Tatu Suhonen

ISO/IEC 27001 -SERTIFIOINNIN HANKINTAPERUSTEET JA SERTIFIOINTIELIMEN VALINTAPERUSTEET

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2019

TIIVISTELMÄ

Suhonen, Tatu
ISO/IEC 27001 -sertifioinnin hankintaperusteet ja sertifiointielimen valintaperusteet
Jyväskylä: Jyväskylän yliopisto, 2019, 85s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja(t): Siponen, Mikko

ISO/IEC 27001 -sertifikaatti on vapaaehtoinen tietoturvan johtamisjärjestelmäsertifikaatti, joka voidaan myöntää standardin vaatimukset täyttävälle organisaatiolle. Sertifikaatilla organisaatio voi osoittaa, että sen toimintatavat tietoturvan osalta ovat johdettuja, suunniteltuja ja jatkuvia. ISO/IEC 27001 -standardi on yksi tunnetuimmista tietoturvaan liittyvistä standardeista, mutta siihen liittyvä tutkimus on ollut melko vähäistä, etenkin sertifioinnin osalta. Sen vuoksi tässä tutkimuksessa selvitettiin syitä sille, miksi erilaiset organisaatiot päättävät hankkia ISO/IEC 27001 -sertifikaatin ja ylläpitää sitä. Lisäksi pyrittiin selvittämään tekijöitä, jotka vaikuttavat sertifioinnin suorittavan sertifiointielimen valintaan, sillä aihe on vielä käytännössä tutkimaton. Tutkimus toteutettiin laadullisena monitapaustutkimuksena, jonka avulla pyrittiin löytämään tekijöitä, jotka vaikuttavat tutkimuskysymyksissä viitattuihin ilmiöihin. Sertifioinnin hankintaperusteissa ongelmaa oli käytännöllistä lähestyä etsimällä sertifioinnista saatavia hyötyjä ja haasteita, kun taas sertifiointielimen valintaperusteissa keskityttiin etsimään tekijöitä ja kevyesti vertailemaan niitä. Tiedon kerääminen toteutettiin haastattelemalla jo sertifioituja organisaatioita käyttäen semistrukturoitua haastattelumenetelmää. Analysointi toteutettiin vertailemalla tuloksia aiempiin julkaisuihin aiheista.

Tulosten mukaan sertifioinnin hankintaan ja ylläpitoon vaikuttavat pääasiallisesti tietoturva- ja taloushyödyt, ja näitä täydentävät erilaiset muut hyödyt, kuten lainsäädäntöön liittyvät hyödyt. Hyödyt ovat monissa tapauksissa läheisesti yhteneväisiä monien muiden hyötyjen kanssa. Tietoturvanäkökulmasta suurin hyöty on tietoturvan tason kokonaisvaltainen parantuminen, kun taas taloudellisesti sertifikaatti edistää organisaation luottamusta, helpottaa myyntiä ja mahdollistaa säästöjä. Lisäksi sertifioiutumalla organisaatio voi täyttää lainsäädännöllisiä vaatimuksia, kuten EU:n tietosuoja-asetuksen vaatimuksia.

Sertifiointielimen valintaan liittyviä tekijöitä löytyi useita. Hinnan ja kilpailutuksen merkitys ovat pienempiä kuin auditoijan ammattitaidon ja sertifiointielimen käytännöllisyystekijöiden, mutta niillä on kuitenkin vaikutusta. Lisäksi vaikuttavia tekijöitä voivat olla myös palvelutarjonnan määrä, maine sekä olemassa olevat suhteet sertifiointielimeen.

Asiasanat: ISO/IEC 27001, tietoturvan johtamisjärjestelmä, sertifiointi, sertifiointielin

ABSTRACT

Suhonen, Tatu
Factors that affect the decision to certify against ISO/IEC 27001 and the selection of certification body
Jyväskylä: University of Jyväskylä, 2019, 85 p.
Cyber Security, Master's Thesis
Supervisor(s): Siponen, Mikko

ISO/IEC 27001 -certificate is a voluntary information security management system certificate which can be granted to an organization upon complying with the standard's requirements. Certification acts as a proof that the organization's procedures in terms of information security are managed, planned and continuous. ISO/IEC 27001 is one of the most recognized information security standards, but little research on the subject has been done, especially in the field of certification. Therefore, this study aimed to find factors that affect organizations' decision to aim for a certificate and maintain it. Furthermore, factors affecting the selection of the certification body conducting the certification audits were inspected since practically no research has been made on the subject. The research was conducted as a qualitative multiple case study where factors answering to the research questions were looked for. Factors affecting the decision to certify were identified through benefits of certification whereas factors affecting the selection of the certification body were inspected as such and by comparing them to each other. Information was collected by interviewing certified organizations by using a semi-structured interview method. Analysis was based on comparison between existing literature and results from this study.

The results show that factors affecting the decision to obtain and maintain the certificate are divided into information security and financial benefits which are supplemented with additional benefits, such as legal benefits. Benefits are often closely related and overlapping. From security perspective the main benefit is the overall increase in the level of security while financially the certificate increases trust, increases sales and provides chances for cost savings. Additionally, the certificate might help cover legislative requirements such as the EU General Data Protection Regulation.

The selection of certification body was found to have multiple affecting factors. Price and tendering are affecting the selection but may not be playing a significant role when compared to auditor's competence and practicality matters regarding the certification body. Additionally, the following factors were found in the study: service portfolio coverage, reputation and existing relationship with a certification body.

Keywords: ISO/IEC 27001, information security management system, certification, certification body

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Von Solmsin ja Van Niekerkin (2013) mukaan tietoturvan tavoitteena on varmistaa liiketoiminnan jatkuvuus ja minimoida tietoturvapoikkeamien tuottamat vahingot. Se, miten tämä käytännössä toteutetaan, voi vaihdella hyvinkin suuresti, mutta yleisesti tietoturvaa pyritään Andressin mukaan (2013) tuottamaan CIA-mallilla. Tällä tarkoitetaan informaation suojaamista varjelemalla sen luottamuksellisuutta (confidentiality), eheyttä (integrity) ja saatavuutta (availability). Muun muassa tähän lähestymistapaan perustuen on syntynyt erilaisia tietoturvan hallintaan ja toteutukseen tarkoitettuja standardeja, joilla pyritään tuottamaan yhtenäistettyjä ja hyväksi todettuja toimintatapoja tiedon turvaamiseksi. Standardit eivät takaa täydellistä tietoturvaa, mutta ne ovat Posthumusin ja Von Solmsin (2004) mukaan hyviä tapoja ottaa käyttöön maailmanlaajuisesti käytettyjä tietoturvan hallintakeinoja ja ne auttavat lisäämään luottamusta organisaation ja sen viiteryhmien kanssa. Lisäksi ne auttavat tehostamaan organisaation toimintaa ja vähentämään tietoturvasta aiheutuvia kustannuksia. (Posthumus ja Von Solms, 2004.)

Yksi tunnetuimmista tietoturvan hallinnan tietoturvastandardeista on ISO/IEC 27001. Sen pyrkimyksenä on auttaa organisaatioita luomaan tietoturvan johtamisjärjestelmä, joka toimii johdon työkaluna tietoturvan hallintaan. Käytännössä johtamisjärjestelmä koostuu erilaisista prosesseista ja määritellyistä toimintavoista, sekä tietoturvakontrolleista, joilla tietoturvauhkia pyritään hallitsemaan. Uhat ja niistä koituvat riskit ovat ISO/IEC 27001 -standardin lähtökohta, sillä standardin toiminta perustuu organisaation omaan kykyyn riskien tunnistamisessa ja hallinnassa. Lambon (2006) mukaan ISO/IEC 27001 on vakiinnuttanut asemansa tietoturvastandardien keskuudessa niin sanottuna de facto -standardina, eli se on yksi tunnetuimmista, luotetuimmista ja käytetyimmistä standardeista. Humphreysin (2011) mukaan organisaatio voi osoittaa standardin vaatimusten täyttämisen hakemalla siitä kertovaa sertifikaattia. Sertifikaatti on jonkin kolmannen osapuolen myöntämä todistus siitä, että kohdeorganisaation määritellyt osat ja toiminnot täyttävät standardin vaatimukset (Humphreys, 2011). Sertifikaatin saaminen edellyttää auditointia, eli tarkastusta, jossa kohdeorganisaation tietoturvan johtamisjärjestelmä tarkastetaan standardin

vaatimuksia vasten. Vaatimukset täyttäessään organisaatio saa sertifikaatin. Sertifikaatin hankkiminen on kuitenkin täysin vapaaehtoista, joten miksi organisaatiot päättävät hankkia sen?

Parkin, Jangin ja Parkin (2010) mukaan sertifioinnin tehokkuudesta kertovat hyödyt ovat vielä melko tuntemattomat. Ongelmallista on muun muassa se, miksi organisaatiot päättävät hankkia pelkän implementoinnin lisäksi vielä sertifikaatin, joka on maksullinen lisäinvestointi. Luonnollinen johtopäätös on se, että sertifikaatti tuottaa organisaatiolle pelkkään implementointiin verrattuna paljon suurempia hyötyjä, mutta näistä hyödyistä ei ole selkeää varmuutta. Sertifikaatin hankkiminen on kuitenkin tietoturvainvestointi, jolle täytyy löytää investointiperuste ja tapa mitata sitä, mikä sertifikaatin tuoma lisäarvo organisaatiolle on. Näin ollen sertifikaatin hankkiminen on tiukasti yhteydessä organisaation tietoturvainvestointistrategiaan.

Koska sertifikaatti on maksullinen, on sen ympärille luonnollisesti syntynyt liiketoimintaa. Sertifiointiliiketoiminta on liiketoiminta-alana mielenkiintoinen, sillä toiminnan on oltava riippumatonta ja puolueetonta. Toisin sanoen, sertifikaatteja myöntävien sertifiointielinten toimintaa säätelevät määräykset siitä, miten auditointeja, eli arviointeja, tulee tehdä. Näin ollen auditoinnin tulos tulisi olla aina sama arvioijasta riippumatta. Tällöin sertifikaatin hankkimispäätökseen vaikuttaisi vain hinta. Käytännössä tilanne ei kuitenkaan näytä toimiva näin. Auditointitoiminta on runsaasti tietotaitoa vaativa ala, jossa ammattitaito heijastuu työn laatuun. Täten on mielenkiintoista selvittää myös sitä, miten organisaatiot tekevät päätöksiään sertifiointielimen valintaan liittyen. Valitaanko sertifiointielin siten, mistä sertifikaatti saadaan halvimmalla, helpoiten vai kenties sieltä, mistä saadaan paras arvioija? Näiden kahden ongelman perusteella tutkimukseen valikoituivat seuraavat kaksi tutkimuskysymystä:

- Miksi yritykset päättävät hankkia ISO/IEC 27001 -sertifioinnin ja ylläpitävät sitä?
    - Mitä hyötyjä sertifioinnista on?
- Mitkä tekijät vaikuttavat sertifiointielimen valintaan?

Tutkimus toteutettiin laadullisen tutkimuksen menetelmin monitapaustutkimuksena haastattelemalla sopivien organisaatioiden edustajia. Empiirisessä osiossa syntyneitä tuloksia analysoitiin ensin siten, että niistä tunnistettiin vaikuttavat tekijät, minkä jälkeen tuloksia vertailtiin olemassa olevaan kirjallisuuteen yhteneväisyyksien ja poikkeamien havainnoimiseksi. Aihepiiriin liittyviä olemassa olevia julkaisuja etsittiin verkosta löytyvien materiaalien joukosta hyödyntäen tieteellisiä julkaisuja indeksoivia palveluita ja suoria materiaalihakuja. Lähdemateriaaliksi pyrittiin valitsemaan mahdollisimman tunnetuista lähteistä löytyvää materiaalia ja yksittäisten julkaisujen luotettavuutta arviointiin myös viittausmäärien mukaan.

Tutkimuksen pääpyrkimyksenä oli selvittää tutkimuskysymyksiin vastaavia tekijöitä, eikä niinkään syvällisesti vertailla niitä keskenään, sillä tutkimusongelma on sen verran niukasti tutkittu, että tutkimuksessa oli mielekkäämpää selvittää tekijät, jotka vaikuttavat sertifikaatin hankkimiseen ja ylläpitämiseen, sekä

sertifiointielimen valintaan. Tutkimuksen tulokset osoittavat, että sertifioinnin hankkimiseen ja ylläpitämiseen vaikuttavat niin tietoturva- kuin taloushyödyt. Sertifikaatin koetaan nostavan organisaation tietoturvan tasoa, mutta samalla se lisää luottamusta organisaatiota kohtaan. Kasvanut luottamus taas lisää liiketoimintamahdollisuuksia ja edistää myyntiä. Toisaalta sertifiointi myös tehostaa organisaation toimintaa, jolloin se voi saavuttaa sertifikaatin avulla säästöjä. Lisäksi sertifikaatti tuottaa yleisiä hyötyjä, sillä sen avulla organisaation on helpompi täyttää standardin vaatimuksia sivuavaa lainsäädäntöä ja muita standardeja. Sertifiointielimen valintaan liittyen taas vaikuttavat monet muutkin tekijät kuin raha, kuten sertifiointielimen ja auditoijan ammattitaito, palveluntarjonnan laajuus ja maine. Lisäksi käytännöllisyystekijät, kuten yhteinen kieli, voivat olla merkittäviä tekijöitä sertifiointielintä valittaessa.

Tämä tutkimus on jaettu johdannon lisäksi kuuteen lukuun, minkä lisäksi tutkimuksen lopusta löytyvät käytetyt lähteet sekä liitemateriaali. Tutkimuksen kirjallisuuskatsausosiossa luvuissa kaksi ja kolme tutustutaan aiheesta löytyvään olemassa olevaan lähdemateriaaliin. Luvussa kaksi käsitellään tärkeimpiä käsitteitä, ISO/IEC 27001 -standardin toimintaa, sertifioitumisprosessia ja tietoturvaan investointeja. Luvussa kolme esitellään olemassa olevan tutkimuksen näkemyksiä sertifikaatin hankkimiseen ja ylläpitämiseen liittyvistä tekijöistä sekä sertifiointielimen valintaan liittyvistä tekijöistä. Luku neljä esittelee tutkimuksessa käytetyn tutkimusmenetelmän ja sen soveltamisen tässä tutkimuksessa. Viidennessä luvussa esitellään tutkimuksen tulokset ja kuudennessa, pohdinnan sisältävässä luvussa, analysoidaan tutkimuksen tuloksia olemassa olevan tutkimuksen kanssa. Seitsemäs luku summaa tutkimuksen johtopäätökset yhteenvedon muodossa ja käsittelee tutkimuksen rajoitteita ja jatkotutkimusaiheita.

2 ISO 27001 -SERTIFIOINTI JA TIETOTURVAINVESTOINNIT

Tämä luku käsittelee tutkimuksen taustaa sekä tärkeimpiä sovellettavia käsitteitä, jotka helpottavat tutkimuksen teoreettisen taustan ymmärtämisessä. Aluksi käsitellään ISO/IEC 27001 -standardia tutkimalla sen taustaa ja keskeisiä toimintaperiaatteita. Standardin esittelyn jälkeen perehdytään ISO/IEC 27001 -sertifiointiin ja siihen liittyvään sertifiointiprosessiin. Lopuksi tutustutaan tietoturvainvestointien perusteorioihin ja niiden ominaisuuksiin. Tietoturvainvestointien ymmärtäminen on tärkeää, jotta voidaan ymmärtää markkinoilla kilpailevien organisaatioiden investointikäyttäytymistä tietoturvakontekstissa. Luvun luettuaan lukijalla tulisi olla ymmärrys tutkielman aihepiirin keskeisistä käsitteistä ja niiden välisistä suhteista.

2.1 ISO/IEC 27001

Tietojärjestelmät ja tietoliikenne ovat nykyisin tärkeä osa lähes kaikkien organisaatioiden liiketoimintaa. Distererin (2013) mukaan datan merkityksen kasvu, sekä liiketoimintaympäristön verkottuminen asettavat organisaatiot tilanteeseen, jossa ne kohtaavat riskejä, jotka koskevat dataa, tietojärjestelmiä ja verkkoja (Disterer, 2013). ISO/IEC 27000 -standardin (2018) mukaan riskit voivat olla hyvin monimuotoisia ja erilaisista alkulähteistä: Ne voivat olla esimerkiksi ihmisten toimintaan, tietomurtoihin, tiedon käsittelyvirheisiin tai luonnonkatastrofeihin liittyviä ja olla lähtöisin niin organisaation sisä- kuin ulkopuolelta. Kaikille riskeille yhteistä niiden hyvinkin erilaisista piirteistä huolimatta on kuitenkin se, että ne perustuvat haavoittuvuuksin, jotka voivat aiheuttaa organisaatiolle sekä rahallista vahinkoa, että imagohaittaa. Tietoon ja tiedonkulkuun liittyviä riskejä minimoidakseen organisaation on investoitava tietoturvaan. Riskien välttämisen lisäksi tietoturvaan investoimalla organisaatio pyrkii myös saavuttamaan sen johdon asettamat tavoitteet organisaation liiketoiminnalle, sekä noudattamaan lakien vaatimuksia ja suojelemaan organisaation julkisuuskuvaa. (ISO/IEC 27000, 2018.)

Tietoturvan toteuttamiseen ja hallintaan on useita menetelmiä, mutta nykyisin erilaiset tietoturvastandardit ovat vakiinnuttaneet paikkansa monien organisaatioiden tietoturvan hallinta- ja toteutuskeinona (Disterer, 2013). Hsun (2009) mukaan tietoturvastandardit voidaan jakaa kahteen ryhmään, teknologia- ja johtamisorientoituneisiin standardeihin. Teknologiaorientoituneet standardit keskittyvät informaatioteknologian fyysisten ja loogisten ominaisuuksien hallintaan, kun taas johtamisorientoituneet keskittyvät hyvään tietoturvan johtamiseen. Johtamiseen keskittyviä standardeja kutsutaan myös johtamisjärjestelmästandardeiksi. (Hsu, 2009.) Yksi tunnetuimmista ja eniten käytetyimmistä tietoturvan johtamisjärjestelmästandardeista on ISO/IEC 27001 (Humphreys, 2008 &

Watkins, 2013). ISO/IEC 27001 on kansainvälinen standardi, joka auttaa organisaatioita ylläpitämään ja kehittämään omaa tietoturvaympäristöään. Standardi on kahden organisaation, International Organization for Standardizationin (ISO) ja International Electrotechnical Comissionin (IEC), yhteisesti kehittämä ja ylläpitämä. Standardin kehittämisestä vastaa edellä mainittujen organisaatioiden ylläpitämä komitea nimeltä Joint Technical Committee 1 (ISO/IEC JTC1), joka saa hyväksynnän standardiin tehtyihin muutoksiin komitean maakohtaisilta standardoimiskumppaneilta. (ISO/IEC 27001, 2017.) Suomessa standardin suomenkielisestä kehittämisestä ja ylläpitämisestä vastaa Suomen Standardoimisliitto SFS (ISO, 2019b). Standardi on käytössä maailmanlaajuisesti, sillä ISO:n (2018) tuottaman vuosittaisen kyselyn mukaan vuonna 2017 standardin vaatimuksenmukaisuudesta kertovia sertifikaatteja on myönnetty tai ylläpidetty 160:ssä eri maassa ja sertifikaatteja oli maailmanlaajuisesti yhteensä 39501. Suomessa myönnettyjä sertifikaatteja oli 72. Lisäksi kasvu on ollut voimakasta viime vuosina, sillä kansainvälisesti mitattuna vuosittainen kasvu on keskimäärin ollut 10 % - 20 % kymmenen viimeisen vuoden aikana. (ISO, 2018.)

Tällä hetkellä tuorein versio ISO/IEC 27001 -standardista on vuodelta 2017. Tyypillisesti standardi uusiutuu muutamien vuosien välein, mutta muutokset eivät kuitenkaan välttämättä ole kovin merkittäviä, vaan tarkennuksia, lisähuomioita ja korjauksia jo olemassa oleviin vaatimuksiin. Distererin (2013) mukaan ensimmäinen ISO/IEC 27001 -standardin versio on julkaistu vuonna 2005, mutta sen juuret ulottuvat jo 90-luvun alkupuolelle, kun brittiläinen British Standards Institute (BSI) julkaisi vuonna 1995 kansallisen standardin nimellä ”BS 7799-1 IT—Security techniques—Code of practice for information security management”. BS 7799-1 standardin lisäosasta BS 7799-2:sta kehittyi sittemmin ISO 27001. BS7799-1 tunnetaan nykyisin nimellä ISO/IEC 27002. Nykyisin ISO 27000 -sarjan standardiperheeseen kuuluu lukuisia eri standardeja, mutta sen selkärangan muodostavat ISO 27001 ja 27002. (Disterer, 2013.)

ISO/IEC 27001:2017 -standardiin kuuluu 10 vaatimuskokonaisutta, jotka jokaisen sertifiointiin pyrkivän organisaation täytettävä, sekä liitteessä A mainituista tietoturvakontrolleista, joita organisaatio oman riskipohjaisen arvionsa mukaan implementoi minimoidakseen siihen kohdistuvia tietoturvariskejä. (ISO/IEC 27001, 2017.) Standardin vaatimukset ovat:

1. Soveltamisala
2. Velvoittavat viittaukset
3. Termit ja määritelmät
4. Organisaation toimintaympäristö
5. Johtajuus
6. Suunnittelu
7. Tukitoiminnot
8. Toiminta
9. Suorituskyvyn arviointi
10. Parantaminen

    Lisänä Liite A Hallintatavoitteiden ja -keinojen viiteluettelo (tietoturvakontrollit)

Standardin vaatimuskokonaisuuksiin kuuluu useampia vaatimuksia, jotka sisältävät tarkentavia alavaatimuksia. Liite A:n tietoturvakontrollit ovat peräisin ISO/IEC 27002 -standardista, joka kuvailee tietoturvallisuuden hallintakeinojen menettelyohjeet. Yhdessä Liite A:n ja ISO/IEC 27001 -standardin vaatimusten kanssa organisaatio pystyttää itselleen tietoturvan johtamisjärjestelmän, joka sisältää teknisiä tietoturvakontrolleja, prosesseja ja toimintaa kuvaavia tietoturvapolitiikkoja.

2.1.1 Tietoturvan johtamisjärjestelmän toiminta

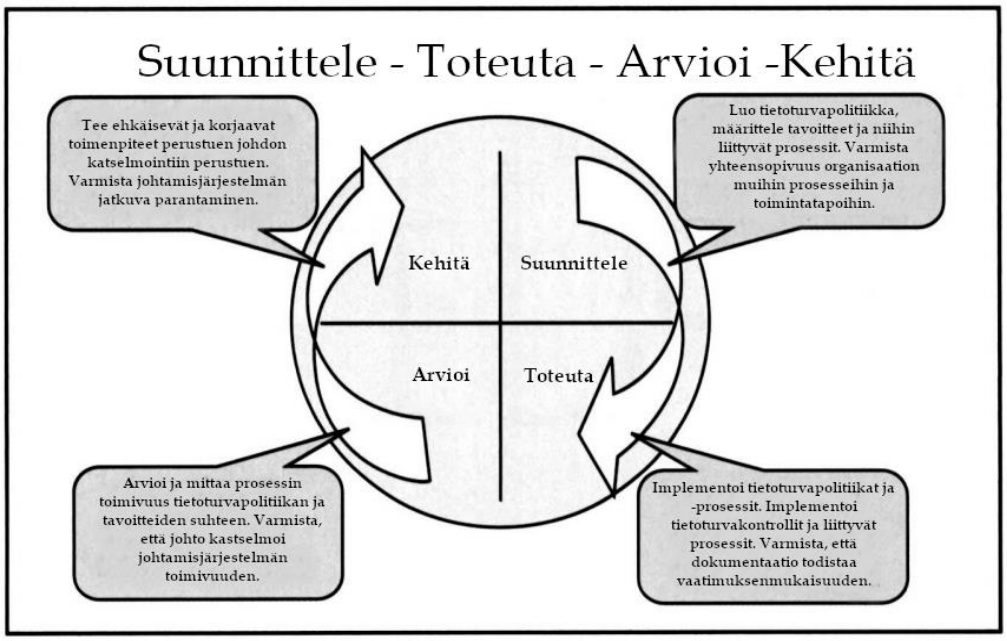
ISO/IEC 27001 on johtamisjärjestelmästandardi. Tämä tarkoittaa sitä, että standardin avulla organisaatio pystyttää osaksi organisaatiotaan tietoturvan johtamisjärjestelmän (Information Security Management System, ISMS), jonka avulla se hallitsee tietoturvaympäristöään. ISO/IEC 27000 -standardin (2018), joka määrittelee ISO/IEC 27000 -standardisarjan yleiset periaatteet ja sanaston, mukaan johtamisjärjestelmä ei sellaisenaan tarkoita mitään tiettyä tietoturvatuotetta, vaan organisaation systemaattista lähestymistapaa tietoturvan hallinnolliseen ja säännönmukaiseen suunnitteluun, toteutukseen, ylläpitoon ja kehittämiseen. Johtamisjärjestelmän tehtävänä on olla johtamisen työväline, jonka toiminnan tuloksena syntyy erilaisia prosesseja, politiikkoja ja teknisiä toteutuksia, joiden tarkoituksena on suojata organisaation suojattavia omaisuuseriä. Johtamisjärjestelmän tulisi perustua riskiarvioon, jossa arvioidaan organisaatioon ja sen omaisuuseriin kohdistuvia riskejä, sekä organisaation määrittämiin riskitasoihin, joiden perusteella riskejä hallitaan. (ISO/IEC 27000, 2018.) Riskejä hallitaan implementoimalla tietoturvakontrolleja, joita löytyy muun muassa velvoittavasta ISO/IEC ISO 27001 -standardin Liite A:sta. Liite A:n kontrollit ovat implementointiohjeita tarjoavasta ISO/IEC 27002 standardista, mikä osoittaa standardien läheisen suhteen toisiinsa.

ISO/IEC 27000 -standardin (2018) mukaan johtamisjärjestelmän onnistunut toteutus perustuu seuraaviin välttämättömiin perusperiaatteisiin:

a. Ymmärrys tietoturvan tarpeesta
b. Tietoturvavastuiden nimeäminen organisaatiossa
c. Johdon ja tärkeimpien sidosryhmien sitoutuminen tietoturvaan
d. Yhteiskunnallisten arvojen vahvistaminen
e. Riskiarvioperusteinen tietoturvakontrollien valitseminen, jotta riskitasot saadaan organisaation hyväksymälle tasolle
f. Tietoturvan yhdistäminen olennaiseksi osaksi organisaation tietoverkkoja ja -järjestelmiä
g. Riskien realisoitumisesta aiheutuva tietoturvatapahtumien aktiivinen estäminen ja havainnointi
h. Tietoturvan kokonaisvaltaisen hallinnan varmistaminen
i. Jatkuva tietoturvan tason uudelleenarviointi ja tarvittavien korjausten tekeminen.

Standardi on pyritty luomaan hyvin yleisluontoiseksi ja sovellettavaksi, jotta se sopisi hyvin kaikentyyppisiin organisaatioihin, mutta muun muassa Barletten, Fominin ja Vriesin (2008) mukaan sen soveltuvuudesta pieniin ja keskisuuriin organisaatioihin on ollut epäilyksiä. Tätä näkemystä vastaan voidaan kuitenkin Brennerin (2007) mukaan jossain määrin esittää eriäviä mielipiteitä: Standardin lähestyminen tietoturvaan on agnostinen, sillä se ei esitä mitään tiettyyn teknologiaan riippuvaisia vaatimuksia. Tämän takia ISO/IEC 27001:n vaatimukset voidaan skaalata hyvin erikokoisille ja eri toimialoilla toimiville organisaatioille. (Brenner, 2007.) Vaatimukset ovat myös määritelty siten, että ne eivät aina suoraan määrittele vaatimuksen toteutustapaa. Tämä antaa organisaatiolle liikkumavaraa vaatimusten toteuttamiseen oman organisaation koon ja toiminnan luonteen mukaan. Standardin yleisluontoiset vaatimukset ovat kuitenkin myös saaneet kritiikkiä. Siposen ja Willisonin (2009) mukaan hyvin yleisluontoisten vaatimusten ongelma on se, että ne eivät ota huomioon erilaisten organisaatioiden erityistarpeita ja -ominaisuuksia, jolloin tietoturvastandardin vaatimukset eivät välttämättä vastaa tietoturvatarpeisiin.

Standardinmukaista johtamisjärjestelmän toimintaprosessia voidaan pitää melko yksinkertaisena. Brennerin (2007) mukaan ISO/IEC 27001:n mukainen johtamisjärjestelmä noudattaa ISO/IEC 27000 -standardissa määriteltyä, ja muun muassa ISO 9000 laatujärjestelmästandardissa käytettävää, jatkuvaa ja toistuvaa nelivaiheista PDCA-prosessia: Suunnittele (Plan) – Toteuta (Do) – Arvioi (Check) – Kehitä (Act), joka on esitelty alla olevassa kuviossa (kuvio 1). Toimintamallia ei enää mainita sanallisesti standardin uusimmassa SFS:n julkaisemassa versiossa, mutta malli on silti edelleen käytössä laajasti.



KUVIO 1 PCDA-prosessi Brennerin (2007) mukaan

Prosessin suunnitteluvaiheessa tunnistetaan organisaation toiminnassa käytettävät ja siihen riippuvaiset omaisuuserät, sekä omaisuuseriin liittyvät tietoturvavaatimukset. Omaisuuseriin voi kohdistua vaatimuksia niin organisaation liiketoiminnasta, sopimuksista, lainsäädännöstä kuin itse standardista. (ISO/IEC 27000, 2018.) Kun omaisuuserät on tunnistettu, organisaatio suorittaa riskiarvion, jossa arvioidaan riskien todennäköisyyttä ja niiden vaikutuksia eri omaisuuseriin (Brenner, 2007). Riskienhallintaan on olemassa erilaisia menetelmiä, mutta tietoturvakontekstissa on yleistynyt tapa mitata omaisuuseriin kohdistuvia riskejä niiden vaikutuksilla tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen (Andress, 2014). ISO/IEC 27000 (2017) myös suosittelee käyttämään riskiarviossa mittareina riskin kustannuksia, hyötyjä, lainsäädännön ja sidosryhmien asettamia vaatimuksia, sekä muita organisaation hyvinä katsomia mittareita. Brennerin (2007) mukaan on myös tyypillistä mitata riskejä niiden todennäköisyyden ja vaikutuksen kautta. Jotta niin riskienhallinta, kuin muutkin tietoturvan johtamisjärjestelmän prosessit alkavat toimia halutusti, täytyy organisaation johdon määrittää tarvittavat roolit ja niihin liittyvät vastuut, sekä huolehtia tarvittavista resursseista, jotta johtamisjärjestelmä voi toimia tehokkaasti (Brenner, 2007).

Brennerin (2007) mukaan riskiarvion jälkeen toteutusvaiheessa organisaatio päättää, miten se aikoo käsitellä havaittuja riskejä. Tyypillisesti organisaatio valitsee implementoitavaksi riskeihin vaikuttavia tietoturvakontrolleja. (Brenner, 2007.) Tietoturvakontrollien valintaan ISO/IEC 27000 (2018) suosittelee ISO/IEC 27002:n määrittelemiä tietoturvakontrolleja, mutta ei erikseen kiellä muiden tietoturvakontrollien käyttämistä. Kuitenkin kontrolleja valitessaan organisaation tulisi huomioida kansallisen ja kansainvälisen lainsäädännön vaatimukset, organisaation omat päämäärät, oman operatiivisen toiminnan asettamat vaatimukset ja rajoitteet. Lisäksi organisaation tulisi arvioida implementoitavan tietoturvakontrollin kustannusta ja kustannuksen suhdetta riskiin. Johtamisjärjestelmän toimivuuden kannalta on tärkeää tietoturvakontrollin mitattavuuden ja seurattavuuden varmistaminen. (ISO/IEC 27000, 2018.) Tietoturvakontrollit tulisi ISO/IEC 27001 -standardin (2017) mukaan dokumentoida Statement of Applicability (SoA) -dokumenttiin, jossa kuvataan kontrollin valintaperuste, toteutustapa ja sen vaikutus. ISO/IEC 27000 -standardin mukaan valmiiden tietoturvakontrollien lisäksi riskejä voi käsitellä myös erilaisilla politiikoilla, kuten esimerkiksi kieltämällä sellaisten toimintojen suorittamisen, jotka synnyttävät organisaatiolle riskejä. Riskejä voi myös jakaa esimerkiksi sopimuksilla tai vakuutuksilla, jolloin taakka organisaatiolle on pienempi, kun riski on hajautettu. Riskin voi myös jättää käsittelemättä ja hyväksyä sen olemassaolon, jos organisaatio hyväksyy havaitun riskitason eikä koe sitä liian suurena uhkana. Tärkeintä kuitenkin on, että kaikki riskit käsitellään ja riskienhallinta on toimiva ja jatkuva prosessi. (ISO/IEC 27000, 2018.)

Arviointivaiheessa järjestelmän toiminnan tehokkuutta tarkkaillaan ja tarkastetaan johtamisjärjestelmän kehittämiskohteiden löytämiseksi. Tarkastaminen sisältää säännöllisen johtamisjärjestelmän ja tietoturvakontrollien toimivuuden testaamisen, sekä riskiarvion säännöllisen päivittämisen (Brenner, 2007). ISO/IEC 27000 -standardin (2018) mukaan tarkastusten tulisi tuottaa

dokumentoitua informaatiota johdon katselmoitavaksi, jotta se voi arvioida järjestelmän toimivuutta ja kehityskohteita. Dokumentaatio toimii myös todisteena havainnoista, tehdyistä korjauksista, ennaltaehkäisevistä ja kehittävistä toimista. (ISO/IEC 27000, 2018.)

