Eeva Mäki-Maukola

ISO 27000 -TIETOTURVASTANDARDISARJA OSANA NYKYPÄIVÄN YRITYSTEN TIETOTURVALLISUUDEN HALLINTAA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Mäki-Maukola, Eeva
ISO 27000 -tietoturvastandardisarja osana nykypäivän yritysten tietoturvallisuuden hallintaa
Jyväskylä: Jyväskylän yliopisto, 2023, 62 s.
Kyberturvallisuus, Pro Gradu -tutkielma
Ohjaaja: Lehto, Martti

Tämän tutkimuksen tavoitteena oli selvittää, miten ISO 27000 -tietoturvastandardisarja on osana nykypäivän yritysten tietoturvallisuuden hallintaa. Tutkimuksessa keskitytään standardeihin ISO 27000, ISO 27001 sekä ISO 27002, joista ISO 27001 -standardia käsiteltiin yrityksille myönnettävän ISO 27001 -sertifikaatin avulla. Näkökulma tarkasteluun valittiin kyseisten standardien myötä, sillä ne keskittyvät olennaisesti yritysten tietoturvallisuuden hallintaan sekä sen suunnitteluun, toteutukseen, ylläpitoon ja parantamiseen. Tutkimuksen rajaus kohdistettiin Suomessa toimiviin eri liiketoiminta-alan yrityksiin, jotka ovat viime vuosien aikana saavuttaneet ISO 27001 -sertifikaatin.

Tutkimuksen kirjallisuuskatsaus muodostuu yritysten tietoturvallisuuden hallinnasta sekä tietoturvapolitiikan ja tietoturvan hallintajärjestelmän viitekehyksestä. Kirjallisuuskatsauksessa keskitytään myös ISO 27000 -tietoturvastandardisarjaan ja erityisesti standardeihin ISO 27000, ISO 27001 ja ISO 27002, sekä niiden historiaan ja kehitykseen aina nykyhetkeen asti.

Tämä tutkimus toteutettiin laadullisena tutkimuksena ja laadullisen aineiston keräämiseen käytettiin sähköistä kyselylomaketta, johon vastasivat tutkimukseen osallistuneet yritysten edustajat. Tutkimuksen tulosten tavoitteena oli selvittää, kuinka tutkimukseen osallistuvat yritykset käyttävät standardeja ISO 27000 ja ISO 27002 tietoturvallisuutensa hallinnassa sekä sen ohjaamisessa. Tulosten tavoitteena oli myös tarkastella yritysten saavuttaman ISO 27001 -sertifikaatin hakuprosessia muun muassa sen keston ja haastavuuden näkökulmista.

Tutkimukseen osallistui neljä yritystä, joten otanta oli pieni. Tämän takia yleistävien päätelmien teko Suomessa toimivien eri liiketoiminta-alan yritysten tietoturvallisuuden hallinnasta ei voida tehdä. Tutkimustulokset kuitenkin antavat yleiskatsauksen juuri tämän tutkimukseen osallistuneiden yritysten tietoturvallisuuden hallinnasta ISO 27000 -tietoturvastandardin avulla.

Asiasanat: ISO 27000, ISO 27001, ISO 27002, tietoturvastandardisarja, tietoturvastandardi, tietoturva, tietoturvan hallintajärjestelmä, ISO 27001 -sertifikaatti, tietoturvapolitiikka

ABSTRACT

Mäki-Maukola, Eeva
The ISO 27000 set of information security standards as part of today's organization information security management
Jyväskylä: University of Jyväskylä, 2023, 62 pp.
Cyber Security, Master of Science Thesis
Supervisor: Lehto, Martti

The aim of this study was to find out how the ISO 27000 series of information security standards is part of today's organizations information security management. The research focuses on the standards ISO 27000, ISO 27001, and ISO 27002, of which the ISO 27001 standard was handled with the help of the ISO 27001 certificate granted to organizations. The perspective for the review was chosen along with the standards in question, as they essentially focus on the management of organizations information security and its planning, implementation, maintenance and improvement. The scope of the research was focused on organizations operating in various business sectors in Finland, which have achieved the ISO 27001 certificate in recent years.

The literature review of the research consists of the information security management of organizations and the reference framework of the information security policy and information security management system. The literature review also focuses on the ISO 27000 series of information security standards and especially the standards ISO 27000, ISO 27001 and ISO 27002, as well as their history and development up to the present.

This study was carried out as a qualitative study and an electronic questionnaire was used to collect qualitative data, which was answered by the representatives of the organizations that participated in the study. The aim of the results of the study was to find out how the organizations participating in the study use the standards ISO 27000 and ISO 27002 in managing and directing their information security. The goal of the results was also to examine the application process for the ISO 27001 certificate achieved by the companies, for example from the perspective of its duration and challenge.

Four organizations participated in the study, so the sample was small. Because of this, it is not possible to make generalizing conclusions about the information security management of organizations operating in different business sectors in Finland. The research results, however, give an overview of the information security management of the organizations that participated in the research using the ISO 27000 information security standard.

Keywords: ISO 27000, ISO 27001, ISO 27002, information security standard set, information security standard, information security, information security management system, ISO 27001 -certificate, information security policy

KUVIOT

KUVIO 1 Digitaalisen turvallisuuden toteutusalueet (DVV, 2023)..... 17
KUVIO 2 Tietoturvapolitiikan käyttöönottoprosessi (mukaillen Karyda ym., 2004) 22
KUVIO 3 Tietoturvan hallintajärjestelmän toteuttaminen PDCA-mallin mukaisesti (mukaillen Susanto ym., 2011)..... 23
KUVIO 4 Standardien ISO 27000, ISO 27001 ja ISO 27002 kehitys vuosien saatossa (Disterer, 2013). 27
KUVIO 5 ISO 27001 -sertifiointiprosessi (mukaillen Talib ym., 2012)..... 32

TAULUKOT

TAULUKKO 1 Yritysten ISO 27001 -sertifikaatin saavuttamisvuosi..... 40
TAULUKKO 2 Yritysten ISO 27001 -sertifikaatin hakuprosessin kesto..... 41
TAULUKKO 3 Yritysten kokemus ISO 27001 -sertifikaatin hakuprosessin haastavuudesta 41
TAULUKKO 4 Yritysten kokemat tärkeimmät tekijät, jotka vaikuttivat ISO 27001 -sertifikaatin hakupäätökseen..... 43

SISÄLLYS

TIIVISTELMÄ
ABSTRACT
KUVIOT JA TAULUKOT

1 JOHDANTO 7
1.1 Tutkimuksen tausta ja tavoitteet 9
1.2 Tutkimukseen osallistuvat yritykset 10
1.3 Tutkimusmenetelmä ja tutkimuksen tulokset 11
1.4 Tutkielman rakenne 13

2 TIETOTURVALLISUUDEN HALLINTA YRITYKSESSÄ 14
2.1 Yritykset ja tietoturvallisuus 14
2.1.1 Tietoturvallisuuden toimintaympäristö 14
2.1.2 Tietoturvallisuus vs. kyberturvallisuus 16
2.1.3 Yrityksiin kohdistuvat tietoturvauhkat 18
2.2 Tietoturvapolitiikka 20
2.3 Tietoturvan hallintajärjestelmä (ISMS) 22

3 ISO 27000 -TIETOTURVASTANDARDISARJA 26
3.1 ISO 27000 28
3.2 ISO 27001 29
3.2.1 ISO 27001 kuvaus 29
3.2.2 ISO 27001 -sertifikaatti ja sen hakuprosessi 31
3.3 ISO 27002 33

4 TIEDONKERUUMENETELMÄ 35
4.1 Tiedonkeruumenetelmän valinta ja toteutus 35
4.2 Keskeiset haasteet ja riskit 36
4.3 Aineiston analyysi ja luotettavuus 37

