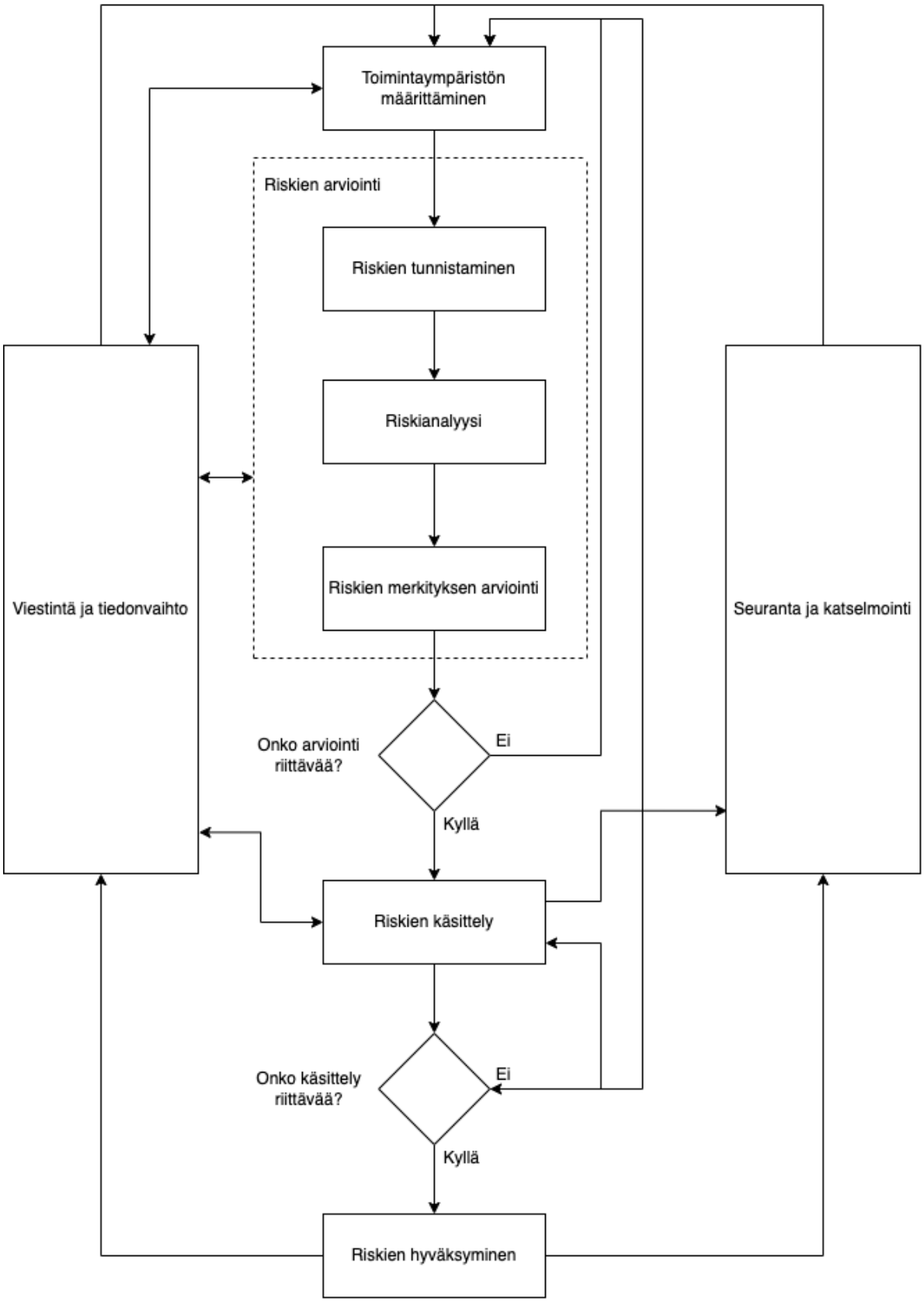
2.3 Riskienhallinta

Riskienhallinnalla tarkoitetaan organisaation toimia, joilla se tunnistaa ja arvioi riskejä sekä käsittelee niiden vaikutusta organisaation tavoitteiden saavuttamiseen [31, s. 15]. Riskienhallintaprosessi onkin yksi tietoturvan hallintajärjestelmän keskeisistä tekijöistä, sillä tietoturvariskien pienentäminen ja uhkiin varautuminen vaatii tietoturvariskien systemaattista tunnistamista ja arviointia. Riskienhallintaprosessin määrittely on myös yksi ISO/IEC 27001 -standardin vaatimuksista, jonka mukaan organisaation on määriteltävä ja toteutettava tietoturvariskien arviointiprosessi sekä käsittelyprosessi [27, s. 8-10].

2.3.1 ISO 27005

ISO/IEC 27005 -standardi esittelee ohjeistusta tietoturvariskien hallintaan ja sen tarkoitus on auttaa organisaatioita edistämään tietoturvan tasoa riskienhallintaan perustuvan toimintamallin avulla. Se perustuu ISO 31000 -standardiin, joka on tarkoitettu riskienhallintaan yleisemmällä tasolla. ISO/IEC 27005 on tarkoitettu kaikentyyppisille organisaatioille, kuten kaikki muutkin ISO/IEC 27000 -standardiperheen standardit. ISO/IEC 27005:n keskeisimmät kohdat ovat toimintaympäristön määritteleminen, riskien arviointi, riskien käsittely, riskien hyväksyminen, riskien viestiminen sekä riskien seuraaminen ja katselmointi. Riskienhallintaprosessi on esitelty kuvassa 2.2.

Toimintaympäristön määrittely tarkoittaa tietoturvariskien hallinnassa tarvittavien peruskriteerien asettamista, laajuuden ja rajojen määrittämistä sekä riskienhallintaan liittyvän organisaation määrittelyä tai perustamista. Riskienhallintaa varten organisaation on valittava toimintamalli, jolla tarkastellaan peruskriteerejä. Peruskriteereillä tarkoitetaan riskien merkityksen arviointikriteerejä, vaikutuskriteerejä sekä hyväksymiskriteerejä. Arviointikriteerejä määriteltäessä olisi otettava huomioon mm. liiketoimintaprosessien strateginen arvo, suojattavien kohteiden kriittisyys, luottamuksellisuuden, eheyden ja saavutettavuuden



Kuva 2.2. *ISO/IEC 27005 mukainen tietoturvariskien hallintaprosessi, perustuu lähteeseen 27005:2020 [31]*

tärkeys liiketoiminnan kannalta sekä sidosryhmien odotukset ja maineeseen kohdistuvat haitalliset seuraukset. Edellä mainittuja voidaan käyttää riskien käsittelyn tärkeysjärjestystä määriteltäessä. Vaikutuskriteereillä voidaan arvioida tietoturvatapahtuman aiheuttaman vahingon tai kustannusten suuruutta. Niiden määrittelyssä olisi otettava huomioon suojattavan kohteen arkaluontoisuus, tietoturva-aukot, vahingoittuneet toiminnot, liiketoiminnalle aiheutuneet rahalliset tappiot, suunnitelmien ja aikataulujen häiriöityminen sekä maineen vahingoittuminen. Riskien hyväksymiskriteerit liittyvät riskien hyväksymistasoon ja ne riippuvat organisaation tavoitteista, toimintaperiaatteista sekä mahdollisesti myös sidosryhmien näkemyksistä. Niiden määrittelyssä olisi otettava huomioon organisaation toimiala, toiminnot, liiketoimintakriteerit, lainsäädännön asettamat vaatimukset sekä sosiaaliset ja inhimilliset tekijät. Tietoturvariskien hallinnan laajuuden ja rajojen määrittelyllä pyritään varmistamaan, että kaikkeen olennaiseen omaisuuteen liittyvät riskit huomioidaan riskien arvioinnissa. Niiden määrittelyssä olisi huomioitava organisaation liiketoimintatavoitteet, strategiat ja toimintaperiaatteet, liiketoimintaprosessit, organisaation rakenne ja tietoturvapolitiikka, suojattavat kohteet, toimipaikkojen sijainnit sekä niiden maantieteelliset piirteet, organisaatioon vaikuttavat rajoitukset ja sidosryhmien odotukset. Riskienhallintaprosessia suorittava organisaatio olisi joko perustettava tai siihen liittyvät vastuut olisi määriteltävä. Organisaation vastuulle kuuluu riskienhallintaprosessin kehittäminen, sidosryhmien tunnistaminen ja analysointi, suhteiden muodostaminen mm. organisaation ja sidosryhmien sekä muiden asiaan kuuluvien toimintojen ja hankkeiden välille. [31, s. 10-13]

Riskien arviointiin kuuluu kolme riskienhallinnan kannalta oleellista toimintoa: riskien tunnistaminen, riskianalyysi sekä riskien merkityksen arviointi. Riskien tunnistamisen aikana pyritään määrittämään seuraukset mitä voisi tapahtua jos riski toteutuisi, mikä voi aiheuttaa tappioita sekä miten, missä ja miksi tappiot voisivat syntyä. Riskien tunnistaminen lähtee liikkeelle suojattavan omaisuuden tunnistamisella ja luetteloimisella. Omaisuudelle olisi määriteltävä omistaja, jotta siihen liittyvät vastuut voidaan määritellä. Omistajuudella ei tarkoiteta tässä yhteydessä omistusoikeutta, vaan vastuuta esimerkiksi omaisuuden kehittämisestä, ylläpidosta, käytöstä ja turvallisuudesta. Omaisuuden tunnistamisen jälkeen on vuorossa omaisuuteen liittyvien uhkien tunnistaminen. Uhka voi vahingoittaa omaisuutta ja uhkat voivat olla luonnollisia tai ihmisen joko tahattomasti tai tahallisesti aiheuttamia ja ne voivat ilmetä joko organisaation sisältä tai sen ulkopuolelta. Uhkan tunnistamisen yhteydessä on arvioitava sen toteutumisen todennäköisyys. Uhkien tunnistamisen jälkeen olisi tunnistettava jo nykyisellään käytössä olevat hallintakeinot, jotta organisaatio voi välttää tarpeettoman työn tekemisen. Hallintakeinojen toimivuus olisi varmistettava tunnistamisen yhteydessä, esimerkiksi katselmoimalla niihin liittyvät asiakirjat tai tarkastamalla omaisuuden omistajan tai käyttäjien kanssa, että hallintakeinot on todella käytössä. Riskien tunnistamisen toiseksi viimeinen vaihe on haavoittuvuuksien tunnistaminen, jossa on tarkoituksena tehdä luettelo omaisuuteen, uhkiin ja hallintakeinoihin

liittyvistä haavoittuvuuksista. Haavoittuvuus voi liittyä organisaatioon, prosesseihin, henkilöstöön, teknisiin konfiguraatioihin, fyysiseen ympäristöön, ohjelmistoihin ja laitteistoon tai riippuvuuteen ulkoisista tahoista. Riskeihin liittyvien seurausten tunnistamisvaiheessa aikana olisi tunnistettava mitä seurauksia luottamuksellisuuden, eheyden ja saatavuuden menettämisellä voi olla suojattavalle omaisuudelle. Seurauksia voi olla esimerkiksi tutkimiseen ja korjaamiseen kuluva aika ja rahalliset kustannukset, liiketoiminnalle aiheutuvat tappiot sekä maineen menettäminen. [31, s. 14-18]

Riskianalyysin aikana arvioidaan riskien toteutumisen seurauksia, häiriöiden syntymisen todennäköisyyttä ja määritetään tietoturvariskeille riskitasot. Riskien toteutumisen seurausten arvioinnin aikana olisi arvioitava tietoturvahäiriöiden vaikutukset organisaation liiketoiminnalle ja arvioitava tietoturvarikkomuksen seuraukset suojattavalle kohteelle. Liiketoimintaan kohdistuvat vaikutukset voidaan arvioida laadullisesti ja määrällisesti, mutta yleensä vaikutukset on kannattavampaa arvioida rahallisena arvona, sillä se tuottaa enemmän tietoa päätöksentekoa varten. Rahallisen arvon määrittelyssä voidaan ottaa huomioon palauttamistoimenpiteiden ja tiedon korvaamisesta aiheutuvat kustannukset sekä suojattavan kohteen vaarantumisesta tai menettämisestä liiketoiminnalle aiheutuvat seuraukset. Häiriön todennäköisyyden arvioinnissa olisi arvioitavat kunkin skenaarion todennäköisyys. Arvioinnissa voidaan ottaa huomioon käytössä olevat hallintakeinot, tahalliset uhkat, tahattomat uhkat sekä uhkan todennäköisyyttä koskeva kokemus ja mahdollisesti siihen liittyvät tilastot. Riskianalyysin viimeinen vaihe on riskitason määrittäminen, jonka aikana jokaiselle riskille arvioidaan riskitaso perustuen todennäköisyyksiin ja arvioituihin seurauksiin. Riskitason määrittämisessä voidaan huomioida myös kustannushyödyt sekä sidosryhmien näkemykset. [31, s. 18-20]

Riskien arvioinnin viimeinen toiminto on riskien merkityksen arviointi, jossa riskitasoja verrataan arviointikriteereihin ja hyväksymiskriteereihin. Sen aikana olisi otettava huomioon suojattavan kohteen tietoturvaominaisuudet sekä niiden tärkeys liiketoiminnan kannalta. Toiminnon seurauksena tulisi olla luettelo riskeistä, jotka on asetettu tärkeysjärjestykseen. [31, s. 20-21]

Riskien käsittelyssä valitaan, mitä riskille tehdään. Vaihtoehtoja on neljä: riskin muokkaaminen, säilyttäminen, välttäminen ja jakaminen. Vaihtoehdot eivät ole toisiaan poissulkevia ja joskus niiden yhdistelemisestä voi olla organisaatiolle hyötyä. Lopputuloksena tulisi olla riskinkäsittelysuunnitelma sekä jäännösriskit, jotka voidaan viedä organisaation johdolle päätettäväksi ja hyväksyttäväksi. Mikäli jäännösriski ei täytä riskien hyväksymiskriteerejä, riskien käsittely saattaa olla tarpeen toistaa. [31, s. 21-25]

Riskien käsittelyn jälkeen organisaation johdon olisi hyväksyttävä riskit perustuen riskinkäsittelysuunnitelmaan sekä jäännösriskien arviointiin ja päätökset olisi kirjattava. Joissakin tapauksissa riskien hyväksyminen saattaa olla houkuttelevaa, sillä riskien mukana saatavat hyödyt voivat olla vastustamattomia tai riskien muokkaamisen kustannukset

nousisivat liian suuriksi. Riskien käsittelyn lisäksi riskeistä olisi tärkeä viestiä päätöksentekijöiden ja muiden sidosryhmien kanssa, jotta riskienhallinnan toteuttamisesta vastaava organisaatio ja muut merkitykselliset tahot ymmärtävät, miksi tiettyjä toimenpiteitä tarvitaan ja mihin päätökset perustuvat. Organisaation olisi myös varauduttava viestintäsuunnitelmien avulla hätätilanteita varten, mutta myös viestittävä niistä osana arkipäiväistä toimintaa. [31, s. 25-26]

Koska uhkat, haavoittuvuudet, todennäköisyydet ja seuraukset voivat muuttua jatkuvasti, riskejä olisi seurattava jatkuvasti. Organisaation olisi seurattava jatkuvasti mm. uusia suojattavia kohteita, uusia uhkia sekä organisaation sisältä että ulkopuolelta, tietoturvahäiriöitä ja tunnistettuja haavoittuvuuksia. Riskien seuraamisen lisäksi olisi seurattava ja katselmoitava riskienhallintaprosessia, jotta sitä voidaan parantaa jatkuvasti tarvittavalla tavalla sekä varmistua sen tuottavan oikeaa, toistettavaa ja merkityksellistä tietoa. Esimerkiksi kilpailuympäristöä, suojattavien kohteiden arvoa ja luokittelua, vaikutus-, arviointi ja hyväksymiskriteerejä olisi seurattava ja katselmoitava jatkuvasti. [31, s. 26-28]

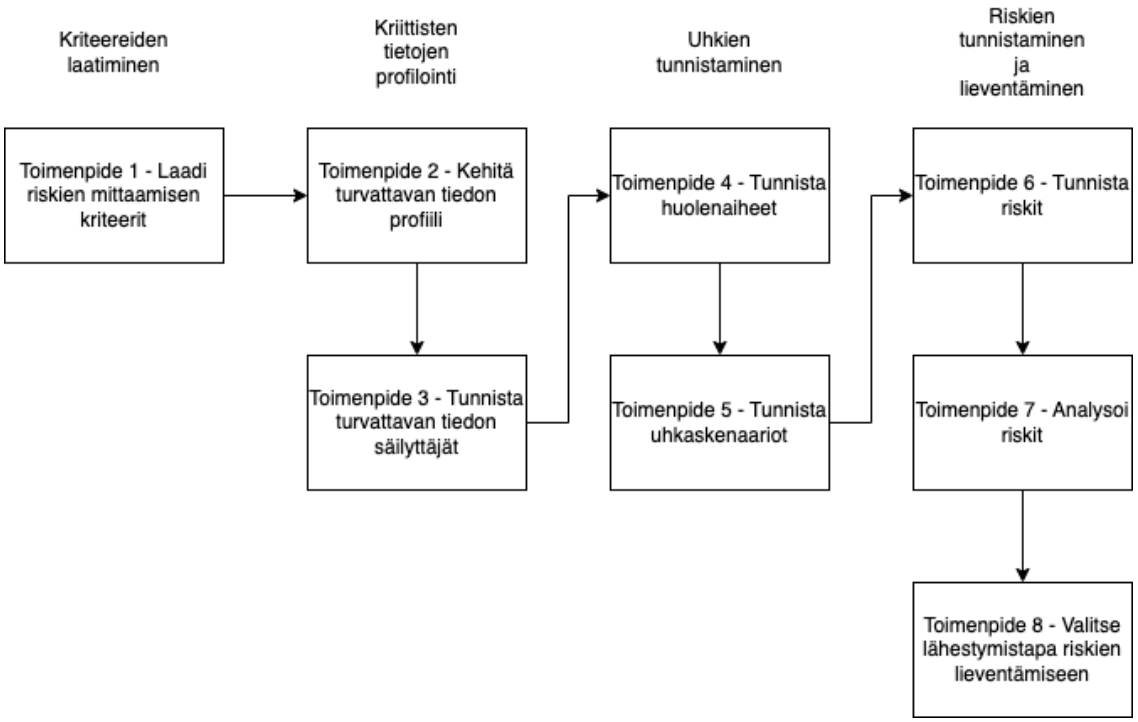
2.3.2 OCTAVE Allegro

Yhdysvaltalainen Carnegie Mellonin yliopisto kehitti tietoturvan riskienhallintaan keskittyvän OCTAVE:n (Operationally Critical Threat, Asset, and Vulnerability Evaluation) 1990-luvulla ja se julkaistiin vuonna 1999. Alkuperäinen OCTAVE-menetelmä on tarkoitettu yli 300 hengen organisaatioille, joilla on monikerroksinen hierarkia, jotka hallitsevat omaa IT-infrastruktuuria ja joilla on kyky käyttää haavoittuvuuksien arviointityökaluja sekä tulkita haavoittuvuuksien arvioinnin tuloksia. Tämän jälkeen OCTAVE-menetelmästä on julkaistu kaksi uutta versiota: alle sadan hengen organisaatioille suunniteltu OCTAVE-S vuonna 2003 sekä OCTAVE Allegro vuonna 2007. OCTAVE Allegro eroaa aiemmista menetelmistä siten, että se keskittyy organisaation suojattaviin kohteisiin siinä yhteydessä, miten niitä käytetään ja missä niitä kuljetetaan, säilytetään ja käsitellään sekä miten ne voivat altistua uhkille, haavoittuvuuksille sekä häiriöille. Kaikkia kolmea menetelmää voidaan käyttää osana työpajatyöskentelyä ja niitä varten on luotu valmiit dokumenttipohjat, kysymyspatteristot sekä ohjeistus niiden käyttöön.