Syklin viimeinen vaihe, kehitys, pyrkii siihen, että johtamisjärjestelmää parannetaan ja ylläpidetään aktiivisesti. Se tarkoittaa muun muassa sitä, että tarkastusvaiheessa löydettyjen parannuskohteiden eteen tehdään ehkäiseviä ja korjaavia toimenpiteitä. Lisäksi tehdyistä muutoksista on hyvä kommunikoida organisaation sisällä, sekä oppia tehdyistä virheistä. (Brenner, 2007). Kun prosessin neljäs vaihe on suoritettu, alkaa sykli uudestaan ensimmäisestä vaiheesta, millä varmistetaan järjestelmän jatkuva ylläpitäminen ja parantaminen. ISO/IEC 27000 -standardin mukaan johtamisjärjestelmän tehokkuus ja toiminta täytyy pystyä tarvittaessa osoittamaan, minkä takia järjestelmän ylläpito vaatii aktiivista työskentelyä, koska muuten jatkuvan parantamisen vaatimus ei täyty. Tyypillisesti prosessi voidaan käydä läpi esimerkiksi kerran vuodessa, mutta tarvittaessa se voidaan toistaa tiheämmin. (ISO/IEC 27000, 2018.)

ISO/IEC 27000 (2018) määrittelee joitakin kriittisiä tekijöitä, jotka vaikuttavat organisaation tietoturvan johtamisjärjestelmän onnistumiseen: Ensinnäkin organisaation määrittelemien tietoturvapolitiikkojen, -tavoitteiden ja toimintojen on oltava linjassa organisaation yleisten tavoitteiden kanssa. Organisaatiolla täytyy myös olla systemaattinen ja organisaatiokulttuurin mukainen lähestymistapa ja viitekehys tietoturvan suunnitteluun, implementointiin, seurantaan, ylläpitoon ja kehitykseen. ISO/IEC 27001 (2017) korostaa myös johdon vahvaa sitoutumista tietoturvaan, erityisesti korkeimman johdon osalta, jotta järjestelmällä on tosiasiallinen mahdollisuus vaikuttaa ja toimia. ISO/IEC 27000 -standardin (2018) mukaan organisaation on myös ymmärrettävä riskienhallinnan avulla saavutettava hyöty omaisuuseriä suojatessa. Organisaatiossa tulisi myös käyttää resursseja siihen, että sillä olisi toiminnassa tietoturvatietoisuutta lisäävä tietoturvakoulutus. Tietoturvakoulutuksella pyritään lisäämään työntekijöiden sekä muiden tärkeiden yhteistyökumppaneiden tietoisuutta organisaation tietoturvapolitiikoista ja toimintatavoista, sekä myös motivoimaan toimimaan niiden mukaisesti. Erilaisten tietoturvatapahtumien varalle organisaatiolla tulisi olla valmiiksi määritelty prosessi, jotta se ei lamaannu riskin aiheuttamasta haitasta. Lisäksi organisaation tulisi varautua pitkän aikavälin kriisinkestävyyteen ja palautumiseen suunnittelemalla jatkuvuudenhallintaan liittyviä toimenpiteitä. Viimeisenä kriittisenä tekijänä ISO/IEC 27000 mainitsee mittaus- ja arviointisysteemin tietoturvan hallinnan tehokkuuden mittaamiseksi ja kehitysehdotuksien tuottamiseksi. (ISO/IEC 27000, 2018.)

2.1.2 ISO/IEC 27001 -sertifiointi

Vaatimuksenmukaisuuden standardin vaatimuksiin voi osoittaa kolmella eri tavalla: Itsearviolla, toisen osapuolen arvioinnilla, tai kolmannen osapuolen arvioinnilla. Näitä arviointeja kutsutaan auditoinneiksi. Humphreysin (2011) mukaan itsearvio on organisaation oma sisäinen auditointi, joka kuuluu osaksi

ISO/IEC 27001 -standardin vaatimiin vuosittaisiin toimenpiteisiin. Sisäinen auditointi pyrkii havainnoimaan tarvittavat muutoskohteet johtamisjärjestelmässä, sekä pyrkii varmistamaan johtamisjärjestelmän jatkuvan parantamisen ja ylläpidon. Toisen osapuolen auditointi voi olla esimerkiksi organisaation toimittajan tai asiakkaan tekemä tai teettämä auditointi, jolla pyritään varmistamaan auditoitavan organisaation vaatimustenmukaisuus. Kolmannen osapuolen auditointi on riippumattoman sertifiointielimen tekemä auditointi, jonka läpäistyään organisaatio voi hakea sertifikaattia, eli todistusta standardin vaatimusten täyttämisestä. (Humphreys, 2011.) Brennerin (2007) mukaan ISO/IEC 27001 -sertifikaatilla organisaatio voi osoittaa, että se suhtautuu vakavasti tietoturvaan ja että organisaation tietoturvan taso on todettu todistetusti hyväksi. Sertifikaatti toimii todisteena siitä, että organisaation sertifikaatissa määritellyt osat ja toiminnot ovat standardin vaatimusten mukaisia.

ISO/IEC 27001 johtamisjärjestelmän auditointi toteutetaan kaksivaiheisesti perustuen siitä annettuihin vaatimuksiin dokumenteissa ISO/IEC 17021 *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements* ja ISO/IEC 27006 *Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems*:

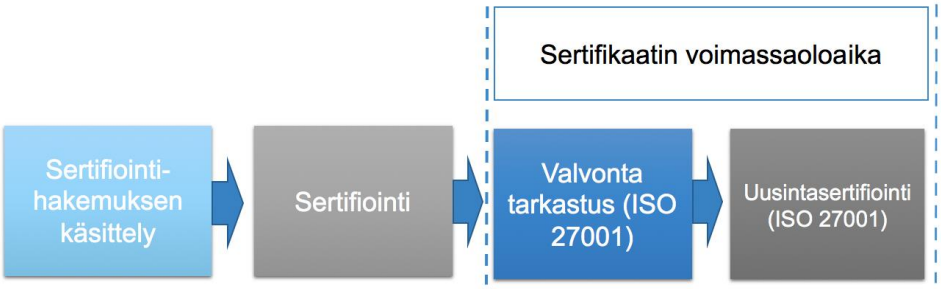
1. Dokumentaatio ja haastattelut (Vaihe 1): Tarkastetaan standardin vaatima dokumentaatio ja haastatellaan tarvittava henkilöstö, jotta varmistutaan standardin vaatimusten täyttyminen.
2. Todentaminen (Vaihe 2): Tarkastetaan auditoitavan organisaation prosessit ja implementoidut tietoturvakontrollit, jotta varmistutaan standardinmukaisesta toiminnasta. Todennusmenetelmiä voivat olla muun muassa haastattelut, dokumentaatio, havainnointi ja tekninen testaus.

ISO/IEC 17021:n (2015) ja sitä täydentävän ISO/IEC 27006:n (2015) mukaan ensimmäisen vaiheen tavoitteena on saavuttaa riittävä ymmärrys ja varmuus auditoitavan organisaation johtamisjärjestelmän olemassaolosta ja toimivuudesta tutkimalla dokumentaatiota ja haastattelemalla tarvittavat henkilöt, kuten organisaation johto ja johtamisjärjestelmästä vastaavat henkilöt. Vaiheessa yksi tarkastetaan siis, että auditoitavan organisaation johtamisjärjestelmä täyttää kaikki standardin vaatimukset 1-10. Kun auditoinnin ensimmäinen vaihe on suoritettu hyväksytysti siten, että tarvittavat korjaukset on tehty, käydään läpi vaihe kaksi, jossa todennetaan vaatimuksiin liittyvien prosessien toiminta ja implementointi. Käytännössä tämä tarkoittaa auditoitavan organisaation SoA-dokumentissa määriteltyjen tietoturvakontrollien tarkastamista erilaisilla todennusmenetelmillä, joita voivat olla muun muassa haastattelut, dokumentaation tarkastelu, havainnointi ja tekninen testaus. SoA (Statement of Applicability) on johtamisjärjestelmän havaitsemien riskien hallintaan käytettävä dokumentti, johon dokumentoidaan tietoturvakontrollit, niiden valintaperusteet (tai valitsematta jättämisperusteet), suojatavat omaisuuserät ja toteutusmenetelmät. Todentamisvaiheen tarkoitus on nimensä mukaisesti olla ensimmäisen vaiheen tulosten todentaminen, jolla varmistutaan siitä, että johtamisjärjestelmän prosessit todella

toimivat ja organisaation riskiperusteinen arvio tarvittavista tietoturvakontrolleista on auditoijan mielestä riittävä ja oikea. (ISO/IEC 17021, 2015 & ISO/IEC 27006, 2015.)

Auditoinnin tuloksena syntyy kirjallinen auditointiraportti, joka sisältää keskeiset löydökset ja auditoinnin tuloksen. Auditointiprosessiin kuuluu kahden edellä mainitun vaiheen lisäksi myös muita tehtäviä, kuten aloitus- ja lopetuskokoukset, sekä sertifiointihakemuksen katselmointi ja sertifiointipäätöksen tekeminen. Sertifiointiprosessiin voi auditoinnin havaintojen perusteella tulla kuitenkin useampia lisätarkastuksia, jos auditoinnin aikana löytyy puutteita, joita joudutaan korjaamaan vaatimusten täyttämiseksi. Kun auditoitava organisaatio on läpäissyt auditoinnin hyväksytysti, voi se hakea sertifikaattia todistukseksi vaatimusten täyttämisestä. Sertifikaatin myöntäminen tapahtuu sertifiointihakemuksen perusteella, jonka sertifikaatin myöntävä organisaatio käsittelee. Myönnetty sertifikaatti on voimassa sen myöntämispäivästä lähtien, ja on voimassa sertifikaatin elinkaaren mukaisesti. (ISO/IEC 17021, 2015 & ISO/IEC 27006, 2015.)

ISO/IEC 27001 -sertifikaatin elinkaari perustuu ennalta määrättyyn sykliin, joka on kolmivuotinen. Sykli on esitelty alla olevassa kuviossa (kuvio 2).



KUVIO 2 Sertifioinnin elinkaari (Nixu Certification, 2019)

ISO/IEC 17021 -standardin (2015) mukaan syklin ensimmäinen vuosi alkaa sertifioinnin myöntämisen jälkeen. Sertifikaatin ylläpitämiseksi sertifioidun organisaation on läpäistävä vuosittaiset valvontatarkastukset, eli vuosiauditoinnit, jotka eivät ole laajuudeltaan yhtä kattavia kuin ensimmäinen auditointi. Valvontatarkastuksilla pyritään varmistamaan organisaation standardin mukainen toiminta, erityisesti jatkuvan parantamisen ja kehittämisen toimivuus. Syklin lopussa, eli kahden vuosiauditoinnin jälkeen, tulee sertifikaatin ylläpitämiseksi läpäistä uusintasertifiontiauditointi, joka on laajuudeltaan verrattavissa ensimmäiseen sertifiointiauditointiin. (ISO/IEC 17021, 2015.)

2.2 Sertifiointielimet

ISO/IEC 27001 -sertifikaatteja voi käytännössä myöntää kuka tahansa, mutta uskottavuutta ja luotettavuutta lisätäkseen johtamisjärjestelmiä sertifioivat toimijat, eli sertifiointielimet (certification body), voivat hakea kansalliselta

akkreditointipalvelulta akkreditointia toimintaansa. Suomessa johtamisjärjestelmien sertifioinneista vastaavien sertifiointielinten akkreditoinneista vastaavan Suomen akkreditointipalvelu FINAS:in (Finnish Accreditation Service) (2016) mukaan akkreditointi tarkoittaa sitä, että sertifiointielimen toimintatavat ja prosessit on todettu päteväksi akkreditointipalvelua suorittavan toimijan toimesta. ISO/IEC 27001 -sertifioinnin osalta akkreditointi velvoittaa sertifiointielimiä noudattamaan standardia ISO/IEC 17021 ja sitä täydentävää ISO/IEC 27006 -standardia. Edellä mainitut muun muassa velvoittavat sertifiointielimiä huolehtimaan puolueettomuudesta ja riittävästä osaamisesta osana auditointitoimintaa, sekä noudattamaan standardien määrittämää auditointiprosessia ja muita auditointiin liittyviä vaatimuksia. Sertifiointiauditoinnin tarkoitus on olla puolueeton kolmannen osapuolen auditointi, joten akkreditointi toimii osaltaan merkkinä siitä, että auditointi on suoritettu asianmukaisesti, sillä akkreditoidut sertifiointielimet ovat myös jatkuvan seurannan alaisia. (FINAS, 2016.)

Suomessa on tällä hetkellä kolme FINAS:in akkreditoimaa sertifiointielintä, jotka myöntävät ISO/IEC 27001 -sertifikaatteja (FINAS, 2019). Näiden lisäksi Suomessa toimii ulkomaisia sertifiointielimiä, joilla voi olla ulkomainen akkreditointi. Tyypillisesti sertifiointielinten palveluihin voi kuulua myös muita standardeja ja osaamisalueita. Suomessa sertifiointielinten on muun muassa mahdollista hankkia FINAS:lta akkreditointi tietoturvallisuuden arviointilaitokseksi, jota säätelee Laki tietoturvallisuuden arviointilaitoksista (1405/2011), ja jonka hyväksynnästä ja valvonnasta vastaa Traficom (entinen Viestintävirasto). Tietoturvallisuuden arviointilaitokset voivat tehdä toimeksiantona muun muassa Katakri- ja VAHTI-auditointeja ja myöntää niihin liittyviä todistuksia, jos arviointilaitoksella on niihin myönnetty pätevyys. Arviointilaitosten on mahdollista tarjota myös muita palveluita. (Viestintävirasto, 2018.)

2.3 Tietoturvainvestoinnit

Tietoturvaloukkauksen tapahtuessa organisaatio voi kokea merkittäviä taloudellisia menetyksiä ja erilaisia muita haittoja, kuten maineen menettämisen. Sen vuoksi organisaatioiden on tehtävä riittäviä investointeja, jotta ne välttäisivät tietoturvaloukkaukset ja niiden seuraukset. Tietoturva on investointi siinä missä muutkin organisaation investoinnit ovat, sillä niiden avulla organisaatio pyrkii saavuttamaan hyötyä suhteessa panostettuihin resursseihin. Tietoturvainvestoinnit voivat vaihdella yksittäisistä pienistä investoinneista suuriin hankkeisiin, kuten johtamisjärjestelmän pystyttämiseen. Cavusoglun, Raghunathanin ja Yuen (2008) mukaan tietoturvainvestointien ongelma on kuitenkin se, että niiden onnistumista on hankala mitata panostuksen ja saadun hyödyn välisellä suhteella, mikä on yleisesti merkittävä investointipäätökseen vaikuttava tekijä. Investoinnilla ei siis usein ole suoraan rahassa mitattavia tuottoja, tai investoinnille on muutoin haastavaa osoittaa sopivia mittareita kulutettujen resurssien ja saadun hyödyn suhteesta. Tällä tarkoitetaan siis sitä, että tietoturvaan sijoitetun pääoman tuottoasteen (Return on Security Investment, ROSI) arvioiminen on

hankalaa. (Cavusoglun ym., 2008.) Kiistatonta on se, että tietoturvaan sijoittaminen tuottaa jossain määrin arvoa, sillä tietoturvainvestoinneilla voidaan pienentää tai jopa poistaa tietoturvariskeistä koituvia kustannuksia ja laskea riskin toteutumisen todennäköisyyttä. Ongelmaksi muodostuu kuitenkin sopivan investointitason määrittäminen, sillä investointi ei ole kannattava, jos se kustantaa liian paljon suhteessa riskin todennäköisyyteen ja riskin realisoitumisesta syntyviin kustannuksiin. Toisaalta myös alimitoitettu tietoturvainvestointi on organisaatiolle rasite, sillä se ei suojaa organisaatiota riskin realisoituessa ja lopputilanteessa investoinnin ja vahingon kokonaiskustannukset ovat suuremmat kuin ilman investointia.

Tietoturvainvestointien optimaalisen tason mittaamiseen ja määrittämiseen on kehitetty erilaisia teorioita, joista monet lähestyvät ongelmaa riskienhallinnan kautta. Tyypillisesti investointiteoria jakautuvat kuitenkin kahteen eri luokkaan. Cavusoglun ym. (2008) mukaan organisaatioiden johto näkee tietoturvainvestoinnit tyypillisesti samanlaisena kuin muutkin IT-investoinnit ja soveltaa niihin päätösteorian mukaisia päätöksentekomalleja. Parmigianin ja Inouen (2009) mukaan päätöksentekoteoria on päätöksentekoon hyödynnettävä malli, jossa voidaan hyödyntää erilaisia tilastollisia menetelmiä optimaalisen valinnan löytämiseksi erilaisten vaihtoehtojen joukosta. Käytännössä se tarkoittaa sitä, että riskien ja valintojen tuottama hyöty kvantifioidaan, jotta ihminen voi tehdä rationaalisen päätöksen kahden tai useamman vaihtoehdon väliltä. Organisaatiotasolla päätöksentekoteoriaa voidaan käyttää esimerkiksi riskienhallinnan osana: Arvioidaan erilaisten tietoturvakontrollien kustannusta ja toimivuutta suhteessa riskiin ja valitaan niistä halutulla mittarilla mitattuna tehokkain. (Parmigiani ja Inoue, 2009.)

Cavusoglun ym. (2008) mukaan päätöksentekoteoria ei kuitenkaan ole kaikista tehokkain tapa tietoturvainvestointien tekemiseen ongelman strategisen luonteen takia. Tämä tarkoittaa sitä, hakkerit ja muut organisaatiota kohti hyökkäävät hyökkääjät muuttavat toimintatapojaan tilanteen mukaan oppiessaan organisaation heikot kohdat. Tämän vuoksi he kehittivät peliteoriaan perustuvan lähestymistavan tietoturvan optimaalisen investoinnin määrittämiseksi. Peliteoriassa organisaation täytyy käyttää strategista ajattelua ja suorittaa päättelyketjuja tietoturvaa suunnitellessaan, koska hyökkääjät muuttavat toimintatapojaan tilanteen muuttuessa. Peliteorian mukaisessa lähestymistavassa pyritään tekemään ennaltaehkäiseviä tietoturvaratkaisuja siten, että organisaatio pyrkii löytämään hyökkääjän oletetut seuraavat liikkeet ja estämään ne, ennen kuin hyökkääjä kerkeää käyttämään niitä. Täten organisaation tietoturvan taso kehittyy jatkuvasti ja se löytää järkevät investointikohteet organisaatiostaan. Vaikka teoria on sinänsä todistettu toimivaksi, on sen ongelmana kuitenkin melko vähäinen levinneisyys käytäntöön organisaatioiden käyttöön, koska sen käyttö koetaan haastavammaksi verrattuna perinteisiin ja yksinkertaisempiin päätöksentekoteorioihin. (Cavusoglu ym., 2008.)

Peliteorian sijaan on siis tyypillisempää käyttää päätöksentekoteoriaa tietoturvainvestoinnin optimaalisen tason määrittämiseksi. Yksi tunnetuimmista teorioista on Gordonin ja Loebin vuonna 2002 kehittämä matemaattinen malli

tietoturvainvestointien optimaalisen tason laskemiseksi. Mallin tärkeimpänä pyrkimyksen on määrittää taso, jossa saadut hyödyt investoinnista ovat korkeammat kuin kustannukset. Malli perustuu kolmeen parametriin: Datan arvoon tietomurron sattuessa (potentiaalinen rahallinen tappio), tietomurron todennäköisyyteen ja tietoturvainvestointien vaikutukseen tietomurron todennäköisyyteen. Mallin tuloksena syntyi johtopäätös, jonka mukaan tietoturvainvestointien tehokkuus kasvaa aluksi jyrkästi, mutta lisäinvestoinnin positiivinen vaikutus alkaa vähentyä mitä enemmän investointiin kulutetaan resursseja. Teorian yleistyksenä Gordon ja Loeb (2002) tulivat johtopäätökseen, että organisaation optimaalinen tietoturvainvestointi riskiä kohden on tyypillisesti maksimissaan 37 % tai vähemmän potentiaalisesta rahallisesta tappiosta. Toinen mallin päälöydöksistä on, että optimaalisen tietoturvainvestoinnin taso ei myöskään kulje lineaarisesti suhteessa riskiin: Kun mallin mukainen maksimaalinen tietoturvainvestointi suhteessa potentiaaliseen tappioon on saavutettu, alkaa optimaalinen tietoturvainvestoinnin määrä laskea riskin toteutumisen todennäköisyyden lähestyessä 1:tä. Päätelmä on looginen, koska jos tietomurron todennäköisyys on lähes varma, ei siihen kannata investoida. Vaikka teoria on vakiinnuttanut asemansa alan perusteoksena, voi mallille myös esittää perusteltua kritiikkiä. Teoriaa voi olla haastava todentaa käytännössä, sillä Gordonin ja Loebin (2002) mukaan se perustuu hyvin yleistettyyn alkutilanteeseen ja malli sulkee pois monia ulkoisia tekijöitä. Reaalimaailmassa riskeihin ja investointeihin vaikuttavat monet muutkin tekijät kuin määritellyt kolme parametriä. Lisäksi ihminen ei ole päätöksissään rationaalinen. Ihmisten päätöksenteko ei aina perustu järkeen vaan myös tunteeseen ja muihin vaikuttaviin tekijöihin. Toisaalta myös mallin esittämä tarkka luku optimaalisen tietoturvainvestoinnin määrästä on haastava, koska sen todentaminen on hankalaa.

Huang, Hu ja Behara (2008) esittävät omassa tutkimuksessaan jatkoa Gordonin ja Loebin (2002) mallille. He lähestyvät tietoturvainvestointeja riskejä karttavan organisaation näkökulmasta, koska useimmat organisaatiot käyttäytyvät mieluummin riskejä karttaen tai ainakin hallitusti ottaen. Huang ym. (2008) esittelivät tutkimuksessaan kolme väitettä tietoturvainvestoinneista. Ensimmäisen väitteen mukaan on olemassa tietty nollataso, jossa potentiaalisen haitan kustannus on niin pieni, että siihen ei kannata investoida, vaikka riski olisi olemassa. Tämä perustuu siihen, että tarpeeksi harmittomaan riskiin ei kannata tuhlata resursseja, koska potentiaalinen tappio on kuitenkin niin pieni. Kuitenkin heti nollatason jälkeen potentiaalisen tappion kasvaessa alkaa myös optimaalisen investointitason käyrä kohota jyrkästi. Toinen väite on, että optimaalinen investointitaso ei välttämättä kasva, vaikka riskin karttamisen tahtotila kasvaa. Tämä selittyy sillä, että investointiin itsessään liittyy aina riski, esimerkiksi se, että investointi epäonnistuu. Viimeinen kolmesta väitteestä on se, että lisäinvestointi ei aina takaa samassa suhteessa tehokkaampaa suojaa tappioita vastaan, vaan optimitason jälkeen investoinnin tehokkuus kasvaa vähemmän mitä enemmän riskin karttamiseksi investoidaan rahaa. (Huang ym., 2008.)

Tietoturvainvestointeihin liittyvät teorioita on monia ja ne lähestyvät ongelmaa erilaisista näkökulmista. Ongelmaan ei varmastikaan ole yhtä oikeaa

vastausta, mutta se ei tämän tutkimuksen kannalta ole tärkeää. Tämän tutkimuksen osalta on mielenkiintoista tutkia erityisesti sitä, miten tutkittavat yritykset näkevät sertifioinnin ja siihen liittyvät valmistelut investointina. Ollaanko siihen valmiita panostamaan tietoturvan parantamisen takia, vai onko sertifiointi ennemmin kilpailukykyä parantava investointi, joka hankitaan mahdollisimman halvalla? Toisaalta on myös mielenkiitoista koittaa saada selville markkinoilla toimivien yritysten näkemyksiä esimerkiksi siitä, miten he määrittävät ja päättävät riskeihin liittyvien investointien tason.

3 ISO/IEC 27001 -SERTIFIOINNIN HANKINTAPERUSTEET

Kolmas luku käsittelee aiempaa aiheeseen liittyvää tutkimusta yhdistelemällä erilaisia näkökulmia sertifioinnin hyödyistä, haasteista ja yleisistä perusteista, jotka ohjaavat hankkimispäätöstä. Ensin perehdytään sertifikaatin hankkimisesta koituviin hyötyihin talous- ja tietoturvanäkökulmasta, minkä jälkeen perehdytään sertifioitumiseen liittyviin haasteisiin. Tästä muodostuvalla kokonaisuudella pyritään selvittämään syitä sille, miksi organisaatiot päättävät hankkia sertifikaatin itselleen ja päättävät myös ylläpitää sitä. Luvun luettuaan lukijalla on yleisymmärrys aihealueen aikaisemmasta aiheeseen liittyvästä tutkimuksesta ja saa kokonaiskuvan sertifioinnin hankkimisperusteista.

3.1 Johtamisjärjestelmäsertifioinnin hyödyt

Sertifiointi perustuu standardeihin ja niiden noudattamiseen. Kansainvälinen standardoimisorganisaatio ISO (2019a) määrittelee standardien yleiseksi hyödyksi sen, että niillä saadaan yhtenäistettyä yleisesti hyviksi koettuja toimintatapoja niin, että keskinäinen luottamus toimintaan vahvistuu ja markkinoille tulee yhä parempia ja turvallisempia tuotteita ja palveluita. Sertifioinnilla organisaatio voi osoittaa standardinmukaisen toimintansa ulkopuolisille, ja näin ollen vakuuttaa muut omien toimintojensa laadusta. (ISO, 2019a.) ISO:n standardien ollessa kansainvälisesti tunnettuja, on standardien omaksuminen tapa varmistaa kansainvälisesti paljon käytettyjen toimintatapojen käyttäminen organisaatiossa. Mutta mikä erottaa ISO/IEC 27001 -standardin muista tietoturvan hallinta- ja johtamisjärjestelmästandardeista?

Kuten luvussa kaksi todettiin, on ISO/IEC 27001 -sertifiointi kasvanut merkittävää vuosivauhtia ja myönnettyjä sertifikaatteja on jo lähes 40 000 (ISO, 2018). Luvut kertovat sen, että sertifikaatin hankkiminen on yhä yleisempää, mutta ne eivät kuitenkaan kerro mitään siitä, miksi sertifiointi hankitaan. Lukujen avulla voidaan kuitenkin selittää sertifioinnin merkityksen kasvamista, ja toisaalta sitä, että erilaiset standardit ovat yleistyvä tapa lähestyä tietoturvaa. Standardit ovat vapaaehtoisia, mutta joihinkin niistä sertifioidutaan pääosin ulkopuolisen toimijan vaatimana. Näistä standardeista tyypillisiä esimerkkejä ovat maksukorttimaksamisen suojaksi suunniteltu PCI DSS ja kansallinen turvallisuusauditointikriteeristö Katakri. Ulkopuolisen vaatimuksen takia hankittujen sertifikaattien ja todistusten hankintaperuste on sinänsä itsestään selvä, sillä motivointi tulee ulkoisen paineen ja vaatimuksen myötä. Esimerkiksi vaatimustenmukaisuudesta kertova Katakri-todistus voi olla vaatimuksena viranomaisyhteistyölle turvaluokiteltua tietoa käsiteltäessä, mikä sellaisenaan toimii motivoivana tekijänä. Tilanne on kuitenkin varsin erilainen vapaaehtoisuuteen perustuvissa standardeissa. Barletten ym. (2008) mukaan joissain tapauksissa kansallinen

lainsäädäntö tai ohjeistus kannustaa tai pakottaa organisaatiot hankkimaan ISO/IEC 27001 -sertifikaatin, mikä osaltaan selittää sertifikaattien suhteellisen korkean määrän esimerkiksi Japanissa. Kaikilla maksullisen sertifikaatin hankkimista ei kuitenkaan ohjaa pakko, vaan jotkin muut asiat. Tieteellinen tutkimus ISO/IEC 27001 -sertifioinnin hyödyistä on melko vähäistä ja on enemmän keskittynyt yksityisten toimijoiden teettämiin tutkimuksiin. Kuitenkin erilaisia tietolähteitä yhdistelemällä voidaan muodostaa kokonaisuus siitä, miksi organisaatiot päätyvät juurikin ISO/IEC 27001 -sertifiointiin.

Brittiläinen ISO/IEC 27001 -standardiin erikoistunut konsulttitalo IT Governance teki vuonna 2018 kansainvälisen kyselytutkimuksen ISO/IEC 27001 -sertifioinnin hankintaperusteista ja hyödyistä, mihin vastasi 128 eri organisaatiota. Vastauksia tuli ympäri maailmaa, joskin yli puolet vastanneista (64 %) olivat Euroopasta. Vastaajaorganisaatioiden koot olivat kuitenkin laajemmin hajautuneita, joten vastauksia tuli kaikista erilaisista kokoluokista pienistä yrityksistä maailmanlaajuisiin suuriin organisaatioihin asti. Vastaajaorganisaatiot edustivat myös useita eri toimialoja sekä julkiselta että yksityiseltä sektorilta, joten kyselyssä saatiin näkemyksiä varsin erilaisista näkökulmista. Ensimmäinen kysymys kysyi vastaajilta tärkeimpiä syitä ISO/IEC 27001 -standardin implementointiin. Vastauksiin kerättiin vastaajien kymmenen suosituinta vastausta, jotka on esitetty taulukossa 1 alla (taulukko 1).

Taulukko 1 Implementoinnin syyt (It Governance, 2018a)

Syy implementointiin	**Osuus vastaajista**
Tietoturvan tason parantaminen organisaatiossa	72 %
Kilpailuedun kasvattaminen	57 %
Lakien ja muiden velvoittavien vaatimusten täyttämisen varmistaminen	52 %
Toimialan luonne vaatii toteuttamaan tietoturvan parhaita käytänteitä	49 %
EU:n tietosuoja-asetuksen vaatimusten täyttäminen	48 %
Vaatimuksena uuden asiakkuuden saamiseksi	46 %
Organisaation johdon sitouttaminen tietoturvaan	44 %
Kehittyvä kyberuhkien toimintaympäristö	42 %
Nykyisten asiakkaiden vaatimus	40 %
Lain vaatimusten rikkomisesta johtuvien kustannusten välttäminen/alentaminen	21 %

Kysely antaa melko selvän kuvan siitä, mitkä tekijät motivoivat organisaatioita implementoimaan ISO/IEC 27001 -mukaisen johtamisjärjestelmän. Yksinoikeutetusti suurin syy implementointiin on tietoturvan edistäminen, mikä on standardin tärkein tehtävä. Toiseksi suosituin syy liittyy kilpailuedun kasvattamiseen. Kilpailuedun kasvattaminen voidaan nähdä taloudellisena intressinä, joka taas indikoi sitä, että implementoinnin taustalla on myös taloudellisia tavoitteita. Nämä kaksi näkökulmaa, tietoturva ja talous toistuvat myös muissa vastauksissa joko suoraan tai epäsuorasti. Kuitenkaan kumpikaan näkökulma ei erityisesti

erotu toisistaan, vaan vastausten perusteella on havaittavissa, että niiden hyödyt koetaan melko yhtäläisinä. Toisena kysymyksenä It Governancen (2018a) kyselyssä kysyttiin tärkeimpiä ISO/IEC 27001 implementoinnista koettuja hyötyjä. Kahdeksan suosituinta vastausta on esitetty alla olevassa taulukossa (taulukko2).

Taulukko 2 Koetut hyödyt implementoinnista (It Governance, 2018a)

Koettu hyöty ISO/IEC 27001 -standardin implementoinnista	**Osuus vastaajista**
Korkeampi tietoturvan taso	89 %
Paremmat sisäiset prosessit	67 %
Henkilöstön parempi tietoturvaosaaminen	62 %
Kohentunut yrityksen imago/maine	58 %
Uudet liikekumppanit/liiketoimintamahdollisuudet	50 %
Parempi kilpailukyky/suuremmat tuotot	35 %
Olemassa olevien asiakkuuksien säilyttäminen	31 %
Tietomurroista koituvien kustannuksien pienentyminen	24 %

Toisenkin kysymyksen vastauksissa toistuvat teemat tietoturva- ja taloushyötyjen kesken, vaikkakin tietoturvasta saadut hyödyt ovat selkeästi suuremmalla osalla vastaajista yleisempiä. Yleisenä huomiona on huomattava myös se, että ISO/IEC 27001 koetaan hyödylliseksi myös lain ja asetusten velvoitteiden täyttämiseksi. Mielenkiintoinen huomio kyselystä on myös se, että ISO/IEC 27001 -standardin asema on jo nyt markkinoilla sellainen, että se on usein vaatimuksena osana uusia asiakkuuksia. 41 % vastaajista kertoi sertifikaatin olevan jo tavallinen vaatimus uuden sopimuksen solmimiseen ja 33 % kertoi sen olevan vaatimuksena silloin tällöin. (It Governance, 2018a.) Näin ollen voidaan todeta, että markkinoilla alkaa olla jo melko yleistä se, että toimittajan täytyy kyetä osoittamaan tietoturvansa taso jollain mittarilla, esimerkiksi sertifikaatilla, jotta asiakas voi varmistua tietojen turvallisesta käsittelystä.