5 TUTKIMUSTULOKSET 38
5.1 Vastaajien taustatiedot 38
5.2 Yritykset ja ISO 27000 -standardi 38
5.3 Yritykset ja ISO 27002 -standardi 39
5.4 Yritykset ja ISO 27001 -sertifikaatti 39

6 POHDINTA JA JOHTOPÄÄTÖKSET 44
6.1 Tutkimuksen analyysiä 44
6.2 Johtopäätökset 50
6.3 Tutkimuksen vahvuudet ja rajoitteet 52

7 YHTEENVETO 53

LÄHTEET 55

LIITE 1 KYSELYTUTKIMUS.....60

1 JOHDANTO

1.1 Tutkimusongelma ja -kysymys

Yrityksillä on nykypäivänä erilaisia näkemyksiä tietoturvallisuudesta, sen järjestelmistä ja siitä, miten yrityksissä pyritään hallitsemaan tietoturvallisuutta (Hamdi ym., 2019). Tietoturvallisuus käsitteenä voidaan määritellä käytäntönä, jonka tarkoitus on suojata tietovarat ja tietojärjestelmät luvattomalta pääsyltä, käytöltä, paljastamiselta, häiriöltä, muuttamiselta tai tuhoamiselta luottamuksellisuuden, eheyden ja saatavuuden takaamiseksi. Luottamuksellisuus takaa, että yrityksen sisältämät yksityiset tiedot suojataan luvattomilta henkilöiltä. Eheys takaa, että yrityksen tiedot ja järjestelmät luodaan sekä muokataan määritellyllä ja valtuutetulla tavalla. Saatavuus varmistaa, että järjestelmät toimivat ja palvelu pystytään toimittamaan nopeasti niille, joilla on lupa käyttää niitä (Zafar, 2013).

Tietoturvallisuus on moniulotteinen ilmiö, joka auttaa vähentämään tietoon kohdistuvaa riskiä soveltamalla asianmukaista turvakontrollien yhdistelmää (Singh ym., 2014). Tietoturvan keskeinen kysymys on tietoturvallisuusriskien ja mahdollisten vaaratilanteiden rajoittaminen. Tietoturvallisuus on ymmärrettävä huoli nykypäivänä kaikille eri liiketoiminta-alan yrityksille, koska monet niistä tallentavat valtavan määrän tietoa erilaisiin tietokantoihin. Esimerkiksi kehittynyt viestintätekniikka ja avoin pääsy Internetiin lisäävät riskejä, jolloin yritykset voivat kohdata erilaisia välittömiä tietoturvallisuuteen liittyviä tapauksia ja rikkomuksia (Nowak, 2015). Yritysten sisältämä tieto ja niiden käytössä olevat tietojärjestelmät ovat alttiina erilaisille riskeille nykypäivänä yhä enemmän, sillä informaatioteknologian sekä tietotekniikan kysynnän ja tarjonnan lisääntyminen on kasvanut valtavasti eri toiminta-alan yrityksissä. Yritykset voivat käyttää apunaan erilaisia tietoturvastandardeja heidän tietoturvallisuutensa hallintaan, riskien kartoittamiseen sekä kontrollointiin liittyen heidän tietoturvallisuuteensa, tietoturvapolitiikkaansa sekä tietoturvan hallintajärjestelmäänsä.

Tietoturvastandardit ISO 27000, -27001 ja -27002 muodostavat kokonaisvaltaiset puitteet sekä yrityksen tietoturvapolitiikalle että tietoturvan hallintajärjestelmän suunnittelemiseksi, käyttämiseksi ja sen ylläpitämiseksi (Disterer, 2013). Tietoturvapolitiikkaa pidetään yhtenä tärkeänä osana yrityksen tietoturvaa sekä sen hallintaa ja siitä on muodostunut nykyajan yrityksille tärkeä voimavara. Sen avulla yrityksellä on käytössään dokumentoidut tavoitteet, keinot ja menetelmät siitä, miten yrityksessä aiotaan toteuttaa tietoturvaan liittyviä toimia sekä tavoitteita. Tietoturvapolitiikan tarkoitus on myös heijastaa yrityksen halukkuutta toimia yrityksessä valvotulla, toivotulla ja turvallisella tavalla. Myös tietoturvan hallintajärjestelmällä on tärkeä rooli liittyen yrityksen tietovarallisuuteen ja siihen liittyvissä riskeissä, jotka liittyvät fyysisiin, inhimillisiin ja teknologisiin uhkiin. Tietoturvan hallintajärjestelmän käyttöönottoa pidetään yrityksen strategisena päätöksenä. Käyttöönotto on integroitava ja valmisteltava yrityksen tarpeiden mukaisesti, joten suunnittelu ja yritykseen räätälöidyn tietoturvan hallintajärjestelmän toteutuksen tulee perustua organisaatiorakenteeseen ja liiketoimintaprosesseihin (Nowak, 2015).

Edellä mainittujen standardien sekä niiden mukaisen tietoturvapolitiikan ja tietoturvan hallintajärjestelmän avulla yrityksille tarjotaan mahdollisuus yhdenmukaistaa informaatioteknologian menettelyjään sekä varmistaa menetelmät riittävän tietoturvatason varmistamiseksi kansainvälisellä tasolla (Disterer, 2013). Tehokas tietoturva onkin määritelty kyseisissä standardeissa yritysten tietovarojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseksi (Calder & Gerrard, 2013).

Tässä tutkimuksessa tutkitaan neljää eri Suomessa toimivaa yritystä eri liiketoiminnan aloilta, jotka käyttävät yrityksensä tietoturvan ja tietoturvallisuuden hallinnassa jossain määrin ISO 27000 -standardisarjaa ja ovat saaneet käyttöön standardeja 27001 sekä 27002 koskevan kolmannen osapuolen hyväksymän sertifioinnin, joka liittyy keskeisesti yrityksen tietoturvan hallintajärjestelmään.

Tutkimuksen tutkimuskysymys on seuraava:

Miten ISO 27000 -standardisarja ja erityisesti standardit ISO 27000, ISO 27001 ja ISO 27002 ovat osana tietoturvallisuuden hallintaa tutkimukseen osallistuvien nykypäivän yrityksissä?

Tutkimuksen tarkoituksena on selvittää, miten eri Suomessa toimivien liiketoiminta-alan yritysten toimintatavat eroavat käytettäessä kyseisiä standardeja, kun kyseessä on heidän tietoturvallisuutensa sekä tietoturvallisuuden hallinta. Tarkoituksena on myös vertailla tutkimukseen osallistuneiden yritysten tietoturvastandardien käyttöä ja ohjaavatko kyseiset standardit heidän tietoturvallisuutensa hallintaa. Tavoitteena on myös selvittää yritysten eroavaisuuksia liittyen ISO 27001 -sertifiointiprosessiin. Tutkimuksessa tärkeimpänä näkökulmana käytetään ISO 27000 -tietoturvastandardisarjaa ja standardeja ISO 27000, ISO 27001 ja ISO 27002, joiden avulla pyritään tutkimaan tutkimukseen osallistuvien yritysten tietoturvan hallintajärjestelmään liittyvää sertifiointiprosessia, sekä muita menettelytapoja, kokemuksia sekä toimintoja, joita kyseinen standardisarja käsittelee.