OCTAVE Allegron kehittämisellä pyrittiin mm. menetelmän käytettävyyden parantamiseen, vähentämään riskienarvioinnin tekoon vaadittavaa koulutusta ja tietämystä, pienentämään riskienarviointiin tarvittavien henkilöstöresurssien määrää, kannustamaan tekemään riskienarvioinnista säännöllistä ja ottamaan sen osaksi laajempaa riskienhallintaprosessia, mahdollistamaan yhdenmukaisten ja vertailukelpoisten riskienarvioinnin tulosten tuottamisen eri puolilla organisaatiota sekä tukemaan organisaatiota täyttämään lakisääteiset vaatimukset. [6, s. 1-10]

OCTAVE Allegro koostuu neljästä vaiheesta, joihin sisältyy kahdeksan erillistä toimenpidettä. Vaiheet ovat kriteereiden laatiminen, kriittisten tietojen profilointi, uhkien tunnista-

minen sekä riskien tunnistaminen ja toimenpiteet niiden lieventämiseksi. OCTAVE Allegro on esitelty kuvassa 2.3 ja alla on lueteltu Carallin et al. tarkemmat kuvaukset eri vaiheista ja toimenpiteistä. [6, s. 17-20]



Kuva 2.3. *OCTAVE Allegro, perustuu lähteeseen [6, s. 4]*

Ensimmäiseen vaiheeseen kuuluu vain yksi toimenpide ja sen aikana organisaation tulee määritellä toimintansa ja tavoitteidensa mukaiset riskienarviointikriteerit. Riskienarviointikriteerit ovat laadullisia mittareita, joilla kuvataan realisoituneen riskin aiheuttamia vaikutuksia. Riskienarviointikriteerejä ovat esimerkiksi maineen menetys, sakot ja niiden suuruus, liikevaihdon menetys, riskin realisoitumisen johdosta lisääntyneet työtunnit sekä datan menetys. Kriteerien luomisen lisäksi organisaation täytyy priorisoida eri kriteerit, eli päättää mikä niistä on tärkein sen toiminnan ja tavoitteiden kannalta. Tärkeysjärjestys voi vaihdella suuresti organisaatioiden välillä, sillä toiselle organisaatiolle maine voi olla tärkeämpi kuin rahalliset menetykset.

Toisessa vaiheessa eli kriittisten tietojen profiloinnissa on kaksi toimenpidettä. Ensimmäinen on toimenpide 2, jossa organisaation täytyy tunnistaa tiedot (assetit), joihin riskienarvioinnissa keskitytään ja luoda näistä profiilit. Profiili kuvaa suojattavan tiedon yksilöllisiä ominaisuuksia, piirteitä, laatua ja arvoa. Toimenpiteen on tarkoitus varmistaa, että suojattava tieto on kuvattu selkeästi ja johdonmukaisesti ja että sille on määritelty yksiselitteiset rajat ja että sen turvallisuusvaatimukset on määritelty. Lisäksi toiseen vaiheeseen kuuluu toimenpide 3, säilyttäjien (containers) tunnistaminen. Tällä tarkoitetaan esimerkiksi palvelimia, verkkoja, fyysisiä tiloja ja ulkoistettuja IT-palveluita missä tietoja säilytetään, kuljetetaan ja käsitellään. Tämän toimenpiteen aikana suojattava tieto yhdistetään säilyttäjään,

jossa se sijaitsee. Näin suojattavan tiedon ja säilyttäjän olosuhteisiin liittyviä riskejä on helpompi tarkastella.

Vaiheessa kolme eli uhkien tunnistamisessa on kaksi toimenpidettä, joista toimenpiteessä 4 on tarkoitus tunnistaa huolenaiheet, eli tilanteet tai olosuhteet, joissa suojattava tieto voi olla uhattuna. Tämän toimenpiteen tarkoitus on kuvata sellaiset reaalimaailman uhkaskenaariot, jotka tulevat työpajatyöskentelyn aikana henkilöiden mieleen – ei tuottaa täydellistä listaa kaikista suojattavaa tietoa koskevista uhkaskenaarioista. Toimenpide 5 on jaettu kahteen osioon, joista ensimmäisessä pureudutaan tarkemmin edellisessä toimenpiteessä tunnistettuihin huolenaiheisin ja tunnistetaan uhkakuvat kuvaamalla siihen liittyvät yksityiskohdat tarkemmin. Jälkimmäisessä osiossa suojattavaan tietoon liittyviä muita uhkakuvia voidaan tunnistaa käyttämällä apuna uhkapuuta, jonka avulla voidaan käydä läpi ihmisen aiheuttamat ongelmat, tekniset ongelmat sekä muut ongelmat, kuten luonnonilmiöiden aiheuttamat riskit. Lisäksi tämän toimenpiteen aikana on mahdollista arvioida uhkaskenaarion realisoitumisen todennäköisyys, jota voidaan käyttää myöhemmin hyödyksi.

Neljänteen ja viimeiseen vaiheeseen kuuluu kolme toimenpidettä, joista ensimmäinen eli toimenpide 6 on riskien tunnistaminen. Sen aikana kuvataan organisaatiolle aiheutuvat seuraukset, mikäli riski realisoituu. Toimenpiteen aikana on tarkoitus tunnistaa kaikki seuraukset, esimerkiksi organisaation sähköisen mainonnan järjestelmän häiriö voi vaikuttaa organisaation maineeseen sekä sen taloudelliseen tilanteeseen. Toimenpiteen 7 eli riskien analysoinnin aikana riskeille lasketaan yksinkertainen määrällinen arvo, suhteellinen riski, mikä kertoo missä määrin sen toteutuminen vaikuttaa organisaatioon. Arvo lasketaan seurausten sekä organisaation valinnan mukaan myös todennäköisyyden perusteella. Tämän toimenpiteen tarkoituksena on järjestää riskit tärkeysjärjestykseen organisaation toiminnan kannalta ja siinä käytetään toimenpiteen 1 aikana luotuja riskienarviointikriteerejä. Toimenpiteessä 8 organisaatio valitsee mitkä tunnistetuista riskeistä vaativat toimenpiteitä riskien lieventämiseksi sekä kehittävät lieventämisstrategian. Aluksi riskit laitetaan tärkeysjärjestykseen suhteellisen riskin arvon perusteella, minkä jälkeen kehitetään lieventämisstrategiat ottaen huomioon suojattavan tiedon arvo, tietoturvavaatimukset, säilyttäjä sekä organisaation toimintaympäristö.

2.3.3 Sopivuus eri organisaatioille

ISO/IEC 27005 -standardin mukainen tietoturvariskien hallintaprosessi sopii kaikille organisaatioille, ja standardi kertoo sen olevan sovellettavissa ”kaikentyyppisissä organisaatioissa (esim. kaupallisissa yrityksissä, valtion virastoissa, voittoa tavoittelemattomissa organisaatioissa), joissa pyritään hallitsemaan riskejä” [29, s. 6]. Standardin kirjaimellinen noudattaminen vaatii kuitenkin suurempaa paneutumista OCTAVE Allegroon verrattuna.

OCTAVE Allegro sopii kaikille organisaatioille, mutta keveytensä takia se on soveltuva eri-

tyisesti niille, joilla ei ole kattavaa osaamista riskienhallinnasta. Se soveltuu myös yksittäisille henkilöille, jotka haluavat tehdä riskienarvioinnin ilman muun organisaation osallistumista tai panosta. [6, s. 4]

3. MENETELMÄT JA AINEISTOT

Tässä luvussa esitellään tutkimusmetodina käytettävät laadullinen tutkimus ja integroiva kirjallisuuskatsaus. Lisäksi esitellään kirjallisuuskatsauksen aineisto sekä tapaustutkimuksen aineisto ja analyysimenetelmä.

3.1 Laadullinen tutkimus

Laadulliselle tutkimukselle ei ole yhtä tiettyä määritelmää, sillä erilaisia lähestymis- ja analyysitapoja on paljon. Laadullinen tutkimus perustuu aina erilaisiin aineistoihin ja niiden analysointiin, eli se on empiiristä. [13] Laadullisen tutkimuksen perimmäinen tarkoitus on pyrkiä ymmärtämään tutkittavaa ilmiötä. Tyypillisesti tämä tapahtuu analysoimalla kerättyä aineistoa, kuten esimeriksi kirjallisuutta, haastatteluita tai päiväkirjoja. [38]

Tässä työssä laadullinen tutkimusote näkyy sekä kirjallisuuskatsauksessa että empiirisen tapauksen analysoinnissa, sillä tutkimuksessa suositaan laadullista ja luonnollista sekä strukturoimatonta aineistoa. Erityisesti empiirisen tutkimuksen osassa tutkija on läheisessä kontaktissa tutkimuksen kohteen ja siihen liittyvien ihmisten kanssa. Lisäksi tutkimuksessa arvostetaan subjektiivisuutta, eli hyväksytään tutkijan oma subjektiivisuus eikä häneltä vaadita objektiivista, ulkopuolista roolia.

Laadullinen tutkimus auttaa ymmärtämään tarkasteltavaa tapausta kokonaisvaltaisesti sen sijaan että siitä pyrittäisiin eristämään yksittäisiä tekijöitä. Tavoitteena on lisätä ymmärrystä projektien onnistumista edesauttavista tekijöistä osana organisatorista kontekstiaan, minkä johdosta tuloksia ei voida yleistää sovellettavaksi kaikissa organisaatioissa. Työssä käytetään laadullisen tutkimuksen lähestymistapana tapaustutkimusta. Robert Yin mukaan tapaustutkimuksessa ”on kysymys empiirisestä tutkimuksesta, jossa tarkastellaan ajankohtaista ilmiötä syvällisesti sen todellisessa kontekstissa. Tapaustutkimuksessa ilmiön ja kontekstin välinen rajapinta on häilyvä” [21].

3.2 Konstruktiivinen tutkimusote

Tässä työssä käytetään konstruktiivista tutkimusotetta. Lehtirannan et al. mukaan [4, s. 95-106] konstruktiivisen tutkimusotteen tarkoitus on ratkaista käytännön ongelmia sekä tuottaa akateemisia, teoreettisia tuotoksia, eli konstruktioita. Lukan mukaan [15] konstruk-

tio voi olla esimerkiksi prosessi, käytäntöjä, työkaluja, suunnitelmia, tietojärjestelmämalleja tai organisaatiomalleja.

Lehtirannan et al. ja Lukan mukaan konstruktiivisen tutkimusprosessin vaiheet sisältävät käytännön ongelman valitsemisen, joka koetaan tarpeelliseksi ratkaista; kattavan käsityksen hankkimisen tutkimusalueesta; yhden tai useamman tuotoksen eli konstruktion rakentamisen ongelmaa varten; konstruktion soveltuvuuden testaamisen toteuttamisyrityksen avulla; tutkijan ja käytännön edustajien läheistä yhteistyötä; tulosten yhdistämisen takaisin teoriaan ja niiden käytännön soveltuvuuden demonstroimisen sekä tuotosten yleistettävyyden arvioiminen.

Taulukko 3.1. *Konstruktiivisen tutkimusotteen vaiheet sekä niiden toteutuminen tässä työssä [15]*

Vaihe	Selitys	Luku tai luvut jossa käsitellään
1	Etsi käytännössä relevantti ongelma, jossa on mahdollisuus myös teoreettiseen kontribuutioon.	1 ja 3.2.1
2	Selvitä mahdollisuudet pitkän aikavälin tutkimusyhteistyöhön kohdeorganisaation kanssa.	1 ja 3.2.1
3	Hanki syvällinen tutkimusaiheen tuntemus sekä käytännöllisesti että teoreettisesti.	4 ja 6
4	Innovoi ratkaisumalli ja kehitä ongelman ratkaiseva konstruktio, jolla voisi olla myös teoreettista kontribuutiota.	5
5	Toteuta ratkaisu ja testaa sen toimivuus.	6.1
6	Pohdi ratkaisun soveltamisalaa.	6.1
7	Tunnista ja analysoi teoreettinen kontribuutio.	6.2

3.2.1 Kohdeyritys ja tietoturvan hallintajärjestelmän toteutus

Tämän työn tutkimuksen kohteena oli globaalisti toimiva suomalainen huonekaluvalmistaja, joka on laajentanut tarjontaansa myös digitaaliselle puolelle. Sillä on noin 400 työntekijää useissa eri maissa ja asiakkaita lähestulkoon kaikilla mantereilla. Yrityksen liikevaihto vuonna 2021 oli yli 90 miljoonaa euroa ja se on kasvanut viime vuosien aikana voimakkaasti, vaikka COVID-19-pandemia vaikuttikin merkittävästi yrityksen toimintaan. Tässä alaluvussa käydään läpi syitä yrityksen päätökselle lähteä toteuttamaan tietoturvan hallintajärjestelmää, sen rajausta ja yrityksen tietoturvan tilaa ennen hallintajärjestelmän toteutusprojektia.

Yritys julkaisi vuoden 2021 ensimmäisellä vuosipuolikkaalla digitaalisen verkkopalvelun, joka on tarkoitettu käytettäväksi yrityksen myymien fyysisten tuotteiden kanssa ja on tarkoitettu henkilöille, jotka ovat vastuussa kiinteistön hoidosta ja työhyvinvoinnista organi-

saatiossa. Verkkopalvelun käyttäjiä voivat olla esimerkiksi asiakasorganisaatioiden kiinteistöpäälliköt, toimistojen viihtyvyydestä vastaavat tahot esimerkiksi henkilöstöhallinnosta ja asiakkaan IT-ylläpitäjät. Palvelun avulla voidaan mm. visualisoida yrityksen myymien fyysisten tuotteiden käyttöastetta ja käytön jakautumista työpäivien aikana. Asiakkaat pystyvät tämän avulla tekemään päätöksiä tuotteiden sijoittelusta tiloissaan, perustelemaan hankintapäätöksiä organisaation johdolle dataan perustuen. Asiakkaat voivat myös halutessaan yhdistää tuotteet heidän käyttämäänsä Microsoftin tai Googlen kalenterijärjestelmään kalenteri-integraation avulla ja varata tämän avulla tuotteita käyttöönsä vaivattomasti, esimerkiksi palaverin tai videopuhelun ajaksi.

Palvelun julkaisun myötä kohdeyrityksen käsittelemä asiakasdatan ja luottamuksellisen tiedon määrä ja tärkeys kasvoivat merkittävästi, minkä johdosta asiakkaiden vaatimukset tietoturvan suhteen nousivat aivan uudelle tasolle. Aiemmin yritys käsitteli lähinnä asiakkaiden yhteystietoja, tilauksiin ja toimitukseen liittyviä tietoja, laskutustietoja sekä muuta liiketoiminnalle tärkeää, muttei mitään arkaluonteista tietoa. Arkaluonteiseksi tiedoksi luokitellaan tässä yhteydessä mm. asiakkaiden käyttäjien salasanat, joilla he kirjautuvat kohdeyrityksen tarjoamaan verkkopalveluun sekä kalenteri-integraation toiminnan kannalta oleelliset tunnistusavaimet (*token*). Lisäksi yritys varautuu käsittelemään tulevaisuudessa asiakkaiden luottokorttitietoja periäkseen palvelusta kuukausimaksua. Näiden paljastumisella ja vuotamisella luvattomien tahojen haltuun voisi olla haitallisia vaikutuksia organisaatioiden toimintaan ja tällä olisi merkittäviä haitallisia vaikutuksia myös kohdeyritykselle. Tällaisia vaikutuksia voisi olla esimerkiksi maineen ja arvostuksen menetys, sakkoja sekä asiakkaiden kaikkoaminen ja näin ollen liiketoiminnan vaikeutuminen huomattavasti. Asiakkaat alkoivat esittämään kysymyksiä ja vaatimuksia tietoturvasertifikaatteja sekä tietoturvan hallintajärjestelmää koskien jo fyysisten tuotteiden hankintaprosessin aikana. Tietoturvasertifikaateista ja -viitekehyksistä yleisimmin esiin nousivat ISO/IEC 27001 sekä SOC 2-varmennusraportti. Kysymyksissä ja vaatimuksissa nousi esiin myös tietosuojan huomioiminen sekä GDPR.