Tämän tutkimuksen näkökulma ja teoreettinen lähestymiskulma tietoturva- ja talousnäkökulman tarkastelusta perustuu pitkälti myös Parkin ym. (2010) tutkimukseen ISO/IEC 27001 sertifioinnin hyödyistä. Tutkimus toteutettiin kvantitatiivisena tutkimuksena mitaten neljän eri kategorian vaikutuksia sertifioinnin tehokkuuteen teettämällä kyselytutkimus 76:lle tutkimukseen osallistuneelle organisaatiolle. Neljän tutkittavan kategorian mittaamiseen käytettiin kahdeksaa tutkimusolettamaa, kahta kutakin kategoriaa mittaamaan. Analyysi toteutettiin tekemällä regressioanalyysi tutkimuksessa saatujen vastausten perusteella tutkimalla aina kutakin kategoriaa siihen kuuluvilla hypoteeseilla. Tämän tutkimuksen kontekstissa tulokset ovat merkittäviä ja mielenkiintoisia, sillä tutkittavat organisaatiot edustavat eri kokoisia organisaatioita, joiden sertifikaatin ikä vaihtelee myös suuresti ja toisaalta tutkimus myös osaltaan esittää hyviä teoreettisia päätelmiä sertifioinnin hyödyistä. Ensimmäisessä kategoriassa pyrittiin mittaamaan sertifioinnin taloudellisia vaikutuksia. Hypoteeseina olivat väitteet siitä, että sertifiointi lisää sekä tuottoja, mutta samalla myös vähentää organisaation kuluja, jolloin sertifikaatin tuottama arvonlisä on positiivinen. Tutkimuksessa kummatkin hypoteesit hyväksyttiin, sillä tutkittavat organisaatiot

totesivat sertifikaatin tuottavan paremman julkisuuskuvan, joka houkuttelee uusia asiakkaita ja näin ollen tuottaa lisää voittoja. Samalla organisaatiot myös ilmaisivat säästöistä, jotka saavutettiin välttämällä potentiaaliset tietoturvapoikkeamat tuottamalla hyvää tietoturvaa. Toisen kategorian hypoteesina oli se, että vakaan tietoturvatason saavuttaminen ja ylläpitäminen sertifioiutumalla myös lisää organisaation toimintojen luotettavuutta ja jatkuvuutta. Hypoteesit myös todettiin oikeaksi, sillä organisaation omaisuuserien todettiin toimivan vakaammin, kun ne oli sertifioitu. Kolmas kategoria pyrki selvittämään sertifioinnin vaikutuksia asiakkaan ja sertifioidun välisen luottamukseen. Näitä tutkittiin kahdella hieman erilaisella hypoteesilla. Ensimmäinen hypoteesi oletti, että organisaation sertifioinnin myötä tehostuneet prosessit lisäävät asiakkaan luottamusta, ja toinen hypoteesi oletti, että organisaation vastauskyvyn nopeutuminen lisäisi asiakkaan luottamusta. Nämä hypoteesit tuottivat kuitenkin hieman ristiriitaisi tuloksia. Kohentuneet prosessit todettiin tilastollisesti merkittäväksi hyödyksi, mutta vastausnopeuden kasvun ei todettu tuottavan merkittäviä hyötyjä, jolloin hypoteesi myös hylättiin. Neljäs, ja viimeinen, tutkittava kategoria pyrki selvittämään tietoturvatietoisuuden paranemista selvittämällä, onko sertifikaatin tuottamalla tietoturvan suojauskyvykkyydellä ja laadun parannuksella yhteyttä tietoturvatietoisuuden kasvuun. Tutkimus osoitti, että organisaation tietoturvankyvykkyyden kasvulla on myös yhteys tietoturvatietoisuuden kasvuun, mutta toisaalta se ei antanut merkkejä laadun parantumisesta. Tutkimuksesta saadut tulokset on myös esitetty havainnollistavassa taulukossa alla (taulukko 3). (Park ym., 2010.)

Taulukko 3 ISO/IEC 27001 sertifikaatin tuottamat hyödyt (Park, ym. 2010)

Numero	**Hypoteesi**	**Koettu hyöty**	**Regressioanalyysin tulos**
1	Sertifikaatin aiheuttama myynnin lisääntyminen aiheuttaa arvon nousua	14 % kasvua	Hyväksytty
2	Sertifikaatin aiheuttamat säästöt aiheuttavat arvon nousua	30 % säästöjä	Hyväksytty
3	Bisnesmahdollisuuksien lisääntyminen lisää liiketoiminnan tasaisuutta	25 % kasvua	Hyväksytty
4	Asiakasyhteistyön lisääntyminen lisää liiketoiminnan tasaisuutta	39 % kasvua	Hyväksytty
5	Prosessien kehittyminen lisää asiakkaiden luottamusta	53 % kasvua	Hyväksytty
6	Reagointinopeuden kasvu lisää asiakkaiden luottamusta	37 % kasvua	Hylätty
7	Tietoturvan suojaustason parantuminen lisää tietoturvatietoisuutta	68 % kasvua	Hyväksytty
8	Laadun parantuminen lisää tietoturvatietoisuutta	43 % kasvua	Hylätty

Tutkimuksen tärkein anti on se, että sertifiointi tuottaa selkeästi niin taloudellisia kuin tietoturvassa mitattavia hyötyjä. Park, ym. (2010) myös kuitenkin mainitsevat, että tutkimusta ei voida pitää täysin luotettavana muun muassa sen takia, että aikaisemman tutkimustiedon puuttuessa tutkimuksessa sovellettava malli on täysin tutkijoiden itsensä kehittämä. Toinen ongelma liittyy myös tutkittavien käsitteiden mittaamiseen, sillä tutkijat nostivat esille haasteen johtamisjärjestelmästä koettujen hyötyjen muuttamisen mitattaviksi arvoiksi. Täten mitattavat arvot eivät välttämättä mittaa täysin oikeaa asiaa, tai eivät tuota täysin luotettavaa tulosta. Kuitenkin tutkimus antoi yleisellä tasolla selkeän tuloksen siitä, että sertifikaatti tuottaa taloudellista hyötyä ja tietoturvan tason nousua. Lisäksi muun muassa asiakkaiden luottamus organisaatiota kohtaan nousee ja organisaation omat sisäiset prosessit kehittyvät. (Park, ym., 2010.) Tässä valossa on mielekästä tutkia vielä tarkemmin edellä mainitun tutkimuksen puutteet huomioiden ISO/IEC 27001 -sertifikaatin hankitaperusteita tietoturvan ja talouden näkökulmasta.

3.1.1 Taloudelliset hyödyt

On ilmeistä, että varsinkin yksityisellä sektorilla sertifikaatin hankkimista ohjaavat taloudelliset intressit. Sertifikaatti voi olla luottamusta lisäävä tekijä, joka toimii osoituksena hyvästä tietoturvan hallinnasta, joka taas voi toimia kilpailuetuna muihin verrattuna. Humphreysin (2006) mukaan juurikin luottamuksen saavuttaminen on elintärkeää liiketoiminnan jatkuvuuden kannalta. Sertifikaatilla organisaatio voi osoittaa, että sen prosessit ja toimintatavat ovat todettu turvallisiksi, ja että se tekee määrätietoista ja jatkuvaa työtä tietoturvan eteen. Sertifikaatin tuottama luottamus voi olla ratkaiseva tekijä, kun asiakas kilpailuttaa palveluntarjoajia ja sopimuksia. Lisäksi sertifikaatti voi myös auttaa täyttämään sopimusten ja lainsäädännön asettamat vaatimukset ilman, että organisaation tarvitsi erityisesti muuntaa toimintatapojaan ja prosessejaan. Näin ollen sertifioitu organisaatio välttyy kuluilta, jotka jouduttaisiin muuten käyttämään toimintatapojen ja prosessien muuttamiseksi. (Humphreys, 2006.) Myös Disterer (2013) painottaa sertifikaatin tuottamaa luottamusta ja nostaa esille sertifikaattien suuren lukumäärän Aasian markkinoilla. Korkean elintason maissa, jossa tuotantokustannukset ovat korkeat, on paine ulkoistaa toimintoja halvempien tuotantokustannusten maihin. IT-palveluntarjoajat Aasiasta ovat houkuttelevia vaihtoehtoja, sillä niistä kustannukset ovat matalammat, mutta toisaalta paikalliset toimijat ovat usein tuntemattomia. Tällöin tietoturvasertifikaatti voi antaa lisäluottamusta siihen, että ulkoistetun palvelun tuottava kumppani noudattaa hyviä tietoturvakäytäntöjä. (Disterer, 2013.) Luottamuksen lisäksi merkittävää hyötyä tuottaa arvostus, sillä ISO/IEC 270001 -sertifikaatti on markkinoilla arvostettu sertifikaatti. Lambon (2006) mukaan ISO/IEC 27001 -sertifikaatin etu muihin kilpaileviin standardeihin verrattuna on se, että se on kansainvälisesti kaikista tunnetuin tietoturvan johtamisjärjestelmästandardi ja näin ollen toimii niin sanottuna de facto -standardina. Se voi myös osaltaan ruokkia organisaatioiden innokkuutta hankkia juuri ISO/IEC 27001 -sertifikaatti.

Cowan (2011) käsittelee ongelmaa, jossa organisaatio miettii ylläpitääkö se tietoturvan johtamisjärjestelmää ilman aikeita järjestelmän sertifioimisesta, vai kannattaako sen hankkia sertifikaatti. Joissain tilanteissa voi olla täysin riittävää vain ylläpitää ISO/IEC 27001 -mukaista johtamisjärjestelmää ilman sertifiointia, sillä tietoturvan tason pystyy tarvittaessa osoittamaan muutoinkin kuin sertifikaatilla, kuten erilaisilla tietoturvan itsearvioinneilla tai asiakkaan teettämillä kyselyillä. Tällainen järjestely voi sopia joillekin yhteistyökumppaneille, erityisesti pienempien organisaatioiden kohdalla. Kuitenkin ongelmaksi muodostuu se, että organisaation tavoitellessa kasvua, voi sertifikaatti muodostua pakolliseksi suurempien ja rahakkaampien sopimusten saavuttamiseksi. Sertifikaatin tarkoitus on kuitenkin olla markkinointikeino, jonka tuottaman arvon ja vakuutuksen ansiosta organisaation ei tarvitse käyttää ylimääräisiä resursseja oman tietoturvansa tason perustelemiseksi. Organisaation täytyy kuitenkin itse määritellä se, mikä sertifikaatin arvo lopulta on, sillä sertifikaatin arvo ei ole mitenkään absoluuttinen. (Cowan, 2011.)

Sertifiointiin kuluvat kustannukset ovat kuitenkin melko kohtuulliset, jolloin useissa tapauksissa sertifiointi on kannattavampaa ottaen huomioon järjestelmän ylläpitämiseen menevät kulut verrattuna sertifioinnin hintaan. It Governancen (2018a) kyselyn mukaan keskimäärin kyselyyn vastanneista organisaatioista puolet käyttivät ISO/IEC 27001 johtamisjärjestelmän implementointiin keskimäärin 5000 – 20 000 puntaa, 23 % alle 5000 puntaa ja 25 % yli 20 000 puntaa. Implementoinnin lisäksi kokonaiskustannuksiin lisätään sertifikaatin hankkimiseen liittyvät kustannukset, jotka vaihtelevat organisaation koon mukaan, koska suuremmat organisaatiot ja laajemmat auditoitavat ympäristöt vaativat useampia auditointipäiviä. It Governancen (2018b) arvion mukaan pienet ja keskisuuret organisaatiot saavat sertifikaatin keskimäärin muutamalla tuhannella punnalla ja organisaation koon kasvaessa hinta kasvaa sen mukaisesti. Esimerkiksi reilu tuhannen henkilön organisaatio maksaa sertifikaatista keskimäärin hieman yli 13 000 puntaa. (It Governance, 2018b.) Näin ollen kustannukset vaihtelevat suuresti organisaation koon, toimintaympäristön ja auditoitavien kohteiden mukaan. Suhteessa sertifiointi maksaa enemmän pienille organisaatioille, mutta kuitenkin kokonaiskustannuksia voidaan pitää melko kohtuullisina, sillä vaikka investointi ei tuota suoria tuottoja, kokevat organisaatiot investoinnin hyödyllisenä taloudellisesti. It Governancen kyselyssä (2018a) noin puolet vastaajista oli sitä mieltä, että sertifiointiin kuluneet kustannukset voidaan kattaa täysin siitä saaduilla hyödyillä ja noin 30 % vastaajista oli sitä mieltä, että kustannukset ovat linjassa muiden johtamisjärjestelmien kanssa. 16 % vastaajista oli sitä mieltä, että sertifiointiin kuluneet kustannukset olivat liian suuret ja noin 4 % oli sitä mieltä, että sertifiointi on liian kallis pienelle organisaatiolle. (It Governance, 2018a.) Johtopäätöksenä kyselystä voidaan todeta, että kulut eivät ole suurimmalle osalle organisaatioista ongelma, sillä saadut hyödyt koetaan kustannuksia korkeammiksi. Barlette ym. (2008) myös muistuttavat siitä, että sertifikaatti voi vaikuttaa myös esimerkiksi organisaation ottamien vakuutusten hintaan niitä laskevasti, mikä näkyy suorana säästönä vakuutusmaksuihin menevissä kuluissa.

Everettin (2011) mukaan paine hankkia ISO/IEC 27001 -sertifikaatti on lähtenyt hiljalleen kasvuun erityisesti sen takia, että julkiset toimijat, kuten valtiot ovat alkaneet vaatia sertifikaattia niiden tarjoamien sopimusten saamiseksi. Vaatimus on sen jälkeen alkanut yleistymään myös yksityisen sektorin keskuuteen. Aivan yksinkertaista muutos ei kuitenkaan ole ollut, sillä organisaatioilla on ollut hankaluuksia perustella sertifioinnin hyötysuhdetta: Tietoturvainvestoinnit nähdään kuluna ja ne kamppailevat muiden, mahdollisesti suoraa tuottoa tuottavien investointien kanssa samasta rahoituksesta. (Everett, 2011.)

3.1.2 Tietoturvanäkökulma

Vaikka sertifiointi voidaan varsinkin kaupallisten organisaatioiden osalta nähdä taloudellisen päätöksen perusteella tehtynä investointina, on sertifioinnilla myös tietoturvan näkökulmasta havaittavia hyötyjä, jotka voivat olla organisaatiolle tärkeitä. Tärkein hyöty tietoturvan näkökulmasta on kokonaisvaltainen tietoturvan hallinta, joka nostaa tietoturvan tasoa organisaation kaikilla tasolla. Boehmerin (2008) mukaan ISO/IEC 27001:n mukainen johtamisjärjestelmä muodostaa hierarkkisen dokumentaatiojärjestelmän, joka on esitelty seuraavassa kuviossa (kuvio 3).

KUVIO 3 Johtamisjärjestelmän dokumentaatiohierarkia, (Boehmer, 2008)

Pyramidimalli edustaa ISO/IEC 27001 -mukaista johtamisjärjestelmää, jossa tietoturva rakentuu niin johtamisen, dokumentaation kuin prosessien mukaisesti ylhäältä alaspäin. Tämä tarkoittaa sitä, että pyramidin yläosassa määritellään riskienhallinnan ja tietoturvapolitiikan avulla tavoitteet, jotka määrittelevät prosesseja, joilla vastaavasti määritellään halutut toimintatavat. Prosessien seurauksena syntyy tietoturvakontrolleja, joilla voidaan hoitaa teknisellä tasolla tietoturvakontrolleille määriteltyjä tehtäviä. Alimpana pyramidissa ovat tuotetut todisteet siitä, että standardin vaatimukset täyttyvät. Todisteiden avulla mahdollistetaan mittaaminen, seuranta ja jatkuva parantaminen. (Boehmer, 2008.) Pyramidi

kuvaa hyvin sitä, mihin johtamisjärjestelmästandardit perustuvat. Johtamisjärjestelmä ei ole tekninen tuote, mutta sen avulla voidaan saavuttaa kattava tietoturvaympäristö niin hallinnollisesti kuin teknisestikin siten, että se ylettää organisaation kaikille tasoille. Pyramidin jokainen taso koskettaa niin ylintä johtoa kuin hierarkian alimpia työntekijöitä. Esimerkiksi tietoturvapolitiikka ja tekniset tietoturvakontrollit, kuten virustorjunta, koskettavat kaikkia organisaation työntekijöitä. Toisaalta organisaation johdon vastuu korostuu johtamisjärjestelmissä, sillä riittämätön tuki ja huono järjestelmän ylläpito vastaavasti vaikuttavat negatiivisesti kaikkiin järjestelmän osa-alueisiin ja sen käyttäjiin. Kuitenkin hyvin ylläpidetyn tietoturvan johtamisjärjestelmän hyöty tietoturvanäkökulmasta on juurikin se, että se auttaa organisaatioita lähestymään tietoturvaa kokonaisvaltaisesti, jolloin tietoturvaa voidaan kehittää ja ylläpitää tehokkaasti.

Lambon (2006) mukaan ISO/IEC 27001 -sertifikaatin avulla organisaatio voi osoittaa sen, että sen tietoturvan johtamisjärjestelmää ylläpidetään säännönmukaisesti ja se noudattaa standardin vaatimuksia. Standardin noudattamisen kautta taas voidaan saada suoria tietoturvahyötyjä, sillä tehokas järjestelmän ylläpito vähentää riskejä, niiden toteutumisen todennäköisyyttä ja vaikutuksia. Toisaalta sertifikaatti voi myös joissain tapauksissa vähentää esimerkiksi tietomurrosta koituvia sakkoja tai maksuja, jos organisaatio voi osoittaa, että sen toimintatavat ovat olleet standardinmukaisia. (Lambo, 2006.) Kansainvälisesti yhteisesti vakiintuneet käytännöt taas yhtenäistävät toimintatapoja. Von Solms (1999) vertaa standardeja ja sertifikaatteja liikennekulttuuriin: Yhdessä sovitut liikennesäännöt määrittelevät halutut ja sallitut toimintatavat ja ajokortti toimii todisteena siitä, että sen haltija on todistetusti läpäissyt liikennesääntöihin perustuvan testin ja tämän oletetaan myös toimivan sääntöjen mukaisesti. Standardit ovat omassa viitekehyksessään verrattavissa yhdessä sovittuihin liikennesääntöihin ja sertifikaatti toimii todisteena siitä, että sen haltija on läpäissyt vaatimuksiin perustuvan testin (auditointi). (Von Solms, 1999.)

Brennerin (2007) mukaan johtamisjärjestelmästandardin implementointi on organisaatiolle hyvä tapa lähestyä tietoturvaa, sillä yrityksen omaisuuseriin kohdistuvat riskit ovat viime kädessä organisaation johdon vastuulla. ISO/IEC 27001 -standardissa korostuukin organisaation johdon sitoutuminen johtamisjärjestelmän toimintaan, sillä johto mahdollistaa riittävät resurssit, varmistaa riskienhallinnan toimivuuden ja varmistaa järjestelmän jatkuvan ylläpidon ja parantamisen. Perusajatuksena onkin, että tietoturva lähtee organisaation ylimmistä rakenteista ja valuu alaspäin, millä varmistetaan tietoturvan omaksuminen organisaation jokaisella tasolla. (Brenner, 2007.) Tietoturvan johtamisjärjestelmä ei kuitenkaan ei tuota tietoturvaa, jos se ei toimi kunnolla. Tehoton tietoturvan johtamisjärjestelmä ei myöskään ole organisaation liiketoiminnalle kannattavaa, jos se ei kykene auttamaan taloudellisia tavoitteita. Sertifikaatti kuitenkin jossain määrin varmistaa sen, että organisaation johtamisjärjestelmä toimii, koska ulkoinen valvonta pakottaa johdon antamaan järjestelmälle riittävät resurssit ja huolehtimaan siitä, että järjestelmää ylläpidetään aktiivisesti ja laadukkaasti, mikä johtaa väistämättä myös parempaan tietoturvan tasoon.

Barlette ym. (2008) esittävät, että yksi ISO/IEC 27001 -standardin mukaisen johtamisjärjestelmän hyötyjä on tietoturvatietoisuuden kasvaminen, joka johtaa parempaan tietoturvan tasoon. Tietoturvatietoisuuden kasvaminen taas parantaa tehokkaasti organisaation tietoturvan kokonaistasoa, sillä tietoturvassa ihminen on usein heikoin lenkki, kun inhimilliset erheet ja ihmisten välinpitämättömyys mahdollistavat monet erilaiset tietoturvaloukkaukset. Puhakainen ja Siponen (2010) esittävätkin, että oikeanlaisella tietoturvan kouluttamisella voidaan parantaa ihmisten tietoturvakäyttäytymistä ja näin ollen parantaa koko organisaation tietoturvan tasoa. Tietoturvakoulutuksen täytyy kuitenkin olla mielekästä ja kohderyhmälle suunniteltua, jotta se on hyödyllistä. Lisäksi tietoturvan jatkuva kommunikointi organisaatiossa parantaa tietoturvaohjeistuksen omaksumista ja luo parempaa tietoturvakulttuuria organisaatiossa. (Puhakainen ja Siponen, 2010.)

3.2 Johtamisjärjestelmäsertifioinnin haasteet

Yrityksen perimmäinen tehtävä on tavoitella voittoa, joten on loogisesti ajateltuna perusteltua olettaa, että sertifikaatti hankitaan taloudellisin perustein taloudellisen hyödyn saamiseksi. Mutta tuottaako sertifiointi kuitenkaan rahaa? Esimerkiksi Barletten ym. (2008) mukaan ISO 9000 -laatusertifikaatti, joka on myös johtamisjärjestelmäperusteinen ISO/IEC 27001:n tapaan, nostaa yrityksen osakkeen arvoa pörssissä. Hsu, Wang ja Lu (2016) tekivät tutkimuksen, jossa he tutkivat ISO/IEC 27001 -sertifikaatin taloudellisia vaikutuksia organisaation tulokseen vertaillen sertifioituja ja sertifioimattomia organisaatioita. Hypoteesit olivat, että ISO/IEC 27001 -sertifiointi assosioituu positiivisesti organisaation taloudellisen tuloksen kanssa ja se, että ISO/IEC 27001 -sertifiointi vaikuttaa positiivisesti organisaation menestykseen osakemarkkinoilla. Hypoteesien perusteena oli olemassa oleva tutkimus ISO 9001 -laatujärjestelmän tuottavuudesta, koska ISO 9001 -järjestelmän toiminta-ajatus on hyvin samantyyppinen ISO/IEC 27001 -standardin mukaisen johtamisjärjestelmän kanssa. Hypoteeseja tutkittiin kahdella mittarilla: koko pääoman tuottoasteella (Return on Assets, ROA) ja osta-japidä -sijoitusstrategian mukaisilla epänormaalien tuottojen avulla (buy-and-hold abnormal returns, BHAR). Tutkimukseen valittiin ympäri maailmaa niin sertifioituja kuin sertifioimattomia organisaatioita, joiden taloudellista menestystä mitattiin 2 vuotta ennen ja jälkeen sertifioinnin. Tutkimuksen tuloksena tuli ilmi, että kumpikaan mittari ei tarjonnut tilastollisesti merkittävää tukea hypoteeseille, joten suoraa taloudellista hyötyä sertifioinnista ei löytynyt. Tutkijoiden mukaan tämä selittyy sillä, että tietoturvan johtamisjärjestelmän tehtävä on puhtaasti puolustuksellinen, eli estää suurempia tappioita, kun taas laatujärjestelmien, kuten ISO 9001, tehtävä on parantaa tuotteiden laatua ja sen kautta asiakaskokemusta, joka taas lisää organisaation tuloja. Täten ISO/IEC 27001 -sertifioinnin tuottoa ei voi siis mitata rahassa tai tuottavuudessa, sillä onnistunut implementointi ei sellaisenaan tuota rahaa, vaan varmistaa sen, että organisaatio toimii niin kuin sen odotetaankin toimivan. Toisaalta Hsu ym. (2016) myös nostivat esille

sen, että tutkittavat organisaatiot eivät olleet sertifioineet koko organisaatiota, vaan vain osan siitä, jolloin vaikuttavuus ei ole yhtä suuri. (Hsu ym., 2016.)

Tutkimus osoittaa tietoturvainvestointien mittaamisen haasteellisuuden, sillä tietoturvainvestoinnilla ei ole suoraa korrelaatiota tuottoon. Olemassa oleva tutkimus on pyrkinyt etsimään tähän ongelmaan ratkaisuja, josta hyvänä esimerkkinä toimii Boehmerin (2009) kehittämä ISO/IEC 27001:n tehokkuuden mittaamiseen käytettävä suorituskykyindikaattoreihin perustuva teoria. Hsun ym. (2016) tutkimuksessa kuitenkin todettiin myös se, että sertifiointi takaa sen, että organisaatio toimii niin kuin sen odotetaankin toimivan, jolloin sertifiointia voidaan pitää eräänlaisena perusedellytyksenä markkinoilla toimimisessa. Täten sertifioinnin vaikutuksia voidaan pitää taloudellisesti positiivisena, koska lisääntynyt luotettavuus ja sen seurauksena syntyvä potentiaalisten tappioiden estäminen antaa positiivisen viestin organisaation toiminnasta, mikä taas pitkällä aikavälillä mitattuna tuottaa positiivisia vaikutuksia. Tiiviisti kilpailulla alalla organisaatioilla ei ole varaa joutua tietoturvaloukkauksen kohteeksi, sillä maineen menetys ja muut johdannaisvaikutukset voivat vaikuttaa organisaation tulokseen ja toimintaan vielä pitkään. Näitä kenties piilossa pysyviä positiivisia vaikutuksia voi kuitenkin olla vaikea perustella organisaation johdolle, sillä Barletten ym. (2008) mukaan tietoturvalla on samanlainen asema kuin ICT-infrastruktuurilla: Sitä ajatellaan vain sen pettäessä. Ristiriitaista Hsun ym. (2016) kanssa on kuitenkin se, että useat muut lähteet puoltavat sitä, että sertifiointi lisää myös organisaation tarjoamien palveluiden kysyntää ja parantaa organisaation mainetta luotettavana kumppanina. Toisaalta sertifikaatin merkitys suuremmilla yrityksillä, kuten pörssiyhtiöillä voi olla pienempi, koska suuren yrityksen uskottavuus tulee osittain pelkästään suuresta koosta, ja sertifikaatin vaikutus näin ollen pienenee. Lisäksi tietoturva on nykyisin osa kaikkia organisaatioita, joten sertifiointi ei välttämättä ole enää tapa erottautua kilpailijoista, vaan tapa osoittaa, että tietoturvaa hoidetaan asianmukaisesti. On kuitenkin hyvä huomata, että esimerkiksi organisaation suuri koko ei takaa sitä, että tietoturvaloukkaukset eivät vaikuttaisi organisaatioon. Campbell ym. (2003) totesivat jo vuonna 2003, että tietomurroilla voi olla negatiivisia vaikutuksia pörssilistatun organisaation osakkeen arvoon ja sama pätee myös nykyisin, sillä Stepanoksen ja Angelisin (2016) tutkimuksen mukaan tietomurto vaikuttaa lähes poikkeuksetta negatiivisesti tietomurron kohteeksi joutuneen yrityksen osakkeen arvoon.

Sertifikaatin hankkimiseen liittyy kustannuksia, jotka voivat olla ratkaiseva tekijä sille, että hankitaanko sertifikaatti vai ei. Kuten aiemmin todettiin, sertifikaatin hankkimiseen liittyvät kustannukset jakautuvat johtamisjärjestelmän pystyttämiseen ja sertifioinnin hankintaan ja ylläpitämiseen meneviin kustannuksiin. Barlette ym. (2008) esittävät, että erityisesti pienemille organisaatioille kustannukset saattavat olla liian korkeat. Toisaalta tietoturvasertifikaattien yleisyys lisääntyy koko ajan, joten markkinoilla tapahtuu koko ajan muutosta siihen suuntaan, että kaikkien markkinoilla toimivien organisaatioiden täytyy hankkia sertifiointi pysyäkseen kilpailussa mukana. Kuten It Governancen (2018a) kyselyssä kuitenkin todettiin, kokivat kuitenkin useimmat organisaatiot investoinnin hyödyllisenä, ja toisaalta johtamisjärjestelmän ja sertifioinnin kustannukset ovat

suhteutettuna hyötyyn ja potentiaaliseen tappioon hyvin kohtuulliset. Sharman ja Dashin (2012) mukaan etenkin sellaiset organisaatiot, joilla ei ole vahvaa kokemusta tietoturvasta, tekevät investointipäätöksiään usein riittämättömällä osaamisella. Tämä johtaa siihen, että investointipäätökset tietoturvaan tehdään intuitiolla, eikä investointipäätöksien taloudellisia syitä voida perustella mitenkään. Yleensä huono investointi johtuu riittämättömästä kokemuksesta ja riskienhallinnan osaamattomuudesta (Sharma ja Dash, 2012.) Täten on todennäköistä, että etenkin johtamisjärjestelmän pystytysvaiheessa kokemattomilla organisaatioilla voi olla hankaluuksia pitää kustannukset kurissa.

Tietoturvan näkökulmasta sertifikaatin hankkimisprosessissa haasteellista organisaation näkökulmasta on se, että organisaatio voi saavuttaa sertifikaatin, mutta todellisuudessa prosessien ja toimintatapojen jalkauttaminen organisaatioon on haastavaa. Tätä Siponen (2006) selittää sillä, että tietoturvastandardit keskittyvät pääsääntöisesti siihen, että itse prosessi on olemassa, mutta ne eivät määrittele prosessin sisältövaatimuksia tarpeeksi tarkasti. Hsun (2009) tutkimuksessa kyseinen ongelma tuli varsin selkeästi esille organisaation eri tasojen välisessä vertailussa. Organisaation johto oli varsin tyytyväinen sertifiointiprosessiin ja piti sertifikaatin savuttamista erittäin onnistuneena projektina, mutta organisaation alemmissa kerroksissa sertifikaatin tuomat velvoitteet nähtiin lähinnä omaa työtä haittaavina ja ylimääräistä vaivaa aiheuttavina. Tutkimus osoitti hyvin sen, että vaikka organisaation johto koki saavutetut hyödyt suurina ja johto oli standardin vaatimusten mukaisesti erittäin sitoutunut johtamisjärjestelmän toimintaan, ei se taannut tietoturvakontrollien noudattamista organisaation alemmilla tasoilla. Esimerkiksi tietoturvakoulutus nähtiin epäolennaisena ja tylsänä, sekä jotkin tietoturvakontrollit koettiin niin työtä haittaaviksi, että niiden noudattamatta jättäminen oli hyvin yleistä. (Hsu, 2009.) Tämä osoittaa sen, että sertifikaatti ei ole oikotie tietoturvan jalkauttamiseksi. Siihen tarvitaan tietoturvalähtöisen organisaatiokulttuurin kehittämistä, joka voidaan toteuttaa esimerkiksi hyvällä tietoturvakoulutuksella. Puhakaisen ja Siposen (2010) mukaan henkilöstön tietoturvatietoisuus paranee parhaiten jatkuvalla kouluttamisella, joka vaatii myös johdon vahvaa sitoutumista. Koulutuksen tulisi kuitenkin olla työtehtäviin ja osaamiseen nähden relevanttia ja koulutuksessa tulisi pyrkiä jatkuvaan ja osana muuta viestintää tapahtuvaan kouluttamiseen, jolloin tietoturva ei jää irralliseksi kokonaisuudekseen. Tietoturvan kannalta standardien ongelmaksi kiteytyy juurikin aiemmin mainittu keskittyminen prosessiin, eikä sen sisältöön. Siponen (2008) käyttää esimerkkinä jo käsiteltyä tietoturvakoulutuksen ongelmaa. Standardi vaatii, että organisaatiolla on tietoturvatietoisuutta lisäävä ohjelma, joka voi sisältää esimerkiksi tietoturvakoulutusta. Se, että työntekijät käyvät tietoturvakoulutuksen, ei vielä takaa sitä, että työntekijät myös omaksuvat opetetut käytännöt osaksi työntekoa, vaikka standardin vaatimus tietoturvatietoisuuden lisäämisestä täyttyykin. (Siponen, 2008.)

Sertifiointiprosessi vie aikaa, sillä johtamisjärjestelmän pystyttäminen ja sertifioiminen ei tapahdu hetkessä. Distererin (2013) mukaan ISO/IEC 27001 -standardin mukaisen johtamisjärjestelmän pystyttäminen vie organisaation osaamisen mukaan muutamista kuukausista useisiin vuosiin, johon lisätään

vielä sertifiointiprosessiin kuluvat muutamat kuukaudet. Lisäksi organisaation koosta ja kompetenssista riippuen järjestelmän implementointi ja sertifiointi kuluttaa resursseja, joiden varalle organisaatioiden on budjetoitava riittävästi rahaa. Tutkimukset kuitenkin osoittavat, että kokonaisarvion mukaan sertifiointi on organisaatiolle kannattavaa. Selkein todiste tästä on sertifiointien hankkimisen jo vuosia jatkunut kasvava trendi, sillä jos organisaatiot eivät kokisi sertifiointia kannattavaksi, ei sertifikaatteja myöskään myönnettäisi tai ylipäätään ylläpidettäisi. Sertifikaatti ei kuitenkaan itse tuota mitään mutta sillä on kuitenkin suoria ja epäsuoria talous- ja tietoturvavaikutuksia. Sertifikaatti on markkinointiväline, joka mahdollistaa uusien asiakkuuksien saamisena ja edistää kilpailuetua. Sertifikaatti toimii myös todisteena tietoturvan johdonmukaisesta kehittämisestä ja organisaation suhtautumisesta tietoturvaan tärkeänä osana organisaation johtamista ja toimintaa.