Tutkimuksessa selvennetään aiheen kokonaisvaltaisen ymmärtämisen takia ISO 27000 -standardisarjan sisältöä sekä sen historiaa ja käsitellään tarkemmin aiheen laajuuden takia kyseisen sarjan standardeista vain numeroita 27000, 27001 ja 27002 niiden sisältöineen. Tutkimuksessa käsitellään myös tietoturvallisuuden hallintaa yrityksissä esimerkiksi tietoturvapolitiikan sekä edellä mainittujen standardien näkökulmasta ja selvennetään tietoturvan hallintajärjestelmän käsite, joka liittyy olennaisesti myös yrityksen tietoturvallisuuteen ja sen hallintaan. Kyseisen järjestelmän hyvä toteutus noudattaakin juuri ISO 27000 -sarjaa ja erityisesti standardeja 27001 sekä 27002, jotka tarjoavat puitteet parhaille käytännöille, jotka auttavat yrityksiä huolehtimaan omasta tietoturvallisuuden hallinnastaan (Hamdi ym., 2019). Yhdessä oikein rakennettu yrityksen tietoturvan hallinta ja sen järjestelmä, tietoturvapolitiikka, sekä ISO 27000 -standardisarja ja sen standardit 27001 ja 27002, ovat hyvin oleellinen yhtälö käsiteltäessä yritysten tietoturvallisuutta ja sen hallintaa.

1.2 Tutkimuksen tausta ja tavoitteet

Tämän tutkimuksen avulla on tarkoitus suorittaa kyberturvallisuuden maisteriopintokokonaisuuteen kuuluva Pro Gradu -tutkielma. Tutkimuksen avulla on tarkoitus lisätä, tukea sekä vahvistaa tutkielman tekijän jo olemassa olevaa kerättyä tietoa kyseisestä aiheesta. Tutkimuksen taustatekijänä toimii tutkielman tekijän oma mielenkiinto kyberturvallisuuteen, sen ala-aiheisiin sekä aiheen kokonaisvaltainen merkitys nykypäivän kehittyneessä teknologisessa maailmassa. Tutkimuksen taustana on itse tekijän, mutta myös muiden mahdollisten halukkaiden tiedon lisääminen kyseisestä aiheesta. Tutkimuksen avulla myös tutkimukseen osallistuneet yritykset voivat yleisellä tasolla vertailla halutessaan toisiaan ISO 27000 -standardisarjan sekä tietoturvan hallintajärjestelmän näkökulmasta liittyen heidän yritystensä tietoturvallisuuden hallintaan. Tutkimuksen aihe valikoitui tutkimuksen tekijän oman mielenkiinnon kohteiden perusteella. Halu tutustua ISO 27000 -standardisarjaan pintaa syvemmältä on hyvä tapa yhdistää sekä Pro Gradu -tutkielma että uuden ja vanhan oppiminen pintaa syvemmältä. Aikaisempia tutkimuksia liittyen ISO 27000 -standardisarjaan sekä tietoturvan hallintajärjestelmään on tehty eri näkökulmien sekä teorioiden avulla useita erilaisia. Useissa aikaisemmissa tutkimuksissa aihetta on rajattu muutamaan kyseisen tietoturvastandardisarjan standardiin, joita on käsitelty erilaisin tutkimuskysymyksin ja -ongelmin. Esimerkiksi Gillies (2011) tutkii artikkelissaan yritysten tietoturvan hallintajärjestelmien laadun parantamista kaikkien ISO 27000 -standardien avulla.

Gilliesin (2011) tutkimus on maailmanlaajuinen tutkimus, mutta Suomessa toimiviin eri liiketoiminta-alan yrityksiin kohdistuvia aikaisempia tutkimuksia tämän Pro Gradu -tutkielman näkökulmalla sekä tutkimuskysymyksellä ei löytynyt montaa. Lähimpänä tätä tutkimusta aihealueeltaan ovat Suomessa tehty Ilvosen (2006) Pro Gradu -tutkimus, jossa hän tutkii tietoturvallisuutta pirkanmaalaisissa tietointensiivisissä pk-yrityksissä sekä Hytösen ja Sipilän (1987)

tekemä Pro Gradu -tutkimus aiheesta ”Tietoturvallisuus yrityksessä”. Aiempia suomalaisia tutkimuksia juuri edellä mainitun tietoturvastandardisarjan standardeista 27000, 27001 ja 27002 tämän tutkielman tutkimuskysymyksen näkökulmasta ei löytynyt, mutta esimerkiksi Siponen ja Willison (2009) tutkivat tutkimuksessaan ISO 27001 standardiin liittyviä ongelmia sekä ratkaisuja ja Porvari (2012) tutkii väitöskirjassaan tietoturvallisuutta liiketoiminnan johtamisen, prosessien ja henkilöiden toiminnan näkökulmista.

Lähimpänä tätä tutkimusta tutkimuskysymyksen näkökulmasta on Hamdin ym. (2019) tekemä tutkimus Malesiassa, jossa tutkitaan ISO 27000 -tietoturvastandardisarjan näkökulmasta tietoturvan hallintajärjestelmää eri liiketoimintasektoreiden organisaatioissa. ISO 27001 -sertifikaatista on myös tehty lukuisia tutkimuksia ja esimerkiksi Wang ja Tsai (2009) tutkivat ISO 27001 -sertifikaattia yrityksen johdon näkökulmasta, sillä he uskovat sertifikaatin hyödyttävän yritystä sekä sen johtamista positiivisesti. Myös Hsu ym. (2016) tutkivat artikkelissaan ISO 27001 -sertifikaattia yrityksen suorituskyvyn näkökulmasta sekä yrityksen johdon asenteen näkökulmasta.

Tämän tutkimuksen tavoitteena on selvittää, miten ISO 27000 -tietoturvastandardisarja on osana nykypäivän yritysten tietoturvallisuuden hallintaa. ISO 27000 -tietoturvastandardisarjassa on 46 yksittäistä julkaistua standardia, mutta tässä tutkimuksessa niistä käsitellään standardeja numero 27000, 27001 ja 27002. Tutkimuksen tavoitteena on myös selvittää, eroaako yritysten sertifiointiprosessit merkittävästi toisistaan liittyen standardiin ISO 27001.

Tutkimukseen osallistui neljä Suomessa toimivaa yritystä eri liiketoiminnan aloilta. Neljä yritystä sopii tähän tutkimukseen määrältään hyvin, jotta tutkimukseen saataisiin mahdollisimman monta erilaista yritysnäkökulmaa siitä, miten kyseisen standardisarjan standardit ovat kyseisten yritysten tietoturvallisuuden hallinnassa mukana, kuitenkaan keräämättä liikaa aineistoa. Yrityksiä valittaessa tähän tutkimukseen tärkeimpänä osallistumisen edellytyksenä oli se, että yrityksellä on lähivuosina hankittu ISO 27001 -sertifikaatti sekä se, että yrityksellä on tapahtuvaa liiketoimintaa Suomessa. Muuten yritysten valinnassa ei käytetty mitään spesifiä rajausta tutkimukseen osallistumisen suhteen.

1.3 Tutkimukseen osallistuvat yritykset

Tähän tutkimukseen osallistui 4 Suomessa toimivaa eri liiketoiminta-alan yritystä. Kaikkia neljää yritystä lähestyttiin sähköpostin välityksellä, jonka avulla selvitettiin heidän kiinnostuksensa osallistua tutkimukseen yrityksien edustajien kanssa. Tärkein tekijä kartoittaessa sekä lähestyessä yrityksiä ja heidän edustajiaan oli se, että yritys on saanut viime vuosien aikana hankittua itselleen ISO 27001 -sertifikaatin, joka liittyy olennaisesti yrityksen tietoturvallisuuden hallintaan ja täten on merkittävä kriteeri tähän tutkimukseen osallistumiselle. Toinen tärkeä tekijä valittaessa ja lähestyttäessä yrityksiä oli se, että heidän yritystoimintaansa tapahtuu Suomessa. Muita merkittäviä tekijöitä yrityksiä valittaessa ei ollut.

Fingrid Oyj on suomalainen kantaverkkoyhtiö, jonka omistajina ovat Suomen valtio sekä suomalaiset eläkeyhtiöt. Fingrid Oyj:n tehtävänä on turvata suomalaisen yhteiskunnan ja asiakkaiden varma sähkö kaikissa eri tilanteissa, kantaa vastuu Suomen sähköjärjestelmän tasapainosta sekä edistää puhdasta ja markkinaehtoista sähköjärjestelmää. Fingrid Oyj:n maailmanlaajuisen kantaverkon kautta kulkeekin noin 77 % Suomessa käytetystä sähköstä. Yhtiö on perustettu vuonna 1996 ja vuonna 2021 yrityksen liikevaihto oli 1090,2 miljoonaa euroa (Fingrid).