Kasvaneiden asiakasvaatimusten myötä kohdeyrityksessä pohdittiin keinoja täyttää asiakkaiden toiveet ja vaatimukset tietoturvan osalta. Kohdeyritys selvitti erilaisia lähestymistapoja ongelman ratkaisuun, joista päätyi valitsemaan ISO/IEC 27001 -standardin mukaisen tietoturvan hallintajärjestelmän toteuttamisen ja sen sertifioimisen standardia vasten. Muita vaihtoehtoja oli mm. SOC 2 ja NIST CSF -viitekehyksen mukaisten hallintakeinojen käyttöönotto. Tietoturvan hallintajärjestelmän toteuttamisen nähtiin olevan paras tapa kohentaa verkkopalvelun ja siihen liittyvien prosessien tietoturvaa sekä tuovan systemaattisen lähestymistavan tietoturvan ylläpitoon, kehitykseen, monitorointiin ja jatkuvaan parantamiseen. Lisäksi hallintajärjestelmän toteuttamisen uskottiin luovan samalla edellytykset asiakasvaatimusten täyttämiseen sekä pienentävän vasteaikaa vastaamiseen asiakkailta tuleviin tietoturva-aiheisiin kysymyksiin. Lisäksi se mahdollistaa sertifikaatin tavoittelemisen, jonka uskottiin parantavan mainetta ja kasvattavan luottamusta, kun tietoturvan hal-

lintajärjestelmä on auditoitu ulkopuolisen, riippumattoman sertifiointitahon toimesta. Sertifikaatin nähtiin olevan myös yksi valttikortti, jota voitaisiin käyttää tulevaisuudessa sekä markkinoinnissa että kilpailutuksissa. Näin ollen tietoturvan hallintajärjestelmän toteuttamisen nähtiin olevan myös pidemmällä aikajänteellä tarkasteltuna paras ratkaisu kohdeyrityksen kannalta. Lisäksi kansainvälisesti tunnustettuun standardiin perehtymisen myötä yrityksessä tehtiin johtopäätös, että tietoturvan hallintajärjestelmän toteutusprojektin myötä oppeja pystytään jalkauttamaan muulle organisaatiolle ja täten parantamaan ja tehostamaan toimintaa sekä prosesseja, kehittämään tietoturvan eri osa-alueita ja näin ollen parantamaan koko yrityksen sietokykyä tietoturva-uhkia vastaan. Hallintajärjestelmän toteutusprojektista vastasi tämän työn kirjoittaja. Toteutusprojektia esitellään tarkemmin luvussa 5. Toteutusprojektin kokemusten ja kirjallisuuskatsauksen löydösten perusteella työssä kehitetään konstruktio. Se on malli, joka esittelee onnistumistekijöitä, jotka huomioimalla organisaatiot voivat edesauttaa tietoturvan hallintajärjestelmän toteutusprojektin onnistumista. Malli esitellään luvussa 6.

3.2.2 Aineisto

Hallintajärjestelmän toteutusprojektista kertynyttä aineistoa ovat mm. tämän työn kirjoittajan omat muistiinpanot, Jira-tiketit, Jiran roadmap-ominaisuuden avulla tehty tiekartta sekä havainnot ja muistiinpanot riskienarviointi-työpajasta. Lisäksi toteuttamisprojektin aikana käytettiin aineistona ISO/IEC 27000 -standardiperheen eri standardeja sekä ISO/IEC 27001 Lead Implementer -kurssin materiaaleja. Konstruktion kehittämiseen liittyy Salmen ja Järvenpään mukaan [23, s. 265-266] aina monipuolista aineistoa, kuten teoriaa, havaintoja sekä ymmärrystä organisaation toiminnasta.

3.3 Kirjallisuuskatsaus

3.3.1 Integroiva kirjallisuuskatsaus menetelmänä

Teoreettisen viitekehyksen muodostamiseksi työssä käytetään integroivaa kirjallisuuskatsausta. Integroiva kirjallisuuskatsaus tehtiin, jotta voitaisiin muodostaa kattava, dokumentoitu käsitys tietoturvan hallintajärjestelmän toteuttamiseen ja sen onnistumiseen liittyvästä aiemmasta tutkimuksesta. Integroiva kirjallisuuskatsaus on kuvailevan kirjallisuuskatsauksen orientaatio narratiivisen kirjallisuuskatsauksen lisäksi. Integroivalla kirjallisuuskatsauksella on yhtymäkohtia systemaattiseen kirjallisuuskatsaukseen ja sitä käytetään, kun tutkittavaa ilmiöltä halutaan kuvata monipuolisesti. Systemaattiseen katsaukseen verrattuna integroiva kirjallisuuskatsaus tarjoaa laajemman kuvan aihetta käsittelevästä kirjallisuudesta ja se auttaa kirjallisuuden kriittisessä arvioinnissa, syntetisoinnissa ja tarkastelussa. Integroivassa katsauksessa tutkimusaineistoa ei seulota niin yksityiskohtaisilla valintakriteereillä kuin systemaattisessa katsauksessa eikä se rajaa erilaisin meto-

disin lähtökohdin tehtyjä tutkimuksia, vaan se sallii kaikki tutkimukset analyysin pohjaksi. Tämän seurauksena aiheesta on mahdollista kerätä laaja otos. Integroivassa katsauksessa on viisi vaihetta: tutkimusongelman asettelu, aineiston hankkiminen, arviointi, analyysi ja tulkinta sekä tulosten esittäminen. [24, s. 8]

Integroivan kirjallisuuskatsauksen tekoon ei ole olemassa yhtä tiettyä mallia, vaan tutkimuksen tekijällä on mahdollisuus toteuttaa tutkimus oman tahdon mukaan [36, s. 359]. Tässä tutkimuksessa kirjallisuuskatsaus toteutetaan edellä mainitussa järjestyksessä. Tutkimuksessa käytettyjen julkaisujen luotettavuutta on arvioitu Julkaisufoorumin julkaisukanavahaun avulla.

3.3.2 Kirjallisuuskatsauksen aineisto

Tässä tutkimuksessa käytetyt tietokannat ovat ProQuest Central, IEEE Xplore, ACM Digital Library, SpringerLink ja ScienceDirect. Artikkelit valittiin hakutuloksista alustavaan tarkasteluun otsikon perusteella, minkä jälkeen luettiin valittujen artikkeleiden tiivistelmät. Mikäli artikkeli vaikutti tiivistelmän perusteella relevantilta, artikkeli käytiin läpi tarkemmin. Haut tuottivat yhteensä 3191 osumaa, joista 97:n tiivistelmät luettiin ja kokonaisuudessaan 46 artikkelia otettiin lähempään tarkasteluun. Lähemmän tarkastelun jälkeen osa artikkeleista rajautui pois, sillä niiden sisältö ei ollut relevanttia tämän tutkimuksen kannalta. Näin ollen 46 artikkelista valittiin lopulta 10 artikkelia sisällytettäväksi kirjallisuuskatsaukseen. Kirjallisuuskatsaukseen valittiin vain artikkelit, jotka olivat saatavilla maksutta Tampereen yliopiston opiskelijoille, vertaisarvioitu ja joiden julkaisukieli oli englanti. Kirjallisuuskatsaukseen ei otettu mukaan useita mielenkiintoiselta vaikuttavia artikkeleita, joiden JUFO-luokitus oli 0 tai niiden julkaisualustoja ei ollut arvioitu ollenkaan. Käytetyt hakusanat on esitelty taulukossa 3.2 ja hakutulokset on esitelty taulukossa 3.3.

Taulukko 3.2. *Hakusanat*

Hakuindeksi	Hakusana
A	(ISO 27001 OR 27001 OR ISO 2700* OR ISO2700*) AND (implementati* OR establish* OR introduct*)
B	("ISO 27001"OR "ISO27001") AND (implementati* OR establish* OR introduct*)
C	(ISO 27001 OR 27001 OR ISO 2700* OR ISO2700*) AND (success* OR enable*)
D	("ISO 27001"OR "ISO27001") AND (“CSF” OR “critical success factor”)

Taulukko 3.3. *Hakutulokset*

Tietokanta	**Hakusanat**	**Rajaukset**	**Hakujoukko**	**Tiivistelmää luettu**	**Artikkelia käyty läpi**
ProQuest	A, B, C, D	Vain vertaisarvioidut ja tietelliset artikkelit	317	17	8
IEEE Xplore	A, B, C, D		145	19	10
ACM	B, C, D		298	8	6
SpringerLink	B, C, D	Konferenssijulkaisut, artikkelit	1266	21	11
Emerald	B, C, D	Konferenssijulkaisut, artikkelit	383	20	7
ScienceDirect	B, C, D	Tutkimusartikkelit	782	12	4
Yhteensä			**3191**	**97**	**46**

4. KIRJALLISUUSKATSAUS

Tässä luvussa tehdään integroiva kirjallisuuskatsaus. Kirjallisuuskatsauksessa keskitytään onnistumistekijöihin, joten kirjallisuuden analyysistä on jätetty pois muista näkökulmasta mahdollisesti relevantteja asioita, kuten esteet sekä yksityiskohtaiset projektinhallintakäytännöt toteutusprojekteissa sekä organisaatiokulttuuriin liittyvät arvot ja perusoletukset. Lopuksi tässä luvussa esitellään kirjallisuuskatsauksen yhteenveto. Konstruktiivisen tutkimusotteen kolmas vaihe, eli tutkimusaiheen syvällisen teoreettisen tuntemuksen hankkiminen sijoittuu tähän lukuun.

4.1 Onnistumistekijät tietoturvaan ja IT:n hallintaan liittyvissä toteutusprojekteissa

Kriittisistä onnistumistekijöistä käytetään englannin kielessä termiä CSF (critical success factors). Bullenin ja Rockartin määritelmän mukaan [5, s. 7] kriittiset onnistumistekijät ovat organisatorisia tekijöitä, joiden riittävän tason avulla organisaatiot voivat saavuttaa menestyksekkään kilpailukyvyn, jonka avulla liiketoiminta kukoistaa ja organisaatio kykenee saavuttamaan tavoitteensa.

Alreemyn et al. tekemässä vuonna 2016 julkaistussa tutkimuksessa [2] tarkasteltiin kirjallisuuskatsauksen avulla kriittisten onnistumistekijöiden roolia organisaatioiden IT:n hallintatapaan (*IT governance*) liittyvissä toteutusprojekteissa. Tutkimuksen mukaan onnistumistekijöiden huomioiminen voi auttaa IT:n hallintatapaan liittyvien toteutusprojektien tavoitteiden saavuttamisessa, mutta niiden puuttuminen voi vaikeuttaa tavoitteiden saavuttamista. IT:n hallintatapa kattaa mm. tietoturvan, IT:n palveluidenhallinnan, ohjelmistokehityksen sekä projektinhallinnan. Tutkimuksessa jaotellaan toteutusprojektit kolmeen osaan: toteutusta edeltävään vaiheeseen, toteutusvaiheeseen sekä toteutuksen jälkeiseen vaiheeseen.

Alreemyn et al. mukaan toteutusta edeltävässä vaiheessa on tärkeää kiinnittää huomiota valmisteluun. Tällä tarkoitetaan esimerkiksi kaikkien prosessien ja käytäntöjen kartoittamista, sidosryhmien, käyttäjien ja työntekijöiden valmennusta käytäntöihin. Myös pääelementtien analysointi sekä roolien ja vastuiden määrittely ovat tärkeitä.

Toteutusvaiheessa onnistumistekijöitä ovat mm. sidosryhmien osallistaminen, johdon tu-

ki, taloudellinen tuki, organisatoriset vaikutukset, strateginen yhdenmukaisuus IT:n ja liiketoiminnan välillä, IT:n henkilöstön hallinta, IT:n rakenne sekä toteutusprojektin hallinta. Sidosryhmien osallistamisella tarkoitetaan kaikkien projektiin liittyvien oikeiden henkilöiden osallistamista, jolloin he pääsevät vaikuttamaan projektiin liittyviin päätöksiin sekä sen kulkuun. Johdon tuki liittyy oleellisesti sidosryhmien osallistamiseen ja sen puuttuminen voi vaikeuttaa merkittävästi toteutusprojektin kulkua. IT-projektien kustannukset ovat usein suuria, minkä takia niiden rahoitukselle täytyy olla jatkuva tuki sekä varattu budjettia, jotta projektit onnistuvat. Alreemyn et al. mukaan taloudellinen tuki ei ole kuitenkaan kaikille organisaatioille oleellinen seikka. Toteutusprojektien organisatoriset vaikutukset tulisi ottaa huomioon, sillä projekteilla on usein monia vaikutuksia koko organisaatioon, kuten niiden toimintatapoihin tai kulttuuriin. Organisaation liiketoiminnan ja IT:n tulisi olla yhteisymmärryksessä toistensa tarpeista ja päämääristä. Tämä voidaan saavuttaa hyvällä viestinnällä ja se tulisi ottaa huomioon toteutusprojektissa. IT:n henkilöstön resurssien riittävyys, ammattitaito ja kyvykkyydet ovat merkittävä tekijä toteutusprojekteissa. Tutkimuksen mukaan ammattitaidon ja koulutuksen puute voi olla merkittävä este toteutusprojektien arvon realisoitumiselle. Myös IT:n rakenteen, prosessien, roolien ja vastuiden tulisi olla selkeät ennen toteutusprojektin aloittamista. Tutkimuksessa mainitaan myös hyvän projektinhallinnan olevan suuressa roolissa toteutusprojektien onnistumisen kannalta, sillä hyvällä projektinhallinnalla voidaan vaikuttaa esimerkiksi ajankäyttöön.

Almeidan et al. vuonna 2019 julkaistussa tutkimuksessa [1] tutkittiin GDPR:n käyttöönottoon liittyviä kriittisiä onnistumistekijöitä systemaattisen kirjallisuuskatsauksen keinoin. Kriittiset onnistumistekijät jaettiin mahdollistajiin, joiden avulla projektien toteutuminen helpottuu ja jotka ovat kriittisiä niiden toteutumiselle sekä esteisiin, jotka voivat aiheuttaa projektien epäonnistumisen. Mahdollistajiksi tutkimuksessa todettiin mm. käyttöönoton yksityiskohtaisen tiekartan teko sekä tietosuojan ja tietoturvan tärkeyden ymmärtäminen organisaatiossa. Esteiksi ja haasteiksi puolestaan Almeida et al. totesivat GDPR:n kompleksisuuden sekä yksityiskohtaisten ohjeiden puuttumisen, GDPR:n vaatiman runsaan ajan ja henkilöstöresurssit, rahoituksen puutteen GDPR:n huomioimiselle toiminnassa sekä tietosuojan osaamisen ja ammattitaidon puutteen organisaatioissa.

Othmanin ja Chanin tutkimuksessa [19] käsitellään IT:n hallintaan ja sen käytäntöön viemiseen liittyviä esteitä laadullisen tutkimuksen avulla. Vuonna 2013 julkaistun tutkimuksen löydöksiä olivat muutosvastarinta, käytäntöjen sekä projektien – kuten tietoturvan hallintajärjestelmän toteuttamisen – kompleksisuus sekä organisaation sisäiset valtataistelut, jolla tarkoitetaan oman edun tavoittelua organisaation edun sijaan. Myös keskijohdon tuen puuttuminen mainittiin yhdeksi esteeksi. Se liittyy organisaation sisäisiin valtataisteluihin ja sillä tarkoitetaan organisaation ylimmän johdon ja suorittavan portaan välissä olevan johdon – yleisemmin keskijohdon – tuen puutetta. Kolmas johtoon liittyvä este on johdon vaihtuminen, jolla tarkoitetaan johtajien siirtymistä toisiin tehtäviin, mikä aiheuttaa muutoksia johtamistavoissa sekä jatkuvien parannusyritysten katkeamista

uusien johtajien ottaessa roolin haltuun. Myös henkilöstön tiedon ja ammattitaidon puute, suuret maantieteelliset etäisyydet sekä vastaanottavaisuus määräyksille mainittiin esteiksi. Viimeksi mainittu koskee erityisesti organisaatioita, joissa käskyt ja määräykset jaetaan ylhäältä alaspäin ja jossa työntekijöitä motivoi vain heidän lähimpien esihenkilöidensä välittämät käskyt.

Gillies käsittelee vuonna 2011 julkaistussa tutkimuksessa [9] tietoturvan hallintajärjestelmän laadun parantamista ISO 27000 -standardiperheen avulla. Gilliesin mukaan yksi este ISO 27001 -standardin omaksumiselle on korkeat kustannukset, jotka johtuvat esimerkiksi konsulttien käyttämisestä toteutusprojektin yhteydessä.

Stewartin ja Jürgensin tutkimuksessa [34] käsitellään tietoturvan hallintaa ja inhimillisten tekijöiden roolia organisaatioissa. Vuonna 2017 julkaistussa tutkimuksessa tuodaan esiin viisi avaintekijää, jotka vaikuttavat tietoturvan hallinnan onnistuneeseen käyttöönottoon: kiinnostuksen puute tietoturvaa kohtaan, tietoturvakoulutusten puute, laitteiston ylläpidon puute, johdon tuen puute sekä tietoturvapolitiikan puuttuminen.