3.3 Sertifiointielimen valintaperusteet

Sertifiointielimen valinta pitäisi teoriassa olla merkityksetöntä, sillä auditoinnin tulisi olla puolueetonta ja lopputuloksen tulisi olla aina sama auditoijasta riippumatta. Kuitenkaan käytännössä näin ei ole, sillä sertifiointi on bisnestä ja näin ollen siihen vaikuttavat kilpailulliset tekijät. Aiheeseen liittyvää teoreettista tutkimusta on vielä melko rajoitetusti, mutta aukkoa paikkaavat joidenkin kaupallisten toimijoiden tuottama kokemuspohjainen sisältö valintaperusteisiin vaikuttavista tekijöistä.

ISO Globalin (2019) mukaan hinta on tekijä, jossa voi olla suurta vaihtelua. Hinta on kilpailuttamisen kannalta usein merkittävä tekijä, sillä organisaation intresseissä voi olla saada sertifikaatti mahdollisimman halvalla, jolloin investoinnin kustannus suhteessa hyötyyn paranee. Hinnan merkitys korostuu siinä mielessä paljon, että sertifikaatin elinkaareen sisältyvät vuosittaiset auditoinnit, jotka aiheuttavat kustannuksia vuosittain sertifikaatin hankkimisesta lähtien. (ISO Global, 2019.) Jos organisaation johto ei pidä sertifikaatin merkitystä kovinkaan suurena, voi tällöin hinnan merkitys olla suuri sertifiointielintä valitessa. Jahn, Schramm ja Spiller (2005) toteavat, että sertifiointielimet käyvät markkinoilla ankaraa hintakilpailua, jossa auditointeja saatetaan myydä pahimmillaan jopa tappiollisena. Tämä johtuu siitä, että auditointibisneksessä asiakassuhteet tyypillisesti kestävät useampien vuosittaisten auditointien ajan, jolloin voittomarginaalia voidaan kasvattaa vuosien mittaan, kun asiakassuhde syvenee. Toisaalta tämä taas aiheuttaa sertifiointielimille painetta laskea auditointien kustannuksia alas, jolloin auditoinnin laatu saattaa heikentyä, kun auditointi pitää saada tehtyä tehokkaasti. (Jahn ym., 2005.)

Kuitenkaan hinta ei ole ainoa sertifiointielimen valintaa määräävä tekijä, sillä rahalle täytyy myös saada vastinetta. Kosuticin (2018) mukaan myös maine, kokemus ja erikoisosaaminen ovat tekijöitä, jotka sertifiointielintä valitsevan organisaation tulisi ottaa huomioon. Sertifikaatin tehtävänä on olla markkinointikeino, joten sertifiointiin kannattaa valita kokenut ja hyvämaineinen

sertifiointielin. Täten se nostaa myös sertifikaatin arvoa, sillä hyvämaineisen ja kokeneen sertifiointielimen myöntämä sertifikaatti voi olla parempi todiste asianmukaisesta auditoinnista kuin täysin tuntemattoman sertifiointielimen myöntämä sertifikaatti. Auditoijan kokemus on myös muilla tavoilla hyödyllistä. Kokenut auditoija osaa etsiä kehityskohteita oikeista paikoista, mikä mahdollistaa johtamisjärjestelmän kehittämisen. Lisäksi sertifiointielimellä voi olla myös esimerkiksi toimialaan tai teknologiaan liittyvää erikoisosaamista, joka voi erottaa ne muista sertifiointia tarjoavista sertifiointielimistä. Sertifikaattia hankkivan organisaation kannattaa myös miettiä sitä, hankkiiko se sertifikaatin akkreditoidulta sertifiointielimeltä, sillä akkreditointi ei ole pakollista. Tämä tarkoittaa sitä, että kenellä tahansa on oikeus myöntää sertifikaatteja. Akkreditoidulta toimijalta sertifikaatin hankkiminen on osoitus siitä, että auditointi on suoritettu asianmukaisesti ja täten nostaa sertifikaatin arvoa. (Kosutic, 2018.)

Edellä mainittujen hinnan ja erilaisten auditoinnin laatuun vaikuttavien tekijöiden lisäksi on myös muita tekijöitä, jotka vaikuttavat sertifiointielimen valintaan. Kosuticin (2018) mukaan sertifiointielimien akkreditointialueeseen kuuluu usein muitakin standardeja, jolloin voi olla mahdollista auditoida samalla useita eri standardeja. Tällaisessa järjestelyssä on suora rahallinen etu, kun jokaista johtamisjärjestelmää tai standardia ei tarvitse erikseen auditoida, mutta siinä voidaan saavuttaa myös ajallista hyötyä, sekä yksinkertaistaa ja yhtenäistää järjestelmien toimintaa. Käytännöllisinä asioina sertifiointielimen valintaan voivat vaikuttaa yhteinen kieli, sekä maantieteellinen sijainti. Vaikka ulkomaisen auditoijan voisi saada halvemmalla, ei välttämättä ole järkevää lennättää auditoijaa paikalle, jos toinen vaihtoehto on ottaa paikallinen ja yhteisen kielen omaava auditoija, jonka kanssa käytännön järjestelyistä on helpompi sopia ja joustaa. (Kosutic, 2018.)

Wiander (2008) tutki auditoitavien organisaatioiden henkilöstön tuntemuksia eri auditointien vaiheessa, ja tutkimuksen tulokset tukevat edellä mainittuja valintatekijöitä. Esimerkiksi auditoijan valmistautuminen auditointiin ja ammattitaito auditoinnin aikana koettiin auditointikokemusta parantavana tekijänä, sillä auditoivat kykenivät muun muassa havainnoimaan omia kehityskohteitaan auditoinnin aikana, vaikka auditoija ei suoria kehitysehdotuksia antanutkaan. Vastaavasti heikosti alaa ja auditoitavaa asiakasta tuntenut auditoija koettiin huonoksi, sillä hän ei kyennyt huomaamaan selkeitä epäkohtia organisaation johtamisjärjestelmässä. (Wiander, 2008.)

Prajogo ja Castka (2015) tutkivat omassa tutkimuksessaan valitun sertifiointielimen vaikutuksia ISO 9000 -laatujärjestelmästandardin kontekstissa. Tutkimus on sikäli mielenkiintoinen, että vaikka vastuu järjestelmän implementoinnista ja ylläpitämisestä on auditoitavalla organisaatiolla, voi osaava auditoija vaikuttaa järjestelmän tuottamiin hyötyihin. Tarkemmin tarkasteltuna tulokset eivät kuitenkaan ole mitenkään yllättäviä. Kuten jo aiemmin todettiin, auditoijan laadukkuus edesauttaa järjestelmän kehittämistä ja näin ollen järjestelmän operatiivinen toiminta kehittyy. Taloudellisen vaikutuksen merkitys on kuitenkin vaikutuksista mielenkiintoisempi. Tutkimuksen mukaan sertifiointielimen laadukkuus ja imago markkinoilla vaikuttaa sen sertifioimiin asiakkaisiin positiivisesti.

Näin ollen se hyödyttää molempia osapuolia: sertifiointielimestä tulee houkuttelevampi, kun taas sertifiointielimen myöntämän sertifikaatin arvo nousee. (Prajogo & Castka, 2015.)

Sertifiointielimen valintaan vaikuttaa siis useampi tekijä kuin pelkkä hinta, ja sertifiointielimen valinnassa tulisi noudattaa kokonaisarviota saavutettavista hyödyistä. Vaikka auditointitulos olisi kahdella eri hintaisella sertifiointielimellä sama, ei se silti tarkoita, että auditointi olisi täysin samanlainen. Laadukkuus ja kokemus voivat auttaa auditoitavaa kehittämään tietoturvaa, mutta rahassa mitattuna kalliimpaa auditoijaa voi olla hankala perustella johdolle, jos lopputulos on sama. Olemassa oleva tutkimus liittyen aiheeseen on kuitenkin melko vähäistä, joten tutkimuksen kannalta sertifiointielimen valintaperusteiden selvittäminen on erittäin mielenkiintoista, jotta kysymykseen saadaan tarkempia vastauksia.

4 TUTKIMUKSEN ETENEMINEN

Neljäs luku paneutuu tutkimuksen empiiriseen osuuteen. Ensimmäisenä keskitytään yleisesti tutkimuksen empiirisen osion teorian kuvaamiseen. Se käsittää tutkimuksessa käytettävän tutkimusmenetelmän kuvaamisen esittelemällä tutkimusmenetelmän erilaiset soveltamistavat ja tutkimusmenetelmän rajoitteet. Tämän jälkeen edetään tämän tutkimuksen toteutuksesta kertovaan alalukuun, joka käsittelee tehdyn tutkimuksen toteutustavan ja viimeisenä analysoidaan tehdyn tutkimuksen reliabiliteettia ja validiteettia, joilla voidaan analysoida tutkimuksen luotettavuutta ja tulosten merkitsevyyttä.

4.1 Tapaustutkimus tutkimusmenetelmänä

Tämä tutkimus toteutettiin laadullisena tutkimuksena. Laadullista tutkimusta voi tehdä useilla eri menetelmillä, mutta kenties käytetyin menetelmä on tapaustutkimus, jota sovellettiin myös tässä tutkimuksessa. Saaranen-Kauppisen ja Puusniekan (2009) mukaan tapaustutkimuksen pyrkimyksenä on tutkia rajattua tapahtumaa tai useita tapahtumia käyttämällä monipuolisilla ja eri menetelmillä hankittuja tietoja. Tutkimus siis pyrkii tutkimaan, kuvaamaan ja selittämään tapauksia miten- ja miksi-kysymysten avulla. Tapausten tarkastelussa kiinnostuksen kohteena on usein tapauksiin liittyvät prosessit ja ilmiöt, joita pyritään tarkastelemaan niiden luonnollisessa ympäristössä. Kuvailevat menetelmät eivät kuitenkaan välttämättä pyri selittämään täydellisesti ilmiöiden välisiä yhteyksiä, testaamaan hypoteeseja tai tekemään ennusteita, vaan pyrkivät tutkimuskohteiden ominaispiirteiden systemaattiseen ja totuudenmukaiseen kuvailuun. (Saaranen-Kauppinen ja Puusniekka, 2009.) Tapaustutkimuksen keskiössä ovat tapaukset, eli tutkittavat yksiköt. Erikssonin ja Koistisen (2014) mukaan tapauksen määritelmiä on olemassa useita, mutta tärkeintä on se, että tapauksen voi rajata muusta kontekstista selkeästi. Tapaukset ovat rajattuja systeemejä, kuten yksilöt, ryhmät ja ohjelmat. Tapaukset voivat olla myös hankalammin määriteltäviä, kuten erilaiset prosessit, mutta tärkeintä on kuitenkin se, että tutkimukseen valittujen tapausten valinta perustellaan tutkimuksen kontekstissa. (Eriksson ja Koistinen, 2014). Tapaukset täytyy myös osata rajata siten, että tutkimuksesta ei tule liian laaja. Baxterin ja Jackin (2008) mukaan hyviä keinoja tapausten rajaamiseen on rajata tapauksia esimerkiksi ajan ja paikan mukaan, ajan ja aktiviteettien mukaan, tai määritelmien ja kontekstin avulla. Valintatavasta riippumatta on tärkeää se, että valitut tutkimukset ovat ominaisuuksiltaan oikeanlaisia tapaustutkimuksen tekemiseen, jotta tutkimuksen tulokset vastaavat tutkimuskysymyksiin. (Baxter & Jack, 2008.)

Tieteellistä tutkimusprosessia voi lähestyä joko teoriaa testaavalla (deduktiivinen) tai teoriaa todisteista synnyttävällä (induktiivinen) tutkimuksella. Tutkimusmenetelmä täytyy perustella riittävän hyvin, sillä se lisää tutkimuksen

luotettavuutta. Eisenhardtin ja Graebnerin (2007) mukaan perinteisesti deduktiivinen tutkimus on ollut suositumpaa, koska sen käyttäminen on helposti perusteltavissa. Eisenhardtin ja Graebnerin (2007) mukaan induktiivinen tapaustutkimus on kuitenkin erinomainen tutkimusmenetelmä, sillä se on yksi parhaista tavoista yhdistää laaja kvalitatiivinen todistusaineisto valtavirran deduktiiviseen tutkimukseen. Tällöin tapauksista tuotettu teoria on todennäköisesti tarkkaa, testattavissa ja mielenkiintoista. Edellä mainitut ominaisuudet syntyvät juurikin induktiivisen tutkimusprosessin tuotteena, sillä tapausten tutkiminen selvittää jotain olemassa olevaa ilmiötä ja ongelmaa, ja vastaavasti ilmiön tutkiminen sopivilla tapauksilla mahdollistaa sen testaamisen ja vahvistaa käsitystä teorian tarkkuudesta. (Eisenhardt & Graebner, 2007.)

Tapaustutkimuksen soveltuvuus täytyy kuitenkin varmistaa, jotta sitä voidaan luotettavasti käyttää. Erikssonin ja Koistisen (2014) mukaan tapaustutkimus kannattaa valita tutkimuksiin, joissa jotkin tai useat seuraavista ehdoista täyttyvät:

- ’Mitä-’, ’miten-’ ja ’miksi-’kysymykset ovat keskeisellä sijalla.
- Tutkijalla on vähän kontrollia tapahtumiin.
- Aiheesta on tehty vain vähän empiiristä tutkimusta.
- Tutkimuskohteena on jokin tämän ajan elävässä elämässä oleva ilmiö.

Tässä tutkimuksessa kaikki edellä mainitut kohdat täyttyivät, sillä tutkimuskysymykset ovat ’mitä-’ ja ’miksi-’kysymyksiä ja pyrkivät etsimään vastauksia tapauksiin liittyvän ilmiön syihin. Lisäksi tutkijalla ei ollut tutkittaviin tapahtumiin mitään kontrollia, vaan tutkija tutki tapahtumia ulkopuolelta ilman vaikutusta tapausten käyttäytymiseen. Aiheesta on lisäksi hyvin vähän aikaisempaa empiiristä tutkimusta ja tutkittava tutkimuskohde on elävässä elämässä oleva ilmiö, sillä tutkimusongelma on luotu markkinoilla olevan ongelman selvittämiseksi.

Tapaustutkimus ei kuitenkaan ole mikään yksittäinen tarkoin määriteltymenetelmä, vaan siihen kuuluu erilaisia tyyppejä, joilla tapauksia voidaan tutkia. Tapaustutkimus voidaan jakaa esimerkiksi kuvailevaan ja selittävään tutkimukseen. Erikssonin ja Koistisen (2014) mukaan kuvaileva tutkimus pyrkii tiheän kuvauksen tuottamiseen, jossa tarkoituksena on kertoa tapahtumaan liittyvistä kulttuurisista merkityksistä. Kuvaileva tutkimus voi myös keskittyä kuvaamaan havaittua tai innovatiivista käytäntöä arkipäivän tilanteessa. Toinen menetelmä on selittävä tutkimusmenetelmä. Selittävä tutkimus pyrkii selittämään tapausta ja syitä siihen miksi tapaus on juuri sellainen kuin se on. Selittävä tutkimus on myös kiinnostunut selittämään tosielämän monimutkaisten tapahtumien välisiä kausaalisia suhteita tai niihin liittyviä mekanismeja. (Eriksson ja Koistinen, 2014.) Tapaustutkimus viittaa nimensä mukaisesti vain yhteen tapaustutkimukseen, mutta tapauksia voi olla myös monia, jolloin menetelmää kutsutaan monitapaustutkimukseksi. Baxterin ja Jackin (2008) mukaan monitapaustutkimuksen ero yksittäisen tapauksen tutkimiseen on se, että monitapaustutkimuksessa tutkittavia tapauksia on useita ja jokaisella tapauksella on erilainen konteksti, joka tuottaa

hieman erilaisia tuloksia. Useita tapauksia voidaan käyttää joko tuottamaan samanlaisia tuloksia, jolloin kontekstin vaikutus ei muuta tulosta, tai vastaavasti tuottamaan eroavaisia tuloksia, jolloin kontekstin merkitys vaikuttaa myös lopputulokseen. Monitapaustutkimus tuottaa sellaisenaan usein luotettavampia tuloksia kuin yhden tapauksen tutkiminen, mutta on paljon kalliimpaa ja aikaa vievää. (Baxter & Jack, 2008.)

Tutkimusprosessina tapaustutkimus on selkeä ja etenee loogisesti vaihe kerrallaan. Eisenhardtin (1989) mukaan teorian muodostaminen tapauksista tapahtuu kahdeksanvaiheisen prosessin mukaisesti. Aloitusvaiheessa määritellään tutkimusongelma ja -kysymykset sekä tarvittavat käsitteet. Tutkimusongelmaan pitää valita sopivat tutkittavat tapaukset, joita voi olla joko yksi tai useampi. Yhden tapauksen tutkimuksissa tapaus täytyy olla ongelmaan erityisen hyvin sopiva ja perusteltu, kun taas monia tapauksia käsitellessä on mahdollisuus tuoda ilmi tapauksien eroja ja yhteneväisyyksiä. Tapausten valintaan voi käyttää tilastollisia menetelmiä, mutta yleisempää on valita tutkimusongelmaan hyvin sopivia tapauksia. (Eisenhardt, 1989.) Eisenhardtin ja Graebnerin (2007) mukaan tapausten valintaan on hyvä soveltaa teoreettista otantaa, sillä tapaustutkimuksen tavoitteena on tuottaa teorioita, eikä testata niitä. Tyypillistä on siis valita mahdollisimman hyvin ongelmaan sopiva tapaus. Monien tapausten kohdalla teoreettisen otannan suorittaminen on kuitenkin haastavampaa, sillä valinta ei välttämättä perustu tapauksen uniikkiin luonteeseen, vaan tuotettavan teorian tukemiseen. Käytännössä se tarkoittaa sitä, että tutkimukseen valitaan tapauksia, jotka tuottavat keskenään identtisiä vastauksia, kehittävät teoriaa pidemmälle, eliminoivat kilpailevia teorioita tai tuottavat vastakkaisia tuloksia vertailun tekemiseksi. (Eisenhardt & Graebner, 2007.)

Eisenhardtin (1989) mukaan tapausten valinnan jälkeen tutkimusprosessissa valitaan tutkimukseen sopivat tiedonkeruumenetelmät, joita laadullisessa tutkimuksessa ovat usein haastattelut, dokumentaation tutkimus ja havainnointi. Lisäksi tutkimukseen voidaan yhdistellä kvantitatiivista tutkimusta. Kun sopivat tiedonkeruumenetelmät on määritetty, voidaan mennä kentälle tekemään tutkimusta, jossa kerätään valituilla menetelmillä dataa. Datan keräämisen jälkeen data täytyy analysoida. Datan analysointiin on olemassa erilaisia menetelmiä, mutta tutkimuksen tulosten kannalta tärkeintä on löytää mielenkiintoiset tiedot mahdollisesti suurista määristä dataa. Analyysi voi tapahtua tutkimalla tarkemmin yksittäisiä tapauksia ja niiden piirteitä, tai tapauksista voidaan koittaa laajemmin tutkimalla etsiä keskenään yhteneviä malleja, jotka ovat tutkimuksen kannalta kiinnostavia. Datan analyysin jälkeen hiotaan hypoteesia, joka tehdään data-analyysin pohjalta Hypoteesin muotoilu auttaa muun muassa löytämään vastauksia 'miksi'-kysymyksiin. Lopuksi tuloksia verrataan olemassa olevaan kirjallisuuteen, josta koitetaan etsiä yhteneväisiä tuloksia tai ristiriitaisia tuloksia. Tutkimus päätetään, kun riittävän kattava tulos on saatu ja tapausten lisääminen tutkimukseen ei tuota merkittävää lisäarvoa. (Eisenhardt, 1989.)

Tapaustutkimusten haasteena pidetään yleistettävyyden haastetta. Erikssonin ja Koistisen (2014) mukaan yleistämisen ongelma liittyy nimenomaisesti tilastolliseen yleistämiseen, sillä tapaustutkimus keskittyy yleensä yhden tai

muutaman tapauksen tutkimiseen, jolloin koko populaatiota kuvaavan luotettavan tilastollisen yleistämisen tekeminen on lähes mahdotonta. Tapaustutkimuksessa voidaan kuitenkin pyrkiä analyyttiseen yleistämiseen, jonka tarkoitus on tutkimuksessa luotujen teoreettisten käsitteiden ja mallien avulla selittää uusia tapauksia, joka taas auttaa ymmärtämään ja selittämään laajempia joukkoja tapauksia. (Eriksson & Koistinen, 2014.) Flyvbjerg (2006) toteaa muun muassa monen fysiikan lain syntyneen yksittäisten tapausten testaamisesta, mutta korostaa kuitenkin myös sitä, että tapausten täytyy olla tutkittavaan ongelmaan hyvin sopivia. Tapaustutkimuksen liittyy myös kuitenkin muitakin haasteita. Tutkimusta voi tehdä teoriaa luovalla tutkimuksella induktiivisesti tai teoriaa testaavalla tavalla deduktiivisesti. Tapaustutkimukset pyrkivät usein etsimään uutta tietoa tutkittavista ilmiöistä, jolloin teorian luominen tapausten pohjalta täytyy perustella hyvin, sillä tutkimustapaa pidetään perinteisesti huonompana tapana tuottaa teorioita. Eisenhardtin ja Graebnerin (2007) mukaan teorioiden tuottaminen tapauksista ei ole yhtä tarkkaa, objektiivista ja täsmällistä kuin laajamittainen hypoteesien testaaminen. Heidän mukaansa ongelman yksi tärkeimmistä vastauksista on tutkimuskysymyksen hyvä perustelu sekä selitys siitä, miksi olemassa oleva teoria ei kykene vastaamaan ongelmaan. Kilpailevan teorian tuottaminen ei kuitenkaan sellaisenaan riitä, vaan tutkimusongelman on oltava kohderyhmälle erityisen kiinnostava ja toisaalta täytyy myös pystyä osoittamaan, että olemassa oleva tutkimus ei tarjoa vastausta ongelmaan tai vastaus on potentiaalisesti epätosi. (Eisenhardt & Graebner, 2007.)

4.2 Tutkimuksen toteutus

Siponen ja Baskerville (2018) toteavat, että tietojärjestelmätieteessä tietoturvaan liittyvä tutkimus on perinteisesti noudattanut kaavaa, jossa tutkimuksen lähtökohtana on jokin käytännön ongelma, jonka ratkaisemiseksi ehdotetaan hypoteesia tai teoriaa. Ehdotettua teoriaa pyritään empiirisesti todistamaan teorian/hypoteesin todentamiseksi. (Siponen & Baskerville, 2018.) Tämä tutkimus noudattaa osin tätä kaavaa, sillä tutkimuksen avulla pyritään todentamaan olemassa olevan tutkimuksen tuottaman teorian toimivuutta, mutta toisaalta tapaustutkimukselle tyypilliseen tyyliin tutkimus myös tuottaa uutta teoriaa aihepiiristä.

4.2.1 Tutkittavien tapausten valinta

Eisenhardtin (1989) mukaan monitapaustutkimuksessa on yleensä toimivinta tutkia neljästä kymmeneen tapausta. Alle neljä tapausta ei yleensä ole tarpeeksi tuottamaan tarpeeksi monipuolista teoriaa, mutta toisaalta yli kymmenen tapauksen tutkimisesta tuotettu data saattaa käydä liian kompleksiseksi ja näin ollen kokonaisuuden hallinta käy hankalaksi. (Eisenhardt, 1989.) Tämän perusteella tutkimukseen valikoitui tutkittavaksi viisi tutkimusasetelmaan sopivaa tapausta. Tutkittavia tapauksia, eli kohdeorganisaatioita, lähdettiin kartoittamaan

tunnetuista ISO/IEC 27001 -sertifioiduista organisaatioista hyödyntäen olemassa olevia kontakteja ja verkon hakukoneita. Jälkimmäinen tapa löytää kohdeorganisaatioita perustui siihen, että monet organisaatiot mainostavat sertifikaattejaan verkkosivuillaan ja näin ne löytyvät usein hakukoneella haettaessa. Lisäksi sertifioituja organisaatioita ja niiden sertifikaatin voimassaoloa etsittiin ja varmistettiin sertifikaattihaulla, jota osa sertifiointielimistä tarjoaa vapaasti, johtuen akkreditoitujen sertifiointielimien toimintaa ohjaavan ISO/IEC 27021 -standardin vaatimuksesta sertifikaattitietojen julkisuudesta.

Valituille kohdeorganisaatioille asetettiin tietyt vaatimukset, jotka niiden täytyi täyttää, jotta ne sopisivat tutkimuksen tarkoitukseen ja vastaisivat tutkimusongelmaan mahdollisimman hyvin. Ensimmäinen valintakriteeri oli se, että kohdeorganisaatio on tehnyt päätöksen ISO/IEC 27001 -sertifioinnin hankkimisesta ja tällä hetkellä myös ylläpitää riippumattoman kolmannen osapuolen tarjoamaa sertifiointia. Toinen edellytys tutkimusorganisaatiolle oli se, että sillä täytyy olla toimintaa Suomessa ja sertifikaatissa mainittujen toimintojen täytyy olla ainakin osittain Suomessa. Edellytyksen syy on tutkimuksen kontekstissa, sillä tämän tutkimuksen rajoitteissa ei ollut tarkoituksenmukaista laajentaa tutkimusta ulkomaille, sillä Suomessa on riittävä populaatio tutkimuksen tekemiseksi. Tuloksissa tämä kuitenkin täytyy huomioida, sillä vaikka osa kohdeorganisaatioista oli kansainvälisiä toimijoita, voivat sertifikaatin hyödyt ja hankintaperusteet olla Suomessa erilaiset kuin jossain toisessa maassa. Näiden kahden pakollisen yhdistävän tekijän lisäksi otoksen suurin yhteneväisyys oli se, että kaikkien tutkimukseen osallistuneiden sertifioitujen organisaatioiden liiketoiminta perustuu nykyisin joko päätoimisesti tai osittain teknologiapohjaisten palveluiden tuottamiseen. Ominaisuus korostuu siksi, että ISO:n julkaiseman ISO Surveyn (2018) mukaan ISO/IEC 27001 -sertifikaattien määrästä suurin osa, eli noin 61 % on myönnetty informaatioteknologian parissa liiketoimintaa tekeville organisaatioille. Lisäksi tähän osuuteen täytyy vielä lisätä muut toimialat, jotka ovat kyselyssä eroteltu, mutta ovat nykyisin teknologiapainotteisia, kuten finanssiala ja insinööripalvelut.

Jotta tutkimuksen teoreettista perustaa voidaan arvioida tarkemmin, on tapauksiin valittu tietyiltä osin hyvin eroavaisia tutkimuskohteita, jotta niiden väliltä voidaan etsiä eroja ja ristiriitoja. Tutkittavien tapausten erot ovat pääasiassa eroja koossa, sillä tutkimuksen pienimmän organisaation henkilöstömäärä mitataan kymmenissä ja vastaavasti suuremmat haastateltavat organisaatiot kuuluvat keskisuureen tai suureen kokoluokkaan ja työntekijöiden määrä mitataan sadoissa ja ylimmillään tuhansissa. Lisäksi tutkimuskohteiden omistussuhteissa on eroa, sillä yksi tutkittavista organisaatioista on valtio-omisteinen ja julkisen valvonnan kohteena, kun taas muut tutkittavat organisaatiot ovat ainakin pääosiltaan yksityisessä omistuksessa. Tutkittavat organisaatiot toimivat osittain eri liiketoiminta-aloilla, joissa vaikuttavat alalle ominaiset vaatimukset, kuten toimialakohtainen valvonta ja lainsäädäntö, tai alalle muodostuneet käytännöt. Yksittäisen tapauksen toimialaa ei tuoda tässä tutkimuksessa ilmi anonymiteetin säilyttämiseksi, mutta yleisellä tasolla tutkittavat organisaatiot tuottavat muun muassa teknologiapalveluita, kapasiteettipalveluita ja ohjelmistokehitystä. Pääosin

tutkimuskohteet toimivat B2B-markkinalla, eli yritysten välisellä markkinalla, mutta toimintaa on myös kuluttajamarkkinalla. Tutkittavat organisaatiot on lyhyesti esitelty myös alla olevassa taulukossa (taulukko 4), jonka tarkoitus on tuoda esille tutkittavien organisaatioiden perustiedot tutkimuksen kannalta tärkeiden ominaisuuksien osalta.

Taulukko 4 Tutkimusorganisaatioiden ominaisuudet

Numero	Kokoluokka	Sertifikaatin ikä	Käytettyjen sertifiointielinten määrä
1	Keskisuuri	3-9 vuotta	1
2	Pieni	0-3 vuotta	1
3	Suuri	Yli 10 vuotta	1
4	Suuri	Yli 10 vuotta	>1
5	Suuri	Yli 10 vuotta	>1

4.2.2 Tiedon kerääminen haastattelemalla

Yksi laadullisen tutkimuksen tiedonkeruumenetelmistä on haastattelu. DiCicco-Bloomin ja Crabtreen (2006) mukaan haastattelutyypit tyypillisesti jaetaan karkeasti kolmeen eri tyyppiin, strukturoituihin, semistrukturoituihin ja strukturoimattomiin haastattelutyyppeihin sen mukaan, kuinka paljon haastattelijalla vapauksia poiketa haastattelun etenemisjärjestyksestä ja sisällöstä. Tähän tutkimukseen sopivimmaksi valikoitui semistrukturoitu haastattelu, sillä DiCicco-Bloomin ja Crabtreen (2006) mukaan se perustuu ennalta määriteltyyn kysymysrunkoon, jota täydennetään haastattelutilanteessa tarkentavilla kysymyksillä. Tätä haastattelutyyppiä hyödyntämällä kyettiin varmistamaan se, että kaikissa haastatteluissa käsiteltiin samat aiheet ja haastattelusuunnitelmaan kirjatut kysymykset, mutta tarvittaessa mielenkiintoisia vastauksia voitiin tarkentaa sopivilla lisäkysymyksillä haastattelijan ohjatessa keskustelua keskustelunomaisesti.

Haastattelut toteutettiin jokaisen kohdeorganisaation kanssa siten, että organisaatiota edusti relevantissa työtehtävässä työskentelevä työntekijä. Haastateltavan työntekijän tehtävävaatimukseksi asetettiin organisaation tietoturvan johtamisjärjestelmän ylläpitämiseen liittyvä tehtävä, jotta tutkittavien henkilöiden asiantuntemus saatiin varmistettua. Haastattelu toteutettiin neljän kohdeorganisaation kanssa kasvotusten ja yhden kohdeorganisaation kanssa haastattelu toteutettiin internetin välityksellä neuvottelusovellusta hyödyntäen. Kaikissa haastatteluissa käytettiin kuitenkin samaa haastattelurunkoa, joka on tämän tutkimuksen liitteenä (Liite 1), joten kaikki haastattelut olivat keskenään hyvin yhteneväisiä. Haastattelut nauhoitettiin tulosten analysointia varten yhtä haastattelua lukuun ottamatta tutkimuskohteiden luvalla.

Haastattelu koostui kahdesta teemasta, joista ensimmäisessä tutkittiin ISO/IEC 27001 -sertifioinnin hankintaperusteita tietoturva- ja talousnäkökulmista, ja toisessa tutkittiin sertifiointielimen valintaperusteita tutkimalla erilaisia valintaan vaikuttavia tekijöitä. Haastattelutilanteessa teemoja käsiteltiin ensin

yleisellä tasolla siten, että haastateltavat saivat kuvailla hankintaperusteita ja sertifiointielimen valintaperusteita ilman haastattelijan johdattelevia kysymyksiä, jonka jälkeen haastattelijan olemassa olevaan tutkimukseen perustuvia kysymyksiä käytettiin täydentämään haastateltavien vastauksia tutkittavien teemojen osalta. Lopuksi haastateltavat henkilöt saivat vielä itse mahdollisuuden täydentää vastauksiaan ja kysyä haastattelijalta aiheeseen ja tutkimukseen liittyviä kysymyksiä. Johtopäätöksenä haastattelujen katsottiin onnistuneen hyvin ja ongelmitta.

4.2.3 Tulosten analysointi

Eisenhardtin (1989) mukaan tulosten analysointivaihe on tapaustutkimuksissa sen tärkein, mutta samalla haastavin vaihe, sillä suuren laadullisen datamäärän analysointi kattavasti perustellen on erittäin haastavaa ja toisaalta myös tutkijasta riippuvaisempaa verrattuna esimerkiksi kvantitatiivisen tutkimuksen määrämuotoisempiin analyysimenetelmiin. Myös Eriksson ja Koistinen (2014) painottavat sitä, että laadullinen tutkimus nojaa aina jossain määrin tutkijan omaan tulkintaan, mutta painottavat myös sitä, että laadulliseen tutkimukseen on kehitetty erilaisia analysointitapoja, kuten suora tulkinta, aineiston koodaus, kaavan etsiminen ja selittäminen, aikasarja-analyysi ja teoreettisten käsitteiden kehittäminen, joilla analyysin tekeminen on systemaattisempaa.

Tähän tutkimukseen analyysimenetelmäksi valikoitui aineiston koodaaminen, jota hyödynnettiin yksittäisten tapausten analysointiin (within-case analysis) ja tapausten välisien suhteiden analysointiin (cross-case pattern analysis). Eriksonin ja Koistisen (2014) mukaan koodaus tarkoittaa sitä, että aineistossa oleville sisällöllisille asioille annetaan nimet, eli koodit, jotka kuvaavat erilaisia tutkimuskysymyksiin vastaavia ominaisuuksia tai asioita. Koodaus johtaa yleensä käsitteellisiin luokkiin, jotka voivat perustua kerättyyn aineistoon tai olemassa olevaan teoriaan. (Eriksson ja Koistinen, 2014.) Tämän tutkimuksen osalta koodauksen tavoitteena oli muodostuneiden käsitteiden avulla kuvata tutkimusongelmassa etsittäviä sertifioinnin hyötyjä ja hankkimisperusteita sekä sertifiointielimen valintaperusteita. Koodauksessa käytettävien käsitteiden määrittelyssä käytettiin pääasiassa olemassa olevaa teoriaa, sekä aineistossa toistuvia käsitteitä.