Gofore Oyj on suomalainen digitaalisten palveluiden kehittämiseen ja suunnitteluun keskittynyt yhtiö. Gofore Oyj haluaa selvittää, miten ihmiset ja teknologia parhaiten palvelevat toisiaan ja kuinka voidaan rakentaa ratkaisuja, jotka parantavat ihmisten arkea. Yritys tarjoaa muun muassa sovelluskehitystä, mobiilikehitystä, tietoturvaa, UX- ja UI-suunnittelua sekä testiautomaatiota ja laadunvarmistusta. Yrityksen liikevaihto vuonna 2021 oli yli 204 miljoonaa euroa (Gofore).

Magic Cloud Oy on suomalainen pilvipalveluja tarjoava yritys. Yritys huolehtii kokonaisvaltaisesti pilvialustoista sekä vastaa pilvialustojen teknisestä käytettävyydestä, laadusta ja turvallisuudesta. Yritys tarjoaa muun muassa pilven huolenpitopalveluita, pilvi-infrapalveluita, pilvihallittua yritysverkkoa sekä pilvi-infran optimointia. Magic Cloud onkin yksi Suomen johtavista virtuaalityöpöytien tarjoajista. Yrityksen liikevaihto vuonna 2021 oli 2,3 miljoonaa euroa (Magic Cloud).

Yritys X on kokonaisvaltainen IT-palvelutalo, jonka tavoitteena on auttaa asiakkaitaan luomaan mielekkäämmän sekä tuottavamman työympäristön sekä tarjota IT-ratkaisuja ja -palveluita kaiken kokoisille yrityksille ja organisaatiolle. Yritys X on Pohjoismaiden sekä Baltian johtava IT-infrastruktuuritoimittaja, joka toimii myös laajasti Suomessa. Yritys tarjoaa muun muassa IT-ympäristöjen sekä -infrastruktuurin kehittämistä, IT-laitteiden jälleenmyyntiä ja liiketoiminnan digitalisointia. Yritys X:n liikevaihto Suomessa vuonna 2021 oli 339,8 miljoonaa euroa ja koko konsernin liikevaihto vuonna 2021 oli 4,1 miljardia euroa.

1.4 Tutkimusmenetelmä ja tutkimuksen tulokset

Tässä tutkimuksessa tutkimusmenetelmänä käytetään laadullista, eli kvalitatiivista tutkimusmenetelmää ja käsiteltävän aineiston kerääminen tapahtui kyselylomakkeen avulla. Kvalitatiivinen tutkimusmenetelmä valikoitui tähän tutkimukseen sen takia, että se on arvokas tapa tarjota monipuolisia kuvauksia monimutkaisista ilmiöistä sekä saada kerättyä dataa eri toimijoiden toimesta, joilla jokaisella voi olla hyvin erilaisia panoksia ja rooleja (Sofaer, 1999). Varsinkin datan kerääminen eri toimijoiden toimesta on tämän tutkimuksen kannalta olennaista, sillä kyselylomakkeeseen vastanneet yrityksien neljä edustajaa toimivat yrityksissään eri työnimikkeillä.

Tutkimuksessa laadullinen menetelmä on hyödyllinen, kun tarkoituksena on rakentaa ja kehittää teorioita tai käsitteellisiä kehyksiä tai generoida

hypoteeseja (Sofaer, 1999). Tämä tukee myös laadullisen menetelmän valintaa koskien tätä tutkimusta. Eskolan ja Suorannan (1998) mukaan laadullinen tutkimus on keino, jolla voidaan kuvata ilmiötä tai saada parempi käsitys erityisestä toiminnasta. Kvantitatiiviset tutkimusmenetelmät soveltuisivat paremmin tilastollisten yleistysten tekemiseen. Kvalitatiiviselle tutkimukselle on myös tyypillistä, että tutkimussuunnitelma mukautuu tarvittaessa tutkimusprosessiin. Tämä näkyy myös siinä, että kvalitatiivisessa tutkimuksessa tulkinta ulottuu koko tutkimusprosessin läpi. Se näkyy paitsi analysointi- ja keskusteluvaiheessa, myös jo tiedonkeruuvaiheessa ja raportointivaiheessa (Eskola & Suoranta, 1998).

Tämän tutkimuksen tavoitteena on tutkia tutkimukseen osallistuneiden yritysten näkökulmia liittyen heidän tietoturvallisuuteensa sekä tietoturvallisuuden hallintaan, joten kvalitatiivinen tutkimusmenetelmä sopii tähän tutkimukseen erittäin hyvin. Fossey ym. (2002) toteavat, että kvalitatiivisen tutkimuksen tavoitteena on antaa etuoikeus tutkimukseen osallistuneiden näkökulmille ja selkeyttää tutkittavien subjektiivista merkitystä, toimintaa sekä kontekstia. Tällä tavoin tässä tutkimuksessa pyrittiin kvalitatiivisen tutkimusmenetelmän avulla saamaan syvällistä ja asiantuntevaa tietoa yritysten perimmäisistä perusteluista ja vaikuttimista liittyen heidän tietoturvallisuuteensa, tietoturvallisuutensa hallintaan sekä ISO 27000 -tietoturvastandardeihin.

Tutkimuksen tuloksista selviää, että yrityksen edustajat, jotka vastasivat kyselyyn, toimivat yrityksessään työnimikkeillä tietoturvapäällikkö, CISO ja toimitusjohtaja. Kolme neljästä yrityksestä ilmoitti käyttävänsä standardeja ISO 27000 sekä ISO 27002 heidän yrityksensä tietoturvallisuuden hallinnassa jollain tasolla ja kyseiset standardit myös ohjasivat kyseisten yritysten tietoturvallisuuden hallintaa jollain tasolla. Yksi yritys neljästä ilmoitti, ettei yrityksen tietoturvallisuuden hallinnassa tai sen ohjaamisessa käytetä kumpaakaan standardia jollain tasolla. Kaikilla tähän tutkimukseen osallistuneilla yrityksillä on saavutettuna ISO 27001 -sertifikaatti.

Tutkimustuloksista käy lisäksi ilmi, että kaikki neljä yritystä ovat saavuttaneet kyseisen sertifikaatin viimeisen kolmen vuoden aikana. Yritykset pitivät sertifikaattiin liittyvää hakuprosessia sekä haastavana että ei haastavana. Hakuprosessin kesto vaihteli yritysten välillä 0–1 vuodesta 2–3 vuoteen. Tuloksista käy ilmi, että yrityksiin vaikuttaneet tärkeimmät tekijät hakea ISO 27001 -sertifikaattia olivat yrityksen maineen positiivinen edistäminen sekä yrityksen tietoturvaosaamisen sekä tietoturvallisuuden kehittäminen. Vähiten tärkeitä tekijöitä olivat työntekijöiden tietoturvallisuustietoisuuden kasvattaminen, tunnistettujen turvallisuusriskien hallitseminen sekä halu toimia tietoturvallisuuden johtamisen mahdollistajana. Tutkimustulokset osoittavat, että kaikki tähän tutkimukseen osallistuneet yritykset ovat kokeneet ISO 27001 -sertifikaatin vaikuttaneen positiivisesti yrityksen toimintaan sen saavuttamisen jälkeen.