Culotin, Nassimbenin, Podreccan ja Sartorin tekemä tutkimus [7] käsittelee systemaattisen kirjallisuuskatsauksen avulla ISO/IEC 27001 -standardista tehtyä tutkimusta. Culot et al. vuonna 2021 julkaistussa tutkimuksessa organisaatioiden motivaatiotekijät luokitellaan funktionalistisiin sekä institutionaalisiin tekijöihin, joiden takia ne kehittävät tietoturvan hallintajärjestelmää ja pyrkivät sen sertifioimiseen. Funktionalististen motivaatiotekijöiden avulla organisaatiot odottavat saavuttavansa paremman tietoturvan tason sekä parantavansa tuottavuutta kehittämällä ja ylläpitämällä tietoturvan hallintajärjestelmää. Institutionaalisiin motivaatiotekijöihin luokitellaan yrityksen imagon parantaminen, lakisääteisiin vaatimuksiin vastaaminen, markkinoiden vaatimukset sekä paine yhdenmukaisuuteen. Culot et al. käsittelevät tutkimuksessaan myös tietoturvan hallintajärjestelmien toteutusprojektien hallintaa. Tutkimuksen mukaan projekteissa käytetään useita eri lähestymistapoja, joista tyypillisin on aloittaminen pienemmällä, rajatulla pilottivaiheella ja siirtyminen laajamittaiseen käyttöönottoon. Projekteihin liittyen tutkimuksessa mainitaan johdon tuki ja erityisesti se, että vastuu tietoturvan hallintajärjestelmän kehittämisestä on tyypillisesti IT-osastolla ja etteivät tietoturvajohtajat ole useinkaan osa organisaatioiden johtoryhmää. Johdon tuen puute ja vähäinen tietoisuus voi johtaa taloudellisen tuen puuttumiseen. Culot et al. mainitsevat tutkimuksessaan myös konsulttien käytön tietoturvan hallintajärjestelmän toteutusprojektin apuna, mikä johtaa siihen, ettei organisaatiolle kartu osaamista hallintajärjestelmästä, ja voi johtaa epäonnistuneeseen toteutukseen. Lisäksi tutkimuksessa tuodaan esiin, että sertifiointi vaatii merkittävästi resursseja, niin taloudellisia kuin henkilöstön työtuntejakin.

Schinaglin ja Shahimin tietoturvan hallintaa käsittelevä vuonna 2020 julkaistu tutkimus [25] käsittelee kirjallisuuskatsauksen avulla haasteita, jotka estävät tietoturvan hallinnan tehokkaan toteutumisen. Tutkimuksen mukaan suhtautuminen tietoturvaan on useissa or-

ganisaatioissa reaktiivista, tilapäistä ja keskittyy vain välitöntä huomiota vaativiin tapahtumiin, vaikka tietoturvapoikkeamat ovat välttämätön osa digitaalisessa liiketoimintaympäristössä ja jokin osa tietoturvahyökkäyksistä johtaa tietovuotoihin. Organisaatioilla onkin uusi haaste oppia jatkamaan liiketoimintaa myös tietovuodon aikana sekä oppia palautumaan niistä. Schinaglin ja Shahimin tutkimuksessa tuodaan esiin, että tietoturvaa hoitaa usein jokin osa IT-osastosta ja korkein tietoturvajohtaja on vain osa keskijohtoa, mikä johtaa siihen ettei tietoturvaa kehitetä yhdessä liiketoiminnan kanssa. Tietoturvaa ei pitäisi jättää ainoastaan tietoturva-ammattilaisten hoidettavaksi, vaan organisaatioiden tulisi kehittää sitä yhteistyössä liiketoiminnan johdon kanssa ja sen tulisi olla linjassa liiketoiminnan strategian kanssa. Tutkimuksessa todetaan myös, että liiketoiminnan sidosryhmät keskittyvät usein lyhyellä aikavälillä arvoa tuottaviin asioihin, minkä vuoksi tietoturvaa ei huomioida tuotteiden ja prosessien suunnitteluvaiheessa, mikä johtaa toimimattomiin tietoturvaratkaisuihin. Toisaalta myös liiallinen tietoturvaan keskittyminen voi jarruttaa tuotekehitystä ja pidentää markkinoilletuontiaikaa sekä heikentää sovellusten suorituskykyä. Tutkimuksen mukaan tasapainon löytäminen tietoturvan ja liiketoiminnan välillä onkin suuri haaste organisaatioille. Lisäksi Schinaglin ja Shahimin tutkimuksessa mainitaan johdon tuki sekä tietoturvan näkeminen pelkkänä kulueränä investoinnin sijaan. Edellä mainitun syynä on haaste tietoturvainvestointien laskemisessa, sillä niiden tavoitteena on estää tulojen menetys eikä suorat taloudelliset hyödyt.

Hun, Dinevin, Hartin ja Cooken tutkimuksessa [10] käsitellään johdon sekä organisaatiokulttuurin roolia tietoturvapolitiikan ja -ohjeistusten noudattamisen yhteydessä. Hu et al. vuonna 2012 julkaistun tutkimuksen ensimmäinen löydös on, että johdon aktiivisella ja näkyvällä osallistumisella on vaikutuksia kulttuuriin sekä työntekijöiden uskomuksiin, minkä myötä he noudattavat tietoturvakäytäntöjä. Toisen löydöksen perusteella organisaatiokulttuurin rakentamisella on positiivisia vaikutuksia työntekijöiden aikomuksiin noudattaa tietoturvapolitiikkoja. Hu et al. mainitsevat organisaatiokulttuuriin vaikuttaviksi tekijöiksi tavoitteiden selkeän kommunikoinnin, sääntöjen ja käytäntöjen vakiinnuttamisen, työntekijöiden arvioimisen tavoitteiden ja käytäntöjen noudattamisen perusteella sekä palkitsemalla noudattamisesta ja rankaisemalla käytäntöjen ja sääntöjen rikkomisesta. Kolmantena löydöksenä tutkimuksessa tuodaan esiin johdon rooli organisaatiokulttuurin arvojen muokkaamisessa ja tulokset osoittavat, että johdon osallistumisella on suoria ja merkittäviä vaikutuksia organisaatiokulttuuriin sekä tuloshakuisuuteen. Tutkimuksen tulosten perusteella johdon pitäisi olla aktiivisesti ja näkyvästi mukana tietoturvapolitiikkojen ja ohjeistusten määrittelyssä, käyttöönotossa ja toimeenpanossa. Hu et al. ehdottavat Scheinin kuuden jalkautusmekanismin käyttöä tämän apuna. Neljäs löydös liittyy tietoturvakoulutusohjelmiin ja kattavien tietoturvapolitiikkojen implementointiin. Hu et al. väittävät, että koulutusohjelmien tulisi olla räätälöityjä kohderyhmille, jotta niistä saadaan kaikki hyöty irti verrattuna geneerisiin koulutusohjelmiin. Tutkimuksen viidennen ja viimeisen löydöksen perusteella tietoturvapolitiikan noudattamisen seuraaminen organisaatioissa on vaativa

tehtävä, mikä vaatii kokonaisvaltaista lähestymistä. Tietoturvan korkea taso vaatii kattavia tietoturvaohjelmia, hyvää johtamista, tietoturvatietoisuuden kouluttamista, tehokasta viestimistä vaatimustenmukaisuudesta, oppimisteorioihin perustuvien koulutusohjelmien suunnittelua, kurinpitoprosessin luomista ohjeistusten ja politiikoiden noudattamattomuuden varalle sekä vahvan sääntölähtöisen ja tavoitehakuisen organisaatiokulttuurin luomista.

Tietoturvan hallintaa ja sen toteutukseen liittyviä kriittisiä onnistumistekijöitä käsittelevä Tun ja Yanin tutkimus [37] vuodelta 2014 jakaa kriittiset onnistumistekijät kuuteen eri kategoriaan: yhteys liiketoiminnan kanssa (*business alignment*), organisatorinen tuki (*organizational support*), organisaation tietoisuus (*organizational awareness*), IT-osaaminen (*IT competence*), hallintakeinojen kehitys (*security controls development*) sekä suorituskyvyn arviointi (*performance evaluation*). Organisatorisen tuen alle kuuluvia onnistumistekijöitä ovat johdon tuki, sitoutuminen rahoitukseen sekä organisaation rakenne, joka tukee tietoturvan systemaattista kehittämistä, sen raportointia ja viestintää. Henkilöstön tietoisuus ja koulutus sekä tietoturvakulttuuri ovat organisaation tietoisuuteen liittyviä kriittisiä onnistumistekijöitä. IT-osaamisella tarkoitetaan Tun ja Yanin tutkimuksessa kykyjä, joilla IT:n ja liiketoiminnan tavoitteet saavutetaan. Hallintakeinojen kehitykseen liittyviä onnistumistekijöitä ovat tehokas riskienhallinta, tietoturvapolitiikoiden jalkauttaminen sekä tietoturvastandardien noudattaminen. Suorituskyvyn mittaamisella tarkoitetaan tietoturvan hallintajärjestelmään liittyvien tavoitteiden seuraamista ja tarkkailua sekä jatkuvan parantamisen varmistamista.

Tietoturvan kymmentä ”kuolemansyntiä” käsittelevässä tutkimuksessa [32] vuodelta 2004 von Solms ja von Solms väittävät kokemuksiinsa perustuen, että mikäli yksikin tutkimuksessa listatuista seikoista jätetään huomioimatta, se johtaa ongelmiin tietoturvan hallinnassa. Kuolemansynnit ovat:

1. Ei ymmärretä, että tietoturva on yrityksen johdon vastuu.
2. Ei ymmärretä, että tietoturva koskettaa myös liiketoimintaa eikä se ole pelkästään tekninen asia.
3. Ei ymmärretä, että tietoturvan hallinta on monialainen aihe.
4. Ei ymmärretä, että tietoturvan kehityssuunnitelman täytyy perustua tunnistettuihin riskeihin.
5. Ei ymmärretä parhaiden käytäntöjen hyödyntämisen tärkeyttä tietoturvan hallinnassa.
6. Ei ymmärretä, että tietoturvapolitiikka on välttämätön.
7. Ei ymmärretä, että tietoturvakäytäntöjen noudattamisen valvonta ja seuranta on ehdottoman tärkeää.
8. Ei ymmärretä tietoturvan hallintorakenteen olevan ehdottoman tärkeä.

9. Ei ymmärretä käyttäjien tietoturvatietoisuuden merkitystä.
10. Tietoturvasta vastaaville henkilöille ei anneta työkaluja ja tukea, jotta he voisivat hoitaa työnsä menestyksekkäästi.

Von Solms ja von Solms esittelevät tutkimuksessaan myös seuraukset mikäli organisaatio lankeaa syntiin ja jättää mainitut seikat huomioimatta. Seurauksia ovat mm. rahan tuhlaaminen toimimattomiin teknisiin tietoturvaratkaisuihin, tietoturvaratkaisujen keskittyminen vain osaan organisaatiosta ja niiden keskittyminen vaarattomiin riskeihin, jolloin vakavat riskit jäävät huomioimatta. Lisäksi seurauksina mainitaan valheellinen turvallisuuden tunne ja tietoturvajohtajien siirtyminen toiseen työpaikkaan, mikäli heille ei anneta työkaluja ja resursseja hoitaa töitään kunnolla.

4.2 Yhteenveto

Kirjallisuuskatsauksen löydökset on koottu yhteen taulukkoon 4.1.

Taulukko 4.1. *Onnistumistekijät kirjallisuudessa*

	Almeida et al. (2019)	Alreemy et al. (2016)	Culot et al. (2021)	Gillies (2011)	Hu et al. (2012)	Othman & Chan (2013)	Schinagl & Shahimi (2020)	Stewart & Jürgens (2017)	Tu & Yan (2014)	von Solms & von Solms (2004)
Suunnitteluvaihe										
Valmistelu	X	X								
Tietoturvan tärkeyden ymmärtäminen organisaatiossa	X									
Tietoturvan näkeminen investointina							X			
Johdon aktiivinen ja näkyvä rooli					X					
Organisaatiokulttuurin rakentaminen					X				X	
Käyttöönottovaihe										
Sidosryhmien osallistaminen		X								
Johdon tuki		X	X				X	X	X	X

Jatkuu seuraavalla sivulla

Taulukko 4.1 – jatkuu edelliseltä sivulta

	Almeida et al.	Alreemy et al.	Culot et al.	Gillies (2011)	Hu et al.	Othman & Chan	Schinagl & Shahimi	Stewart & Jürgens	Tu & Yan	von Solms & von Solms
Taloudellinen tuki		X	X	X						
Strateginen yhdenmukaisuus IT:n ja liiketoiminnan välillä		X								X
Organisatoriset vaikutukset										X
IT:n henkilöstön hallinta		X								
IT:n rakenne		X							X	
Organisaation sisäiset valtataistelut						X				
Keskijohdon tuki						X				
Johdon vaihtuminen						X				
Muutosvastarinta						X				
Osaava IT-henkilöstö										
Organisaation toimipisteiden lyhyet maantieteelliset etäisyydet						X				
Vastaanottavaisuus määräyksille						X				
Tietoturvakoulutukset					X			X	X	
Kiinnostus tietoturvaa kohtaan								X		
Laitteiston ylläpito								X		
Tietoturvapolitiikan olemassaolo								X		X
Henkilöstön tietoturvatietoisuus									X	X
Kehityssuunnitelman perustuminen tunnistettuihin riskeihin									X	X
Hyvä projektinhallinta		X								

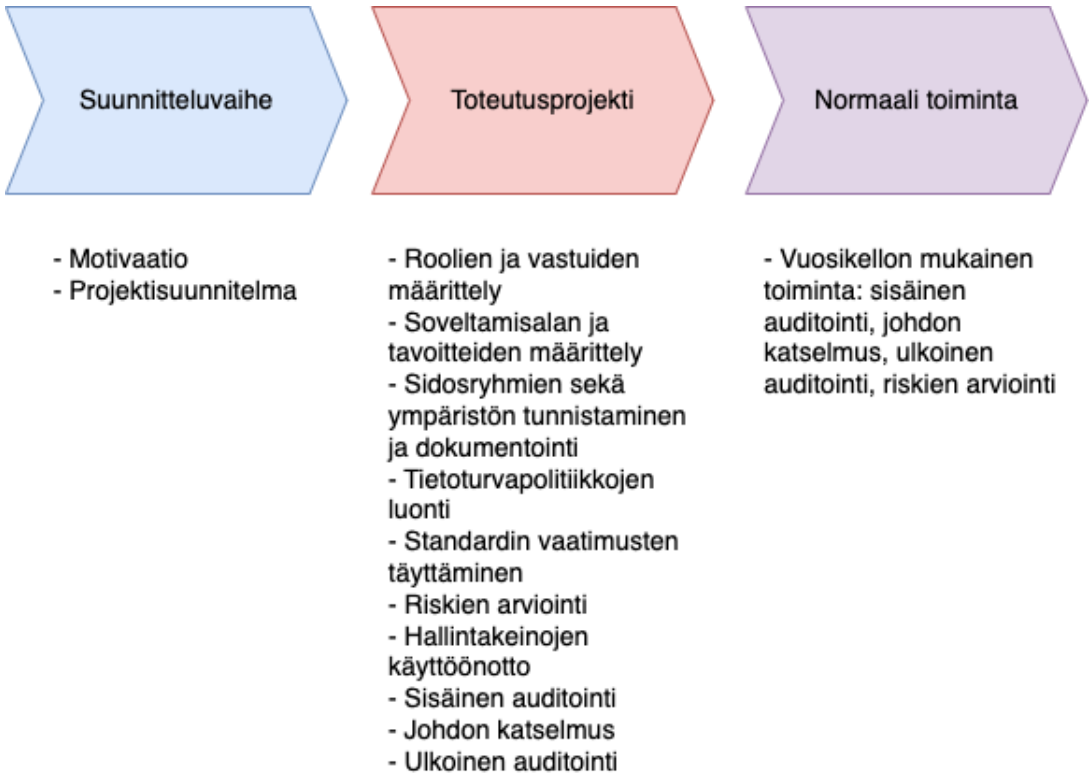
Tietoturvan hallintajärjestelmää, IT:n hallintatapaa ja näihin liittyviä projekteja sekä näihin

liittyviä onnistumistekijöitä, kriittisiä onnistumistekijöitä sekä haasteita on tutkittu 2000-luvun ensimmäisen vuosikymmenen lopulta lähtien. Osa tutkimuksista keskittyy onnistumistekijöihin tai avaintekijöihin [1][2][34][37], mitkä kuvaavat kattavasti asioita, joihin olisi syytä kiinnittää huomiota tietoturvan hallintajärjestelmää toteutettaessa. Osa puolestaan keskittyy esteisiin, kompastuskiviin ja haasteisiin [19][25][32]. Esteet voidaan toisaalta ajatella onnistumistekijöiden vastakohtina ja täten käänteisinä onnistumistekijöinä. Erityisesti suuret kustannukset mainitaan useassa tutkimuksessa [9]. Culot et al. tekemä tutkimus [7] puolestaan nivoo yhteen ISO/IEC 27001 -standardista tehtyä tutkimusta ja siinä käsitellään useita eri näkökulmia. Johdon rooli ja merkitys tuodaan esiin useissa tutkimuksissa [1][2][9][10][19][37], mikä on luonnollista, sillä tietoturvan hallintajärjestelmä keskittyy nimenomaisesti hallintaan ja johtamiseen. Tutkimusmenetelmät vaihtelevat kirjallisuuskatsauksista [1][2][7][25] laadulliseen tutkimukseen [19] ja kyselytutkimukseen tai näiden yhdistelmiin [10][34][37].