Eriksson ja Koistinen (2014) kuitenkin muistuttavat, että koodaus ei sellaisenaan tuota vastauksia vaan mahdollistaa jatkoanalyysin. Tämän vuoksi aineistoa analysoitiin Eisenhardtin (1989) mainitsemilla tavoilla tutkimalla tapauksia ensin erillisinä yksi kerrallaan ja sen jälkeen toisiinsa vertaillen. Tapausten yksittäinen tutkiminen toteutettiin litteroimalla haastatteluista kerätyt äänitallenteet tekstiksi, jotta yksittäisten haastattelujen tuloksista voitiin mahdollisimman tehokkaasti tutkia omina yksittäisinä tapauksina. Yksittäisten tapausten tulokset koodattiin määriteltyihin käsitteisiin, jonka jälkeen tapauksia analysoitiin keskenään yhteneväisyyksien ja ristiriitojen havainnoimiseksi. Keskinäisessä vertailussa otettiin huomioon erityisesti tapausten väliset erot, kuten koko ja sertifikaatin ikä. Näin ollen saavutettiin tutkimuksen kontekstissa laaja käsitys erilaisten organisaatioiden ISO/IEC 27001 -sertifioinnin hankintaperusteista ja

sertifiointielimen valintaan liittyvistä tekijöistä. Lopuksi esiin nousseita tekijöitä verrattiin aiemman tutkimuksen esittämiin näkemyksiin.

4.3 Tutkimuksen reliabiliteetti, validiteetti ja yleistettävyys

Tieteellisessä tutkimuksessa luotettavuudella ja tiedon oikeellisuuden varmistamisella on perinteisesti ollut suuri merkitys. Näitä ominaisuuksia voidaan tutkia reliabiliteetin ja validiteetin avulla. Saaranen-Kauppisen ja Puusniekan (2009) mukaan kummatkin näistä mittaustavoista ovat perinteisesti olleet kvantitatiivisen tutkimuksen tapoja mitata luotettavuutta ja vastaavasti niiden soveltuvuutta laadullisen tutkimuksen arviointiin on kyseenalaistettu. Kuitenkin nykyisin niitä käytetään yleisesti luotettavuuden mittaamiseen joko sellaisenaan tai käsitteiden merkityksiä muokkaamalla paremmin laadullisen tutkimuksen kontekstiin sopivaksi. (Saaranen-Kauppinen & Puusniekka, 2009.)

Reliabiliteetin tarkoitus on mitata sitä, kuinka systemaattisesti yhtäläisiä tuloksia tutkimus tuottaa, eli toisin sanoen, kuinka toistettavissa tutkimuksen tulokset ovat. Golafshanin (2003) mukaan kvantitatiivisen tutkimuksen mukaista käsitystä reliabiliteetista ei suoraan voi soveltaa laadullisen tutkimuksen mittaamisessa, joten sen käsitettä joudutaan muokkaamaan sisältämään asioita kuten tutkimuksen uskottavuus, neutraliteetti, varmistettavuus, johdonmukaisuus ja soveltuvuus. Saaranen-Kauppisen ja Puusniekan (2009) mukaan reliabiliteettia voidaan arvioida kolmen kohdan avulla: metodin, ajallisen ja johdonmukaisuuden reliabiliteetin kautta. Metodin arviointi tarkoittaa käytetyn tutkimusmetodin, kuten tietyn haastattelukysymyksen tuottamien tulosten luotettavuutta tietyissä olosuhteissa, kun taas ajallinen reliabiliteetti tarkoittaa sitä, että mittaukset ja havainnot ovat tosia jossain tietyssä ajan hetkessä. Johdonmukaisuuden arviointi tarkoittaa esimerkiksi eri mittausvälineillä tai -tavoilla saavutettujen tulosten yhdenmukaisuutta. (Saaranen-Kauppinen & Puusniekka, 2009.)

Validiteetti tarkoittaa käytännössä sitä, mittaako ja vastaako tutkimus tutkimusongelmaan oikein tuottaen todellisuutta vastaavia tuloksia. Saaranen-Kauppinen ja Puusniekka (2009) määrittelevät validiteetin tutkimuksen pätevyyden arvioinniksi, jota voidaan mitata muun muassa tutkimuksen perusteellisuuden ja tehtyjen päätelmien oikeellisuudella ja ymmärrettävyydellä. Kuitenkin, etenkin laadullisen tutkimuksen kohdalla, validiteetin määritelmä voidaan joutua käsittämään uskottavuuden tai vakuuttavuuden kautta, sillä tutkimus ei koskaan voi ymmärtää tutkittavaa ilmiötä täysin, vaan tuo siitä ilmi vain osan. (Saaranen-Kauppinen ja Puusniekka, 2009.) Myös Golafshani (2003) nostaa tämän ongelman esille, sillä hänen mukaansa validiteetin mittaamisen sopivuutta on kyseenalaistettu laadullisen tutkimuksen kohdalla, mutta se on kuitenkin jossain määrin mahdollista, muun muassa trianguloimalla dataa, jolloin monista lähteistä ja mahdollisesti eri menetelmillä kerätty data tuottaa todennäköisemmin luotettavampia tuloksia.

Näistä näkökulmista arvioiden tulosten reliabiliteettia ja validiteettia voidaan arvioida melko kattavasti. Kaikkiin haastatteluihin sovellettiin samaa kysymysrunkoa, joka perustui aikaisemmasta tutkimuksesta kerättyyn lähdemateriaaliin. Haastattelutilanne oli olosuhteiden kannalta kaikissa tapauksissa hyvin samankaltainen sillä erotuksella, että yksi haastattelu toteutettiin internetin välityksellä. Tällä ei kuitenkaan nähty olevan suurta vaikutusta, sillä haastattelu ja tulosten analysointi tapahtui samalla tavalla kaikissa tapauksissa. Esimerkiksi kohdehenkilöiden äänenpainoja ja asennoitumista yksittäisiin kysymyksiin kyettiin havainnoimaan kaikissa tapauksissa yhtäläisesti. Haastatteluihin valikoituneet kohdeorganisaatiot valittiin tutkimusongelmaan sopivasti siten, että niillä kaikilla oli määritellyt pakolliset yhteneväiset ominaisuudet ja toisistaan eroavat ominaisuudet monipuolisten tulosten varmistamiseksi. Osaan tutkimukseen osallistuneista henkilöistä oli myös olemassa olevia kontakteja, jotka edesauttoivat positiivista suhtautumista tutkimukseen osallistumisesta. Myös ajallisesti mitattuna tutkimusta voidaan pitää luotettavana, sillä kaikki haastattelut toteutettiin kolme viikon aikavälillä, jota voidaan pitää tutkimuksen kontekstissa niin lyhyenä aikana, että ajan vaikuttavuutta eri haastattelutulosten välillä voidaan pitää lähes olemattomana. Lisäksi haastattelutulokset ovat tuoreita, jolloin niitä voidaan pitää nykytilaa kuvaavina. Tutkimuksen empiirisen osuuden tuloksia verrataan myös dokumentoituun lähdeaineistoon, jolloin tutkimuksen tuloksia varmistetaan useiden kanavien kautta.

Haastattelutilanteen osalta tutkimuksesta pyrittiin minimoimaan erilaisten haittaavien tekijöiden vaikutusta. Myersin ja Newmanin (2007) mukaan tällaisia haittaavia tekijöitä ovat muun muassa haastattelun keinotekoisuus, ajan ja luottamuksen puute, kohdehenkilön sopivuus, hawthorne-efekti ja väärinymmärrykset. Haastattelun keinotekoisuus tarkoittaa sitä, että haastattelija on haastateltavalle täysin tuntematon, jolloin tämä saattaa vaikuttaa haastateltavan vastauksiin, erityisesti aikapaineen alla. Hawthorne-efekti taas tarkoittaa sitä, että haastateltava itse ei pysy neutraalina, vaan alkaa kontrolloimaan ja johdattelemaan keskustelua siten, että se vaikuttaa haastateltavan vastauksiin haastattelijan mieltymysten mukaisesti. (Myers & Newman, 2007.) Näitä ongelmia pyrittiin välttämään sillä, että haastattelutilanteesta pyrittiin tekemään haastateltavalle mahdollisimman helppo ja paineeton. Kaikkiin haastateltaviin oli luotu keskusteluyhteys jo ennen haastattelua ja itse haastattelutilanne järjestettiin haastateltavan haluamassa paikassa, esimerkiksi haastateltavan työpaikalla. Haastatteluille varattiin riittävästi aikaa siten, että haastatteluissa ei tarvinnut kiirehtiä, eikä yksikään haastattelu jäänyt kesken. Kohdehenkilöt taas olivat kaikissa tapauksia sopivia, sillä kaikista tapauksissa kohdehenkilön työtehtäviin kuului haastattelun aiheen mukaiset tehtävät. Hawthorne-efekti on haastattelijalle itselleen vaikea havaittavaksi, etenkin kun puolistrukturoitu haastattelutyyli mahdollistaa keskustelevan ja haastattelun kulkua muokkaavan tyylin. Kuitenkin arvion mukaan efektiä ei ollut, tai sen vaikutukset arvioitiin hyvin pieniksi, sillä haastateltavilla oli aina mahdollisuus perustella vastauksiaan ja haastattelu kulki keskustelunomaisesti. Lisäksi mahdollisten väärinymmärrysten kohdalla haastattelija pyrki varmistamaan haastateltavan sanoman joko heti haastattelutilanteessa tai haastatteluja

litteroidessa. Vaikka reliabiliteetti ja validiteettivaatimukset täyttyvät tämän tutkimuksen kohdalla hyvin, on tutkimukseen liittyvät rajoitteet ja haasteet kuitenkin ymmärrettävä. Rajoitteita ja haasteita kuvataan tarkemmin tutkimuksen yleistettävyyttä käsittelevässä osiossa 7.3.

5 TUTKIMUKSEN TULOKSET

Tämä luku esittelee tutkimuksessa saatuja tuloksia ja pyrkii esittelemään niin eri tapauksista löytyneitä yksittäisiä mielenkiintoisia havaintoja, suurempia yhteneväisiä kokonaisuuksia ja selkeitä eroja. Ensin esitellään ensin sertifikaatin hankintaperusteisiin liittyviä tekijöitä niin tietoturva- kuin talousnäkökulmasta esittelemällä hankintaan liittyviä hyötyjä, mahdollisuuksia ja haasteita. Kolmannessa alaluvussa keskitytään sertifiointielimen valintaperusteisiin liittyviä tekijöihin. Tuloksia esitellään niin tekstinä kuin taulukkomuodossa, sekä haastatteluissa tulleita mielenkiintoisia sitaatteja esitellen. Sitaateissa on viitattu haastateltuja henkilöitä taulukossa 4 esitellyn organisaatiota kuvaavan numeron mukaisesti, siten että haastateltava H1 viittaa organisaation numero 1 ja vastaavasti H2 viittaa organisaatioon numero 2.

5.1 Sertifioinnin hankintaan ja ylläpitoon vaikuttavat tekijät tietoturvanäkökulmasta

ISO/IEC 27001 -standardin implementoinnin hyödyt organisaation tietoturvan tasoon ovat todistetut, sillä standardin laaja levinneisyys ja aiempi tutkimus puoltavat tätä. Kuitenkin melko vähän on tietoa siitä, miten sertifiointi vaikuttaa tietoturvahyötyihin. Näitä hyötyjä kuvaavia tekijöitä kuitenkin löytyi tutkimuksessa laaja-alaisesti, vaikkakin ne olivat usein yhteydessä standardin yleisesti tuottamiin hyötyihin.

5.1.1 Tietoturvan hallinnan kokonaisvaltainen parantuminen eri osa-alueilla

Kaikki haastateltavat organisaatiot kokivat, että ISO/IEC 27001 -standardin mukainen johtamisjärjestelmä on kohottanut organisaation tietoturvan tasoa laaja-alaisesti. Yleisesti tietoturva koettiin kaikissa organisaatioissa tärkeäksi ja osaksi organisaatiokulttuuria, mikä näkyi myös päivittäisessä toiminnassa. Haastateltavien arvion mukaan ISO/IEC 27001 tarjoaa tietoturvan hallintaan ja johtamiseen hyvän viitekehyksen ja työkalun. Yleisesti haastatteluissa tuli ilmi myös käsitys siitä, että ISO/IEC 27001 on tietoturvastandardien keskuudessa niin kutsuttu ”de facto” -standardi, joka tunnetaan yleisesti ja sitä pidetään jossain määrin tietoturvan perusteoksena, joka toimii hyvänä mallina tietoturvan toteuttamiselle.

Kun haastateltavat saivat ensin vapaasti kuvailla organisaation kokemia tietoturvahyötyjä, tuli esiin paljon erilaisia hyödyiksi koettuja tekijöitä. Yksi selkeä viite tietoturvahyödyistä kaikkien organisaatioiden kohdalla oli se, että ISO/IEC 27001 -standardi tarjoaa hyvän perustan tietoturvalle ja tarjoaa hyvän työkalun tietoturvan hallintaan organisaatiossa.

> ”Kyllä tämä ISO tarjoaa hyvän framen siihen, että nimenomaan tietoturvan hallintajärjestelmän pystyttämisen ja hallinnointiin ja varsinaisen tietoturvan ja kontrollien jalkauttamiseen.” (H1)

> ”ISO 27001 -standardi on hyvä malli asioita ja sen avulla näitä asioita tulee ajateltua syvemmin. Se itsessään antaa tietoturvan kannalta lisää työkaluja.” (H5)

Eräässä tapauksessa ISO/IEC 27001 -standardi nähtiin jopa organisaatiomuutoksen loppuun viemisen mahdollistavana työkaluna. Haastateltava koki, että koko uusi, laajentunut organisaatio saatiin saman hallintajärjestelmän alle, jossa pätevät yhtenäiset tavat toimia.

> ”Kun useampi organisaatio yhdistyi ja scope laajentui, niin sen jälkeen meillä on yksi tapa, ja nimenomaan yhteismitallinen tapa toimia. Ilman muuta se on hyvä työkalu tässä integraation loppuun viemisessä.” (H3)

Kuitenkaan mikään johtamisjärjestelmä ei voi toimia tehokkaasti, ellei sillä ole johdon tukea, ja tämä käsitys sai vahvaa tukea myös haastattelujen kautta, sillä kaikissa organisaatioissa sertifikaatille ja tietoturvalle yleensä oli vahva tuki. Johdon tuki myös miellettiin ennemmin omaehtoiseksi ja kannustavaksi kuin standardin vaatimusten pakottamana.

> ”Kyllä siinä hallitus ja toimitusjohtaja nukkuu rauhallisemmin, kun tämä (sertifikaatti) on. Ei ole enää uskon varassa se, että asiat ovat hoidossa. Ja se (tietoturva) on dokumentoidusti hoidossa. Ja totta kai sillä on vastuukysymyksiinkin viime kädessä vaikutusta. Se (sertifikaatti) on vahva osoitus siitä, että asioihin on kiinnitetty asianmukaista huomiota.” (H2)

> ”Luulen, että liikkeenjohdolla on sellainen näkemys, että me ei voida jättää sertifikaattia pois.” (H1)

Kun haastateltavilta kysyttiin standardin ja sertifioinnin vaikutuksia hallintajärjestelmän prosesseihin ja jalkauttamiseen, nousi ihmisten tietoturvatietoisuus yhtenä tekijänä ilmi. Tämä korostui ehkä siksi, että tietoturvatietoisuuden parantamista käytettiin esimerkkinä prosessien parantumisena, mutta kaikki haastateltavat olivat kuitenkin sitä mieltä, että myös muista hallintajärjestelmän prosesseista on ollut hyötyä ja ne ovat ajan saatossa kehittyneet.

> ”Esimerkiksi tietoturvatietoisuus, niin kyllä standardi ajaa siihen suuntaan, että meidän pitää sitä edistää.” (H1)

> ”Työntekijöiden awareness (tietoturvatietoisuus) nousee ja myös prosesseihin löydetään parannuksia.” (H4)

> ”Kyllä standardilla on positiivinen vaikutus ihmisten tietoturvaosaamiseen. Myös meille se on työkalu, että meillä on tällainen tietty vaatimus täällä, mikä on kaikkien

> hyväksi. Se on paljon parempi peruste kuin, että tietoturva (liiketoimintayksikkö) nyt vaan haluaa." (H5)

5.1.2 Jatkuva parantaminen

Yksi ISO/IEC 27001 -standardin kantavista periaatteista on jatkuva parantaminen, mikä varmistaa tietoturvan johtamisjärjestelmän jatkuvan ylläpitämisen ja mahdollistaa sen kehittämisen. Kehittämisen myötä organisaation on mahdollista tunnistaa sitä koskevat riskit entistä tarkemmin, sekä mahdollistaa johtamisjärjestelmän tehokkaamman toiminnan. Tiedon keräämisvaiheessa jatkuva parantaminen nousi myös aktiivisesti esille kaikkien haastateltavien kanssa.

> "Kun asiat laitetaan kuntoon, se antaa hallittavuuden ja helppouden, niin voi keskittyä jatkuvaan parantamiseen ja pystyy seuraamaan sitä, missä ollaan menossa ja samalla pystytään priorisoimaan paremmin niitä parannettavia osa-alueita." (H1)

Jatkuva parantaminen ei kuitenkaan aina tarkoita sitä, että tietoturvaan laitettaisiin aina enemmän resursseja ja tehtäisiin asioista entistäkin turvallisempia. Eräs haasteltava koki, että heidän organisaatiossaan jatkuva parantaminen on optimointia, jonka avulla tietoturvalle voidaan löytää sopiva tasapainopiste, missä kaikille tietoturvan osa-alueilla koitetaan jatkuvan parantamisen avulla löytää tasapainopiste riittävän turvallisuuden ja panostetun työmäärän ja resurssien suhteen. Kuitenkin haastateltava korosti, että tietyissä asioissa, jotka ovat organisaatiolle tärkeitä, resursseja laitetaan vastaavasti enemmän.

> "Meille tärkeitä on maine- ja jatkuvuusriskit. Jos järjestelmät on alhaalla, niin me menetetään rahaa, ja paljon. Niin, me ollaan ajateltu, että se jatkuva parantaminen on optimointia. Se tarkoittaa, että me voidaan jotain juttua tietoisesti huonontaa ja se parantaa meidän toimintaamme. Meidän ei kannata esimerkiksi tiettyyn juttuun panostaa niin paljon, kun vähemmälläkin pärjätään, ja se on jatkuvaa parantamista." (H3)

5.1.3 Sertifikaattiin liittyvät velvollisuudet ja auditointi

Tämän tutkimuksen kontekstissa oli erityisen mielenkiintoista tutkia sertifioinnin merkitystä organisaatioiden tietoturvaan. Kun haastatteluissa haastateltavia pyydettiin arvioimaan nimenomaisesti sertifioinnin vaikutusta tietoturvaan, toistuivat siinä kaikkien haastateltavien kohdalla samat tekijät, jotka liittyvät sertifikaatin ylläpitämiseen liittyviin velvoitteisiin, mikä on luonnollista, sillä suurin sertifikaatin tuoma ero sertifioimattomaan johtamisjärjestelmään on velvollisuus noudattaa sertifikaatin elinkaaren mukaisia auditointi- ja ylläpitovelvollisuuksia. Sertifiointi pohjautuu kolmannen osapuolen arviointiin, joten sertifiointisyklin mukaisesti sertifioitu organisaatio joutuu vuosittain valmistautumaan vuosiauditointiin tai uusintasertifiointiin, tai joskus jopa erikoisauditointiin. Jatkuva

valvonta oli kaikkien haastateltavien mukaan yksi tekijä, joka varmistaa johtamisjärjestelmän ylläpitämisen ja jatkuvan parantamisen.

> ”On tietyt prosessit ja tietyt asiat, jotka tulee mietittyä paljon pidemmälle, kun on sertifikaatti. Siinä mielessä on hyvä, että uudelleen arviointia ja sertifiointia tehdään, että sitä (johtamisjärjestelmää) tulee koko ajan ylläpidettyä ja on sitten jatkuvaa se kehittäminen. Lisäksi malli (ISO 27001) on niin laaja, että ilman auditointia voisi olla, että joitain asioita ei tulisi käytyä läpi sillä tasolla kuin nyt.” (H1)

> ”On sillä jonkinlainen vaikutus, tosin siinä täytyy todeta, että meillä oli jo ennen sertifiointia asiat ihan hyvällä tolalla, mutta kyllä totta kai dokumentaatio on ihan eri tasolla. Nyt dokumentaatio viety sille tasolle, kun sen kuuluukin olla.” (H2)

Yksi haastateltavista arvioi, että itse auditointi ei enää vaikuta suuresti organisaation tietoturvan tasoon, sillä organisaatiolla on ollut sertifikaatti jo useita vuosia ja täten auditoijan on haastava tehdä havaintoja, joita organisaatio ei itse jo tietäisi.

> ”Sertifiointi pakottaa määrämuotoisuuteen ja siihen, että asiat on kuvattu. Auditointi ei kuitenkaan enää meillä merkittävästi vaikuta tietoturvan tasoon. Perustelen tätä sillä, että meillä on pitkä kokemus näistä auditoinneista ja harvoin se auditoija, kun se kerran vuodessa tulee kylään, niin ei se sieltä mitään sellaista löydä mitä me ei jo tiedettäisi. Aika skeptinen olen sen auditoinnin suhteen. Toki standardissa on hyviä vaatimuksia, ja jos niiden noudattamista vahditaan niin siinä mielessä kyllä se auditointi vaikuttaa” (H3)

Toisaalta kyseinen haastateltava kuitenkin oli sitä mieltä, että auditointi pakottaa tiettyyn määrämuotoisuuteen ja siihen, että asiat, kuten politiikat ja prosessit on kuvattu riittävän hyvin, mikä helpottaa esimerkiksi uusien henkilöiden kouluttamista. Myös kaksi muuta haastateltavaa viittasivat sertifikaatin luomaan pakkoon, vaikka pakkoa ei tietoturvamielessä nähty huonona asiana. Pakko nähtiin ennemmin toimimiseen velvoittavana tekijänä, joka taas vaikuttaa siihen, että standardin velvollisuudet on täytetty huolellisemmin. Eräs haastateltava kuvaili asiaa myös siten, että standardin vaatimusten kanssa ei voi oikoa, tai ainakin sen perustelu on sertifioinnin sisältämän kolmannen osapuolen valvonnassa hankalampaa.

> ”Sit on vaikeampi perustella itselleen, miksi jostain oiotaan ja näin ollen on täytettävä huolellisemmin kaikki vaatimukset. Toki silloin voi tulla mukana jotain ei välttämätöntä mukana, mutta esimerkiksi meidän tapauksessamme kaikki vaatimukset mitä sertifikaatin mukana on tullut, on ihan relevantteja. Lisäksi sehän on ennakoitavissa mitä auditoija sieltä edellyttää, niin osataan valmistautua, mutta juuri se prosessi on se hyödyllinen” (H2)

> "Ehkä tämä sertifiointi aiheuttaa sen, että ne asiat tulee todennäköisemmin tehtyä, että vaadittavat dokumentit ja toiminta saadaan aikaiseksi. Antaa myös toisaalta minulle työkaluja, jotta saadaan täällä organisaatiossa aikaiseksi tarvittavat muutokset.” (H1)

Haastateltava H4 korosti sitä, että auditointeja tehdään juuri siksi, että niissä löytyy havaintoja, joista organisaatio voi oppia ja siten parantaa tietoturvansa tasoa. Lisäksi myös se, että auditoija tulee organisaation ulkopuolelta, ja näin ollen pystyy arvioimaan johtamisjärjestelmää ilman ennakkokäsityksiä ja puolueettomasti, auttaa parantamaan tietoturvan tasoa. Tämän koettiin myös näyttäytyvän positiivisena asiakkaiden suuntaan, kun auditoinnin suorittaa kolmannen osapuolen toimija.

> ”Kyllä parantaa, koska silloin kun ulkoisen silmin katsotaan, niin nähdään eri silmin asioita. Sen takia auditointeja tehdään, että sieltä opitaan. Löydöksiä ei pidä pelätä. Ilman auditointia sisäiset prosessit rapautuisivat ja toisaalta auditointi varmistaa sen, että mistään ei oiota.” (H4)

Haastateltava H5 toi ilmi näkemyksen, jonka mukaan auditointi tarjoaa mahdollisuuden laajempaan syvempään ajatteluun tietoturvan osalta, koska tietyt, ehkä vähemmän relevantit tai haastavammat osa-alueet standardista voivat muuten jäädä vähemmälle huomiolle. Tällöin valmiit kriteerit ja niiden noudattaminen helpottavat ylläpitämään kokonaisvaltaista tietoturvan johtamisjärjestelmää, jossa tietoturvaa ajatellaan monelta eri osa-alueelta.

5.2 Sertifioinnin hankintaan vaikuttavat tekijät taloudellisesta näkökulmasta

Koska ISO/IEC 27001 -sertifikaatti on vapaaehtoinen, ovat sertifikaatin hankkimiseen johtavat perusteet ainakin osittain taloudellisesti määräytyviä. Näitä tekijöitä löytyikin melko runsaasti. Ne vaihtelevat laajasti säästöistä tuottoihin ja asiakassuhteiden luomiseen ja ylläpitämiseen.

5.2.1 Asiakkaiden vaatimus

Kolmella haastateltavalla nousi esiin puhtaasti vaatimus sertifikaatille asiakkaan suunnasta. Lisäksi vaatimus tuli epäsuorasti kahden muun haastateltavan kohdalla, toisella näistä omien toimittajien suuntaan siten, että sitä vaaditaan omilta toimittajilta. Vaatimus sertifikaatille oli yleisesti siitä syystä, että sen odotettiin toimivan ikään kuin vakuutena siitä, että toinen osapuoli on luotettava ja se huolehtii tietoturvasta asianmukaisesti.

> ”Selkein syy sertifikaatin hankkimiseen oli se, että asiakkaat, jos ei suoraan edellytä sitä, niin arvostaa sitä. Myöskin painopiste on siltä osin muuttunut, että jos sitä (sertifikaattia) ei ole, niin jossain kohti tulee vaikeeta.” (H2)

> ”Jos tätä sertifikaattia ei olisi, niin osa asiakkaistamme ei tulisi meidän asiakkaiksemme. Sitä vaativat niin yksityisen kuin julkisen sektorin toimijat.” (H4)

> ”Alun perin sertifikaatti hankittiin ihan tarpeen vuoksi, eli meidän partnerit ja asiakkaat sitä vaativat. Nykyään ISO 27001 tulee joka paikassa jo vaatimuksena. Jos haluaa olla uskottava ja toimia oikein niin se on yksi syy.” (H5)

5.2.2 Toimialakohtainen vaatimus

Yhdellä kohdeorganisaatioista ISO/IEC 27001 -sertifikaatti oli pohjavaatimus omalla toimialla vaadittavaan sertifiointiin, joka edellytetään kaikilta toimintaan osallistuvilta organisaatioilta. Täten heidän kohdallaan yksi merkittävimmistä syistä ISO/IEC 27001 -sertifioinnin hankkimiselle, ja ennen kaikkea sen ylläpitämiselle, on kyseinen toimialakohtainen vaatimus. Haastattelussa kuitenkin myös tuli ilmi, että sertifioinnista ei luovuttaisi, vaikka toimialakohtainen vaatimus poistuisi, koska sertifioinnista saadaan muita hyötyjä.

5.2.3 Kilpailuetu

Yksi mielenkiintoinen aspekti sertifikaattiin liittyen on sen tuottama kilpailuetu, ja tässä vastanneiden organisaatioiden näkemykset erosivat suuresti. Enemmistö, kolme viidestä vastaajasta oli sitä mieltä, että sertifikaatti on aiemmin ollut kilpailuetu, mutta sen merkitys on viime vuosina laskenut osittain siksi, että sertifikaattien määrä on kasvanut ja kilpailuetu on vaihtunut alan olettamaksi.

> ”Vielä pari vuotta siten se oli selkeästi erottava tekijä, luonnollisesti nyt se erottuvuus alkaa laimentua, kun sertifikaatteja on laajemmin” (H2)

> ”Joskus ollut kilpailuetu, mutta ei enää ole, sillä nykyään tietoturva-alan sertifikaatti on de facto-juttu tällä alalla.” (H1)

> ”Kyllä sanoisin, että sertifikaatti on vakiintunut käytäntö, koska meidän toimialallamme se on monesti vaatimus, että voi olla toiminnassa mukana.” (H3)

Kuitenkin kaksi haastateltavaa otoksen suurta koko luokkaa edustavista organisaatioista oli sitä mieltä, että sertifikaatti on vielä merkityksellinen ja varsinkin suurilla kansainvälisillä markkinoilla siitä on etua, etenkin jos sertifikaatti kattaa organisaation kaikki osat. Kuitenkin näissäkin tapauksissa haastateltavat tunnistivat ilmiön, että kilpailuetu on hiljalleen kaventunut.

> ”Sertifikaatti on lisenssi operoida. Kansainvälisillä markkinoilla käytetään globaaleja standardeja ja isoilla organisaatioilla sertifikaatti on ollut jo pitkään. Tilanne on ollut tällainen jo pitkään. Viime aikoina ilmeisesti pienemmätkin toimijat ovat alkaneet hankkia sertifikaatteja.” (H4)

> ”On se kilpailuetu vielä, koska ei sitä kaikkialla vielä ole, varsinkaan sillä laajuudella kuin meillä on.” (H5)

5.2.4 Luottamus ja uskottavuus

Ylivoimaisesti eniten haastateltavien kanssa keskusteluissa tuli ilmi luottamukseen ja uskottavuuteen liittyvät tekijät ja niistä usein keskusteltiin ajallisesti eniten ja tekijät tulivat usein epäsuorasti ilmi monien muidenkin tekijöiden kautta. Kaikki kohdeorganisaatioiden edustajat olivat sitä mieltä, että sertifikaatilla oli luottamusta ja uskottavuutta nostava vaikutus. Tämä on kuitenkin ymmärrettävää, sillä sertifikaatin tehtävä on toimia osoituksena vaatimuksenmukaisuudesta ja sen kautta tuottaa luottamusta ja uskottavuutta. Luottamuksen merkitys korostui etenkin pienemmillä organisaatioilla. Yksi haastateltavista organisaatioista oli myös sitä mieltä, että sertifikaatti lisää työnhakijoiden luottamusta organisaatiota kohtaan rekrytointitilanteessa. Yhdellä kohdeorganisaatiolla toiminta perustuu pitkälti kuluttajamarkkinaan, jolloin loppuasiakkaan luottamukselle sertifikaatilla ei haastateltavan mukaan ollut juurikaan merkitystä, mutta toisaalta he edellyttivät standardinmukaista toimintaa heidän omilta toimittajiltaan, jolloin sertifikaatin merkitys sinne suuntaan on merkittävä.

> ”Mä uskon, että se sertifikaatin hankkiminen oli sellainen strateginen valinta, eli sillä saadaan uskottavuutta tällaisessa toiminnassa ja silloin (hankkimisvaiheessa) jo nähtiin että meidän pitää laajentaa tätä liiketoimintaa, niin tämä antaa semmoisen uskottavan taustan sitä varten.” (H1)

> ”Pienen yhtiön uskottavuuden kannalta on huima merkitys, etenkin silloin kun sertifikaatti saatiin ja niitä ei juuri vielä näkynyt” (H2)

> ”Alun perin sertifikaatin hankkimisen syynä oli se, että tämä meidän toimialamme on luottamusbisnestä, joten haluttiin osoittaa, että tietyllä tasolla hoidetaan asioita. Sanotaan, että asiakkaiden luottamus on kaiken a ja o, ja jos me se luottamus menetetään, niin se näkyy euroissa saman tien.” (H3)

> ”Sertifikaatti luo luottamusta myös asiakkaisiin, kun tiedetään että käy ulkopuolinen katsomassa.” (H4)

> ”Se (sertifikaatti) on merkki siitä, että se on ulkopuolisen tekemä arviointi. Se ei ole pelkkää mainospuhetta, vaan siellä on todellista perää.” (H5)

Kun haastateltavien kanssa keskusteltiin sertifikaatin vaikutusta uusiin ja olemassa olevien asiakkuus- ja yhteistyösuhteisiin, tuli selkeästi ilmi, että sertifikaatilla on suuri merkitys uuden asiakkuus- tai yhteistyösuhteen syntymisessä, mutta sertifikaatti auttaa lisäämään luottamusta myös olemassa olevien suhteiden aikana. Uusien asiakkaiden hankkimiseen liittyvää luottamusta on käsitelty myös tutkimuksen luvussa 5.2.6, joka käsittelee myynnin edistämistä.

> ”Uusien asiakkaiden kohdalla on helppo heti näyttää, että asiat on kunnossa” (H4)

> ”Mielestäni on nähtävissä, että sekä uudet että olemassa olevat asiakkaat on viime aikoina alkaneet kysyä yhä enemmän ja enemmän tietoturva-aiheisia kysymyksiä ja

> siellä näen, että tämä sertifikaatti auttaa näyttämään, että ollaan huolehdittu asioista ja toimintatavat on laitettu kuntoon." (H1)

Olemassa olevien suhteiden kohdalla sertifikaatin vaikutus kuitenkin pienenee, mutta toisaalta sertifikaatin avulla voidaan viitata tietoturvaan liittyviin asioihin ja niitä on helpompi käsitellä yhdessä. Kuitenkin kaikilla haastateltavilla oli näkemys siitä, että sertifikaatin tuottaman luottamuksen merkitys on uusien asiakkuussuhteiden luomisen kohdalla suurempi kuin olemassa olevien suhteiden kohdalla.