1.5 Tutkielman rakenne

Tämän tutkielman rakenne koostuu kuudesta luvusta ja näiden lukujen alaluvuista. Tutkimus alkaa johdannolla, jonka tarkoituksena on johdattaa lukija aihealueeseen. Johdannossa kuvataan lyhyesti tutkimuksen tausta, ongelmat, tutkimuksen tarkoitus ja tarve perusteluineen, tavoitteet, tutkimusmenetelmä sekä saavutetut tulokset ja niiden merkitys. Johdannossa esitellään myös tutkimukseen osallistuneet neljä yritystä kuvauksineen. Toisessa luvussa käsitellään tietoturvallisuuden hallintaa yrityksessä sekä käsitellään tietoturvallisuuden ja kyberturvallisuuden välistä suhdetta tämän tutkimuksen aiheen näkökulmasta. Luvussa käydään myös läpi yrityksiin kohdistuvia mahdollisia tietoturvauhkia sekä avataan tietoturvapolitiikan sekä tietoturvan hallintajärjestelmän merkitys yritysmaailmassa ISO 27000 -standardisarjan sekä standardien ISO 27000, ISO 27001 ja ISO 27002 avulla. Kolmannessa luvussa keskitytään tarkemmin ISO 27000 -tietoturvastandardisarjaan ja erityisesti edellä mainittuihin standardeihin 27000, 27001 ja 27002, sekä niiden historiaan ja kehityskaareen aina nykyhetkeen asti. Samassa luvussa käsitellään myös ISO 27001 -tietoturvastandardin sekä tietoturvan hallintajärjestelmän yhteys toisiinsa ja ISO 27001 -standardiin liittyvä sertifiointiprosessi liittyen yrityksen tietoturvan hallintajärjestelmään. Neljännessä luvussa käydään läpi tämän tutkimuksen tiedonkeruumenetelmä, sen valinta ja toteutus. Samassa luvussa käsitellään myös keskeisiä haasteita ja riskejä liittyen tiedonkeruumenetelmään. Luvussa analysoidaan myös kerätty aineisto sekä sen luotettavuus. Viidennessä luvussa esitetään tutkimuksen aikana saadut ja kerätyt tutkimustulokset, jonka jälkeen kuudennessa luvussa pohditaan ja analysoidaan saatuja tutkimustuloksia kirjallisuuden avulla. Samassa luvussa käydään läpi myös tämän tutkimuksen vahvuudet sekä rajoitteet. Tutkimuksen päättää yhteenveto, jossa kootaan tutkimuksen ydin yhdeksi kokonaisuudeksi.

2 TIETOTURVALLISUUDEN HALLINTA YRITYKSESSÄ

2.1 Yritykset ja tietoturvallisuus

2.1.1 Tietoturvallisuuden toimintaympäristö

Yritykset ovat nykyään riippuvaisempia kuin koskaan informaatioteknologiasta, koska se tukee niiden päivittäistä toimintaa sekä lukuisia muita kriittisiä liiketoimintatoimintoja (Flowerday & Tuyikeze, 2008). Tämän takia tietoturvan hallinnalla sekä tiedolla ja sen oikeaoppisella suojaamisella on erittäin tärkeä rooli eri liiketoiminta-alan yrityksissä. Se on huomattava voimavara, joka ohjaa yritystä päätöksenteossa, ongelmien ratkaisemisessa, tietoturvallisuuden hallinnassa ja tietoturvan hallintajärjestelmän kehittämisessä sekä sen ylläpidossa (Hamdi, 2019).

Yrityksen tietoturvallisuuden hallinta sisältää joukon toimia, jotka liittyvät resurssien konfigurointiin yrityksen tietoturvatarpeiden täyttämiseksi. Tietoturvallisuuden hallinnan ydintavoitteena on mukauttaa turvallisuustavoitteet yrityksen liiketoiminnan tarpeisiin. Tietoturvaa hallitaan yrityksessä kolmella tasolla: strategisella (politiikkalähtöinen), taktisella (ohjeistuslähtöinen) ja operatiivisella (toimenpiteisiin perustuvalla) tasolla. Tämän takia esimerkiksi yrityksen tietoturvan hallintajärjestelmä koostuu käytännöistä, menettelyistä, ohjeista, toiminnoista ja niihin liittyvistä resursseista, joita yritys hallinnoi yhdessä suojatakseen tieto-omaisuuttaan (Singh ym., 2013). Tietoturvallisuuden hallinnan olennaisia haasteita on epätäydelliset tiedot yrityksen turvallisuusriskeistä sekä käytettävissä oleva valvonta niiden ratkaisemiseksi (Meriah ym., 2019). Monet väärinkäsitykset liittyen yrityksen tietoturvallisuuteen johtuukin usein sen puutteesta tai väärästä päättelystä. Monesti ajatellaan, että yrityksen tietoturvallisuus ja sen hallinta on vain tietynlainen väliaikainen tila, vaikka kyseessä on jatkuvasti käynnissä oleva ja muuttuva prosessi (Hoffman ym., 2016).

Tietoturvallisuus kasvaa yrityksissä koko ajan kohti laajempaa kokonaisuutta ja siitä on tullut tärkeä osa eri liiketoiminta-alojen liiketoimintaprosesseja sekä yrityskokonaisuutta. Tavoitteena on yritysten tietovarojen luottamuksellisuuden, eheyden ja saatavuuden lisäksi myös tuottaa todellista liiketoimintahyötyä samalla suojellen ja helpottaen valvotun tiedon jakamista ja niihin liittyvien riskien hallitsemista koko ajan muuttuvassa uhkaympäristössä. Tällaisen painotuksen muutos tarkoittaa, että yrityksessä on myös monia rooleja erilaisilla toimintatasoilla liittyen tietoturvaan. Tietoturva käsitteenä on kehittynyt sekä leveydessään että syvyydessään, sillä nykyään sen tulisi olla yrityksessä sulautettu toiminto. Yrityksen johdolla onkin merkittävä rooli liittyen tietoturvallisuuteen ja tietoturvan hallintajärjestelmään, sillä johdon tehtävänä on määritellä tietoturvapolitiikan tavoitteet ja kuinka kyseisiä tavoitteita voidaan saavuttaa tehokkaasti ja johdonmukaisesti (Ashenden, 2008).

Yritykset käyttävätkin erilaisia tietojärjestelmiä ja työkaluja, jotka on tarkoitettu auttamaan yritystä liiketoiminnan kannalta merkittävissä prosesseissa. Tietojärjestelmien turvallisuuden hallinta onkin johtamistoimintojen virta, jonka tavoitteena on turvata kyseiset järjestelmät ja luoda puitteet, joissa tietojärjestelmät toimivat yrityksen odottamalla tavalla. Tietojärjestelmien sekä tietovarojen turvallisuuden hallinta pyrkii minimoimaan riskit ja sisältääkin useita eri vaiheita, kuten suunnitteluvaihe, toteutusvaihe ja auditointivaihe (Karyda ym., 2004).

Erilaisten tietojen kerääminen, tallentaminen ja analysointi ilman asianmukaista tietoturvamittausta tekee yrityksestä erittäin haavoittuvan tietoturvarikollisille (Hamdi ym., 2019). Tietoa ja tietojärjestelmiä on hallittava oikein, jotta yritykset voivat parantaa toimintaansa, sillä ilman oikeaa tiedon hallintaa ja säilyttämistä yritykset tekevät ja tulevat tekemään varmasti virheitä. Kyseiset virheet voivat kostautua erilaisina tietoturva-aukkoina ja ongelmina, jotka voivat vaarantaa muun muassa yrityksen toiminnan jatkuvuuden, prosesseja sekä mainetta (Hamdi ym., 2019).

Tekniset ratkaisut, joiden tarkoituksena on estää tietojärjestelmien vaarantuminen, on lisääntynyt. Tämä on johtanut siihen, että tietoturvarikolliset ja -hyökkääjät ovat joutuneet myös kehittämään ja löytämään uusia keinoja saavuttaakseen tavoitteensa. Uusien tapojen läsnäolo tietoturvan vaarantamisessa on saanut yritykset kiinnittämään huomiota kokonaisvaltaisempaan lähestymistapaan liittyen oman tietoturvan hallintaan. Kokonaisvaltaista tietoturvallisuuden hallinnan lähestymistapaa korostaa inhimillisen tekijän huomioon ottaminen varmistaessa koko yrityksen tietoturvaa (Rocha ym., 2014). Goodman ym. (2008) toteavatkin, että tietoturvallisuus suojaa nykyään kokonaisvaltaisesti yrityksen toimintakykyä.