5. TIETOTURVAN HALLINTAJÄRJESTELMÄN TOTEUTTAMINEN KOHDEYRITYKSELLE

Tässä luvussa käydään läpi tietoturvan tilaa kohdeyrityksessä ennen tietoturvan hallintajärjestelmän toteutusprojektia, projektin kulkua ja sen aikana tunnistettuja onnistumistekijöitä. Konstruktiivisen tutkimusotteen neljäs vaihe, eli ratkaisumallin innovoiminen ja konstruktion kehittäminen sijoittuu tähän lukuun.

Tietoturvan hallintajärjestelmän elinkaari ja sen toteuttaminen voidaan jakaa [2, s. 911-912] karkeasti kolmeen osaan: suunnitteluvaihe, toteutusprojekti ja hallintajärjestelmän normaali toiminta. Elinkaari on esitelty kuvassa 5.1.



Kuva 5.1. *Tietoturvan hallintajärjestelmän elinkaari*

Seuraavaksi tarkastellaan verkkopalvelun lähtötilannetta kohdeyrityksessä, minkä jälkeen alaluvusta 5.2 alkaen analysoidaan projektin onnistumistekijöitä kuvassa 5.1 esitellyissä kolmessa eri projektin vaiheessa.

5.1 Tietoturvan tila ennen hallintajärjestelmän toteutusprojektia

Tietoturvan nykytilalla on merkittävä vaikutus hallintajärjestelmän toteutusprojektin etenemiseen ja sen työmäärään. Mikäli tietoturvaa on kehitetty organisaatiossa suunnitelmallisesti jo pidemmän aikaa, toteutusprojekti voi olla kevyt, sillä oletettavasti organisaatio on omaksunut ja ottanut käyttöön alan parhaita käytäntöjä, joiden myötä tietoturvan tila on vähintäänkin kohtuullisella tasolla. Seuraavissa alaluvuissa käydään läpi kohdeyrityksen sekä sen kehittämän verkkopalvelun tietoturvan tilaa. Näin on mahdollista ymmärtää tämän tutkimuksen lähtötilannetta.

5.1.1 Tietoturvan tila koko organisaatiossa

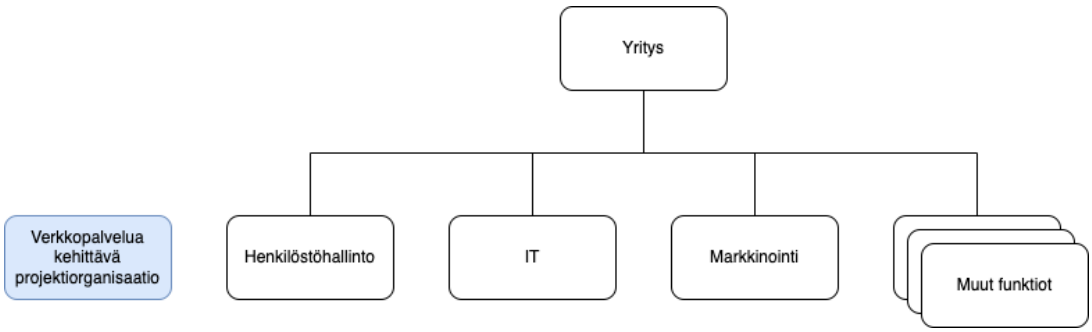
Päävastuu yrityksen tietojärjestelmien ja tiedon tietoturvasta kuuluu IT-osastolle, jonka vastuualueeseen kuuluu myös tietojärjestelmien hankinta organisaation tarpeiden perusteella. Lisäksi tietoturva ja tietosuoja-asiat kuuluvat tietyille henkilöstöhallinnon työntekijöille, juristille sekä kiinteistöön liittyvistä asioista vastaavalle henkilölle. Yrityksessä tietoturvan kehitys on ollut aiemmin pääosin IT-lähtöistä, mikä on seurausta yrityksen kulttuurista, jossa jokaisella työntekijällä on vapaus ja vastuu kehittää omaa työtä ja tehdä siihen liittyviä päätöksiä. Tämän perusteella kukin työntekijä saa ja voi – tiettyjen rajojen puitteissa – päättää oman työnsä yksityiskohdista, kunhan se palvelee yrityksen päämääriä. Yrityksessä pyritään välttämään tarpeetonta byrokratiaa ja käskyjen sanelemista ylhäältä päin. Käytännön tasolla, eli esimerkiksi tietoturvan kehittämisessä IT-osaston henkilöstö on hionut tietoturvan eri osa-alueita oma-aloitteisesti ja päämäärätietoisesti ajanut tietoturvaprojekteja eteenpäin saaden niihin rahoituksen. Kehitys on painottunut isoimpiin tunnistettuihin riskeihin ja tekniseen tietoturvaan, kuten identiteetin- ja pääsynhallintaan, verkon turvallisuuteen, päätelaitteiden turvallisuuteen ja fyysiseen turvallisuuteen. Järjestelmällinen ja säännöllinen riskienhallintaprosessi on kuitenkin puuttunut, vaikka IT-osasto onkin tehnyt riskienarviointia säännöllisesti. Tunnistettujen riskien seuraaminen ja päätettyjen sekä toteutettujen lievennystoimenpiteiden vaikuttavuuden katselmointi on puuttunut.

Tietoturvan hallintajärjestelmän toteuttamisen kannalta yritykseltä löytyi valmiina toimivat prosessit ja työkalut identiteetin- ja pääsynhallintaan, prosessit henkilöstöhallinnon osalta olivat kunnossa samoin kuin työntekijöiden puhelinten ja tietokoneiden hallintakeinot. Identiteetin- ja pääsynhallinnan työkalut ja prosessit ovat olleet yksi mahdollistava asia yrityksen kasvun kannalta, sillä kyvykkäiden ja monipuolisten työkalujen avulla iso osa työntekijöiden ja ulkoisten tahojen identiteettien elinkaareen liittyvistä eri vaiheista on pystytty automatisoimaan ja näin vapauttamaan IT-osaston työntekijöiden aikaa muihin työtehtäviin.

5.1.2 Tietoturvan tila verkkopalvelun osalta

Verkkopalvelun tietoturva oli huomioitu jo projektin alusta asti arkkitehtuurin suunnittelussa, kerättävän tiedon määrässä, käytettävien teknologioiden valinnassa ja ohjelmointikäytännöissä. Käytössä oli alan parhaita käytäntöjä, mutta dokumentointi oli luonnollisista ja ymmärrettävistä syistä puutteellista – yritykselle ei ollut täysin selvää, mikä verkkopalvelun vastaanotto olisi asiakkaiden keskuudessa ja vastaisiko yrityksen visio asiakkaiden tarpeita. Tämän johdosta myös laajempimuotoisen dokumentaation teko ennen projektin ja palvelun tulevaisuuden selkeytymistä oli nähty käytettävissä olevien henkilöiden työajan hukkaamiseksi.

Verkkopalvelua rakennettiin alkuvaiheessa lähestulkoon täysin omana projektinaan ja eristettynä kohdeyrityksen muusta organisaatiosta, jolloin projektiorganisaatio toimi ikään kuin omana yrityksenä yrityksen sisällä. Palvelua kehittänyt henkilöstö koostui pääosin ohjelmistokonsulteista, jotka työskentelivät hyvin itsenäisesti, mutta kuitenkin yrityksen henkilöstön ohjauksessa. Projektiorganisaation suhdetta yritykseen on havainnollistettu kuvassa 5.2. Tämän johdosta kohdeyrityksen tietoturvaprosessit ja -käytännöt eivät näkyneet palvelua rakentaneen projektiorganisaation päivittäisessä tekemisessä tai prosesseissa.



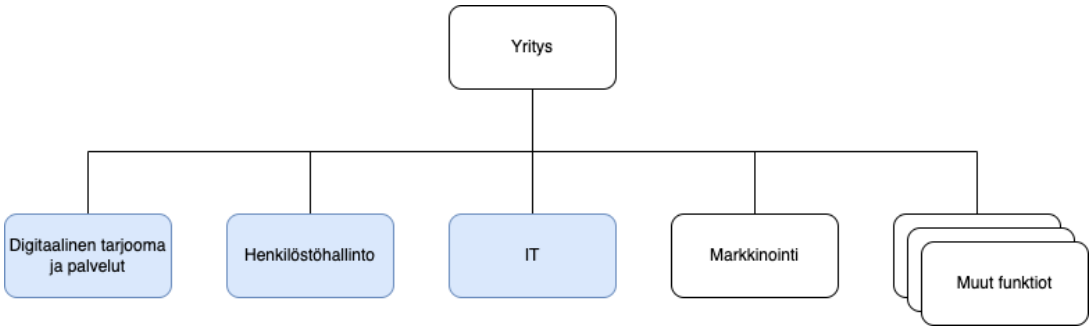
Kuva 5.2. *Verkkopalvelua kehittänyt projektiorganisaatio*

5.2 Suunnitteluvaihe

Analyysissä tunnistettiin useita onnistumista edesauttaneita tekijöitä jo suunnitteluvaiheesta. Onnistumistekijöiksi voidaan nimetä laadukas valmistelutyö, johdon aktiivinen ja näkyvä rooli tietoturvaan liittyen, tietoturvamyönteisen organisaatiokulttuurin rakentaminen, hallintajärjestelmän soveltamisalan rajaaminen koskemaan vain pientä osaa organisaatiosta sekä tietoturvan näkeminen investointina.

Suunnitteluvaihe käynnistyi kesällä 2021, jolloin yritys kartoitti eri vaihtoehtoja tietoturvan tason ja sen maineen parantamiseen. Selvitystyön perusteella yritys valitsi ISO/IEC 27001 -standardin mukaisen tietoturvan hallintajärjestelmän kehittämisen ja lähetti tämän työn kirjoittajan ISO/IEC 27001 Lead Implementer -kurssille.

Tietoturvan hallintajärjestelmä rajattiin koskemaan ainoastaan funktiota, jonka vastuulle digitaalisten palveluiden, kuten verkkopalvelun kehittäminen, operointi ja ylläpitäminen kuuluu. Lisäksi hallintajärjestelmän piiriin määriteltiin kuuluvan yrityksen tukitoimintoja tuottavat oleelliset osat, eli henkilöstöhallinto sekä IT-tiimi. Tietoturvan hallintajärjestelmän soveltamisalaa organisaatioon on havainnollistettu kuvassa 5.3



Kuva 5.3. *Yrityksen organisaatiokaavio, jossa korostettu hallintajärjestelmän piiriin kuuluvat funktiot*

Toteutusprojektin suurimmiksi riskeiksi arvioitiin mm. sisäisen resurssoinnin riittävyys, erityisesti konflikti ohjelmistokehittäjien työajan priorisoinnin kanssa, sillä oli selvää, että heidän arvokasta työpanosta tarvittaisiin myös itse verkkopalvelun kehittämisen parissa. Myös hallintajärjestelmän kehittämisestä vastuussa olevan henkilön työkuorma sekä hallintajärjestelmän soveltamisalan (*scope*) määrittely liian laajaksi arvioitiin yhdeksi merkittäväksi riskiksi. Analyysin perusteella riskiarviointi onnistui ja ottamalla tunnistetut riskit tekijät huomioon jo suunnitteluvaiheessa, riskit eivät realisoituneet projektin edetessä.

Projektin merkittävimmiksi kustannuksiksi todettiin projektiin osallistuvan henkilöstön palkat ja muut työntekijäkulut sekä sertifioinnista koituvat kulut. Täten toteutusprojekti oli myös merkittävä investointi yritykselle ja yritys oli halukas investoimaan tietoturvaan.

Yrityksen johto tuki projektia alusta asti ja esimerkiksi yrityksen toimitusjohtaja on kiinnostunut tietoturva-asioista ja ymmärtää vastuunsa tietoturvaan liittyen. Yrityksessä on jo pidempään ymmärretty ja tiedostettu tietoturvan sekä tietosuojan tärkeys liiketoiminnalle. Tietoturvariskien realisoitumisen vaikutukset liiketoiminnalle on tiedostettu ja mm. IT-osasto tekee riskienarviointia säännöllisesti, vaikka kattava riskienhallintaprosessi onkin puuttunut.

Onnistumista edesauttoivat sekä sisäiset että ulkoiset motivaatiotekijät. Sisäisinä motivaattoreina oli tietoturvan paremman tason tavoittelu sekä proaktiivisen tietoturvakulttuurin luominen jo verkkopalvelun alkuvaiheessa. Lisäksi yritys halusi pienentää vastausaikaa asiakkaiden kysymyksiin, sillä tietoturvan hallintajärjestelmän myötä useita teknisiä asioita vaaditaan dokumentoitavaksi. Ulkoisina motivaatiotekijöinä oli yrityksen imagon parantaminen, asiakkaiden vaatimukset sekä sertifikaatin saaminen, jota voidaan käyttää markkinoinnissa sekä tarjouskilpailuissa yhtenä kilpailuvalttina.

5.3 Toteutusprojekti

Toteutusprojektin osalta onnistumistekijöiksi voidaan nimetä johdon tuki ja taloudellinen tuki, hyvä projektinhallinta, sidosryhmien osallistaminen, strateginen yhdenmukaisuus liiketoiminnan kanssa ja tietoturva-asioista kiinnostunut henkilöstö.

5.3.1 Projektin järjestäytyminen ja projektinhallinta

Hallintajärjestelmän toteutusprojekti alkoi suunnitteluvaiheen jälkeen alkuvuodesta 2022, jolloin projektiorganisaatio perustettiin, luotiin projektisuunnitelma ja projektista viestittiin tärkeimmille sidosryhmille. Projektiin kuului mm. roolien ja vastuiden määrittely, sidosryhmien sekä ympäristön tunnistaminen ja dokumentointi, standardin vaatimusten täyttäminen sekä auditoinnissa todettujen poikkeaminen korjaaminen. Toteutusprojektista oli päävastuussa tämän työn kirjoittaja, joka toimi samalla projektipäällikkönä ja pääasiallisena toteuttajana. Projektin ohjausryhmään kuului digitaalisen tarjooman funktion johtaja, ohjelmistokehityksen johtaja sekä IT-osaston johtaja. Tärkeitä henkilöitä projektin toteutuksen kannalta olivat IT-osaston tietyt työntekijät, avainrooleissa olleet ohjelmistokehittäjät sekä juristi. Merkittäviä sisäisiä sidosryhmiä projektin kannalta olivat myös ns. ”tietoturvanyrkki”, johon kuuluu edustajia eri puolilta organisaatiota, kuten henkilöstöhallinnosta ja IT-osastolta. Yrityksellä oli jo entuudestaan ISO 9001 -standardin mukainen laatujärjestelmä, ISO 14001 -standardin mukainen ympäristöjärjestelmä sekä ISO 45001 -standardin mukainen työterveys- ja työturvallisuusjärjestelmä, joiden myötä sidosryhmät sekä ympäristö oli hyvin pitkälti jo valmiiksi tunnistettu. Kuitenkin tietoturvaan liittyvien erityisten sidosryhmien – kuten tietosuojavaltuutettu ja yrityksen sisäinen tietoturvanyrkki – ja heidän odotustensa tunnistaminen ja määrittely olivat osa toteutusprojektia.