> "Kyllä olemassa olevatkin asiakkaat kyselevät sertifikaatin perään. Ja kyllä asiakkaat aina sertifikaatista todistusta pyytävät uusintasertifointien kohdalla. (H5)

> "Jos mietitään asiakkaita, jotka oli jo ennen sertifiointia, niin kyllä se sitä heidän luottamustaan vahvistaa, mutta hirveän suuri se vaikutus ei ole" (H2)

> "Jos me ajatellaan meidän loppuasiakkaitamme, niin niille se ei varmaan ole merkittävä, mutta jos ajatellaan meidän toimittajia, niin niiltä me vaaditaan standardin noudattamista ja siellähän se varmasti vaikuttaa." (H3)

5.2.5 Sertifikaatti markkinointikeinona

Kun sertifikaatin haastatteluissa keskityttiin sertifikaatin käyttämiseen markkinointivälineenä, tuli haastatteluissa ilmi hieman eriäviä mielipiteitä. Kaikki haastateltavat olivat pääosin sitä mieltä, että sertifikaatin päätoiminen tehtävä on toimia markkinointikeinona, mutta sen hyödyntämisen suhteen eroja oli melko paljon, sillä muun muassa standardin tunteminen vaikuttaa julkisuuskuvan muotoutumiseen.

> "Kun lähdetään tuotetta ulkomaille myymään, niin on siitä etua, että on sertifioitu talo." (H3)

> "Ne, jotka eivät sertifikaattia tunne, niin eivät sen merkitystä ymmärrä, mutta ne, jotka ymmärtävät, niin niiden kohdalla se parantaa organisaation julkisuuskuvaa." (H4)

> "Julkisuuskuvaan sertifikaatilla pelkästään positiivisia ja luottamusta herättäviä vaikutuksia. Ehkä alussa sertifikaattia käytettiin enemmän markkinointikeinona, nykyisin ei enää niin paljon, kun se on jo perusvaatimus." (H1)

Yhden kohdeorganisaation kohdalla organisaatio oli tehnyt päätöksen, että he eivät julkisesti ainakaan kovin aktiivisesti sertifikaattia mainosta sen vuoksi, että heidän arvionsa mukaan sertifikaatin aktiivinen mainostaminen saattaisi innoittaa hyökkääjiä yrittämään entistä innokkaammin ikään kuin näyttääkseen kyvykkyytensä. Lisäksi organisaatio kokee olevansa kohteena ehkä keskimääräistä organisaatiota kiinnostavampi.

> "Meillä sertifikaattia ei aktiivisesti mainosteta, vaikka siitäkin on jonkin verran puhuttu. Mulla silläkin tavalla on vähän mietitty, että olemme hakkerointimielessä

> mielenkiintoinen kohde. Ja jos taas mainostaisimme, että olemme tietoturvasertifioitu organisaatio, niin innostuisiko siitä joku hakkeri kahta kauheammin yrittämään murtautumaan sisään. Siinä mielessä on ehkä järkevä pitää matalaa profiilia" (H3)

5.2.6 Myynnin edistäminen

Myynnin edistäminen, jolla tarkoitetaan sertifikaatin potentiaalia hankkia uusia asiakkaita, tai myyntiprosessia helpottavaa vaikutusta, oli kaikille kohdeorganisaatioille yhteinen tekijä, joka koettiin sertifikaatista saatuna hyötynä. Hyöty oli vahvasti yhteydessä seuraavassa alaluvussa esiteltyyn taloudellisen säästön tuomaan hyötyyn. Käytännössä kuitenkin sertifikaatin kyky edistää myyntiä korostui esimerkiksi ulkomaisella markkinalla toimiessa, jossa luottamuksen saaminen saattaa olla haasteellisempaa. Tällöin myyntiprosessi muuttuu yksinkertaisemmaksi, kun tarjousvaiheesssa tietoturva-aspektin voi osoittaa sertifikaatilla.

> "Jos tätä sertifikaattia ei olisi, niin osa asiakkaistamme ei tulisi meidän asiakkaiksemme. Sitä vaativat niin yksityisen kuin julkisen sektorin toimijat." (H4)

> "Mielenkiintoista kyllä, täällä kotimaassa siitä on vähemmän hyötyä kuin sitten tuolla Läntisessä-Euroopassa, mutta kyllä se niin kuin edellytys on sille, että näiden isojen kansainvälisten toimijoiden kanssa ylipäätään päästään kauppaa tekemään." (H2)

> "Sertifiointi vaatii resursseja, mutta se vähentää resurssitarvetta myyntiprosessin aikana. Minulle kohdistuvat kysymykset ovat ainakin pienempiä ja myyjillä on helpompi työ myydä" (H1)

> "Ilman muuta sertifikaatilla on myyntiä edistävä vaikutus, sillä kun meidän asiakkaamme sitä kyselee, niin ilman sertifikaattia meidän olisi hankalampi tarjota meidän palveluitamme ja todentaa asioita." (H5)

Yksi haastateltavista organisaatioista ei kokenut sertifikaatilla olevan suurta myyntiä edistävää vaikutusta, koska organisaation pääasiallinen toiminta tapahtuu kuluttajamarkkinoilla, jossa sertifikaatin merkitys on vähäinen. Organisaatio kuitenkin tunnisti potentiaalin tilanteessa, jossa se alkaisi myydä omia tuotteitaan ulkomailla toimiville saman alan organisaatiolle.

> "On mietitty, että alettaisiin myydä meidän omia tuotteitamme myös ulkomaille, ja siinä sertifikaatista olisi varmasti hyötyä." (H3)

5.2.7 Taloudelliset säästöt

Taloudelliset säästöt jakautuivat jossain määrin jo edellä esitetyn myynnin edistämiseen liittyviksi säästöiksi myyntiprosessin aikana. Tällä tarkoitetaan tarkemmin sitä, kun tarjousvaiheessa organisaatio voi joutua osoittamaan omaa tietoturvansa tasoa erilaisilla kyselyillä, niin sertifikaatilla kyetään kuittaamaan suuri osa kyselyn vaatimuksista. Tämä taas suoraan vähentää tarjousten tekemiseen vaadittavaa työmäärää ja säästää resursseja muuhun. Muun muassa yksi

haastateltavista vastasi kysymykseen sertifikaatin mahdollisuudesta tuottaa taloudellisia säästöjä seuraavasti:

> ”Tuottaa juu, konkreettisimmin hyötyä tarjousprosesseissa, kun siellä tulee semmoinen raamatun paksuinen tietoturvakysely. Siitä selviää aika paljon helpommalla, jopa lyhyellä lomakkeella.” (H2)

Kolme haastateltavaa organisaatiota näki sertifikaatin tuottavan säästöjä myös muilla tavoin. Sertifikaatti muun muassa vähentää auditointien määrää, kun asiakkaat eivät erikseen tule auditoimaan sertifioitua organisaatiota ja näin ollen myös riski tiedon leviämisestä pienenee.

> ”Sertifikaatti pitää kontrollin itsellä ja tällöin ulkopuoliset (asiakkaat) eivät tule auditoimaan. Myös löydöksistä oppiminen, riskien tunnistaminen ja vahinkojen estäminen tuottavat säästöjä.” (H4)

Toisaalta tietoturva voidaan nähdä osana liiketoimintaa tukevia prosesseja, eli tietoturva ei ole vain pakollinen kuluerä, vaan myös liiketoimintaa mahdollistava investointi.

> ”Tietoturva on nähty ehkä sellaisena business prevention departmentina, mutta totta kai sen tehtävä on tukea liiketoimintaa.” (H1)

Sertifikaatti ja sen tuoma riskipohjainen ajattelu myös auttaa organisaatiota miettimään kulutus- ja investointitarpeita tehokkaammin, kun se kykenee arvioimaan uhkia ja kustannuksia entistä tarkemmin.

> ”Mun mielestä se tuo säästöjä, koska me on tehty riskiarviot ja arvio siitä tarpeesta, mikä meille riittää, niin sitä kautta me on pystytty helpommin sanomaan mikä meille on tarpeellista ja mikä ei ole.” (H5)

Kuitenkin yhden organisaation kohdalla sertifikaatilla ei nähty olevan suoria säästöjä omassa toiminnassa, mutta omien toimittajien kokema hyöty sertifikaatin esittämisestä kuitenkin tunnistettiin.

> ”Ei se säästöjä tuota. Kulujahan siinä on, mutta tämän kokoisessa firmassa ne eivät ole mitenkään merkittäviä. Mutta toki, kun me valitsemme omia toimittajiamme, kun meillä on tietoturvavaatimuksia, niin sillä he pystyvät kuittaamaan asioita meidän suuntaan.” (H3)

5.2.8 Yrityksen arvo

Kaikki haastateltavat henkilöt olivat sitä mieltä, että organisaation arvo nousee sertifioinnin myötä. Arvonnousu nähtiin pääasiallisesti kolmannen osapuolen tarkastuksen tuoman luottamuksen kautta.

> ”Mielestäni sertifikaatti nostaa yrityksen arvoa, koska se on kuitenkin kolmannen ja riippumattoman osapuolen todistus siitä, että asiat hoidetaan hyvin.” (H3)

> ”Kyllä se sertifikaatti nostaa arvoa, koska silloin on panostettu asioihin ja saadaan meihin lisää luottamusta, kun sertifikaatti on voimassa.” (H4)

5.2.9 Sertifikaattiin liittyvät investoinnit

Eräs tämän tutkimuksen päämääristä oli tutkia sitä, miten organisaatiot suhtautuvat tietoturvaan liittyviin investointeihin. Ensin organisaatioita pyydettiin kuvailemaan johdon suhtautumista tietoturvainvestointeihin ja tulos oli varsin selkeä, sillä kaikissa organisaatiossa tietoturvainvestointeihin suhtauduttiin siinä mielessä positiivisesti, että investoinnit olivat kaikissa organisaatioissa helppo perustella.

> ”Liikkeenjohdolle on hyvin helppo perustella kustannukset ja ennemminkin se tuli minulle annettuna tehtävänä, joka pitää hoitaa.” (H1)

> ”Hallitus kyllä olisi sertifiointia kyllä vaatinut, ellei päätöstä olisi jo aiemmin tehty” (H2)

> ”En tiedä onko koskaan tarvinnut tietoturvabudjetista johdon kanssa keskustella. Meidän kokoluokan firman mittakaavassa se määrä on pieni, melkein verrattavissa kiinteään kuluun.” (H3)

> ”Osa (sertifikaatin kattamista osista) kuuluu tarjottuihin palveluihin, joten sitä kautta ne on riskiarvion perusteella helppo perustella.” (H4)

> ”Koska sitä (sertifiointia) halutaan ylläpitää, niin kyllähän se päätös johdolta on tullut, että sitä ylläpidetään.” (H5)

Haasteltavien kanssa keskusteltiin myös siitä, miten kohdeorganisaatiot investoivat tietoturvaan. Kaikissa kohdeorganisaatioissa tietoturvainvestoinnit olivat suunniteltuja ja riskipohjaisesti perusteltuja. Kohdeorganisaatiossa tietoturvaan halutaan investoida sen verran rahaa, että se varmasti riittää, mutta toisaalta investointitasoa pyritään optimoimaan riskienhallinnan ja sertifikaatin vaatiman tason perusteella. Kaikki kohdeorganisaatiot myös kokivat sertifikaatin tuottavan enemmän hyötyä ja tuottoa kuin se vaatii investointia, vaikka erotusta rahallisesti välttämättä arvioitu sen tarkemmin.

> ”Tietoturva pitää nähdä vakuutustoimintana, eli joka tapauksessa pitää laittaa rahaa likoon, että mahdollisia infiltraatioita estetään. Meillä sitä priorisointia lähdetään hakemaan riskienhallinnan kautta, josta kulut saadaan perusteltua liiketoimintatavoitteilla, eli yksittäisestä tietoturvakontrollista voidaan se polku vetää sinne ylös asti, että se kontrolli on tämmöisen liiketoimintatavoitteen takia. Eli tuki pitää löytyä ylhäältä alas ja jopa toiseen suuntaan.” (H1)

> ”tehdään välttämättömyydestä hyve, ja nyt ollaan ennemmin ylläpitomoodissa ja sen eteen tehdään sen verran kuin se vaati, mutta ei välttämättä enempää. Investoinnit ovat suuruusluokaltaan sellaisia, että niistä kyllä selvitään ja toisaalta jos mietitään että tietoturva ei olisi kunnossa, niin mikä sen merkitys olisi liiketoimintaan, niin siinä

suhteessa investoinnit ovat pieniä. Sitä ei edes tarvitse laskea tuottaako sertifikaatti enemmän kuin se kustantaa." (H2)

"Me on onnistuttu, kun ei olla jouduttu julkisuuteen negatiivisessa valossa ja ne ovat meille niitä perimmäisiä mittareita. Meillä on varaa ottaa safetyn puolelta, eli ei tarvitse miettiä sitä, että satsataanko tietoturvaan, vaan me voidaan hoitaa se kunnolla." (H3)

"Investoinnit arvioidaan riskien kautta. Mikä on riskin seuraus, kustannus ja brändivaikutus. Tietoturvabudjetti pyritään määrittelemään mahdollisimman konkreettisesti, jotta se on helppo ymmärtää." (H4)

"Meillä on myös omat minimivaatimukset tietoturvan osalta, jotka kulkee aika hyvin käsi kädessä ISO 27001:n kanssa, mikä tarkoittaa sitä, että tietyllä investoinnilla on tietyt vaatimukset tietoturvan osalta. Meidän on täytettävä vaatimukset, ja sitä kautta sertifikaatti myös vaikuttaa niihin tekemiimme hankintoihin." (H5)

"Sertifikaatti on kustannuksiin nähden kannattava" (H5)

Kun haastateltavien kanssa keskusteltiin erilaisista tietoturvan investointiteorioista, niin hieman sama teema toistui vastauksissa, kuin tietoturvainvestointien mittaamisessa: Haastateltavissa organisaatioissa investointeja ei sellaisenaan ajateltu investointeja minkään teorian pohjalta, mutta niissä vahvasti sovellettiin osia tai periaatteita tunnetuimmista teorioista. Teoriat olivat myös monilta osin tuntemattomia, vaikka organisaation oma toiminta saattoi olla hyvin lähellä jonkin teorian mukaista mallia. Kuitenkin kaikissa organisaatioissa investointeja ajateltiin standardin lähestymismallin mukaisesti organisaatiota koskevien riskien kautta.

"Se mitä suojellaan vaikuttaa investoinnin määrään ja tasoon, eli konteksti vaikuttaa. Näkökulmia on kuitenkin monia, eikä pelkästään numeroilla asiaa voi varmistaa." (H4)

"Päätöksentekoteoria se varmasti on mitä käytämme" (H2)

"Kyllä tässä päätöksentekoteoriasta voisi puhua, olen myös jalkauttanut tänne sellaista frameworkia kuin SABSA." (H1)

"Ehkä pöytäharjoittelua (peliteoriaa) harrastetaan incident response-puolella, mutta muuten ilman muuta riskiperusteisesti toimitaan." (H3)

"Käytetään sekä päätöksentekoteoriaa, mutta omassa sovelluskehityksessä threat modeling -työkaluna käytetään peliteoriaa mallintamaan erilaisia riskejä ja tilanteita." (H4)

"Riskienhallinta on vahvasti joka paikassa mukana" (H5)

5.3 Muut tekijät

5.3.1 Lain vaatimusten täyttäminen

Haastatteluissa kysyttiin myös ISO/IEC 27001 -standardin mukaisen johtamisjärjestelmän ja sertifikaatin vaikutusta lainsäädännön asettamien vaatimusten täyttämisessä. Erityisesti Euroopan Unionin tietosuoja-asetus GDPR nousi vahvasti esille. Haastateltavat näkivät kuitenkin muitakin yhteyksiä lainsäädäntöön. Tämä yhteys ei kuitenkaan välttämättä ollut täysin suora, vaan standardi ja sertifikaatti avustivat lainsäädännön asettamien vaatimusten täyttämisessä epäsuorasti. Yhdessä tapauksessa organisaatio ei kokenut sertifikaatista suoraa apua, vaan koki, että kahdenväliset sopimukset ovat parempia hoitamaan vastuukysymyksiä.

> ”GDPR:ssä ja ISO 27001 on paljon samaa, eli tietosuoja-asetusta on helppo seurata.” (H5)

> ”GDPR:n hanskaaminen on verrattomasti helpompaa” (H2)

> ”Joo, kyllä ilman muuta sertifikaatista on ollut GDPR:n täyttämiseen apua, kun siellä on niitä tietoturvaan liittyviä vaatimuksia.” (H3)

> ”Asiakkaiden kautta tulee muun muassa finanssivalvonnan valvomia huolellisuusvelvotteita, niin kyllähän se (sertifikaatti) on verraton apu.” (H2)

> ”Meillä on viikoittain useampia palavereja valvovien viranomaisten kanssa ja sertifiointi kyllä auttaa varmasti tässä.” (H3)

> ”Laissa ja määräyksissä ylätason vaatimukset ovat yhdistettävissä sertifikaatteihin.” (H4)

> ”Meille ei tule suoraan laista vaatimuksia, mutta asiakkaiden kautta voi tulla jotain, jotka vaikuttavat myös meihin, mutta pitkälti nämä vastuuasiat hoidetaan kahdenvälisillä sopimuksilla.” (H1)

5.3.2 Muiden standardien implementointi

Koska ISO/IEC 27001 koetaan alan yleiseksi standardiksi, joka sisältää tietoturvan perusvaatimuksia, oli aiheellista tutkia onko sertifikaatin avulla helpompi siirtyä muihin standardeihin useampia sertifiointeja varten. Kaikki haastateltavat näkivät yhteyden ja potentiaalin, joten ISO/IEC 27001 voi toimia linkkinä muiden tietoturvasertifikaattien saavuttamiseksi.

> ”Musta ISO 27001 on tietoturvan perusteita, ja vielä suurin osa hyvin valittuja. Samahan se on myös muissa standardeissa, eli perusteet niissäkin on samaa, varmaan 50-60-70 % samoihin spekseihin vietävissä.” (H5)

”Kyllä se auttaa, koska on päällekkäisiä kontrolleja. Tietyn teollisuudenalan sertifikaattien suorittamiseen saattaa olla helpompaa tai ainakin suoraan verrata sertifikaattia siihen.” (H4)

”Kyllä se sertifiointi helpottaa, koska vaatimukset on kuitenkin aika pitkälle yhteneväiset monessa standardissa” (H1)

”Kyllä se voisi auttaa ISO 9001 hankkimisessa, mutta nykyinen sertifiointi korvaa sen” (H2)

”Meillä on myös PCI-sertifiointi, ja näen että siinäkin se auttaa, esimerkiksi tietoturva-tietoisuuteen liittyvät asioissa.” (H3)

5.3.3 Vakuutusmaksujen aleneminen

Haastateltavilta kysyttiin myös muista mahdollisista eduista, kuten kybervakuutuksen hintaan vaikuttamisesta. Muita tekijöitä ei ilmennyt ja vakuuttamisestakin näkemykset olivat enemmän arvelevia kuin varmaa tietoa, joten tulosten perusteella vakuutusten osalta sertifikaatin vaikutus on pieni, tai haastateltavat eivät tiedä siitä, sillä vakuutukset eivät kuulu heidän vastuualueelleen.

”Suoraan sertifikaattia ei ole vakuutusta hankkiessa kysytty, mutta viittasimme kyllä sertifikaattiin joidenkin kysymysten kohdalla.” (H1)

”Vakuutuksissa kysytään tiettyjä asioita, jotka alentavat vakuutusmaksuja, ainakin näin luulisin etenkin kybervakuuttamisessa.” (H4)

”Olen kuullut, että jossain tämmösiä on, ja että sillä on vaikutusta, joten luulisin että näin on.” (H5)

5.4 Sertifioinnin haasteet ja syyt luopua sertifikaatista

Haastateltavilta kysyttiin myös syitä luopua sertifikaatista ja sertifikaatin ylläpitämiseen liittyvistä suurimmista haasteista, jotka aiheuttavat eniten ongelmia sertifikaatin ylläpitämisessä. Vastauksissa tuli ilmi kaksi tekijää, jotka nousivat esille: Sertifikaatin sopivuus organisaatiolle ja sertifikaatin ylläpitämiseen liittyvät velvoitteet.

5.4.1 Sopivuus

Yksikään tutkittavista organisaatioista ei ollut valmis luopumaan sertifikaatista, mutta kaksi organisaatiota ilmaisi, että olisivat ehkä valmiita miettimään jotain toista sertifiointia, jos se koettaisiin paremmin sopivammaksi tai hyödyllisemmäksi.

> ”Ollaan mietitty, että onkohan tämä se oikea sertifikaatti, mitä me tarvitaan, koska asiakkailta on tullut sitten kyselyä myös muista sertifioinneista, jotka on kattavampia. Esimerkiksi SOC, Katakri ja VAHTI.” (H1)

> ”En usko, että luovuttaisiin sertifikaatista, ellei tulisi joku vastaava hallintamalli, joka katsotaan jostain syystä meillä toimivammaksi.” (H5)

5.4.2 Sertifioinnin ylläpitoon liittyvät velvoitteet

Kaikilla organisaatioilla kuitenkin nousi esiin haasteena se työ, mitä vuosittaisen syklin mukainen toiminta vaatii, jotta sertifiointi saadaan ylläpidettyä hyväksytysti. Esiin nousseita teemoja olivat muun muassa jatkuva parantaminen, integraatio ja jalkauttaminen.

> ”Jatkuva parantaminen siltä osin, että kaikilla osa-alueilla on näytettävissä se, että ollaan menossa parempaan suuntaan.” (H1)

> ”Sehän nyt (sertifikaatti) vaatii jonkun verran erityispanostusta vuosisyklin mukaan” (H2)

> ”Integraatio organisaatiomuutoksen jälkeen on meille se suurin haaste” (H3)

> ”Scopen laajentaminen on tällä hetkellä puheissa ja organisaation sisäiset muutokset aiheuttavat lisätöitä.” (H4)

> ”Jalkautuksen osalta ISO 27001 aiheuttaa lisätyötä esimerkiksi yritysostojen kohdalla.” (H5)

5.5 Sertifiointielimen valintaperusteet

Tämän tutkimuksen toinen päätutkimuskysymys keskittyi sertifiointielimen valintaperusteisiin. Valintaperusteissa keskityttiin etsimään erilaisia tekijöitä, jotka vaikuttavat sertifiointielimen valintaan ja samalla myös tutkittiin niiden merkitystä ja painoarvoa osana valintaa.

5.5.1 Kilpailutuksen merkitys

Ensimmäisenä haastateltavien kanssa keskusteltiin sertifiointielimen valintatilanteessa tapahtuvasta kilpailuttamisesta, ja tulokset osoittivat, että kilpailutusta tapahtuu melko vähän, tai se tehdään kevyesti.

> ”Aina on ollut sama, ja sertifiointielintä ei ole kilpailutettu välissä, koska se ehkä on ollut organisaation tapa toimia eikä päätöstä ole toisaalta ole haastettu. Se myös ehkä nähtiin hyötynä, että sitä historiatietoa on.” (H1)

”kilpailutettiin kevyesti, otettiin luotettavaksi tiedettyjä toimijoita kilpailutukseen” (H2)

”Ei olla kilpailutettu, koska haluamme kaikki auditoinnit samasta paikasta, ja tällä hetkellä se on mahdollista vain yhdestä paikasta.” (H3)

”Kilpailutusta on aina arvioitu syklin lopussa, mutta nyt on pitkään ollut sama, koska auditoija tuntee organisaatiomme.” (H4)

”Meidän kohdallamme on muutama iso ja kriteereihimme sopiva toimija, joista sertifiointielin valitaan.” (H5)

5.5.2 Sertifiointielimen maine

Kaksi haastateltavaa toi ilmi maineen vaikutuksen. Ensimmäinen haastateltavista pohti sertifiointielimen maineen vaikutusta organisaation markkina-alueella, kun taas toinen toi ilmi omien asiakkaiden kiinnostuksen sertifikaatin myöntäjään. Kummatkin näistä tekijöistä tulevat asiakkailta, joten sertifiointielimen maine voi näyttäytyä asiakkaan suuntaan merkittävänä.

”Pyrittiin keskustelemaan vain sellaisten toimijoiden kanssa, joilla on hyvä maine. Siinä nyt ehkä mielenkiintoisin nyt on se, että onko se (sertifiointielin) suomalainen vai ulkomaalainen, kun toimitaan eurooppalaisella kentällä. Siinä voisi olla, että joku ulkomainen toimija voisi tuoda lisäuskottavuutta, mutta toistaiseksi ei ole millään tavalla vaikuttanut” (H2)

”Melko usein meiltä kysytään kuka sen sertifioinnin on tehnyt, koska joillekin asiakkaille sillä voi olla merkitystä.” (H5)

Yksi haastateltavista organisaatioista toi ilmi vaatimuksen sille, että sertifiointielimen pitää olla virallinen, joka viittaa sertifiointielimen akkreditointiin. Myös tämä tekijä katsottiin olevan sertifiointielimen maineeseen viittaava tekijä.

5.5.3 Olemassa olevat suhteet

Kaikkien haastateltavien organisaatioiden kohdalla nousi esille olemassa olevien suhteiden vaikutus, mutta näkemykset olivat kuitenkin kaksijakoisia. Toisaalta olemassa olevat suhteet nähtiin hyvinä siinä mielessä, että yhteistyötä oli helppo jatkaa tunnettujen ihmisten kanssa hyödyntäen edellisten vuosien kokemuksia. Toisaalta kuitenkin auditoijan vaihtaminen nähtiin mahdollisuutena saada uusia näkemyksiä, mikä voisi tuottaa uusiin löydöksiin ja johtamisjärjestelmän kehittymiseen.

”Historiatieto nähtiin hyötynä. Vaikka sertifioinnissa ei konsultointinäkökulmaa tuoda mukaan, niin siellä on annettu aikaisemmin semmoisia hyviä vinkkejä asioista, mihin kannattaa kiinnittää huomiota.”(H1)

”Jos vaihtaisin sertifiointielintä, niin ehkä se menisi enemmän henkilökemiaan liittyvistä syistä, mutta sellaista syytä ei ole tullut vastaan.” (H1)

”Meidän nykyinen sertifiointielimemme tuntee meidän organisaatiomme. Että jos nyt otettaisi joku muu, niin 2-3 vuotta menisi siihen, että he kysyisivät sellaisia ikään kuin tyhmiä kysymyksiä, mitä nykyisen auditoijan ei tarvitse kysyä. Nyt päästään nopeammin itse asiaan, kun heillä on kokemusta meidän organisaatiostamme.” (H3)

”Yksi syy miksi voisimme vaihtaa auditoijaa, on se, että tulisi uutta näkemystä. Nyt auditoija tuntee meidät ja me tunnetaan auditoija. Kun auditoija tulee paikalle kerran vuodessa ja juodaan kahvia ja jutellaan, niin voisi olla hyvä, että joku tulisi uutena ja tuorein silmin paikalle.” (H5)

5.5.4 Ammattitaito

Auditoijan ammattitaito tunnistettiin kaikissa haastatteluissa tärkeäksi tekijäksi. Ammattitaitoista auditoijaa pyrittiinkin sen vuoksi etsimään jo hankintavaiheessa, koska jos auditoija ei osaa tehdä oikeita löydöksiä asiakas ei saa auditoinnista kaikkea hyötyä irti. Tällöin houkutus vaihtaa auditoijaa nousee, koska organisaation intresseissä on saada johtamisjärjestelmästään turvallisempi.

”Se on merkittävä juttu, että auditoija osaa löytää oikeita juttuja. Edelliskerralla tuntui, että auditoija kiinnitti ehkä hieman erikoisiin yksityiskohtiin huomiota, joka sai miettimään, että pitäisiköhän koittaa vaihtaa auditoijaa.” (H1)

”Pyrittiin keskustelemaan vain sellaisten toimijoiden kanssa, joilla on hyvä maine.” (H2)

”Auditoijan ammattitaito on hyvä asia, koska minä katson asiaa tietoturvan kannalta ja mitä paremmin me saadaan asioita löydettyä niin sen parempi minulle.” (H5)

5.5.5 Hinta

Hinnan merkitys tunnistettiin kaikkien organisaatioiden keskuudessa, mutta sen merkitys koettiin pääasiassa erittäin pieneksi verrattuna esimerkiksi laatuominaisuuksiin. Erityisesti suuremmat organisaatiot kokivat muut tekijät, kuten kyvykkyyden toimia globaalisti suurempana. Lisäksi haastateltavien mukaan markkinoilla hinnat ovat melko tasaisia, joten erottuvuus tulee sertifiointielinten välillä muista tekijöistä.

”Hintaerot oli pieniä, joten ei suurta vaikutusta, mutta ulkomaisilla tulee toki aina matkakuluja, joka aina vaikuttaa.” (H2)

”Hinta kyllä vaikuttaa, mutta isona organisaationa kykenemme kyllä neuvottelemaan hinnasta.” (H4)

”Meidän tapauksessamme hinta ei voi olla ainut peruste, sillä sertifiointielimeltä vaaditaan myös muita ominaisuuksia.” (H5)

5.5.6 Käytännöllisyys ja mukautuminen

Käytännöllisyys ja mukautuminen tarkoittavat tässä tutkimuksessa sitä, että sertifiointielin kykenee joustamaan ja tarjoamaan palveluitaan mukautuen asiakkaan tarpeisiin. Käytännössä se voi tarkoittaa yhteistä natiivia kieltä, kykyä toimia paikallisesti eri paikoissa tai vaikkapa kykyä reagoida nopeasti erilaisiin muutoksiin.

> ”Luulen, että se yhteistoiminta on helpompaa suomalaisten kanssa, etenkin kun meillä on dokumentaatiota paljon suomen kielellä.” (H1)

> ”Jos oletetaan, että laadulliset tekijät on suurin piirtein samalla viivalla, niin sitten käytännön asioilla on vaikutusta, mutta jos perustekijöissä eroa, niin joustavuuskysymykset jäävät sekundaarisiksi.” (H2)

> ”Ilman muuta käytännön asioilla on merkitystä. Meillä on esimerkiksi dokumentaatio suomeksi. Vaikuttaa myös haastatteluihin, vaikka kaikki periaatteessa osaa englantia, niin kyllä oman asian kertominen englanniksi on hankalampaa.” (H3)

Kahden suuren ja kansainvälisen organisaation kohdalla käytännöllisyysasiat koskivat lähinnä sitä, että sertifiointielin kykenee toimimaan globaalisti siellä, missä organisaatioilla on omaa toimintaa. Lisäksi kyky toimia eri kielillä nähtiin positiiviseksi asiaksi, vaikka englanti toimisi pääkielenä.

> ”Hankintaosastomme arvioi toimiiko sertifiointielin globaalisti ja kykeneekö se tekemään työn englanniksi. Lisäksi auditoijalta vaaditaan kyvykkyyttä toimia paikallisesti maissa, joissa meillä on toimintaa.” (H4)

> ”Meidän tapauksessamme kilpailutukseen vaikuttaa laajuus ja kansainvälisyys. On kuitenkin hyvä, jos haastattelut voidaan tehdä natiivilla kielellä.” (H5)

5.5.7 Palvelutarjonta

Palvelutarjonnalla tarkoitetaan tässä yhteydessä sertifiointielimen kykyä tarjota useampia sertifiointi- ja auditointipalveluita asiakkaalle siten, että asiakkaan ei tarvitse hankkia niitä usealta eri toimijalta. Tämä ominaisuus nähtiin pääasiassa hyvänä, mutta käytännön rajoitteet usein estävät sen, että kaikki halutut ja vaaditut sertifioinnit voitaisiin hankkia samasta paikasta. Lisäksi sertifiointielinten kykyyn tarjota kaikkia palveluita ammattitaitoisesti epäiltiin.

> ”Kyllä minä ainakin ehdottaisin, että saisimme yhdestä paikasta täytettyä niitä muitakin tarpeita. Yhdeltä luukulta on tähänkin mennessä asioita hoidettu.” (H1)

> ”Jos tilanne olisi se, että joku voisi tarjota kaikki tarvitsemamme sertifioinnit, niin olisihan se kiva, mutta kun se ei teoriassa ole mahdollista niin en näe tällä kovin suurta merkitystä.” (H2)

”Meilläkin on vain yksi hallintajärjestelmä, eikä erillistä laatu- ja tietoturvan hallintajärjestelmää. Ne standardit, jotka ovat läheisesti yhteydessä toisiinsa, niin ne sertifioinnit on hyvä hankkia samasta paikasta.” (H3)

”ISAE:ssa ja ISO:ssa on muutama suuri toimija, joista se auditoija valitaan, koska ne voivat tarjota meille ne palvelut, joita tarvitsemme.” (H4)

”Yksi syy hankkia sertifiointeja eri paikoista voi olla yksinkertaisesti esimerkiksi osaaminen, eli onko sertifiointielimen mahdollista ylläpitää niin laajaa osaamista, että siellä kaikki standardit hallitaan sitten.” (H5)

5.5.8 Valintaperusteiden merkitsevyys

Haastattelun lopussa haastateltavia pyydettiin järjestämään neljä ennalta määritettyä valintaperustetta tärkeysjärjestykseen. Neljä viidestä haastateltavasta valitsi tärkeimmäksi tekijäksi auditoijan ammattitaidon. Niin ikään, neljä viidestä valitsi toiseksi tärkeimmäksi käytännöllisyyteen ja mukautumiseen viittaavat tekijät. Olemassa olevat suhteet ja hinta jakautuivat tasaisesti kolmanneksi ja neljänneksi tärkeimmäksi tekijäksi. Tulokset on esitelty alla olevassa Taulukossa 5.