Tietotekniikan sekä informaatioteknologian merkityksen kasvaessa yritykset ovat käsittäneet kiireellisen tarpeen riittäville tietoturvatoimille. Järjestelmällinen tietoturvan hallinta on yksi informaatioteknologian hallinnan tärkeimmistä aloitteista yritysmaailmassa ja eri liiketoiminta-alan yritykset ovatkin tunnustaneet vastuunsa tietovarojen suhteen (Disterer, 2013). On olemassa erilaisia valvontatoimia ja toimenpiteitä, joiden avulla voidaan toteuttaa tehokasta työskentelyä yrityksen tietoturvan hallinnan, tietovarojen sekä tietoturvallisuuden

parissa. Nämä keinot ja toimenpiteet vaihtelevat teknisistä ratkaisuista ja sopimusmääräyksistä aina yrityksen tietoisuuteen riskeistä, uhkista ja haavoittuvuuksista (Höne & Eloff, 2002).

Esimerkiksi tietoturvastandardeja voidaan käyttää ohjeena tai viitekehyksenä riittävän tietoturvan ja tietoturvallisuuden hallintajärjestelmän kehittämiseen ja ylläpitämiseen. Ne eivät ole kuitenkaan pakollisia. Tietoturvallisuuden hallintastandardit, kuten ISO 27000 -tietoturvastandardisarja tarjoaa erilaisia ohjeita, joiden avulla yritykset voivat arvioida heidän tietonsa turvallisuuttaan jatkuvasti. Standardit ohjaavat tietoturvatoimintaa myös yritysten johtamis- ja prosessilähestymistavassa. Esimerkiksi standardit ISO 27000, 27001 ja 27002 ovat kansainvälisiä standardeja, jotka saavat jatkuvasti kasvavaa tunnustusta ja hyväksyntää. Niitä kutsutaankin järjestöjen yhteiseksi kieleksi ympäri maailmaa ja ne ovatkin suosituimpia standardeja, kun käsitellään yrityksen tietoturvaa, tietoturvapolitiikkaa sekä tietoturvallisuuden hallintajärjestelmää (Disterer, 2013).

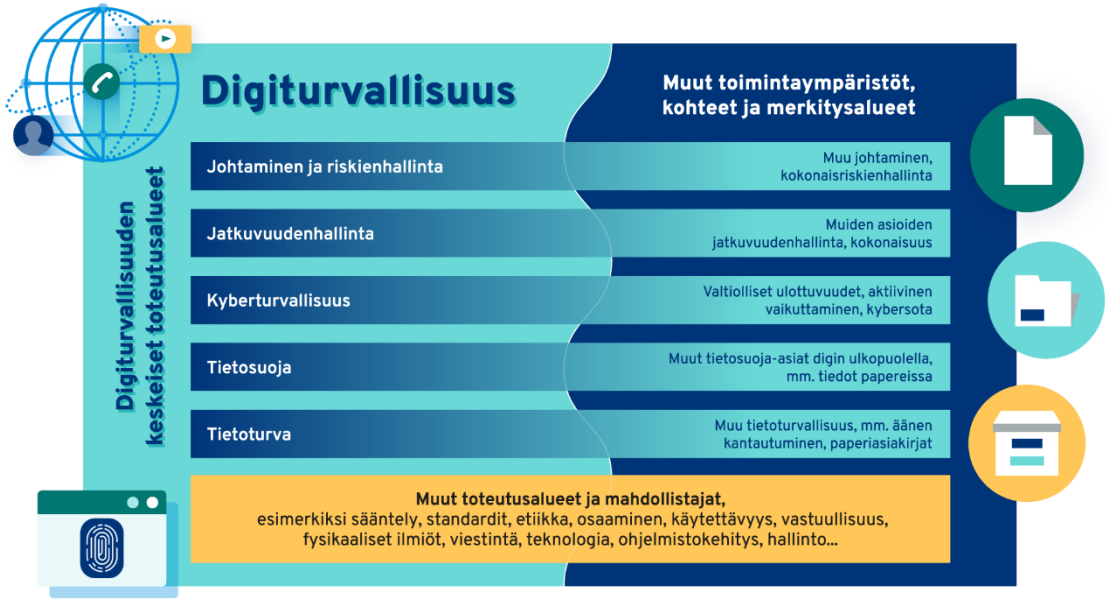
ISO 27000 -tietoturvastandardisarja sisältääkin useita sääntöjä, jotka mahdollistavat lisääntyvien uhkien vähentämisen, olemassa olevien turvallisuusongelmien ratkaisuja ja parantaa turvallisuustavoitteita yleisesti (Meriah ym., 2019). Kyseinen standardisarja sisältää myös ohjeet ja käytänteet yrityksen tietoturvapolitiikalle sekä tietoturvan hallintajärjestelmän rakentamiselle ja ylläpidolle (Hoffmann ym., 2016). Yhdet tärkeimpiä toimenpiteitä toteuttaa yritysten tehokasta tietoturvallisuutta ovatkin edellä mainitut tietoturvapolitiikka sekä tietoturvan hallintajärjestelmä, joiden avulla voidaan kontrolloida yrityksiin kohdistuvia mahdollisia tietoturvauhkia.

2.1.2 Tietoturvallisuus vs. kyberturvallisuus

Vaikka tässä tutkimuksessa keskitytään yritysten tietoturvallisuuteen, koettiin tarpeelliseksi myös käsitellä tietoturvallisuuden ja kyberturvallisuuden suhdetta toisiinsa tämän tutkimuksen aiheen näkökulmasta. Tietoturvallisuus ja kyberturvallisuus liittyvät läheisesti toisiinsa ja niitä käytetään usein vaihtokelpoisesti sekä kirjallisuudessa että yrityksissä (Alexei & Alexei, 2023).

Digi- ja väestötietovirasto (DVV) on tuottanut määritelmän digitaalinen turvallisuus. Sen viisi keskeistä toteutusaluetta ovat tarpeellisia kattavan digitaalisen turvallisuuden varmistamiseksi. Nämä eri osa-alueet ovat johtaminen ja riskienhallinta, jatkuvuudenhallinta, kyberturvallisuus, tietosuoja ja tietoturvallisuus. Digitaalisella turvallisuudella pyritään varmistamaan, että digitaalinen toimintaympäristö on luotettava, turvallinen ja saatavilla. Tässä kontekstissa DVV:n mukaan ”Tietoturvallisuus eli tietoturva tarkoittaa toimia, joilla pyritään varmistamaan tietojen luottamuksellisuus, eheys ja saatavuus. Tietoturvalla pyritään takaamaan se, että ainoastaan asianmukaiset tahot pääsevät käsiksi tarvitsemiinsa tietoihin” (DVV, 2023).

Kuviossa 1 on esitetty Digi- ja väestötietoviraston malli digitaalisesta turvallisuudesta ja sen osa-alueista.



KUVIO 1 Digitaalisen turvallisuuden toteutusalueet (DVV, 2023)

Kuten edellä on mainittu, tietoturvallisuus keskittyy muun muassa tietojen suojaamiseen luvattomalta käytöltä, paljastumiselta, häiriöiltä, muuttamiselta tai tuhoamiselta, riippumatta siitä mihin tietovälineeseen tieto on tallennettu. Kyberturvallisuuden ajatellaan olevan tietoturvallisuuden osajoukko, joka käsittelee erityisesti Internetin yhdistettyjen järjestelmien suojaamista kyberuhkilta. Toisin sanoen kyberturvallisuus on tietoturvatyyppi, joka käsittelee digitaalisen omaisuuden suojaamista kyberuhkilta. Tietoturvallisuudessa painotetaan vahvasti tiedon suojaamista sekä fyysisesti että digitaalisesti, kun taas kyberturvallisuus tarkoittaa kaikkea kyberavaruuteen kuuluvaa omaisuutta (Alexei & Alexei, 2023).