Toteutusprojektille varattiin aikaa 11 kuukautta ja alkuperäisen tavoitteen mukaan ulkoisen auditoinnin ensimmäinen vaihe tapahtuisi kymmenen kuukauden kuluttua projektin alkamisesta. Toteutusprojekti jaettiin alkuperäisessä projektisuunnitelmassa yhdeksään eri vaiheeseen:

1. Soveltamisalan ja tavoitteiden määrittely sekä sidosryhmien tunnistaminen
2. Nykytila-analyysi
3. Tietoturvapolitiikkojen luonti
4. Riskienhallintaprosessin kehittäminen ja riskiarvioinnin teko
5. Hallintakeinojen valinta
6. Hallintakeinojen käyttöönotto
7. Hallintajärjestelmän validointi
8. Sisäinen auditointi

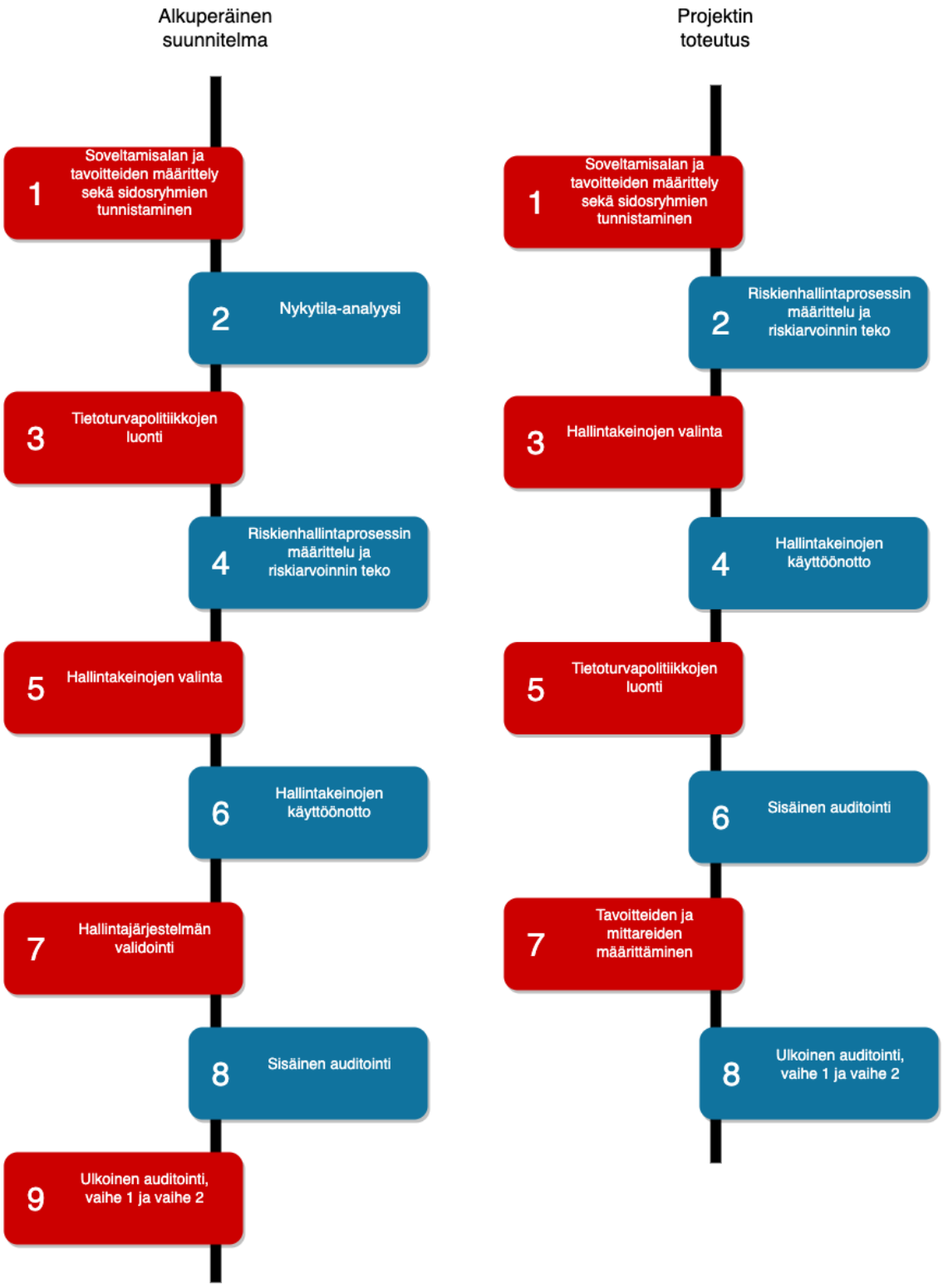
9. Ulkoinen auditointi, vaiheet 1 ja 2

Projektin edetessä eri vaiheita yhdistettiin toisiinsa, sillä niiden eri työvaiheilla todettiin olevan huomattavia yhteneväisyyksiä, joten niiden yhdistäminen koettiin järkeväksi ja myös jälkikäteen tarkasteltuna viisaaksi ratkaisuksi. Alkuperäinen projektisuunnitelma sekä lopullinen projektin kulku on esitelty kuvassa 5.4. Varsinaista nykytila-analyysiä ei tehty ollenkaan, sillä tietoturvan tila oli hyvin tiedossa projektin avainhenkilöillä. Myös eri vaiheiden paikkaa siirrettiin sekä aikataulusyistä että priorisointisyistä – tietoturvapolitiikkojen kirjoittaminen jätettiin viimeiseksi vaiheeksi ennen sisäistä auditointia, sillä projektin edetessä todettiin olevan järkevämpää ottaa ensin käyttöön riskejä pienentäviä teknisiä hallintakeinoja kuin keskittyä kirjoittamaan tietoturvan hallintaan liittyviä dokumentteja. Hallintajärjestelmän tavoitteiden ja mittareiden määrittäminen siirtyi samoista syistä sisäisen auditoinnin jälkeiseen ajankohtaan. Hallintajärjestelmän toteuttamisessa käytettiin apuna ISO/IEC 27003 -ohjestandardia.

Projektinhallintaan kiinnitettiin huomiota alusta alkaen ja projektin suunnitteluun panostettiin sen alkuvaiheessa. Projektinhallinnassa käytettiin apuna Jira-projektinhallintatyökalua, jonka avulla projektille muodostettiin etenemissuunnitelma ja projektin kulku pilkottiin pieniin osiin, aivan yksittäisen hallintakeinon toteuttamistasolle asti. Työkalun avulla hallintakeinojen toteuttamisvastuita jaettiin eri työntekijöille ja projektin eri työvaiheiden etenemistä oli helppo seurata. Analyysin perusteella toteutusprojektin projektinhallinta onnistui hyvin, sillä projekti pysyi tavoiteaikataulussa, joskin aikataulua muutettiin kerran ja ulkoisen auditoinnin tavoitteellista ajankohtaa siirrettiin kahdella kuukaudella eteenpäin. Syynä tälle oli projektiin liittymättömät yllättävät työtehtävät, ns. musta joutsen, joka vaati välitöntä reagointia. Projektiin liittyviä yllättäviä käänteitä ei ilmennyt.

Projektiin osallistettiin ja siihen osallistui henkilöitä eri puolilta organisaatiota: pääosin digitaalisesta tarjoomasta vastaavan funktion työntekijöitä, mutta myös henkilöstöhallinnosta sekä IT-osastolta. Ihmiset ovat yrityksessä kaiken kaikkiaan vastaanottavaisia, muutosvastarintaa ei ole juurikaan havaittavissa ja he ovat kiinnostuneita tietoturva-asioista. He haluavat parantaa tietoturvaan ja tietosuojaan liittyviä käytäntöjä sekä kehittää palveluita, joiden tietoturvaan on panostettu. Osalla henkilöstöstä on myös aiempaa kokemusta tietoturvan parista, joten henkilöstön voidaan katsoa olevan osaavaa ja ammattitaitoista myös tämän projektin osalta.

Tietoturvan hallintajärjestelmällä on selkeä yhteys liiketoiminnan kanssa, minkä myötä tietoturvaan liittyvät asiat nähdään mahdollisuutena eikä uhkana liiketoiminnalle. Näin ollen kaikki ymmärtävät tietoturvan merkityksen ja panostukset siihen, vaikka se voikin osaltaan hieman hidastaa ja vaikeuttaa liiketoiminnan arkea. Henkilöstö tietää ja ymmärtää, että yrityksen asiakkaisiin kuuluu maailman isoimpia yrityksiä ja merkittäviä organisaatioita, joilla on kovat vaatimukset heidän käyttämiensä verkkopalveluiden tietoturvalle.



Kuva 5.4. *Alkuperäinen projektisuunnitelma ja toteutunut projektin kulku*

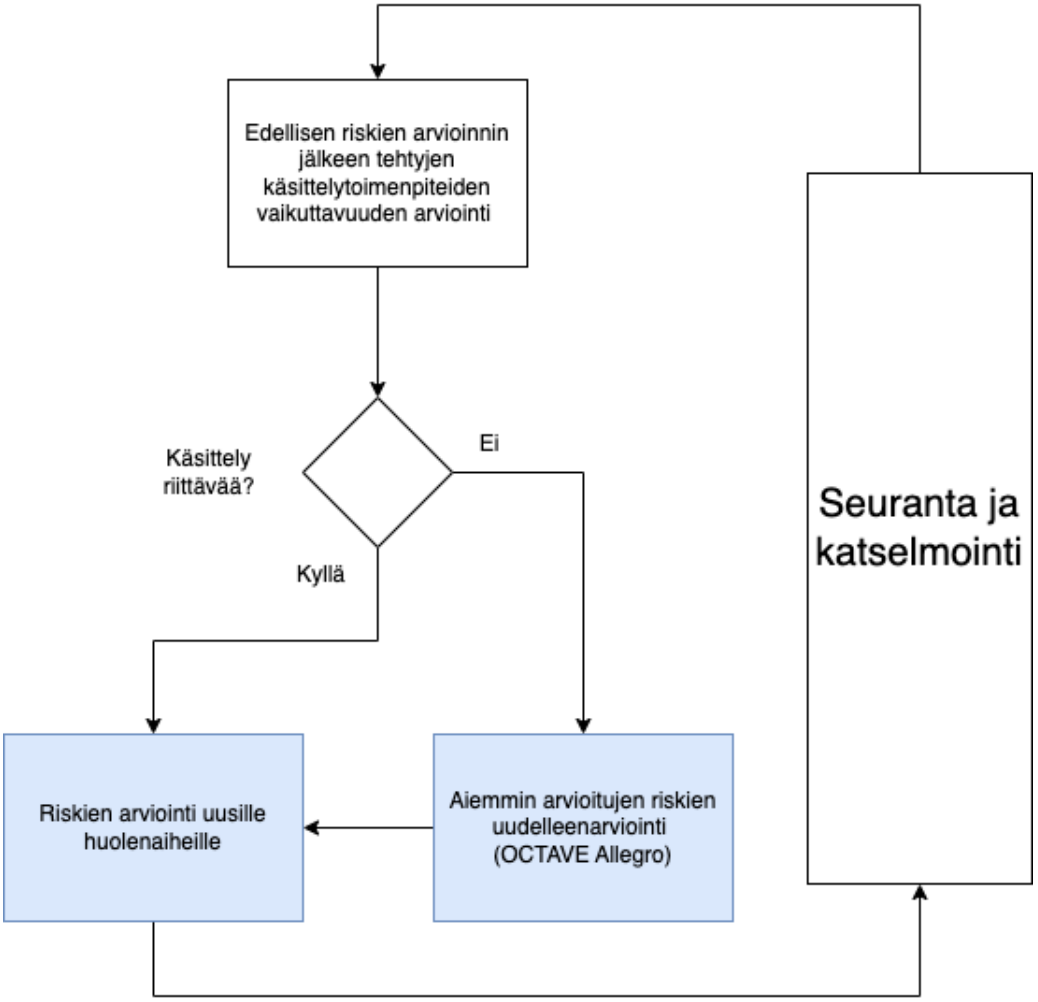
5.3.2 Riskienhallintaprosessi

Riskienhallintaprosessin kehittäminen sekä sen ensimmäinen testaaminen riskienarvioinnin teon yhteydessä oli yksi projektin merkittävimpiä ja työläimpiä yksittäisiä vaiheita. Ris-

kienarviointimenetelmäksi valittiin OCTAVE Allegro, sillä se sopii työpajatyöskentelyyn, on käytössä tietoturva-alan ammattilaisten keskuudessa ja sopii organisaatioille, joilla ei ole erillistä riskienhallintaan keskittyvää osastoa. Riskienhallintaprosessi kokonaisuudessaan on yhdistelmä luvussa 2 esitellyistä ISO/IEC 27005:n mukaisesta tietoturvariskien hallintaprosessista sekä OCTAVE Allegrosta. Projektin aikana kehitetty riskienhallintaprosessi on esitelty kuvassa 5.5. Tavoitteena oli yhdistää OCTAVE Allegron ketterä riskienarviointimenetelmä ISO/IEC 27005:n kokonaisvaltaiseen riskienhallintaprosessiin. Tämän avulla itse riskienarviointityömenetelmä on mahdollista kouluttaa ohjelmistokehittäjille ja muulle henkilöstölle, jolloin he voivat tehdä riskienarviointia itsenäisesti. Heillä nähdään olevan paras tietämys järjestelmiin liittyvistä riskeistä, joten on luonnollista, että he myös pääsevät arvioimaan niitä ja saavat täten kanavan tuoda huoliaan esille.

OCTAVE Allegron toimenpide 1 vastaa ISO/IEC 27005:n toimintaympäristön määrittelyä, mutta prosessia kehitettäessä todettiin, että mittarit muuttuvat todella harvoin, joten niiden laatimista ei tarvitse suorittaa jokaisen riskien arvioinnin yhteydessä. Samalla tavalla OCTAVE Allegron toimenpiteet 2-7 vastaavat hyvin pitkälle ISO/IEC 27005:n mukaista riskien arviointia ja toimenpide 8 ISO/IEC 27005:n mukaista riskien käsittelyä sekä hyväksymistä. Edellisen riskien arvioinnin jälkeen tehtyjen käsittelytoimenpiteiden vaikuttavuutta arvioidaan jokaisen riskienarviointi-työpajan yhteydessä, jolloin arvioidaan ovatko esimerkiksi lieventämistoimenpiteet tuottaneet toivotun tuloksen ja pienentäneet organisaatiolle aiheutuvaa riskiä. Mikäli ei ole, riski otetaan uudelleen käsiteltäväksi.

Prosessin kehittämisen jälkeen sitä testattiin yhden työpäivän mittaisessa riskienarviointityöpajassa. Työpajaan osallistui seitsemän henkilöä, joista kukaan ei ollut aiemmin kuullutkaan OCTAVE Allegrosta. Tästä huolimatta tai juuri sen takia työpajatyöskentely koettiin mielekkääksi ja malli hyväksi, sillä sen avulla uhkien tunnistaminen oli ketterää, eri osa-alueet oli vaivatonta pilkkoa pienempiin paloihin ja työpajaan osallistuneet pääsivät myös arvioimaan liiketoiminnalle aiheutuvia vahinkoja, mikäli riskit realisoituisivat. Osallistamalla ohjelmistokehittäjät mukaan riskien arviointiin kohdeyritys sai arvokasta tietoa verkkopalvelun teknisistä parannuskohteista, teknisestä velasta, hyökkäysvektoreista ja palvelun eri osien keskinäisistä riippuvuuksista. Yhden päivän mittaisen työpajan huonoiksi puoliksi osallistujat totesivat yksimielisesti sen raskauden, sillä uuden menetelmän opiskeleminen ja soveltaminen saman päivän aikana vaatii häiriötöntä keskittymistä. Noin puolet osallistui työpajaan etäyhteyden avulla ja tämän todettiin vaikeuttavan ryhmätyöskentelyä ja keskustelun seuraamista. Työpajan päätteeksi pidetyssä keskustelussa todettiin, että jatkossa vastaavat tilaisuudet kannattaa järjestää kahdessa osassa ja kaikkien osallistujien on hyvä olla samassa huoneessa, jotta tilaisuuden potentiaali saadaan hyödynnettyä parhaiten.



Kuva 5.5. *Kohdeyritykselle kehitetty riskienhallintaprosessi, jossa korostettu OCTAVE Allegron osuus*

5.3.3 Hallintakeinojen toteuttaminen ja auditoinnit

Riskienarvioinnin pohjalta valittiin hallintakeinot ISO/IEC 27001 -standardin liitteestä A ja priorisoitiin järjestys niiden käyttöönotolle. Hallintakeinojen toteuttamisvastuu delegoitiin eri tahoille, minkä jälkeen alkoi kuukausien mittainen toteuttamistyö. Hallintakeinojen toteuttamisessa käytettiin apuna ISO/IEC 27002 -ohjestandardia. Alkuperäisen suunnitelman mukaan tavoitteena oli validoida koko hallintajärjestelmä projektiorganisaation toimesta ennen sisäistä auditointia, mutta projektiin liittymättömien, muiden yllättävien työtehtävien vuoksi validoinnille ei kuitenkaan jäänyt aikaa ennen sisäistä auditointia.

Sisäisen auditoinnin jälkeen määritettiin tavoitteet ja niitä seuraavat mittarit, joilla arvioidaan tietoturvan toteutumista ja tietoturvan hallintajärjestelmän vaikuttavuutta. Eri tavoitteita vuosille 2022–2023 määritettiin seitsemän, joista kahdelle kehitettiin mittarit. Näistä ensimmäisen tavoitteena on varmistaa, että työntekijät ovat asianmukaisesti koulutettuja kehittämään ja ylläpitämään turvallisia ja luotettavia digitaalisia palveluita. Sitä mitataan

seuraamalla työntekijöiden suorittamien tietoturvakurssien määrää. Toinen tavoite on nolla tietoturvapoikkeamaa, minkä mittarina on tietoturvapoikkeamien määrä. Tämän yhteydessä määritettiin myös seuranta- ja raportointitaajuus sekä vastuuhenkilöt seurannalle ja mittaamiselle.

Tämän jälkeen oli vuorossa ulkoisen auditoinnin ensimmäinen vaihe, joka oli yhden työpäivän mittainen ja sen suoritti sertifiointiyrityksen auditoija. Ulkoisen auditoinnin ensimmäisen vaiheen tarkoituksena on varmistaa tietoturvan hallintajärjestelmän tilan olevan sellainen, että auditoinnin toinen vaihe on mahdollista ja järkevää suorittaa. Auditoinnin ensimmäisessä vaiheessa auditoija totesi hallintajärjestelmän dokumentoinnin ja muun tilan olevan sillä tasolla, että auditoinnin toinen vaihe voidaan suorittaa aikataulutettuna ajankohtana. Auditoinnin toinen vaihe oli kestoltaan viisi työpäivää, minkä aikana auditoijat haastattelivat hallintajärjestelmän piirissä työskenteleviä henkilöitä, kuten henkilöstöhallinnon, IT-osaston ja ohjelmistokehityksen työntekijöitä sekä yrityksen johtoa. Auditoinnin aikana havaittiin muutamia lieviä poikkeamia ja kohdeyritys sai ISO 27001 -sertifikaatin esiteltyään poikkeamien korjaussuunnitelman. Hallintakeinojen käyttöönotto jatkui ulkoisen auditoinnin toiseen vaiheeseen asti sekä myös sen jälkeen.