Taulukko 5 Sertifiointielimen valintaperusteet tärkeysjärjestyksessä

Numero	**1**	**2**	**3**	**4**
H1	Olemassa olevat suhteet	Käytännöllisyys	Ammattitaito	Hinta
H2	Ammattitaito	Hinta	Olemassa olevat suhteet	Käytännöllisyys
H3	Ammattitaito	Käytännöllisyys	Olemassa olevat suhteet	Hinta
H4	Ammattitaito	Käytännöllisyys	Hinta	Olemassa olevat suhteet
H5	Ammattitaito	Käytännöllisyys	Hinta	Olemassa olevat suhteet

5.6 Tulokset kootusti

Tulokset kerättiin lopuksi vielä yhtenäisiin taulukoihin kuvaamaan sitä, mitkä tekijät koettiin haastateltavien kanssa vaikuttaviksi organisaation omalla kohdalla. Merkintä pyrittiin laittamaan vain silloin, kun haastateltava antoi vahvan osoituksen tekijän merkittävyydestä, joten esimerkiksi pelkkää veikkausta tai arvelua jonkin tekijän vaikuttavuudesta ei kelpuutettu luotettavaksi tekijän merkittävyyttä arvioidessa. Alla olevassa taulukossa (Taulukko 6) on esitelty sertifioinnin hankintaan ja ylläpitoon vaikuttavat tekijät ja niiden esiintyminen eri kohdeorganisaatioiden kohdalla. Taulukko on jaettu eri näkökulmien mukaan neljään osaan.

Taulukko 6 Sertifioinnin hankintaan ja ylläpitoon vaikuttavat tekijät

Tekijä	**H1**	**H2**	**H3**	**H4**	**H5**
Tietoturvanäkökulma					
Tietoturvan hallinnan parantuminen	X	X	X	X	X
Jatkuva parantaminen	X	X	X	X	X
Sertifikaattiin liittyvät velvollisuudet	X	X	X	X	X
Taloudellinen näkökulma					
Asiakkaiden vaatimus	X	X	X	X	X
Toimialakohtainen vaatimus			X		
Kilpailuetu				X	X
Luottamus ja uskottavuus	X	X	X	X	X
Sertifikaatti markkinointikeinona	X	X	X	X	X
Myynnin edistäminen	X	X		X	X
Taloudelliset säästöt	X	X		X	X
Yrityksen arvo	X	X	X	X	x
Sertifikaattiin liittyvät investoinnit	X	X	X	X	X
Muita tekijöitä					
Lain vaatimusten täyttäminen	X	X	X	X	X
Muiden standardien implementointi	X	X	X	X	X
Vakuutusmaksujen aleneminen	X			X	
Luopumiseen liittyvät tekijät					
Sopivuus	X				X
Sertifioinnin ylläpitoon liittyvät velvoitteet	X	X	X	X	X

Toiseen taulukkoon (Taulukko 7) kerättiin sertifiointielimen valintaperusteisiin liittyvät tekijät. Myös tässä taulukossa tekijät on kirjattu haastateltavien organisaatioiden vastausten mukaan siten, että organisaation arvion mukaan selkeästi merkittävät tekijät päätyivät taulukossa valituiksi.

Taulukko 7 Sertifiointielimen hankintaan vaikuttavat tekijät

Tekijä	**1**	**2**	**3**	**4**	**5**
Kilpailutus	X	X		X	X
Maine		X		X	X
Olemassa olevat suhteet	X		X		
Ammattitaito	X	X	X	X	X
Hinta				X	X
Käytännöllisyys ja mukautuminen	X	X	X	X	X
Palvelutarjonta	X	X	X	X	

Taulukoista voidaan huomata, että tulokset ovat melko yhteneväiset ja erot vastauksissa ovat melko vähäisiä. Tuloksia on tarkemmin eritelty seuraavassa luvussa, jossa yksittäisten tekijöiden taustoja avataan tämän tutkimuksen kontekstissa.

6 POHDINTA

Tässä luvussa tutkimuksen tuloksissa esiteltyjä löydöksiä analysoidaan suhteessa teoriaosuudessa esitettyyn aiempaan teoriaan. Luku noudattelee tutkimuskysymysten mukaista järjestystä siten, että ensin käsitellään sertifioinnin hankkimisen ja ylläpitämisen perusteena olevien tekijöiden merkitystä, minkä jälkeen esitellään sertifiointielimen valintaan liittyviä tekijöitä.

6.1 ISO/IEC 27001 -sertifikaatin hankkimiseen ja ylläpitämiseen vaikuttavat tekijät

Tämän tutkimuksen kahdesta päätutkimuskysymyksestä toinen kysyy: Miksi yritykset päättävät hankkia ISO/IEC 27001 -sertifioinnin ja ylläpitävät sitä? Jotta tätä kokonaisuutta pystyttiin lähestymään järkevästi, määriteltiin tälle kysymykselle apututkimuskysymys, joka pyrkii selvittämään sertifioinnista saatavia hyötyjä, joilla voitaisiin selittää sertifioitujen organisaatioiden käyttäytymistä. Hyvin nopeasti ilmeni, että hyötyjä on pääasiassa kolmea eri luokkaa: tietoturvahyötyjä, taloudellisia hyötyjä ja muita näihin luokkiin sopivia hyötyjä, jotka epäsuorasti periytyvät kahdesta ensimmäisestä. Toisaalta olemassa on myös tekijöitä, jotka saattavat vaikuttaa sertifikaatista luopumiseen. Tutkimuksen empiirisessä osuudessa tekijöitä löytyi yhteensä 17, joista kolme liittyi tietoturvahyötyihin, yhdeksän taloudellisiin hyötyihin, kolme muihin hyötyihin ja kaksi luopumiseen liittyviin tekijöihin. Vaikka tämä tutkimus ei ollut tyypiltään määrällinen, toistui myös tässä tutkimuksessa jossain määrin jo Parkin ym. (2010) kuvaama haaste siitä, että tietoturvan johtamisjärjestelmästä saatavien hyötyjen mittaaminen on haastavaa. Erityisesti ilmi tuli piirre siitä, että hyödyt ovat keskenään riippuvaisia, niitä voi olla vaikea erotella tarpeeksi pieniksi osiksi ja hyötyjen vertailu keskenään on haastavaa. Sertifioinnista saatavat hyödyt ovatkin laajoja ja toisiinsa sidonnaisia.

Tietoturvanäkökulmaan liittyen tässä tutkimuksessa löytyi kolme tekijää, tietoturvan hallinnan kokonaisvaltainen parantuminen, jatkuva parantaminen ja sertifikaattiin liittyvät velvollisuudet. Näistä ensimmäinen on juuri melko geneerinen kokoelma erilaisia tietoturvahyötyjä, koska hyödyt voivat olla toistensa tuotteita. Esimerkiksi prosessien kehittyminen voi johtaa tietoturvatietoisuuden kasvamiseen, joka itsessään on hyöty. Kuitenkin tuloksissa tuli ilmi, että organisaatiot kokivat tietoturvan johtamisjärjestelmän hyödylliseksi hallintatyökaluksi, joka tarjoaa hyvän mallin tietoturvan perusteita ja mahdollistaa tietoturvan jalkauttamisen tehokkaasti koko organisaation tasolle. Yksi organisaatio jopa näki ISO/IEC 27001 -mukaisen johtamisjärjestelmän erinomaisena työkaluna kahden tai useamman organisaation integraation loppuun saattamisessa. Nämä positiiviset tekijät parantavat organisaation tietoturvan tasoa monella mittarilla mitattuna. Näitä mittareita olivat muun muassa kehittyneet sisäiset prosessit ja

ihmisten kasvanut tietoturvatietoisuus. Toisaalta johtamisjärjestelmän toiminta oli vahvasti riippuvainen organisaation johdon vahvasta tuesta, joka tuli ilmi kaikissa organisaatioissa. Löydökset ovat vahvasti yhteneväiset olemassa olevan tutkimuksen kanssa, sillä muun muassa It Governancen (2018a) vastaavat tutkimukset hyödyistä ovat saman suuntaisia, muun muassa arvottaen tietoturvan tason parantumisen suurimmaksi hyödyksi ja sisäisten prosessien parantumisen toiseksi. Myös muut tekijät voidaan yhdistää löydettyihin tekijöihin: Brennerin (2007) mukainen johdon sitoutumisen merkitys oli selkeästi havaittavissa tutkimuksen analyysissä, sekä Barletten ym. (2008) huomio tietoturvatietoisuuden kasvusta oli helposti havaittavissa myös tämän tutkimuksen tuloksista. Lisäksi Parkin ym. (2010) esittämä väite tietoturvan suojaustason parantumisen vaikutuksesta tietoturvatietoisuuteen tuli tämän tutkimuksen tuloksissa selkeästi osoitetuksi.

Toinen läheisesti tietoturvan hallinnan parantumiseen liittyvä tekijä oli jatkuva parantaminen, joka liittyy tietoturvan parantumiseen, mutta on kokonaisuutena merkittävä, joten se käsitellään erikseen. Muun muassa Lambo (2006) ja Brenner (2007) korostavat jatkuvan parantamisen tähtäävän siihen, että prosessien kehittyessä riskiarvion mukaiset riskit pienenevät ja organisaation tietoturvan taso kasvaa. Kuitenkin tässä tutkimuksessa jatkuvan parantamisen kokeminen koettiin kaksijakoisesti. Pääosin pyrkimys oli juurikin tietoturvan jatkuvassa parantamisessa, mutta jatkuva parantaminen nähtiin myös mahdollisuutena tiedostettuun riskin kasvattamiseen. Tämä toki myös perustui riskiarvion ja käytettävien resurssien painoarvon laskemiseen, jolloin organisaatio kykeni tehostamaan omaa toimintaansa muilla mittareilla optimoimalla omaa tietoturvan hallintaansa hallitusti. Kuitenkin jatkuvan parantamisen käsite saa täysin erilaisen merkityksen, vaikka sen kokeminen hyötynä ei muutu.

Kolmantena merkittävänä ja selkeästi nimenomaisesti sertifioinnista saatavana tietoturvahyötynä nähtiin sertifioinnin tuomat velvoitteet tietoturvan hallinnan osalta. Myös tällä tekijällä oli polveutuvia vaikutuksia kahteen ensimmäiseen tekijään, sillä sertifikaatin velvoitteet tuottivat myös tietoturvahyötyjä. Organisaatiot muun muassa kokivat, että standardin vaatimukset täyttyvät sertifioinnin seurauksena paljon tarkemmin ja organisaation oma ajattelu kattaa standardin paljon laajemmin. Tämä johtaa dokumentaation ja prosessien parantumiseen ja saa toiminnan määrämuotoiseksi. Syynä sertifioinnista koettuihin tietoturvahyötyihin nähtiin auditointi, koska siinä ulkoinen toimija tarkastelee riippumattomasti johtamisjärjestelmää ja pyrkii arvioimaan sen toimivuutta. Tällöin organisaatiolla on tietty pakko ylläpitää johtamisjärjestelmää tarkemmin ja jatkuvasti. Toisaalta myös se, että arvioija tulee organisaation ulkopuolelta ja tekee arvionsa tuntematta organisaatiota ja johtamisjärjestelmää, mahdollistaa uusien näkemysten ja heikkouksien havainnoinnin. Huomionarvoista tuloksissa oli se, että vaikka pakko koettiin aktivoivaksi tekijäksi, sitä ei koettu kovin negatiiviseksi. Syy oli siinä, että organisaation sitoutuessa tietoturvan parantamiseen, se myös koittaa aktiivisesti tehdä töitä sen eteen, sillä tietoturvan edistäminen on sen intresseissä.

Taloudellisia tekijöitä sertifioinnin hankkimisen ja ylläpitämisen syiksi löytyi selkeästi eniten, eli yhdeksän. Tässä tutkimuksessa tuli ilmi, että kaikilla tutkittavilla organisaatioilla sertifikaatin hankkimista ohjasivat tietoturvatekijöiden lisäksi myös taloudelliset intressit, eli sertifikaatilla haettiin organisaation liiketoimintaa edistäviä vaikutuksia. Tässä ei kuitenkaan pidä tehdä oletusta siitä, että sertifikaatti olisi täysin vapaaehtoisesti hankittu. Esimerkiksi Barlette ym. (2008) mainitsevat, että sertifiointi on joissain tapauksissa lainsäädännön vaatima. Suomessa lainsäädäntö ei nimenomaisesti velvoita hankkimaan ISO/IEC 27001 sertifiointia, mutta se on kuitenkin joillain aloilla pakollinen osa markkinoilla toimimiseen. Tässä tutkimuksessa yhden organisaation syy sertifikaatin hankkimiseen oli nimenomaisesti toimialan vaatimus sertifioinnille, sillä ISO/IEC 27001 toimii pohjana toimialan omalle pakolliselle sertifioinnille. Pakollisuuden sijaan muilla sertifikaatin hankkimista ohjasi asiakkaiden vaatimus. Muun muassa Cowan (2011) ja Everett (2011) mainitsevat sertifikaatin osana asiakasvaatimuksia. Tuloksissa kävi ilmi selkeästi se, että sertifikaatin hankkimista on ajanut vaatimus asiakkuuksien saamiseksi. Sertifikaattia vaaditaan nähtäväksi yleensä jo tarjousvaiheessa ja on edellytyksenä sopimuksen syntymiseksi. Täytyy kuitenkin muistaa se, että kaikilla toimialoilla ISO/IEC 27001 sertifikaatti ei ole vaatimus, mutta sitä arvostetaan. Tästä nousikin esiin sertifikaatin hankkimiseen ja ylläpitämiseen viittaava tekijä, joka viittaa kilpailuetuun. It Governancen (2018a) tekemässä kyselyssä 57 % vastaajista koki kilpailuedun kasvattamisen syyksi implementoida tietoturvan johtamisjärjestelmä. Vastaajista kuitenkin vain 35 % koki saavansa johtamisjärjestelmän avulla kilpailuetua. Tämän tutkimuksen tulokset heijastavat myös tätä kehitystä. Kaksi vastaajaa oli selkeästi sitä mieltä, että sertifikaatti on edelleen kilpailuetu, kun muut olivat sitä mieltä, että sertifikaatin merkitys kilpailuetu on laantunut. Jälkimmäinen ryhmä kuitenkin tunnisti sertifikaatin olleen aikaisemmin kilpailuetu, mutta sertifioinnin yleistymisen myötä siitä on tullut vakiintunut käytäntö kilpailuedun sijaan. Tätä näkemystä myös tukee sertifikaattien määrän vahva kasvu, sillä ISO:n (2018) tuottaman ISO Survey -kyselyn mukaan sertifikaattien määrä on viimeisten vuosien aikana kasvanut yli 10 % kasvuvauhtia.

Luottamus ja uskottavuus olivat tekijöitä, jotka nousivat joko suoraan tai epäsuorasti ylivoimaisesti eniten esille keskusteluissa, sillä luottamuksella oli useita johdannaisia hyötyjä. Humphreysin (2006) mukaan sertifikaatin tehtävänä on nostaa luottamusta organisaatiota kohtaan. Sertifikaatista saavutettu luottamus syntyy kolmannen osapuolen osoituksesta siitä, että sertifioitu organisaatio toimii standardin vaatimusten mukaisesti ja sen johtamisjärjestelmän ja prosessit on todettu toimiviksi. (Humphreys, 2006.) Tutkimuksen tuloksissa ilmeni, että luottamuksen merkitys oli korkeampi pienemmillä organisaatioilla, sillä ne kokivat, että niiden oli muuten vaikea saavuttaa uskottavuutta. Tämä löydös on yhteneväinen Hsun ym. (2016) kanssa siitä, että erityisesti pienille organisaatiolle organisaatioille sertifikaatti voi olla elintärkeä. Esimerkiksi suuremmilla organisaatioilla on luonnostaan luotettavampi asema, sillä ne ovat pelkästään kokonsa puolesta merkittävämpiä ja vaikutusvaltaisempia toimijoita markkinoilla, kun taas pienten organisaatioiden täytyy pystyä osoittamaan toimintansa

luotettavuus muilla keinoilla. Kuitenkin kaikki tutkittavat organisaatiot olivat sitä mieltä, että liiketoiminta perustuu luottamukseen, joten yhteistyökumppaneita ja asiakkaita tavoiteltaessa sertifikaatin merkitys luottamusta lisäävänä tekijänä ei voi ohittaa. Luottamus syntyy kolmannen osapuolen vakuutuksesta siitä, että sertifioitu organisaatio todella toteuttaa standardin vaatimuksia vastaavasti ja suhtautuu tietoturva-asioihin vakavasti. Luottamuksella on vahva vaikutus niin uusiin kuin olemassa oleviin asiakkuus- ja toimitussuhteisiin. Sertifikaatin merkitys olemassa oleviin suhteisiin kuitenkin pienenee, sillä luottamussuhde on syntynyt jo sopimusta tehdessä. Tässä tapauksessa It Governancen (2018a) tutkimus ja tämän tutkimuksen tulokset ovat yhteneväiset, sillä It Governancen tutkimuksessa 31 % vastaajista koki sertifikaatilla olevan vaikutusta olemassa oleviin asiakkuuksiin. Vaikka tässä tutkimuksessa jo pelkästään otoksen koon takia samanlaista prosentuaalista vertausta ei voida tehdä, oli haastateltavien viesti kuitenkin saman suuntainen, eli merkitys on pienempi, mutta se voidaan kuitenkin havaita. Sertifikaatilla on luottamussuhdetta ylläpitävä vaikutus, sillä sen avulla organisaation on helppo käsitellä tietoturva-aiheisia kysymyksiä ja tarvittaessa osoittaa jonkin tietoturva-aiheisen vaatimuksen kattaminen sertifikaatilla. Näin ollen sertifikaattia on järkevää ylläpitää, vaikka organisaatio ei aktiivisesti etsisikään uusia kumppanuussuhteita.

Uusien asiakkuuksien kohdalla sertifikaatin luottamus auttaa erityisesti myynnin edistämiseen. Kuten Parkin ym. (2010) tutkimuksessa todettiin, prosessien kehittyminen lisää asiakkaiden luottamusta, mikä taas vaikuttaa siihen, että organisaation arvo ja liiketoiminnan tasaisuus kasvavat kohonneen myynnin lisääntyessä. Tämä voidaan todentaa myös It Governancen (2018a) tekemästä tutkimuksesta, jossa puolet vastanneista organisaatiosta koki saaneensa sertifikaatista uusia liikekumppaneita ja implementoinnin syynä se oli lähes puolella juurikin asiakkuuden saavuttamisen takia. Myös tämän tutkimuksen tuloksissa on vahva indikaatio samoista vaikutuksista. Kävi ilmi, että sertifikaatti on joissain tapauksissa vaatimus jo tarjousvaiheessa, tai että sen avulla voidaan välttää pitkiä ja monimutkaisia tietoturvakyselyitä, kun vaatimukset voidaan kuitata sertifikaatilla. Myyntiä edistävä vaikutus oli havaittavissa niin kotimaassa kuin ulkomailla, mutta vaikutus oli merkittävämpi ulkomaille suuntautuessa, sillä silloin suomalaisen organisaation on hankalampi saavuttaa luottamusta vieraalla markkinalla toimiessa.

Uusien asiakkaiden hankkimiseen ja julkisuuskuvan ylläpitämiseen sertifikaattia voidaan käyttää markkinointikeinona, sillä lopulta sertifikaatti kiteytyy todistukseen organisaation seinällä tai sähköiseen versioon organisaation verkkosivuilla. Tutkimuksen tulokset osoittavat, että markkinointikäytössä sertifikaatista koetut hyödyt ovat vahvasti organisaation oman arviosta riippuvaisia. Sertifikaatin markkinointipotentiaali kyllä tunnistetaan ja sen vaikuttavuutta pystytään arvioimaan muun myyntiä edistävien vaikutusten pohjalta. Kuitenkin organisaatio voi olla hyödyntämättä sertifikaatin markkinointipotentiaalia, kuten yhden tutkittavan organisaation kohdalla oli. Heidän kohdallaan sertifikaattia ei ollut järkevää käyttää markkinointikeinona, sillä oman arvionsa mukaan se

saattaisi olla ärsyke hakkerille koittaa päästä sisään organisaation järjestelmiin osoittaakseen kyvykkyytensä.

ISO/IEC 27001 -sertifikaatti edesauttaa myynnin lisääntymistä, joten se näkyy myös organisaation arvoon. Park ym. (2010) mukaan sertifikaatti nostaa organisaation arvoa kahdella tavalla: myynnin ja säästöjen lisääntymisen kautta. Tässä tutkimuksessa kaikki tutkittavat organisaatiot kokivat sertifikaatin tuottavan arvon nousua. Arvo koettiin muun muassa luottamuksen ja riippumattoman arvioinnin tuottaman todisteen luoman uskottavuuden kautta. Organisaation arvon nousu säästöjen kautta tuotti myös tutkimukseen paljon mielenkiintoisia näkemyksiä. Sertifioinnin tuottamat säästöt ovat usein vahvasti sidoksissa myyntiprosessin selkeytymisestä aiheutuviin resurssisäästöihin, kun organisaation ei tarvitse käyttää aikaa ja resursseja täyttäessään tietoturvavaatimuksia sisältäviä kyselyitä. Toisaalta sertifikaatin kautta organisaatio voi myös oppia optimoimaan omia prosessejaan siten, että niiden tehostuessa syntyy säästöjä. Täten tietoturvan asema organisaatiossa muuttuu pakollisesta kuluerästä liiketoimintaa mahdollistavaksi ja tukevaksi toiminnaksi. Kuten Hsu ym. (2016) toteaa, sertifiointi edistää sitä, että organisaatio toimii niin kuin sen kuuluukin, joten erilaisista tietoturvapoikkeamista syntyvien vahinkojen todennäköisyys laskee ja se tuottaa pitkällä aikavälillä mitattuna säästöjä. Sama näkemys ilmeni tässä tutkimuksessa viittauksena vakuutustoimintaan, eli tietoturvaan laitetaan rahaa sen vuoksi, että sillä estetään laajemmat vahingot. On kuitenkin mahdollista, että organisaatio ei koe sertifioinnista taloudellisia säästöjä, vaan kokee sertifioinnin vain kulueränä. Tällainen näkemys ei kuitenkaan ollut laajasti jaettu.

Kuluista puhuttaessa täytyy käsitellä sertifiointiin liittyviä investointeja. Tässä tutkimuksessa käsiteltiin erilaisia tietoturvainvestointeihin liittyviä teorioita, kuten päätöksenteko- ja peliteoriat, sekä Gordonin ja Loebin (2002) esittämä teoria investointien optimaalisesta tasosta. Kuitenkin tutkimuksessa tuli hyvin selkeästi ilmi se, että sertifioidut organisaatiot eivät sovella näitä teorioita kovinkaan suorasti, tai soveltavat niitä tietämättään. Rationaalisuuteen perustuva päätöksentekoteoria oli useimmissa organisaatioissa tietoturvainvestointien tekemiseen eniten vaikuttava menetelmä, sillä investointeja lähestyttiin riskiperusteisesti ja organisaation liiketoimintatavoitteita ajatellen. Toisaalta peliteoriaa käytettiin erilaisten uhkamallinnusten tekemiseen, mutta investointeja niillä ei määritelty. Yhteistä kaikille organisaatioille oli myös se, että organisaation johto oli vahvasti sitoutunut investointien tekemiseen ja tietoturvabudjetti oli helppo perustella johdolle. Haasteellista kuitenkin oli muun muassa Cavusoglun ym. (2008) kuvaama ongelma tietoturvainvestointien onnistumisen mittaamisessa. Tähän ongelmaan ei tässä tutkimuksessa saatu tarkkaa vastausta. Sertifioitujen organisaatioiden tapa mitata investointeja perustui riskeihin ja vaikutuksiin organisaation liiketoimintaan ja imagoon. Karkeasti arvioituna organisaatiot olivat valmiita investoimaan tietoturvaan mieluummin riittävästi tai liikaa kuin ottamaan turhia riskejä. Yleisesti investointitaso kuitenkin määräytyi sertifikaatin vaatimien kustannusten tasolle, jonka perusteella tehtiin tarpeen mukaan muutoksia. Erityisesti suuremmilla organisaatioilla tietoturvaan on käytettävissä enemmän rahaa, joten niillä on myös varaa tehdä suurempia investointeja tietoturvaan.

Vaikka tietoturvainvestointeja on vaikea ja joskus jopa mahdoton aukottomasti mitata, olivat kaikki tähän tutkimukseen osallistuneet organisaatiot sitä mieltä, että sertifikaatti on investointina kannattava.

Taloudellisten ja tietoturvaan yhdistettävien hyötyjen lisäksi sertifikaatin hankkimiseen voi vaikuttaa myös muita asioita. Esimerkiksi Humphreysin (2006) mukaan sertifikaatin avulla organisaatio voi täyttää lainsäädännön vaatimuksia ilman, että sen tarvitsee merkittävästi muuttaa toimintatapojaan. Myös It Governancen (2018a) tutkimuksessa sertifikaatin todettiin auttavan EU:n tietosuoja-asetus GDPR:n vaatimusten täyttämiseen. Näihin väitteisin saatiin tutkimuksessa vahvaa tukea, etenkin tietosuoja-asetuksen täyttymisen osalta. Muidenkin vaatimusten kohdalla ISO/IEC 27001 -sertifioinnin myös todettiin olevan hyödyllinen. ISO/IEC 27001 -sertifiointi toimii Lambon (2006) mukaan alan de facto-standardina, eli yleisesti hyväksyttynä perustasona tietoturvalle. Näin ollen sitä voidaan käyttää saavuttamaan myös muita sertifiointeja, sillä standardin vaatimukset ovat tietoturvan perusvaatimuksia, joita voidaan täyttää helposti myös tietoturva-alan muissa sertifioinneissa. Standardi on yhteneväinen myös muiden johtamisjärjestelmästandardien kanssa, joten se voi olla helppo integroida esimerkiksi ISO 9001 -laatujärjestelmään. Barlette ym. (2008) mainitsevat, että sertifioinnilla voi alentaa organisaation vakuutusmaksuja. Tutkimuksen tulosten perusteella tätä väitettä ei voitu vahvistaa, mutta tulokset antavat osviittaa siitä, että etenkin kybervakuutusten kohdalla ISO/IEC 27001 -sertifikaatti saattaa alentaa vakuutusmaksuja.

Sertifioinnista luopumiseen vaikuttaa pääosin kaksi tekijää. Joko sertifikaatti ei ole organisaation tarpeisiin sopiva, tai sen ylläpitoon vaadittavat velvoitteet kuluttavat liikaa organisaation resursseja. Sertifikaatin sopivuus riippuu toimintaympäristöstä ja käyttötarpeesta. Esimerkiksi toimialan mukaisesti maksukorttiliiketoiminnan parissa operoivalle organisaatiolle PCI DSS saattaa olla paljon mielekkäämpi kuin ISO/IEC 27001. Toisaalta taas kansallisella tasolla korkean tietoturvan vaatimuksissa Katakri tai VAHTI voi olla soveliaampi asiakasvaatimusten perusteella. Sertifikaatin ylläpitoon vaadittavien velvoitteiden osalta syy luopumiseen on pääasiallisesti rahallinen. Distererin (2013) mukaan ISO/IEC 27001 -standardin mukaisen johtamisjärjestelmän pystyttäminen ja ylläpitäminen vaatii useita kuukausia, ja sertifiointi itsessään vaatii myös muutaman kuukauden ja vuosittaisia toimia. Tähän lisätään sertifioinnin vaatimat toimenpiteet niin puhtaana työnä kuin rahallisena panostuksena, mitkä saattavat vaatia organisaatiolta runsaasti resursseja. Tutkimuksen mukaan organisaatiot kuitenkin ovat melko luottavaisia siihen, että vaikka sertifioinnin ylläpitäminen vaatii resursseja, ne menevät kuitenkin hyvään tarkoitukseen ja kehittävät organisaatiota eteenpäin.

6.2 Sertifiointielimen valintaan vaikuttavat tekijät sertifioinnissa

Toinen tämän tutkimuksen tutkimuskysymyksistä, ISO/IEC 27001 -sertifiointiin liittyen, oli tutkia sertifiointielimen valintaan vaikuttavia tekijöitä.

Kilpailutuksen merkitys oli melko pieni sertifiointielintä valittaessa. Jos olemassa oleva suhde sertifiointielimen kanssa on hyvä, ei kilpailutukselle ole usein tarvetta, tai se tehdään kevyesti. Suomessa toimijoiden lukumäärä on sen verran pieni, että erot niiden välillä eivät ole merkittäviä ja valintaan vaikuttaa usein olemassa olevan suhteen toimivuus. Suurilla organisaatioilla kilpailutus tapahtuu usein ulkomaisten sertifiointielinten kesken, sillä ne ovat kykenevämpiä toimittamaan palveluitaan laajamittaisesti ympäri maailman.

Olemassa oleva suhde sertifiointielimeen oli siis merkittävä tekijä valintaa tehdessä ja se nousi esiin usein tässä tutkimuksessa. Päällimmäinen syy olemassa olevan suhteen merkitsevyyteen on se, että työskentely tutun auditoijan kanssa nähtiin helpoksi, kun auditoija tuntee asiakasorganisaation ja osaa etsiä oikeita asioita keskittymällä tärkeisiin asioihin. Sertifiointielimen vaihtaminen nähtiin juuri tästä syystä usein haastavana, koska silloin auditointi joudutaan aloittamaan vertauskuvallisesti täysin nollatilanteesta. Tämä näkemys voi kuitenkin olla myös hyvä, sillä auditoijan vaihtaminen voi edesauttaa uusien kehityskohteiden löytämisen, mikä taas vie organisaation tietoturvan tasoa paremmalle tasolle.

Jahnin ym. (2005) mukaan hintakilpailu on sertifiointiliiketoiminnassa tiukkaa ja näin ollen hintaerojen tulisi olla maltillisia ja niiden vaikuttavuuden merkitys valinnassa näin ollen pieni. Tämä väite kyettiin tässä tutkimuksessa todentamaan todeksi haastatteluilla, sillä ilmeni, että hintaerot ovat markkinoilla sen verran pieniä, että organisaatiot eivät perusta valintaansa niinkään hintaan. Hinnan sijaan organisaatiot toivovat sertifiointielimeltä muita ominaisuuksia. Se, mitä nämä ominaisuudet ovat, riippuvat hyvin paljon organisaatiosta. Esimerkiksi suurelle organisaatiolle kansainvälisyys voi olla merkitsevää, toiselle taas kyky tarjota useampia palveluita on tärkeämpää. Toisaalta organisaatio voi myös arvostaa joustavuutta ja paikallisuutta. Edellä mainittujen ominaisuuksien lisäksi tärkeää on kuitenkin se, että sertifiointielin tarjoaa palveluitaan ammattitaitoisesti. Wianderin (2008) mukaan auditoijan ammattitaito parantaa auditointikokemusta, kun auditoija tuntee kohdeorganisaation ja löytää oikeat kehityskohteet. Tutkimuksen tuloksissa on selkeästi havaittavissa se, että organisaatiot arvostavat sertifiointielimen tarjoama palvelu on ammattitaitoista. Erityisesti se, että auditoija osaa keskittyä oikeisiin ja relevantteihin asioihin on tärkeää, sillä liian yksityiskohtainen tai irrelevanttien asioiden käsittely voi tuottaa auditoitavalle organisaatiolle tunteen auditoijan ammattitaidottomuudesta ja näin ollen herkentää kynnystä vaihtaa sertifiointielintä.

Sertifiointielimen maine on Kosuticin (2018) mukaan yksi sertifiointielimen valinnassa harkittava asia, sillä sertifikaatin arvo nousee korkeammaksi, jos sen on myöntänyt tunnettu luotettava sertifiointielin. Tämä näkemys on todennettavissa tämän tutkimuksen tulosten perusteella, sillä tutkimuksessa nousi ilmi näkemyksiä siitä, että esimerkiksi ulkomaisilla markkinoilla voi olla hyötyä siitä, että sertifikaatin myöntää jokin paikallinen tai tunnettu toimija. Lisäksi tutkimus antoi osviittaa siitä, että asiakkaat ovat myös kiinnostuneita siitä, kuka sertifikaatin on myöntänyt. Tällöin suuret tunnetut sertifiointielimet voivat olla houkuttelevampia organisaatioille. Haastatteluissa tuli kuitenkin ilmi näkemys siitä, että

suuret sertifiointielimet eivät kuitenkaan välttämättä ole yhtä kiinnostuneita sertifioimaan pieniä organisaatiota, vaan keskittyvät suuriin asiakkuuksiin.

Sertifiointielimen käytännöllisyystekijät nousivat ilmi haastatteluissa, mutta haetut käytännöllisyyteen viittaavat ominaisuudet vaihtelivat jonkin verran organisaation koon ja toiminta-alueen mukaan. Paikallinen auditoija koettiin hyväksi etenkin Suomessa siksi, että dokumentaation ollessa suomeksi, sen auditointi on paljon helpompaa. Myös haastattelujen tekeminen koettiin mielekkäämmäksi natiivilla kielellä, vaikka haastattelujen tekeminen englannin kielellä sinänsä olisi mahdollista. Lisäksi paikalliset toimijat kykenevät toimimaan paikallisesti ja kykenevät reagoimaan muutoksiin paljon paremmin kuin ulkomaiset sertifiointielimet. Lisäksi paikallista toimijaa käytettäessä vältytään suurilta matkakustannuksilta, jos toimintaa on vain yhdessä maassa ja muutamissa toimitiloissa. Toisaalta taas suurten organisaatioiden intressi on käyttää ulkomaisia sertifiointielimiä, jos ne kykenevät palvelemaan asiakasta esimerkiksi paikallistoimistonsa kautta useissa eri maissa niiden omilla kielillä. Täten käytännöllisyys tarkoittaa eri organisaatioiden tapauksessa hieman eri asioita ja näin ollen sertifiointielinten käytännöllisyystekijät ovat erilaisia. Kuitenkin perimmäisenä tekijänä käytännöllisyys viittaa kykyyn toimia paikallisesti ja joustavasti ja sen voidaan todeta vaikuttavan ISO/IEC 27001 -sertifiointia hankkivien organisaatioiden sertifiointielimen valintaan.