Alexei ja Alexei (2023) toteavat, että kyberturvallisuus toimii ikään kuin kattoterminä, joka sisältää sähköisen viestintäverkon ja tietoturvan, fyysisen turvallisuuden, kriittisen infrastruktuurin turvallisuuden, laitteisto- ja sovellusturvallisuuden, henkilöstöturvallisuuden sekä liiketoiminnan prosessien turvallisuuden. Kun tietoturvallisuus keskittyy tietojen luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseen, kyberturvallisuus keskittyy luottamuksellisuuden, eheyden ja saatavuuden säilyttämiseen kyberavaruudessa (Taherdoost, 2022).

Kyberavaruus koostuu kyberjärjestelmistä, jotka edustavat kyberavaruustoiminnan fyysisiä ilmenemismuotoja, joita ihmiset käyttävät vuorovaikutuksessa ja kyberturvallisuus on osa jokaista vuorovaikutusta (Alexei & Alexei, 2023). Kyberturvallisuus sisältää siis erilaisia työkaluja, järjestelmiä, prosesseja, käsitteitä, menetelmiä ja strategioita, joilla pyritään suojelemaan omaisuutta kyberavaruudessa luvatonta pääsyä ja tietojen katoamista vastaan (Taherdoost, 2022), joten kyberturvallisuus keskittyy Internetiin kytkettyjen digitaalisten resurssien ja järjestelmien suojaamiseen.

Alexei & Alexei (2023) toteavat, että kyberavaruus itsessään viittaa linkkien ja suhteiden joukkoon erilaisten kohteiden välillä, joihin pääsee yleisen tietoliikenneverkon kautta, joka mahdollistaa kohteiden haitallisen kauko-ohjauksen

sekä tietojen etäkäytön kyseisessä kyberavaruudessa. Tietoturva on pohjimmiltaan laajempi käsite, joka kattaa sekä fyysisen että digitaalisen tiedon, kun taas kyberturvallisuus on suppeampi käsite, joka keskittyy nimenomaan digitaalisen omaisuuden ja järjestelmien suojaamiseen kyberuhkilta.

Esimerkiksi Taherdoost (2022) toteaa, että tietoturvallisuudella tarkoitetaan tietojen ja kriittisten elementtien suojaamista, mukaan lukien järjestelmät ja laitteistot, jotka käyttävät, tallentavat sekä välittävät tietoa. Edellä mainittujen seikkojen perusteella voidaan päätellä, että vaikka tietoturvallisuus ja kyberturvallisuus liittyvät läheisesti toisiinsa, niin suurin eroavaisuus liittyy tietoon. Tietoturvallisuus on keskittynyt suojaamaan tietoa kaikkialla, kun taas kyberturvallisuus keskittyy erityisesti kyberavaruudessa olevaan tietoon ja sen suojelemiseen.

Taherdoost (2022) toteaakin, että pääsy hallintalaitteisiin, prosessinvalvontaan, vaatimustenmukaisuuden valvontaan ja teknisiin hallintalaitteisiin ovat esimerkkejä tietoturvallisuudesta, kun taas kyberavaruuden sovellusten suojaus, verkkoturvallisuus, pilviturvallisuus ja kriittinen infrastruktuuri ovat esimerkkejä kyberturvallisuudesta. Ottaen huomioon tietoturvallisuuden ja kyberturvallisuuden erot eri näkökulmista, tietoturvallisuus suojaa tietoja miltä tahansa uhkan muodolta riippumatta siitä, että onko se digitaalista tai fyysistä, kun taas kyberturvallisuus suojaa kyberavaruutta kyberhyökkäyksiltä (Taherdoost, 2022).

Täten tietoturvallisuus käsittelee tiedon suojelemista laajemmin. Kaikessa tietoon koskevassa turvallisuudessa on siis kyse arvokkaan omaisuuden suojaamisesta, ja turvallisuusprosessit käsittelevät yleensä valintaa ja toteutusta, jotka auttavat vähentämään tietoturvallisuushaavoittuvuuksien aiheuttamaa riskiä ympäristöstä huolimatta (von Solms & van Niekerk, 2013). Tässä tutkimuksessa kuitenkin haluttiin nimenomaan keskittyä tietoturvallisuuteen yritysmaailmassa, koska aihetta on helpompi käsitellä yrityksien näkökulmasta. Tällöin ei myöskään tarvitse keskittyä käsittelemään yritysten muodostamaa kokonaisuutta kyberavaruudessa, sillä se ei varsinaisesti kuulu tämän tutkimuksen aihealueeseen.

2.1.3 Yrityksiin kohdistuvat tietoturvauhkat

Yritysten tietojärjestelmät ja tietovarat ovat usein alttiina erilaisille uhkille, jotka voivat aiheuttaa erilaisia vahinkoja ja jotka voi johtaa merkittäviin taloudellisiin menetyksiin (Jouini ym., 2014). Uhkalla tarkoitetaan kuvausta mahdollisesta eitoivotusta tapauksesta, eli riskistä, joka voi toteutuessaan aiheuttaa merkittävää vahinkoa yritykselle ja sen tietojärjestelmille (Alhabeeb ym., 2010).

Erilaisten uhkien vaikutukset vaihtelevat huomattavasti, sillä osa niistä vaikuttaa luottamuksellisuuteen tai tietojen eheyteen, kun taas osa voi vaikuttaa suoraan järjestelmän saatavuuteen. Nykypäivänä yrityksillä voi olla vaikeuksia ymmärtää, mitä uhkia heidän tietovaroihinsa voi kohdistua ja kuinka muodostetaan tarvittavat keinot uhkien torjumiseksi (Jouini ym., 2014).

Yrityksiin kohdistuvat tietoturvauhkat voidaan jakaa sisäisiin sekä ulkoisiin uhkiin. Sisäisellä uhkalla tarkoitetaan sitä, kun jollain henkilöllä on valtuutettu pääsy yrityksen verkkoon joko palvelimella olevan käyttäjätilin tai fyysisen pääsyn avulla. Sisäinen uhka voi olla mahdollinen esimerkiksi yrityksen sisäisen työntekijän toiminnan tai organisaatioprosessin epäonnistumisen takia.

Ulkoisella uhkalla tarkoitetaan yrityksen ulkopuolella työskenteleviä henkilöitä, yrityksiä tai valtioita. Heillä ei ole valtuutettua pääsyä tietokonejärjestelmiin tai verkkoon. Sekä sisäiset että ulkoiset uhkat voidaan jakaa inhimillisiin (engl. human), ympäristöllisiin (engl. environmental) ja teknisiin (engl. technological) uhkiin. Inhimillisillä uhkilla tarkoitetaan ihmisten toimia, kuten työntekijöiden tai hakkereiden aiheuttamia uhkia, jotka voivat aiheuttaa vahinkoa tai riskin järjestelmän toiminnassa (Jouini, 2014).

Inhimillinen uhka voidaan jakaa esimerkiksi työntekijöiden ja hakkerien motivaatioon, mahdollisuuksiin ja kykyihin toteuttaa mahdollisia tietoturvauhkia (Colwill, 2009). Ympäristöuhkat ovat muiden tekijöiden kuin ihmisen aiheuttamia uhkia, joita ovat esimerkiksi luonnonkatastrofit. Tekniset uhkat johtuvat usein fyysisistä tai kemiallisista prosesseista. Fyysisiä prosesseja ovat muun muassa fyysisten keinojen käyttö pääsyyn rajoitetuille alueille, kuten rakennukseen tai yhdyshuoneisiin, joissa voidaan aiheuttaa erilaisilla toimilla tietojärjestelmien vahingoittumista. Kemialliset uhkat sisältävät huolimatta nimestään eri laitteiston ja ohjelmistojen eri teknologioita. Kemialliset uhkat sisältävät myös epäsuorat järjestelmätukilaitteet, kuten esimerkiksi virtalähteen. Kaikki kolme edellä mainittua uhkaa, inhimilliset, ympäristölliset ja tekniset, voidaan jakaa vielä ei-haitallisiin ja haitallisiin uhkiin (Jouini ym., 2014).