5.3.4 Projektin päättyminen

Projektin katsotaan päättyneen sertifikaatin saamiseen, vajaa vuosi projektin alkamisen jälkeen. Projektin retrospektiivissä todettiin projektin olleen onnistunut, vaikka se vaikuttikin aluksi suurelta ja pelottavalta. Muiksi positiivisiksi asioiksi todettiin Jiran käyttö hallintakeinojen toteuttamisvastuiden jakamisessa, dokumentaation oikea ja pragmaattinen taso, poikkifunktionaalinen sitoutuminen sekä projektilla olleet selkeät virstanpylväät, joiden avulla kulkua oli helppo seurata. Kehityskohteiksi todettiin mm. hallintakeinojen toteuttamisen delegoinnista viestiminen sekä hallintakeinojen yksityiskohtaisempi selostaminen niitä toteuttaville henkilöille, projektin kulun vähäinen raportointi ohjausryhmälle sekä resursointi IT-osaston puolesta. Yhdeksi haasteeksi todettiin henkilöstön vaihtuminen projektin aikana, sillä kohdeyritys rekrytoi useita työntekijöitä talon sisälle projektin aikana, mikä tarkoitti samalla ohjelmistokonsulttien sopimusten päättymistä. Tämä aiheutti tiettyjä käytännön ongelmia, kuten sen ettei riskien arviointia kannattanut tehdä siinä vaiheessa, kun puolet verkkopalvelun parissa työskentelevistä työntekijöistä oli työskennellyt yrityksessä alle kaksi kuukautta ja käsitys verkkopalvelun teknisestä kokonaisuudesta oli vielä rajallinen.

Projektin aikana kohdatut haasteet olivat odotetunlaisia. Kiireet ja paine muiden työtehtävien parissa aiheuttivat välillä pieniä viivästyksiä, muttei kuitenkaan merkittäviä. Sisäisen resursoinnin riittävyys ja konflikti ohjelmistokehittäjien työajan priorisoinnin kanssa todettiin yhdeksi suurimmista riskeistä projektin suunnitteluvaiheessa. Koska verkkopalvelua tuottava organisaatio on pieni ja tietyt työtehtävät ovat henkilöityneet, tietoturvan ja

sen hallintajärjestelmän parissa voi työskennellä ainoastaan tietyt henkilöt, mikä aiheutti haasteita edellä mainitun työajan priorisoinnin kanssa. Myös kokemattomuus ISO/IEC 27001 -standardista aiheutti pientä epävarmuutta ja toteutukseen liittyviä asioita täytyi varmistaa saatavilla olleista lähteistä useaan otteeseen. Toisaalta tämän myötä organisaatioon tuli rutkasti osaamista ja tietoa hallintajärjestelmästä, joten opiskeluun käytetty aika ei mennyt hukkaan.

Projektille oli johdon tuki koko sen ajan ja johdolle raportoitiin projektin etenemisestä säännöllisesti. Lisäksi projektilla oli taloudellinen tuki koko sen ajan, se oli otettu huomioon jo edeltävänä vuonna seuraavan vuoden budjettia laatiessa ja sen toteuttamiseen oli varattu rahaa sekä otettu huomioon projektien sekä töiden suunnittelussa. Lisäksi kohdeyritys panosti henkilöstön kouluttamiseen lähettämällä projektipäällikön ja pääsääntöisen toteuttajan ISO/IEC 27001 Lead Implementer -kurssille, jonka myötä organisaation sisälle saatiin osaamista ja tietämystä ISO/IEC 27000 -standardiperheestä sekä projektin toteutuksesta. Projekti vaati myös huomattavan määrän työtunteja useilta eri henkilöiltä, joten työntekijäkustannukset nousivat merkittäväksi. Lisäksi sertifiointiauditointi ja siihen liittyvät kulut ovat huomionarvoisia.

5.4 Normaali toiminta

On oleellista muistaa, että työ tietoturvan hallintajärjestelmän parissa ei lopu toteutusprojektin jälkeen, vaan sen jälkeen prosessit ovat osa organisaation normaalia viikoittaista ja päivittäistä toimintaa. Hallintajärjestelmä ei ole koskaan valmis eikä saavuta koskaan lopullista tilaansa, sillä yksi sen tarkoituksista on luoda jatkuvan parantamisen kulttuuri organisaatioon.

Myös organisaation uhkaympäristö muuttuu jatkuvasti, vaikkei välttämättä kovinkaan merkittävästi, ja näin ollen esimerkiksi riskienarviointikriteerit vaativat päivittämistä. Oleellisia vuoden aikana tehtäviä toimenpiteitä ovat riskien arvioinnit, sisäiset auditoinnit, harjoitukset, johdon katselmukset sekä määräaikaisauditointi. Määräaikaisauditointi tulee tehdä kerran vuodessa, jotta organisaatio säilyttää sertifikaattinsa. Lisäksi työ hallintakeinojen parissa jatkuu jos ei päivittäin, niin vähintään viikoittain. Jo aiemmin käyttöönotettujen hallintakeinojen ja prosessien ylläpito sekä jatkuva parantaminen vaativat aikaa ja työpanosta. Lisäksi uusia hallintakeinoja tulee ottaa käyttöön mikäli riskienhallintaprosessi havaitsee niille tarpeen. Jatkuva parantaminen on yksi ISO/IEC 27001 -standardin vaatimuksista ja sen tulee näkyä päivittäisessä toiminnassa, esimerkiksi edellä mainitulla tavalla. Projektin aikana kehitettiin tietoturvan hallintajärjestelmän vuosikello, joka sisältää edellä mainitut toimenpiteet ja se on esitelty kuvassa 5.6.

On tärkeää, että johdon tuki sekä taloudellinen tuki hallintajärjestelmälle säilyy myös toteutusprojektin jälkeen, etenkin jos organisaatio aikoo saada ISO 27001 -sertifikaatin myös jatkossa. Työ hallintajärjestelmän parissa ei lopu toteutusprojektin päättymiseen,

Kuva 5.6. *Kohdeyrityksen tietoturvan hallintajärjestelmän vuosikello*

vaan se vaatii organisaatiosta riippuen päivittäistä tai viikoittaista työtä. Sitä varten tulee varata resursseja ja hallintajärjestelmään liittyvät työt tulee ottaa huomioon töiden suunnittelussa ja eri henkilöiden vastuissa.

6. ONNISTUMISTEKIJÄT TIETOTURVAN HALLINTAJÄRJESTELMÄN KÄYTTÖÖNOTOSSA

Tässä luvussa esitellään malli, joka sisältää kirjallisuuskatsauksen ja tapaustutkimuksen perusteella tunnistettuja onnistumistekijöitä. Myös konstruktiivisen tutkimusotteen kuudes vaihe, eli konstruktion sovellettavuuden arviointi suoritetaan tässä luvussa. Lisäksi tässä luvussa vertaillaan toteutusprojektin aikana tunnistettuja onnistumistekijöitä aiemmissa tutkimuksissa tunnistettuihin onnistumistekijöihin. Konstruktiivisen tutkimusotteen kolmas vaihe, eli tutkimusaiheen syvällisen käytännön tuntemuksen hankkiminen sijoittuu tähän lukuun. Myös konstruktiivisen tutkimusotteen kuudes ja seitsemäs vaihe, eli ratkaisun soveltamisalan pohtiminen sekä teoreettisen kontribuution tunnistaminen ja analysointi sijoittuvat tähän lukuun.

6.1 Onnistumistekijöiden huomioimisella kohti onnistunutta toteutusprojektia

Jotta organisaatio onnistuu tietoturvan hallintajärjestelmän toteuttamisessa, sen tulee kiinnittää huomiota onnistumistekijöihin, jotka ovat sovellettavissa kaikkiin organisaatioihin. Myös hallintakeinojen käyttöönoton onnistumisella on luonnollisesti suuri merkitys toteutusprojektin onnistumiseen, mutta tämä malli ei käsittele niihin liittyviä yksityiskohtaisia ohjeistuksia tai suosituksia niiden tekoon, sillä hallintakeinot ja niiden toteutustavat ovat aina organisaatiokohtaisia. Esimerkiksi ISO/IEC 27002 -standardi tarjoaa ohjeistusta hallintakeinojen käyttöönottoon.

Onnistumistekijöistä toiset ovat merkitykseltään suurempia kuin toiset. Onnistumistekijöiden tärkeysjärjestystä ei voi kuitenkaan yleistää kattamaan kaikkia organisaatioita, sillä niiden merkitys voi vaihdella organisaation koosta ja luonteesta riippuen. Onnistumistekijät on esitelty vaiheittain taulukossa 6.1.

Suunnitteluvaiheessa tärkein onnistumisen edellytys on johdon tuki, sisältäen sekä ylimmän johdon että keskijohdon. On oleellista, että johto ymmärtää projektin tuomat hyödyt sekä sen haasteet. Johdon täytyy olla sitoutunut projektiin ja varata resursseja projektia varten. Johdon näkyvällä ja aktiivisella roolilla esimerkiksi viestinnässä voi olla merkitystä toteutusprojektin onnistumisen kannalta, sillä se voi motivoida ja korostaa tietoturvan

tärkeyttä organisaation työntekijöille. Johdon tuki liittyy läheisesti taloudelliseen tukeen, eli projektille varattavaan rahoitukseen. Projektia varten täytyy budjetoida rahaa ja sen toteuttamiseen tulee varata työtunteja sekä se tulee ottaa huomioon muita projekteja ja töitä suunnitellessa. Tietoturvan näkeminen investointina liittyy myös läheisesti johdon tukeen. Tällä on potentiaalisesti merkittävä vaikutus työntekijöiden motivaatioon ja se liittyy myös tietoturvamyönteisen organisaatiokulttuurin rakentamiseen. Tietoturvan hallintajärjestelmän ja sen toteutusprojektin täytyy olla myös linjassa liiketoiminnan tavoitteiden kanssa. Tämän avulla on mahdollista vähentää potentiaalista muutosvastarintaa.

Johdon tuen täytyy säilyä myös toteutusprojektin aikana ja se onkin eräs tärkeimmistä onnistumistekijöistä toteutusprojektin aikana. Sen avulla voidaan varmistaa, ettei projektille varattuja resursseja suunnata muihin projekteihin. Tästä syystä projektin etenemisestä on hyvä raportoida johdolle säännöllisesti, jotta johdon mielenkiinto projektia kohtaan pysyy yllä. Toinen erittäin tärkeä tekijä on sidosryhmien osallistaminen projektiin. Sen avulla on mahdollista pienentää potentiaalista muutosvastarintaa ja saada asioiden parissa työskentelevät tuntemaan asiat omakseen ja ottamaan niistä vastuuta. Kolmas tärkeä onnistumistekijä on hyvät projektinhallintakäytännöt. Niiden avulla toteutusprojektin onnistumisen edellytykset kasvavat. Projektisuunnitelman on oltava realistinen ja projekti tulee pilkkoa osiin, jonka myötä eri työtehtävien aikatauluttaminen sekä työtehtävien jakaminen helpottuu. Tietoturvan nykytilan tiedostaminen edesauttaa tietoturvan hallintajärjestelmän toteutusprojektia, sillä hallintakeinojen toteuttamisjärjestyksen priorisointi helpottuu, mikäli organisaatiossa ymmärretään olemassa olevien käytäntöjen ja prosessien laatu sekä vaikutukset. Toteutusprojektiin osallistuvan henkilöstön on oltava ammattitaitoista sekä asiantuntevaa ja henkilöstön kouluttamista on syytä harkita, mikäli organisaatiosta ei löydy kokemusta tietoturvan hallintajärjestelmän toteuttamisesta. Apuna on mahdollista myös käyttää ulkopuolista konsulttia tai konsultteja. Tällöin on kuitenkin vaarana, ettei organisaatiolle itselleen kerry syvällistä osaamista tietoturvan hallintajärjestelmästä.

Konstruktiivisen tutkimusotteen kuudennessa vaiheessa arvioidaan konstruktion soveltuvuutta muissa organisaatioissa [15]. Malli ei ole yleistettävissä kaikille organisaatioille, sillä esimerkiksi julkisen sektorin organisaatioissa tietoturvaa ei välttämättä voida nähdä investointina, sillä organisaatio ei tee liiketoimintaa vaan tuottaa julkista palvelua, jonka vaatimukset tulevat lainsäädännöstä. Mallista voisi olla hyötyä organisaatioille, jotka ovat kehittäneet tietoturvaa vuosien ajan keskittymällä suurimpiin riskeihin, mutta vailla ISO/IEC 27001 -standardin tai jonkin muun viitekehyksen mukaista hallintajärjestelmää.

6.2 Teoreettisen kontribuution tunnistaminen ja analysointi

Konstruktiivisen tutkimusotteen seitsemännessä vaiheessa analysoidaan konstruktion teoreettista kontribuutiota ja havaintoja aiempaan teoriaan [15]. Työssä rakennettu konstruktio pohjautuu pitkälti aiempaan teoriaan, eli kirjallisuuskatsauksessa havaittuihin onnistu-

mistekijöihin. Työn tekijän tiedossa ei kuitenkaan ole vastaavankaltaista mallia, joka kokoaisi yhteen onnistumistekijät ja niiden osatekijät, sekä esittelisi nämä vaiheittain.

Työssä tehdyn toteutusprojektin aikana tunnistettiin uusia osatekijöitä. Niitä ovat henkilöstön lisäkoulutus, avoin viestintä sekä henkilöstön pieni vaihtuvuus. Avoimella viestinnällä on mahdollista edistää projektin parissa työskentelevän henkilöstön työrauhaa sekä hallita tietoturvaan liittyviä odotuksia. Henkilöstön lisäkoulutuksen avulla organisaatio saa osaamista organisaation sisälle ja siitä on oletettavasti hyötyä myös projektin jälkeen.

6.3 Toteutusprojektin onnistumistekijöiden analysointi

Pohdittaessa toteutusprojektia ja kirjallisuuskatsauksessa esiin tulleita onnistumistekijöitä, voidaan toteutusprojektista havaituista onnistumistekijöistä löytää useita yhtymäkohtia kirjallisuuskatsauksen löydöksiin. Jo ennen toteutusprojektia tietoturvan tärkeys organisaatiolle ja liiketoiminnalle oli ymmärretty, vaikka selkeää, strukturoitua tietoturvan hallintajärjestelmää ei ollutkaan olemassa [1]. Tietoturvaan oli joka tapauksessa panostettu ja se oli lähtöisin IT-osaston tunnistamista riskeistä ja tarpeista. Organisaatiokulttuuria on rakennettu joko tietoisesti tai tahattomasti tietoturvaa huomioivaan suuntaan esimerkiksi tiedottamalla ajankohtaisista tietoturva-asioista ja huomioimalla tietoturva uusien työntekijöiden perehdytyksissä, mitkä olivat myös aiempien tutkimusten löydöksiä [19][37]. Myös johdolla ja erityisesti toimitusjohtajalla on ollut näkyvä rooli tietoturvasta viestimisessä ja tietoturva-asioiden ajamisessa eteenpäin. Myös verkkopalvelua suunnitellessa tietoturva oli huomioitu, vaikka järjestelmällinen tietoturvan hallinta ja sen kehittäminen puuttuivatkin.

Toteutusprojektille oli vahva sekä ylimmän että keskijohdon tuki sen aikana ja jo sitä ennen, mikä vastaa usean aiemman tutkimuksen löydöksiä [2][7][25][32][34][37]. Tämän johdosta projektia varten oli budjetoitu rahaa ja projektiin liittyviin kuluihin ei tarvinnut hakea erikseen rahoitusta toteutusvaiheen aikana [2][7][9]. Hallintajärjestelmällä on selkeä strateginen yhdenmukaisuus liiketoiminnan kanssa, minkä takia myös johto tuki projektia [2]. Toteutusvaiheessa eri sidosryhmiä osallistettiin esimerkiksi antamalla vaikutusmahdollisuuksia sekä jakamalla toteutusvastuita [2]. Yrityksen henkilöstön tietoturvatietoisuuden taso oli subjektiivisesti arvioituna kohtuullinen jo ennen hallintajärjestelmän toteutusprojektia ja henkilöstö osaavaa. Yritys myös panosti henkilöstön osaamiseen lähettämällä projektin pääsääntöisen toteuttajan ISO/IEC 27001 Lead Implementer -kurssille.

Yrityksen henkilöstö on myös kiinnostunut tietoturva-asioista, ainakin kriittisimpien henkilöiden osalta [34]. Toteutusprojektia helpotti myös se, että yrityksellä on ainoastaan yksi toimipiste, joten henkilöstö työskentelee pääosin samoissa tiloissa sekä työntekijät tuntevat toisensa, jolloin kynnys kysymyksille ja keskusteluille voi olla matalampi [19]. Lisäksi hallintajärjestelmä koskee vain pientä osaa yrityksestä, mikä luultavasti vaikutti toteutusprojektin onnistumiseen.

Taulukko 6.1. *Onnistumistekijät vaiheittain*

Vaihe	Onnistumistekijä	Osatekijä
Suunnitteluvaihe	Valmistelutyö	Aiempi tunnistustyö muita standardeja varten
		Hallintajärjestelmän soveltamisalan oikea rajaaminen
		Toteutusprojektin huolellinen riskienarviointi
	Tiedon ja osaamisen ennakoiva kartuttaminen	Selvitystyö; sopivimman standardin/viitekehyksen valinta
		Henkilöstön lisäkoulutus
	Johdon rooli	Johdon aktiivinen ja näkyvä osallistuminen
		Johdon tuki
		Taloudellinen tuki
		Tietoturvamyönteisen organisaatiokulttuurin rakentaminen
		Tietoturvan näkeminen investointina
	Motiivit hallintajärjestelmän toteuttamiselle	Proaktiivisen tietoturvakulttuurin luominen
		Tietoturvan paremman tason tavoittelu
Toteutusvaihe	Johdon rooli	Johdon tuki
		Taloudellinen tuki
	Projektinhallinta	Sopivat työkalut
		Tehtävien pilkkominen pieniin osiin
		Mahdollisuus ja rohkeus muuttaa aikataulua
	Sidosryhmät & henkilöstö	Henkilöstön osallistaminen
		Vähäinen tai olematon muutosvastarinta
		Avoin viestintä
		Henkilöstön kokemus ja ammattitaito tietoturvaan liittyen
		Henkilöstön kiinnostuneisuus tietoturva-asioihin
		Henkilöstön pieni vaihtuvuus
		Työskentely samoissa tiloissa
Normaali toiminta	Johdon rooli	Johdon aktiivinen ja näkyvä osallistuminen
		Johdon tuki
		Taloudellinen tuki

7. YHTEENVETO

Tutkimuksen lopuksi käydään läpi tutkimuksen kulkua sekä arvioidaan työlle asetettujen tavoitteiden toteutumista. Yhteenvedossa käydään myös läpi kohdeyrityksen tietoturvan hallintajärjestelmään liittyviä jatkotoimenpiteitä.