Käytännöllisyyteen viittaa myös viimeinen identifioitu tekijä, eli palvelutarjonta. Tässä palveluntarjonnalla tarkoitetaan Kosuticin (2018) mukaista sertifiointielimen kykyä tarjota useampaa eri sertifiointia asiakkaalle. Tällöin asiakas voi hankkia yhdeltä luukulta useamman tarvitsemansa sertifioinnin, jolloin siitä voi seurata rahallista ja ajallista hyötyä, kun auditointeja voidaan niputtaa. Tässä kuitenkin tulokset olivat jakautuneita, joten tekijän merkittävyyttä ei voida suoraan arvioida täysin pitävästi. Tutkimuksessa osa vastaajista oli selkeästi halukkaita hankkimaan kaikki tarvittavat palvelut yhdestä ja samasta paikasta sen helppouden takia, mutta toisaalta osa ei kokenut sitä mahdolliseksi saatikka mielekkääksi. Helppouden tuomat edut syntyivät muun muassa hankintaprosessin yksinkertaistumisesta ja edellä mainituista rahallisista ja ajallisista hyödyistä. Lisäksi organisaatioiden välinen kumppanuus syvenee, mikä vaikuttaa olemassa olevan suhteen merkityksen kasvuun sertifiointielintä uudelleen valittaessa. Kuitenkin organisaatioiden tarve erilaisille sertifioinneille voi olla hyvin spesifi ja toimialakohtainen, jolloin sertifiointielimen voi olla haastavaa edes tarjota kaikkia haluttuja palveluita. Yleensä laajimmat palveluportfoliot löytyvät suurilta toimijoilta, mutta nekään eivät välttämättä kata toimialaspesifisiä sertifiointeja, joten täysin palveluja ei voi yhdestä paikasta hankkia.

Kun sertifiointielimen valintaperusteita vertailtiin keskenään tärkeysjärjestykseen, oli järjestys erittäin selkeä. Tärkeimmäksi valintaan vaikuttavaksi tekijäksi valikoitui ammattitaito, joka oli neljällä viidestä tärkein tekijä. Toiseksi tärkein tekijä oli käytännöllisyys, joka niin ikään oli toisiksi tärkein neljällä viidestä vastaajasta. Tämän jälkeen jaetulle kolmannelle sijalle tulivat olemassa olevat suhteet ja hinta. Vertailu osoittaa sen, että sertifiointielimen valinnassa tärkeintä on se, että asiakas saa ammattitaitoista palvelua ja näin ollen saa auditoinnista

myös eniten vastinetta. Toisaalta myös käytännöllisyystekijöiden merkitystä ei voi jättää huomioimatta. Tämä asettaa vaatimuksia sertifiointielimien kykyyn tuottaa räätälöityjä ja paikallisesti tuotettuja palveluita. Olemassa olevien suhteiden merkitys on tämän tutkimuksen perusteella hyvin subjektiivinen, sillä kokemus saadusta palvelusta, ja jopa auditoijan ja asiakkaan välinen henkilökemia voivat vaikuttaa asiaan. Hinnan merkitys koettiin melko pieneksi, sillä muut tekijät koettiin kokonaisuutena tärkeämmiksi. Toisaalta, jos auditointien eroissa olisi enemmän hintaeroa, voisi sen vaikutus valintaan olla suurempi. Hinta kasvaa auditoitavan kohteen mukaan, joten etenkin suurempien organisaatioiden kohdalla hinta voi vaihdella enemmän. Toisaalta pienelle organisaatiolle hinta saattaa olla merkittävä sitä kautta, että organisaation talous pakottaa valitsemaan edullisimman tarjouksen.

7 YHTEENVETO

Tässä tutkimuksessa tutkittiin ISO/IEC 27001 -sertifioinnin hankintaan ja ylläpitämiseen vaikuttavia tekijöitä. Tekijöitä etsittiin tutustumalla olemassa olevaan tutkimukseen aiheesta, ja etsimällä sertifioinnista saatavia hyötyjä ja haasteita. Sertifioinnin hankintaan liittyen tutkittiin myös sitä, mitkä tekijät voivat vaikuttaa sertifikaatin myöntävän sertifiointielimen valintaan. Tutkimuksen empiirinen osio suoritettiin monitapaustutkimuksena, jossa haastateltiin viittä ISO/IEC 27001 -sertifioitua organisaatiota. Tässä luvussa vedetään yhteen tutkimuksen tulokset, sekä arvioidaan tutkimuksen luotettavuutta ja tulosten yleistettävyyttä. Luvun lopussa esitellään vielä mahdollisia jatkotutkimusaiheita.

7.1 ISO/IEC 27001 -sertifikaatin hankintaan ja ylläpitoon vaikuttavat useat tekijät

Sertifikaatin hankinta ja sen ylläpito perustuvat moneen tekijään. Vaikka sertifikaatti hankittaisiinkin aluksi vain yhden tekijän, kuten asiakasvaatimuksen tai ulkopuolisen pakon takia, on sertifioinnissa kuitenkin useita tekijöitä, jotka puoltavat sen hankkimista ja ylläpitämistä. Hankintaperusteita voi jakaa karkeasti tietoturvaperusteisiin ja taloudellisiin syihin, joita tukevat muut yleiset hyödyt. Tietoturvahyödyistä iso osa tulee suoraan standardin implementoinnin mukana, mutta myös sertifioinnilla on vaikutusta organisaation tietoturvan tasoon. Standardin implementointi mahdollistaa sen, että organisaatiolla on työkaluja hallita tietoturvaa. Vahva johdon tuki on elintärkeää johtamisjärjestelmän toiminnan varmistamiseksi, mutta toisaalta myös yksittäisten työntekijöiden panoksella on merkitystä, sillä esimerkiksi tietoturvatietoisuuden hyvä jalkautuminen edistää tietoturvaa merkittävästi. Jatkuvan parantamisen varmistaminen taas edesauttaa sitä, että organisaation tietoturvan johtamisjärjestelmä pysyy ajankohtaisena vallitsevien riskien hallitsemiseksi. Jatkuva parantaminen myös tehostaa järjestelmän toimintaa siten, että se tukee organisaation liiketoimintaa entistä paremmin.

Sertifikaatti toimii vakuutena siitä, että organisaation tietoturvan johtamisjärjestelmä on hallittu, toimiva ja jatkuvasti ylläpidetty. Sertifioinnin myötä organisaation johtamisjärjestelmä kehittyy kokonaisvaltaisesti paremmaksi niin dokumentaation, prosessien kuin tietoturvan jalkautuksen suhteen siten, että tietoturva on integroitu osa koko organisaation toimintaa kaikilla sen kerroksilla. Sertifiointi tuo mukanaan sertifikaatin ylläpitämiseen liittyviä velvoitteita, jotka kannustavat ja pakottavat organisaation toimimaan aktiivisesti tietoturvan hallinnan parissa. Sertifiointisykli sisältää vuosittaiset, kevyemmät, seuranta-auditoinnit ja syklin päättyessä laajempi uusintasertifiointi varmistaa, että sertifioitu organisaatio ylläpitää tietoturvan hallintajärjestelmäänsä standardin vaatimusten mukaisesti. Auditoinnit mahdollistavat ulkopuolisen ja puolueettoman toimijan antaman palautteen järjestelmän kehittämiseksi ja puutteiden löytämiseksi.

Lisäksi auditoinneilla on siinä mielessä pakottava ja painetta luova merkitys, että sertifioidun organisaation on kiinnitettävä erityistä huomiota oman toimintansa tason ylläpitämiseen ja kehittämiseen saadakseen auditoinnista hyväksytyn tuloksen.

Sertifikaatin hankinta on usein taloudellinen päätös, vaikka sertifioinnin pääasiallinen tehtävä on osoittaa organisaation tietoturvan hyvä taso. Sertifiointi on täysin vapaaehtoista, ellei syy sertifioinnille ole pakko, jonka syy voi olla toimialan vaatimuksissa tai lainsäädännössä. Sertifikaatti on markkinointiväline, jolla organisaatio voi vakuuttaa potentiaaliset asiakkaansa siitä, että se huolehtii sitoutuneesti tietoturvasta. Täten sitä voidaan käyttää myyntiä edistäviin tarkoituksiin edistämään myyntiprosessia. Sertifikaatti tuottaa myös säästöjä. Myyntiprosessi selkeytyy, kun asiakkaan tietoturvavaatimuksia voidaan kuitata sertifikaatilla, ja tehostuneet prosessit voivat auttaa organisaatiota vähentämään omia kulujaan. Edellä mainitut tekijät nostavat organisaation arvoa, sillä taloudellisten etujen lisäksi sen julkisuuskuva ja imago parantuvat. Kuitenkaan merkittävää kilpailuetua sertifikaatti ei enää nykyisin välttämättä tarjoa. Kilpailuetu on riippuvainen siitä, kuinka vakiintunut käytäntö ISO/IEC 27001 -sertifiointi toimialalla on. Toisaalta myös organisaation koko vaikuttaa hyvin paljon siihen, miten erilaiset hyödyt koetaan. Pienelle organisaatiolle sertifikaatti voi olla elintärkeä apu luottamuksen rakentamiseksi, kun taas suurelle organisaatiolle sertifikaatti ja tietoturvan johtamisjärjestelmä on tapa hallita suurta organisaatiota ja yleinen markkinoilla toimimisen lisenssi.

ISO/IEC 27001 -sertifikaatin hankinta ja ylläpito vaativat investointeja, mutta nämä investoinnit koetaan kokonaisarviossa hyödyllisiksi ja tuottaviksi. Investointien mittaaminen on haastavaa, mutta niiden perusteluun käytetään yleensä kokonaisarviota riskeistä, tarpeesta, hyödyllisyydestä sekä mainevaikutuksista. Tyypillisesti organisaatiot ovat valmiita investoimaan tietoturvaan varman päälle, eli siten, että investointi on varmasti riittävä. Investoinneissa kuitenkin nojaudutaan myös siihen, mikä on riittävää sertifioinnin ylläpitämiseksi. Investointien kannalta tärkeintä, kuten koko ISO/IEC 27001 standardissa, on se, että johto on niihin sitoutunut ja on valmis määrittämään tietoturvabudjettiin tarpeeksi resursseja. Tarpeellisten resurssien määritelmää voi olla mahdotonta mitenkään aukottomasti määritellä, sillä se perustuu hyvin paljon siihen riskiympäristöön, jossa organisaatio toimii. Luottamukseen perustuvissa, mahdollisesti sensitiivistä dataa käsittelevissä organisaatioissa tietoturvaan joudutaan investoimaan merkittävästi enemmän kuin vähemmän luottamuksellista dataa käsittelevissä organisaatioissa. Luottamus nousee ISO/IEC 27001 -sertifikaatista puhuessa esiin lähes kaikissa yhteyksissä. Sertifikaatin tehtävänä on toimia osoituksena siitä, että organisaatio on luotettava. Monet sertifikaatin tuottamista hyödyistä perustuvat juurikin luottamuksesta syntyvään uskoon organisaation hyvästä toiminnasta tietoturvan suhteen. Sen takia luottamus nousee esiin yhtenä merkittävimmistä tekijöistä sertifikaatin hankinta- ja ylläpitoperusteissa.

ISO/IEC 27001 -sertifikaatista voi saada myös muita yleisiä hyötyjä. Se voi auttaa lainsäädännön ja erilaisten asetusten, kuten GDPR:n vaatimusten täyttämisessä. ISO/IEC 27001:n mukainen johtamisjärjestelmä voi toimia myös hyvänä

askeleena toiseen sertifiointiin, sillä standardin vaatimukset ovat tietoturvan perusvaatimuksia ja yleisiä hyväksi koettuja periaatteita. Lisäksi sertifikaatti voi alentaa erilaisia maksuja, kuten vakuutusmaksuja, jos niiden ehdoissa on tietoturvavaatimuksia.

7.2 Sertifiointielimen hankinta perustuu pääosin muihin tekijöihin kuin hintaan

Sertifiointielimen valinta perustuu moniin tekijöihin, joista yksi on hinta. Hinnan merkitys ei kuitenkaan ole muita tekijöitä tärkeämpi, vaikka sertifiointielinten markkinoilla teoreettisesti sen tulisi olla merkittävin vaikuttava tekijä, sillä toiminta perustuu puolueettomuuteen ja määrämuotoisuuteen. Hinnan merkitys ei kuitenkaan korostu sertifiointielintä valittaessa, ellei hintaero ole merkittävän suuri. Hintaerot markkinoilla ovat kuitenkin melko pieniä, joten monet muut tekijät hinnan ohella vaikuttavat sertifiointielimen valintaan.

Kilpailutuksen merkitys tuntuu olevan melko vähäinen, sillä markkinoilla on melko vähän paikallisia toimijoita ja ulkomaisten sertifiointielimien käyttö on vähäistä etenkin pienillä organisaatioilla, joilla ei ole toimintaa muissa maissa. Jos kilpailutusta ei tehdä, se johtuu yleensä hyvästä olemassa olevasta suhteesta nykyiseen sertifiointielimeen. Toisaalta jos kilpailutusta tehdään, siihen pyritään valitsemaan omiin tarpeisiin sopivat toimijat ja luotettavaksi todetut toimijat. Sertifiointielimen maine on siten yksi vaikuttavista tekijöistä. Akkreditointi itsessään on osoitus luotettavuudesta, mutta mainetta mitataan myös sertifiointielimen tunnistettavuuden kautta. Esimerkiksi suurten sertifiointielinten myöntämät sertifikaatit tunnistetaan paremmin ja niiden arvoa pidetään suurempana. Toisaalta myös se, jos sertifiointielin toimii samalla markkinalla, jossa organisaatio pääasiallisesti toimii, auttaa edistämään sertifikaatin luotettavuutta.

Yhtenä tärkeimmistä tekijöistä on auditoijan ammattitaito. Ammattitaidolla tarkoitetaan auditoijan kykyä auditoida siten, että johtamisjärjestelmän tärkeät kehityskohteet löytyvät ja sitä, että auditoija tuntee standardin hyvin ja osaa tulkita sitä oikein. Auditoijan ei kuitenkaan toivota olevan pikkutarkka, tai keskittyvän epäoleellisiin asioihin, joista ei ole sertifioitavalle organisaatiolle hyötyä. Kun sertifioitu organisaatio miettii sertifiointielimen valintaa, vaikuttavat ammattitaidon ohella merkittävästi myös käytännöllisyystekijät. Käytännöllisyystekijät tarkoittavat sertifiointielimen kykyä mukautua sertifiointielimen tarpeisiin, kuten kykyä toimia paikallisesti siellä, missä auditoitava organisaatio toimii, sekä palvella paikallisella kielellä.

Sertifiointielimelle voi olla etua siitä, että se kykenee tarjoamaan useita palveluita sertifioitavalle organisaatiolle. Useamman sertifioinnin tarjoaminen voi olla auditoitavalle organisaatiolle helpompaa, kun palvelut voidaan hankkia yhdeltä toimittajalta. Tällöin tilanteesta voi seurata hintaetua, ja toisaalta sertifiointielimen ja sertifioitavan organisaation välinen yhteistyösuhde syvenee. Käytännössä kuitenkin organisaatioiden voi olla haastava saada kaikkia haluamiaan

palveluita yhdestä paikasta, joten tekijän merkitys voi jäädä pieneksi verrattuna muihin valintaan vaikuttaviin tekijöihin.

7.3 Tutkimuksen arviointi ja yleistettävyys

Tämän tutkimuksen tuloksia arvioidessa täytyy tiedostaa tutkimuksen rajoitukset ja rajoitusten vaikutukset yleistettävyyteen. Ensimmäinen tutkimukseen liittyvä rajoitus on lähdemateriaalin määrä, joka on verrattain pieni aiheen ollessa uusi ja vähän tutkittu. Riittävän tieteellisen pohjan rakentaminen oli kuitenkin mahdollista, mutta etenkin sertifiointielinten valintaan liittyen lähdemateriaalin vähäinen määrä ja jopa osittainen puuttuminen tuotti haastetta. Toisaalta tämä ei rajoittanut empiirisen tutkimuksen tekemistä, sillä haastatteluissa oli mahdollisuus selvittää vapaan keskustelun kautta myös muita kuin olemassa olevan tutkimuksen määrittelemiä tekijöitä.

Koska pyrkimyksenä oli selvittää tekijöitä, jotka ovat vaikuttaneet haastateltavien organisaatioiden toimintaan, voidaan tuloksia pitää siinä mielessä luotettavina, että kertomukset perustuvat organisaatioiden omaan toimintaan. Kun tekijät ovat peräisin tosielämän toiminnasta, ei niiden vaikuttavuuden merkitystä tarvitse arvioida tulosten luotettavuuden osalta kovin tarkasti. Sen sijaan, on tärkeämpää arvioida sitä, jäikö tutkimuksessa havainnoimatta joitakin mahdollisesti vaikuttavia tekijöitä. Todennäköistä on, että tekijöitä on lisää, mutta tämän tutkimuksen puitteissa niistä löytyi suuri osa. Rajoite liittyy vahvasti tutkimuksessa käytettävissä oleviin resursseihin. Pro gradu -tutkielman kontekstissa resurssit ja niiden riittävyys ja rajoitteet on tiedostettava. Täten myös tässä tutkimuksessa on varmasti aukkoja, jotka vaativat tarkempaa perehtymistä. Tutkijan omien vaikutusmahdollisuuksien piirissä oleviin luotettavuustekijöihin kuitenkin pyrittiin kiinnittämään mahdollisimman paljon huomiota. Kirjallisuuskatsaus toteutettiin huolellisesti ja empiirinen osuus sujui ilman suuria haasteita. Haastattelutilanteista pyrittiin luomaan mahdollisimman helposti lähestyttäviä ja tehokkaita, ja tulosten analysointi tehtiin jokaisen tutkittavan tapauksen kohdalla yksityiskohtaisesti. Näin ollen väärän tai puuttuvan tiedon todennäköisyys tämän tutkimuksen kohdalla voitaneen arvioida pieneksi.

Yleistettävyys voi olla laadullisissa tutkimuksissa, etenkin tapaustutkimuksissa, haastavaa. Tässä tutkimuksessa otos on kohtuullisen pieni, eli viisi. Tällaisen otoksen osalta kaikkien tulosten yleistäminen koko populaatioon voi olla liioiteltua, sillä kaikki tutkimuksessa löytyneet tekijät eivät päteneet kaikkiin tutkittaviin organisaatioihin. Toisaalta monet tekijöistä olivat kaikille organisaatioille yhteisiä, jolloin niiden osalta yleistäminen on helpompaa hyväksyä. Tutkimuksen tärkein päämäärä kuitenkin oli ymmärtää sertifikaatin hankkineiden ja sertifikaatin hankkimista miettivien organisaatioiden käyttäytymistä ja siinä mielessä kaikki löytyneet tekijät ovat arvokkaita löydöksiä, vaikka ne eivät pätisi kaikkiin tapauksiin.

7.4 Jatkotutkimusaiheita

Tässä tutkimuksessa keskityttiin etsimään erilaisia tekijöitä, jotka vaikuttavat ISO/IEC 27001 -sertifioinnin hankintaan ja ylläpitoon, sekä sertifikaatin myöntävän sertifiointielimen valintaan. Hankintaperusteita on tutkittu aikaisemmin erilaisista näkökulmista melko kevyesti ja tämä tutkimus pyrki koostamaan yhtenäisen listauksen, joka kattaisi näitä perusteita kokonaisvaltaisesti. Aihe vaatii kuitenkin vielä laajamittaisempaa tutkimusta, joka tutkisi vielä tässä tutkimuksessa piiloon jääneitä tekijöitä, jotka vaikuttavat sertifikaatin hankkimiseen. Erityisen mielenkiintoista olisi tutkia sitä, miten hankinta- ja valintaperusteet vertautuvat muihin tietoturvasertifikaatteihin ja muihin johtamisjärjestelmästandardeihin kuten laatujärjestelmien sertifiointiin.

Lisäksi vielä piiloon jääneiden tekijöiden lisäksi olisi mielenkiintoista ja erittäin suotavaa selvittää se, minkälainen painoarvo eri tekijöillä on. Tämä tutkimus sivusi aihetta hyvin kevyesti, sillä painopiste oli tekijöiden havainnoimisessa eikä niinkään niiden vertailussa. Joidenkin tekijöiden, kuten luottamuksen merkitystä kyettiin arvioimaan erittäin merkittäväksi sillä perusteella, että se toistui tuloksissa hyvin usein, kun taas esimerkiksi sertifikaatin merkitystä vakuutusmaksujen alenemisessa ei voitu pitää kovin luotettavana tämän tutkimuksen perusteella. Laajamittainen tutkimus suuremmalle otokselle organisaatioita eri tekijöiden merkitsevyydestä olisi erittäin tervetullutta terävöittämään sertifioinnin hankkimiseen ja ylläpitoon liittyvien tekijöiden kartoittamisessa. Lisäksi yksittäisenä sivuhaarana tämän tutkimuksen havainnoista olisi tärkeää selvittää sitä, miten organisaatiot todellisuudessa mittaavat tietoturvainvestointien onnistumista ja sitä, miten tietoturvabudjetti todellisuudessa määräytyy. Tämän tutkimuksen sisällä aiheita tutkittiin hyvin pintapuolisesti, joten aiheessa olisi varmasti vielä paljon mielenkiintoista tutkittavaa.

Sertifiointielinten valintaan liittyvä tutkimus on vielä erittäin olematonta, joten ongelman ympärille tulisi keskittää enemmän tutkimusta. Tämä tutkimus toimi siltä osin pioneerina, että se tuotti listauksen tekijöistä, jotka vaikuttavat sertifiointielimen valintaan. Aihe vaatii kuitenkin myös lisää tutkimusta monesta eri näkökulmasta. Valintaan vaikuttavia tekijöitä on varmasti lisää ja tekijöiden välinen tärkeysjärjestys vaatii vielä jatkotutkimusta.

LÄHTEET

Andress, J. (2014). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress.

Barlette, Y. & Fomin, V. V., Vries, H. (2008). ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption. Teoksessa *Proceedings of the third European conference on Management of Technology (EuroMOT)*.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, *13*(4), 544-559.

Boehmer, W. (2008). Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001. Teoksessa *Emerging Security Information, Systems and Technologies, 2008. SECURWARE'08. Second International Conference on* (pp. 224-231). IEEE.

Boehmer, W. (2009). Cost-benefit trade-off analysis of an ISMS based on ISO 27001. Teoksessa *2009 International Conference on Availability, Reliability and Security* (pp. 392-399). IEEE.

Brenner, J. (2007). ISO 27001: Risk management and compliance. *Risk management*, *54*(1), 24.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-44

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems*, *25*(2), 281-304.

Cowan, D. (2011). External pressure for internal information security controls. *Computer Fraud & Security*, *2011*(11), 8-11.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(02), 92.

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, *40*(4), 314-321.

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of management review*, *14*(4), 532-550.

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of management journal*, *50*(1), 25-32.

Eriksson, P., & Koistinen, K. (2014). *Monenlainen tapaustutkimus*. Kuluttajatutkimuskeskus.

Everett, C. (2011). Is ISO 27001 worth it?. *Computer Fraud & Security*, *2011*(1), 5-7.

FINAS. (2019). *Akkreditoidut toimijat.* Haettu 10.2.2019 osoitteestahttps://www.finas.fi/toimijat/Sivut/default.aspx

FINAS. (2016). *Akkreditoinnin ja sertifioinnin tavoitteet ja merkittävimmät erot.* Haettu 23.1.2019 osoitteesta:

https://www.finas.fi/ajankohtaista/artikkelit/Sivut/Akkreditoinnin-ja-sertifioinnin-tavoitteet-ja-merkitt%C3%A4vimm%C3%A4t-erot.aspx

Flyvbjerg, B. (2006). Five misunderstandings about case-study research. *Qualitative inquiry*, *12*(2), 219-245.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The qualitative report*, *8*(4), 597-606.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438-457.

Huang, C. D., Hu, Q., & Behara, R. S. (2008). An economic analysis of the optimal information security investment in the case of a risk-averse firm. *International Journal of Production Economics, 114(2)*, 793-804.

Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. *ISO Management Systems*, *6*(1).

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *information security technical report*, *13*(4), 247-255.

Humphreys, E. (2011). Information security management system standards. *Datenschutz und Datensicherheit-DuD*, *35*(1), 7-11.

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 certification on firm performance. In *System Sciences (HICSS), 2016 49th Hawaii International Conference on* (pp. 4842-4848). IEEE.

Hsu, C. W. (2009). Frame misalignment: interpreting the implementation of information systems security certification in an organization. *European Journal of Information Systems*, *18*(2), 140-150.

International Organization for Standardization - ISO. (2017). *Information technology -- Security techniques -- Information security management systems -- Requirements* (ISO/IEC Standard No. 27001). Haettu osoitteesta https://www.iso.org/standard/54534.html

International Organization for Standardization - ISO. (2015). *Conformity assessment -- Requirements for bodies providing audit and certification of management systems -- Part 1: Requirements* (ISO/IEC Standard No. 17021) Haettu osoitteesta https://www.iso.org/standard/61651.html

International Organization for Standardization - ISO. (2015). *Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems* (ISO/IEC Standard No. 27006). Haettu osoitteesta https://www.iso.org/standard/62313.html

International Organization for Standardization - ISO. (2018). *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary* (ISO/IEC Standard No. 27000). Haettu osoitteesta https://www.iso.org/standard/73906.html

International Organization for Standardization - ISO. (2018). *ISO Survey 2017.* Haettu 23.1.2019 osoitteesta https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

International Organization for Standardization - ISO. (2019a). *The main benefits of ISO standards.* Haettu osoitteesta https://www.iso.org/benefits-of-standards.html

International Organization for Standardization - ISO. (2019b). *SFS (Finland).* Haettu 28.1.2019 osoitteesta https://www.iso.org/member/1734.html

ISO Global (2019). *How to choose a certification body.* Haettu 10.2.2019 osoitteesta http://www.isoglobal.com.au/how-to-select-a-certification-body/

IT Governance Ltd. (2018a). *ISO 27001 Global Report.* Haettu osoitteesta https://www.itgovernance.co.uk/iso27001-global-report-2018

IT Governance Ltd. (2018b). *Typical ISO 27001 certification costs.* Haettu 10.2.2019 osoitteesta https://www.itgovernance.co.uk/iso27001-certification-costs

Jahn, G., Schramm, M., & Spiller, A. (2005). The reliability of certification: Quality labels as a consumer policy tool. *Journal of Consumer Policy*, *28*(1), 53-73.

Kosutic, D., (2018). *How to choose a certification body*. Haettu 10.2.2019 osoitteesta https://advisera.com/27001academy/knowledgebase/how-to-choose-a-certification-body/

Lambo, T., (2006) ISO/IEC 27001: The future of infosec certification. *The ISSA Journal,* 4(11), 44-45.

Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26

Nixu Certification Oy. (2019) *Nixu Certification Oy.* Haettu 17.2.2019 osoitteesta https://www.nixu.com/fi/nixu-certification-oy

Park, C. S., Jang, S. S., & Park, Y. T. (2010). A study of effect of Information Security Management System [ISMS] certification on organization performance. *IJCSNS International Journal of Computer Science and Network Security*, *10*(3), 10-21.

Parmigiani, G., & Inoue, L. (2009). *Decision theory: principles and approaches (Vol. 812)*. John Wiley & Sons.

Posthumus, S., & Von Solms, R. (2004). A framework for the governance of information security. *Computers & security*, *23*(8), 638-646.

Prajogo, D., & Castka, P. (2015). How do external auditors and certification bodies affect firms' benefits from ISO 9001 certification?".

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS quarterly*, 757-778.

Saaranen-Kauppinen, A. & Puusniekka, A. (2009). *Menetelmäopetuksen tietovaranto KvaliMOTV: Kvalitatiivisten menetelmien verkko-oppikirja* (Toinen vedos.). Tampere: Yhteiskuntatieteellinen tietoarkisto Tampereen yliopisto.

Sharma, N. K., & Dash, P. K. (2012). Effectiveness of ISO 27001, as an information security management system: an analytical study of financial aspects. *Far East Journal of Psychology and Business*, *9*(3), 42-55.

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM*, *49*(8), 97-100.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270.

Siponen, M., & Baskerville, R. L. (2018). Intervention Effect Rates as a Path to Research Relevance : Information Systems Security Example. *Journal of the Association for Information Systems*, 19 (4), 4.

Viestintävirasto. (2018). *Ohje tietoturvallisuuden arviointilaitoksille 210/2016 O*. Haettu 16.2.2019 osoitteesta https://www.traficom.fi/sites/default/files/media/regulation/ohje-tietoturvallisuuden-arviointilaitoksille-210-2016o.pdf

Von Solms, R. (1999). Information security management: why standards are important. *Information Management & Computer Security*, *7*(1), 50-58.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.

Watkins, S. (2013). *An Introduction to Information Security and ISO27001 : 2013 (Vol. 2nd ed).* Ely: IT Governance Publishing.

Wiander, T. (2008). Implementing the ISO/IEC 17799 standard in practice: experiences on audit phases. *In Proceedings of the sixth Australasian conference on Information security-Volume 81* (pp. 115-119). Australian Computer Society, Inc.

LIITE 1 HAASTATTELURUNKO

Yleisesti

1. Mitkä ovat/olivat syyt hankkia ISO/IEC 27001 sertifikaatti?
2. Mitkä ovat syy ylläpitää sertifiointia?
3. Onko jotain syytä, jonka takia sertifikaatista luovuttaisiin?
4. Nostaako sertifikaatti yrityksen arvoa?

Tietoturvanäkökulma

1. Arvioi seuraavaa väitettä: **Auditointi** ja **sertifiointi** parantaa organisaation tietoturvan tasoa.
2. Arvioi vapaasti organisaation sertifioinnista kokemia tietoturvahyötyjä.
3. Onko organisaation tietoturvan johtamisjärjestelmä parempi, kun se on sertifioitu?
4. Minkälaisia vaikutuksia sertifikaatilla on ihmisten tietoturvaosaamiseen?

Taloudellinen näkökulma

1. Arvioi vapaasti organisaation sertifioinnista saamia taloudellisia hyötyjä.
2. Tuottaako sertifikaatti säästöjä?
3. Tuottaako sertifikaatti kilpailuetua, vai onko sertifikaatti alalla jo vakiintunut käytäntö, jonka täyttämistä odotetaan kaikilta?
4. Lisääkö sertifikaatti asiakkaiden luottamusta?
5. Minkälainen vaikutus sertifikaatilla on olemassa oleviin asiakkaisiin?
6. Minkälainen vaikutus sertifikaatilla on uusien asiakkuuksien luomisessa?
7. Miten sertifikaatti vaikuttaa organisaation julkisuuskuvaan?
8. Minkälaista taloudellista arviointia sertifikaatin hankkimiseen/ylläpitämiseen liittyy?
    a. Minkälainen suhtautuminen johdolla on tietoturvainvestointeihin?
    b. Miten tietoturvabudjetti määräytyy?
    c. Miten sertifikaatin hankkimisen/ylläpitämisen kustannuksia mitataan suhteessa hyötyyn, toisin sanoen, miten kustannukset perustellaan? (ROSI, Return On Security Investment)
    d. Miten tietoturvariskien minimoimiseen käytettävä investointi määräytyy?

Muut asiat

1. Auttaako sertifikaatti täyttämään lainsäädännöllisiä vaatimuksia?
2. Auttaako ISO/IEC 27001 täyttämään muita tietoturvavaatimuksia, kuten muita standardeja?

3. Onko sertifikaatti alentanut muita kustannuksia, kuten vakuutusmaksuja?
4. Mitkä ovat sertifikaatin hankkimisen/ylläpitämisen haasteet ja ongelmat?

Sertifiointielimen valintaperusteet

1. Käytettyjen sertifiointielinten lukumäärä:
2. Onko sertifiointia kilpailutettu sitä hankkiessa?
3. Minkälaisiin asioihin kilpailutuksessa kiinnitettiin huomiota?
4. Millä perusteilla sertifiointielin valittiin?
    a. Oliko hinta määräävä tekijä?
    b. Vaikuttiko sertifiointielimen maine?
    c. Vaikuttiko sertifiointielimen ammattitaito?
5. Vaikuttavatko käytännön asiat? (katso tarkennus alakysymyksistä)
    a. Paikallinen toimija vs. kansainvälinen toimija
        i. Yhteinen kieli
        ii. Joustavuus
        iii. Hinta
6. Vaikuttaako sertifiointielimen kyky auditoida useampia standardeja valintaan?
7. Jos olette vaihtaneet sertifiointielintä, mikä on ollut vaihtamisen syy?
8. Mahdollisesti muut valintaperusteisiin liittyvät ja esiin tulevat asiat:

Järjestä valintaperusteet tärkeysjärjestykseen:

- Hinta
- Auditoijan ammattitaito
- Olemassa olevat suhteet sertifiointielimeen
- Sertifiointielimen käytännöllisyys (yhteinen kieli, sijainti yms.)