Lisäksi yhteenvedossa arvioidaan työhön liittyviä rajoitteita sekä arvioidaan työhön liittyviä jatkotutkimuskohteita. Myös tulosten soveltuvuutta muualla arvioidaan.

7.1 Mitä työssä tehtiin

Työssä käytiin läpi tietoturvan ja tietoturvan hallintajärjestelmän teoriaa ja työssä tehty tutkimus koostui kirjallisuuskatsauksesta sekä empiirisestä tutkimuksesta. Työ oli luonteeltaan laadullinen tutkimus ja tutkimusote oli konstruktiivinen.

Työn ensimmäisessä tutkimuskysymyksessä selvitettiin, *”mitkä onnistumistekijät vaikuttavat tietoturvan hallintajärjestelmän toteutusprojektien onnistumiseen?”*. Kysymykseen haettiin vastausta kirjallisuuskatsauksen avulla. Kirjallisuuskatsaus tehtiin integroivana kirjallisuuskatsauksena. Se keskittyi ainoastaan onnistumistekijöihin, joten esimerkiksi projektinhallintakäytännöt sekä organisaatiokulttuurin vaikutus toteutusprojektiin oli rajattu pois. Kirjallisuuskatsauksen löydöksissä korostui johdon rooli sekä tietoturvakoulutusten merkitys. Kirjallisuuskatsauksen yhteenvedossa luotiin synteesi katsauksen löydöksistä ja näin ollen tutkimuskysymykseen saatiin kattava vastaus.

Työn toisessa tutkimuskysymyksessä tutkittiin, *”mitkä syyt johtivat tutkimuksen kohdeyrityksen tietoturvan hallintajärjestelmän toteutusprojektin onnistumiseen?”*. Työssä tehdyn tapaustutkimuksen aiheena oli toteuttaa ISO/IEC 27001 -standardin mukainen tietoturvan hallintajärjestelmä kohdeyritykselle. Toteutusprojekti onnistui ja kohdeyritys sai tavoittelemansa ISO 27001 -sertifikaatin. Tapaustutkimuksen aikana tunnistettiin onnistumiseen johtaneita syitä, joilla on myös yhtymäkohtia kirjallisuuskatsauksen löydöksiin, joten tutkimuskysymykseen saatiin vastaus.

Työn kolmannessa tutkimuskysymyksessä selvitettiin, *”mitä onnistumiseen liittyvää ymmärrystä työssä syvällisesti tarkastellusta yksittäistapauksesta olisi mahdollisesti siirrettävissä muihin konteksteihin?”* Työssä kehitettiin malli, jossa yhdistettiin kirjallisuuskatsauksessa löydetyt onnistumistekijät ja tapaustutkimuksessa tunnistetut onnistumisteki-

jät. Tärkeimmät onnistumistekijät ovat johdon rooli, valmistelutyö, projektinhallinta sekä motiivit hallintajärjestelmän toteuttamiselle. Tärkeimmät yksittäiset osatekijät ovat johdon tuki, henkilöstön lisäkoulutus sekä henkilöstön osallistaminen. Tietoturvan hallintajärjestelmän toteutusta harkitsevat tai toteutusprojektiin ryhtyvät organisaatiot voivat hyödyntää mallia.

Lisäksi työn tavoitteena oli lisätä ymmärrystä tietoturvan hallintajärjestelmästä kohdeyrityksessä ja esitellä hallintajärjestelmän oppeja ja käytäntöjä myös muualle organisaatioon. Työssä kehitettiin riskienhallintaprosessi, jota tietoturvan hallintajärjestelmän piiriin käyttävä organisaation osa käyttää. Lisäksi se on tarkoitus jalkauttaa myös yrityksen IT-osaston käyttöön. Työssä tehdyn toteutusprojektin aikana kehitettiin poikkeamanhallintaprosessi sekä prosessi haavoittuvuuksien seuraamiseen ja hallintaan. Myös IT-osasto voi hyödyntää suoraan näitä prosesseja tai ottaa oppeja kehitetyistä prosesseista.

7.2 Jatkotoimenpiteet

Työn tekemisen jälkeen kohdeyrityksen tietoturvan hallintajärjestelmän kehittäminen jatkuu osana organisaation normaalia toimintaa. Hallintajärjestelmän toteutusprojekti saavutti sille asetetut tavoitteet, kohdeyritys sai ISO 27001 -sertifikaatin ja näin ollen hallintajärjestelmän integroiminen osaksi organisaation normaaleja rutiineja jatkuu.

Merkittävin yksittäinen jatkotoimenpide on riskienhallintaprosessin jalkauttaminen ja kehittäminen. Riskienhallintaprosessiin kuuluvia riskienarviointi-työpajoja tullaan järjestämään vähintään kerran kvartaalissa. Sen kehittäminen sekä riskienarviointikäytäntöjen kouluttaminen muulle henkilöstölle ovat suuressa roolissa tietoturvan hallintajärjestelmän toimivuuden kannalta.

7.3 Rajoitteet ja soveltuvuus muualla

Tutkijan subjektiivisuus on tässä tutkimuksessa tunnistettu, sillä hän on työskennellyt kohdeyrityksessä yli viiden vuoden ajan. Näin ollen tutkijan näkemyksillä ja mielipiteillä voi olla vaikutuksia työn kulkuun ja tuloksiin. Sen vaikutusta on pyritty minimoimaan selostamalla mahdollisimman tarkasti tutkimuksen ja työn kulku, jotta lukijalla olisi mahdollisuus arvioida päätelmien pätevyyttä.

Työ on myös vahvasti kontekstisidonnainen, sillä konstruktio perustuu vain kohdeyrityksen toteutusprojektista saatuihin havaintoihin ja kokemuksiin. Tällä voi olla vaikutusta työn laatuun. Työssä kehitettyä konstruktiota ei ole myöskään testattu toisessa organisaatiossa. Toisaalta vertailu aiempaan kirjallisuuteen osoittaa, että tässä tapauksessa esiin tulleita tekijöitä on monelta osin tunnistettu myös muissa organisaatioissa.

Tutkimus ei tavoittelekaan yleistettävyyttä, koska jokainen organisaatio on monimutkai-

nen kokonaisuus, johon vaikuttaa esimerkiksi henkilösuhteet, kulttuuri, maantieteellinen sijainti sekä koulutustaso. Alaluvussa 6.1 muodostetusta taulukosta voi mahdollisesti olla hyötyä yrityksille, jotka ovat jo panostaneet tietoturvan kehittämiseen vuosien mittaan, mutta joilta puuttuu tietoturvan hallintajärjestelmä ja jotka ovat lähdössä toteuttamaan hallintajärjestelmää.

7.4 Jatkotutkimuskohteet

Työn tekemisen aikana on havaittu useita tietoturvan hallintajärjestelmän toteuttamiseen liittyviä potentiaalisia jatkotutkimuskohteita. Työssä kehitetyn mallin soveltuvuutta olisi luontevaa tutkia yhdessä tai useassa eri organisaatiossa tietoturvan hallintajärjestelmän toteuttamisen yhteydessä esimerkiksi haastattelu-, kysely- tai tapaustutkimuksen avulla. Onnistumistekijöiden soveltuvuus yrityksissä ja julkisissa organisaatioissa olisi niin ikään potentiaalinen tutkimuskohde, sillä mitä luultavimmin eri onnistumistekijät korostuvat eri tyyppisissä organisaatioissa ja jotkut onnistumistekijät voivat olla jopa täysin merkityksettömiä. Myös onnistumistekijöiden merkitys eri toimialoilla saattaa paljastaa eroja niiden välillä tai toisaalta korostaa niiden yleistettävyyttä. Eräs mielenkiintoinen tutkimuskohde olisi onnistumistekijöiden tarkempi analysointi tietoturvan hallintajärjestelmän toteutusprojekteissa, toisin sanoen sen selvittäminen, ovatko jotkin onnistumistekijät kriittisiä.

Onnistumistekijöiden vastapainoksi hallintajärjestelmien toteutusprojekteissa ilmenevien esteiden tai haasteiden tutkiminen voisi tuottaa hyödyllistä tietoa niin yrityksille kuin organisaatioille, etenkin jos ne paljastuisivat yleistettäviksi. Organisaatioille olisi suurta hyötyä, mikäli tutkimus onnistuisi löytämään yleisiä esteitä tai haasteita, joiden poistamiseen organisaatiot voisivat keskittyä ja täten edesauttaa omien toteutusprojektien sujumista.

Myös organisaatiokulttuurin syvällinen tutkiminen ja sen vaikutus tietoturvan hallintajärjestelmään ja toteutusprojekteihin on mielenkiintoinen tutkimuskohde. Eräs tutkimuskohde on myös tutkimuksessa löydettyjen onnistumistekijöiden soveltaminen muihin IT-projekteihin.

LÄHTEET

[1] Gonçalo Almeida Teixeira, Miguel Mira da Silva ja Ruben Pereira. ”The critical success factors of GDPR implementation: a systematic literature review”. *Digital Policy, Regulation and Governance* 21.4 (2019), s. 402–418. URL: https://doi.org/10.1108/DPRG-01-2019-0007 (viitattu 14. 12. 2022).

[2] Zyad Alreemy et al. ”Critical success factors (CSFs) for information technology governance (ITG)”. *International Journal of Information Management* 36.6 (2016), s. 907–916. URL: https://www.sciencedirect.com/science/article/pii/S0268401216303231 (viitattu 14. 12. 2022).

[3] Jason Andress. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice*. 2nd ed. Elsevier Science & Technology Books, 2014. 240 s.

[4] Pasian Beverly ja Turner Rodney. *Design Methods and Practices for Research of Project Management*. Taylor & Francis Group, 2015. URL: https://doi.org/10.4324/9781315270197 (viitattu 29. 12. 2022).

[5] Christine V. Bullen ja John F. Rockart. ”A primer on critical success factors”. *IDEAS Working Paper Series from RePEc* (1981). URL: https://andor.tuni.fi/permalink/358FIN_TAMPO/176jdvt/cdi_proquest_journals_1698779276 (viitattu 27. 12. 2022).

[6] Richard A. Caralli et al. *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process:* 2007. URL: http://www.dtic.mil/docs/citations/ADA470450 (viitattu 06. 12. 2022).

[7] Giovanna Culot et al. ”The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda”. *The TQM Journal* 33.7 (2021), s. 76–105. URL: https://doi.org/10.1108/TQM-09-2020-0202 (viitattu 18. 12. 2022).

[8] *Euroopan parlamentin ja neuvoston asetus (EU) 2016/679*. 4. toukokuuta 2016. URL: http://data.europa.eu/eli/reg/2016/679/2016-05-04/fin (viitattu 23. 11. 2022).

[9] Alan Gillies. ”Improving the quality of information security management systems with ISO27000”. *The TQM Journal* 23.4 (2011), s. 367–376. URL: https://doi.org/10.1108/17542731111139455 (viitattu 14. 12. 2022).

[10] Qing Hu et al. ”Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture*”. *Decision Sciences* 43.4 (2012), s. 615–660. URL: http://onlinelibrary.wiley.com/doi/abs/10.1111/j.1540-5915.2012.00361.x (viitattu 18. 12. 2022).

[11] Edward Humphreys. *Implementing the ISO/IEC 27001:2013 ISMS Standard*. Artech House, 2016. 239 s.

[12] *ISO/IEC 27001: What's new in IT security?* ISO. URL: https://www.iso.org/cms/render/live/en/sites/isoorg/contents/news/2022/10/new-iso-iec-27001.color-C12.html (viitattu 23. 11. 2022).

[13] Timo Kallinen ja Taina Kinnunen. *Laadullisen tutkimuksen verkkokäsikirja*. Tietoarkisto. URL: https://www.fsd.tuni.fi/fi/palvelut/menetelmaopetus/kvali/ (viitattu 29. 12. 2022).

[14] R. S Kaplan ja D. P. Norton. *The balanced scorecard : translating strategy into action*. Harvard Business School Press, 1996.

[15] *Kari Lukka: Konstruktiivinen tutkimusote*. METODIX. 19. toukokuuta 2014. URL: https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/ (viitattu 29. 12. 2022).

[16] *Kyberturvallisuuden sanasto – Turvallisuuskomitea*. URL: https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/ (viitattu 20. 11. 2022).

[17] National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*. 2018. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (viitattu 30. 11. 2022).

[18] *NIST Glossary*. URL: https://csrc.nist.gov/glossary (viitattu 20. 11. 2022).

[19] Mohd Fairuz Iskandar Othman ja Taizan Chan. "Barriers to Formal IT Governance Practice – Insights from a Qualitative Study". Teoksessa: *2013 46th Hawaii International Conference on System Sciences*. 2013, s. 4415–4424.

[20] *Paljastaako pilkutus jotakin Vastaamon kiristäjästä? Miksi hän ei osaa teititellä suomeksi? Tämä tiedetään valtavasta kiristysvyyhdistä*. Yle Uutiset. 26. lokakuuta 2020. URL: https://yle.fi/a/3-11613667 (viitattu 20. 11. 2022).

[21] Anu Puusa, Pauli Juuti ja Iiris Aaltio. *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Publication Title: Laadullisen tutkimuksen näkökulmat ja menetelmät. Helsinki: Gaudeamus, 2020.

[22] Bel G. Raggad. *Information Security Management: Concepts and Practice*. 1. painos. Bosa Roca: Taylor & Francis Group, 2010.

[23] Timo Salmi ja Marko Järvenpää. "Laskentatoimen case-tutkimus ja nomoteettinen tutkimusajattelu sulassa sovussa". *Liiketaloudellinen aikakauskirja* 2 (2000), s. 263–275.

[24] Ari Salminen. *Mikä kirjallisuuskatsaus? : johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasan yliopisto, 2011. URL: https://osuva.uwasa.fi/handle/10024/7961 (viitattu 13. 12. 2022).

[25] Stef Schinagl ja Abbas Shahim. "What do we know about information security governance? "From the basement to the boardroom": towards digital security governance". *Information & Computer Security* 28.2 (2020), s. 261–292. URL: https://doi.org/10.1108/ICS-02-2019-0033 (viitattu 18. 12. 2022).

[26] *SFS-EN ISO/IEC 27000:2020, Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto*. Suomen Standardisoimisliitto SFS ry, 2018.

[27] *SFS-EN ISO/IEC 27001:2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset*. Suomen Standardisoimisliitto SFS ry, 2022.

[28] *SFS-EN ISO/IEC 27002:2022, Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintakeinot*. Suomen Standardisoimisliitto SFS ry, 2022.

[29] *SFS-EN ISO/IEC 27005:2018, Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta*. Suomen Standardisoimisliitto SFS ry, 2018.

[30] *SFS-EN ISO/IEC 27701:2021, Turvallisuustekniikat. Standardien ISO/IEC 27001 ja ISO/IEC 27002 tietosuojalaajennus. Vaatimukset ja ohjeet*. 2021.

[31] *SFS-ISO 31000:2018 — Riskienhallinta. Ohjeet*. 2018.

[32] Basie von Solms ja Rossouw von Solms. ”The 10 deadly sins of information security management”. *Computers & Security* 23.5 (2004), s. 371–376. URL: https://www.sciencedirect.com/science/article/pii/S0167404804001221 (viitattu 21. 12. 2022).

[33] Victor E. Sower. *Essentials of Quality with Cases and Experiential Exercises*. Wiley, 2010. URL: http://ebookcentral.proquest.com/lib/tampere/detail.action?docID=5182164 (viitattu 22. 11. 2022).

[34] Harrison Stewart ja Jan Jürjens. ”Information security management and the human aspect in organizations”. *Information & Computer Security* 25.5 (2017), s. 494–534. ISSN: 2056-4961. URL: https://doi.org/10.1108/ICS-07-2016-0054 (viitattu 18. 12. 2022).

[35] *TEPA-termipankki (erikoisalojen sanasto- ja sanakirjakokoelma)*. URL: https://termipankki.fi/tepa/fi/ (viitattu 20. 11. 2022).

[36] Richard J. Torraco. ”Writing Integrative Literature Reviews: Guidelines and Examples”. *Human Resource Development Review* 4.3 (2005), s. 356–367. URL: https://www.proquest.com/docview/221810269/abstract/71E019388DC946AEPQ/1 (viitattu 13. 12. 2022).

[37] Zhiling Tu ja Yufei Yuan. ”Critical Success Factors Analysis on Effective Information Security Management: A Literature Review”. *Information Systems Security* (2014), s. 13.

[38] Jouni Tuomi. *Laadullinen tutkimus ja sisällönanalyysi*. Yhteistyössä Anneli Sarajärvi. Uudistettu laitos. Helsinki: Tammi, 2018.

[39] *Uutistoimisto STT:n tietojärjestelmiin kohdistui perjantaina laaja hyökkäys, osa järjestelmistä on ajettu varotoimena alas*. Yle Uutiset. 29. heinäkuuta 2022. URL: https://yle.fi/a/3-12556769 (viitattu 20. 11. 2022).