Ei-haitallisilla uhkilla tarkoitetaan niitä uhkia, jotka eivät aiheuta tietojärjestelmille merkittävää vahinkoa ja jotka eivät ilman haitallisia aikomuksia tule aiheuttamaan vahinkoa (Guo ym., 2011). Haitalliset uhkat taas voivat aiheuttaa tietojärjestelmissä merkittävää vahinkoa ja niitä ovat esimerkiksi erilaiset virukset, madot, troijalaiset, vakoiluohjelmat ja kiristyshaittaohjelmat (Ngo ym., 2020). Ei-haitalliset ja haitalliset uhkat voidaan vielä edelleen jakaa ei-tarkoituksellisiin ja tarkoituksellisiin uhkiin (Jouini ym., 2014). Ei-tarkoitukselliset uhkien aiheuttajat ovat yleensä huolimattomia työntekijöitä, jotka tietämättään tekevät virheen esimerkiksi tietokantajärjestelmän merkinnässä tai klikkaavat sähköpostiin saapuneita saastuneita linkkejä epähuomiossa (Gerić & Hutinski, 2007). Tarkoitukselliset uhkat ovat seurauksia haitallisista päätöksistä, kuten esimerkiksi tietokonerikoksista, joiden tarkoituksena on vahingoittaa omaisuutta tai tietoja tarkoituksella (Jouini ym., 2014).

Yritykset voivat vaikuttaa edellä mainittuihin uhkiin yrityksen sisäisellä tietoturvapolitiikalla sekä tietoturvallisuuden hallintajärjestelmällä, jotka voidaan muodostaa ISO 27000 -tietoturvastandardien avulla. Jotta yrityksiin kohdistuvat mahdolliset tietoturvauhkat voidaan tunnistaa, on tärkeää luokitella ja tuntea uhat, jotta tietoturvaresurssit voidaan mahdollisimman hyvin suojata etukäteen (Alhabeeb ym., 2010).

Onnistuneella tietoturvallisuuden hallintajärjestelmällä tämä on mahdollista. Esimerkiksi ISO:n (ISO, 2022b) standardissa 27002 todetaan, että "sopiva, riittävä ja tehokas tietoturvan hallintajärjestelmä varmistaa yrityksen johdolle ja muille asianosaisille, että heidän tietonsa ja muu siihen liittyvä omaisuus on kohtuullisen turvassa ja suojattu uhkia ja haittoja vastaan, jolloin yritys voi saavuttaa asetetut liiketoiminnalliset tavoitteet". ISO 27001 -standardin mukainen tietoturvan hallintajärjestelmä turvaa tiedon luottamuksellisuuden, eheyden ja

saatavuuden riskienhallintaprosessin avulla ja antaa luottamusta siitä, että riskejä sekä uhkia hallitaan yrityksessä asianmukaisesti (ISO, 2022a). Edellä mainittujen standardien avulla yrityksillä on siis merkittävä mahdollisuus kehittää omaa tietoturvauhkien havainnointia sekä analysointia. Täten on tärkeää, että yritysten tietoturvauhkia huomioidessa otetaan myös huomioon sekä käyttöön ISO 27000 -tietoturvastandardit, sillä kyseiset standardit tarjoavat ratkaisuja juuri edellä mainittuihin uhkaolosuhteisiin yritysmaailmassa. Standardien tarjoamat ohjeet ja ratkaisut edesauttavat yrityksiä parantamaan sekä ylläpitämään tietoturvallisuuttansa kokonaisuudessaan positiivisella tavalla.

2.2 Tietoturvapolitiikka

Kuten edellä on mainittu, yritysten tietojärjestelmien ja tietovarojen suojaaminen voi olla vaikeaa. Tämän takia tietoturvapolitiikan soveltamista pidetäänkin välttämättömänä, jotta yritys voi hallita sen liiketoiminnan sujuvuuden kannalta tärkeitä järjestelmiä ja tietovaroja. Onnistunut tietoturvapolitiikka yrityksessä ei kuitenkaan ole yksinkertainen tehtävä ja siihen vaikuttaa useat eri tekijät (Karyda ym., 2004). Karyda ym. (2004) toteavatkin, että tietoturvapolitiikalla on valtava merkitys yrityksille ja tämän seurauksena politiikasta on tullut kriittinen voimavara yrityksille. Tietoturvapolitiikan soveltamista pidetään yhtenä tärkeimpänä mekanismina, kun halutaan hallita yrityksen tietoturvallisuutta (Karyda ym., 2004).

Tietoturvapolitiikka on dokumentoitu selittämään tietoturvallisuuden tarpeet, käsitteet ja toimenpiteet yrityksen tietoresurssien käyttäjille (Höne & Eloff, 2002). Kyseinen politiikka sisältää tietojärjestelmien suojaamiseen liittyvät aikomukset ja prioriteetit, joita yleensä kutsutaan turvallisuuden tavoitteiksi, sekä yleiskuvauksen niistä keinoista ja menetelmistä, joilla kyseiset tavoitteet saavutetaan (Karyda ym., 2004).

Sen tarkoitus on täydentää yrityksen liiketoiminnan tavoitteita ja heijastaa johdon halukkuutta toimia yrityksessä valvotulla, toivotulla ja turvallisella tavalla. Yrityksen tietoturvapolitiikassa pitäisi tulla ilmi tietoturvan tavoitteet ja tietoturvallisuuden hallinnan menetelmät. Kyseisten tavoitteiden ja menetelmien tulee olla selkeät ja niiden tulee liittyä yrityksen yleiseen liiketoimintastrategiaan, tavoitteisiin ja päämääriin. Tärkeitä elementtejä laatiessa yrityksen tietoturvapolitiikkaa on selvittää tietoturvan tarve ja laajuus, tietoturvan ja -politiikan tavoitteet sekä tarkoitus, johdon sitoutuminen tietoturvaan, tietoturvan hyväksymiskäytäntö, tietoturvaperiaatteet, roolit ja vastuut, sekä seuranta ja analysointi (Höne & Eloff, 2002).

On selvää, että tietoturvapolitiikka edistää merkittävästi yrityksen hyvinvointia, kun kyseessä on sen kriittisten tietovarojen suojaaminen. Tehokkaan tietoturvapolitiikan kehittämiseen ja toteuttamiseen liittyvät prosessit voivat olla kuitenkin vaikeita. Tehokkaan tietoturvapolitiikan toteuttaminen ja kehittäminen ei ole aina suoraviivaista, vaan se voi olla ohjattua monien yksityiskohtien,

kuten sääntelyvaatimusten, uusien teknologioiden sekä ulkoisten ja sisäisten uhkien vuoksi (Flowerday & Tuyikeze, 2016).

Tietoturvapolitiikan laatiminen on monitahoinen ja ratkaisevan tärkeä tehtävä, jonka tulee yhdistää tekniset ja turvallisuuteen liittyvät yritystoimenpiteet tietojärjestelmissä, samalla yhdistäen kyseisten järjestelmien toiminnallisuuden suojaamista koskevat vaatimukset. Tehokkaan tietoturvapolitiikan muotoilu voi olla erittäin vaativaa ja monimutkaista toimintaa, vaikka ohjeita kyseisen politiikan laatimiseen on laajasti saatavilla: esimerkiksi tietoturvastandardit (Karyda ym., 2004).

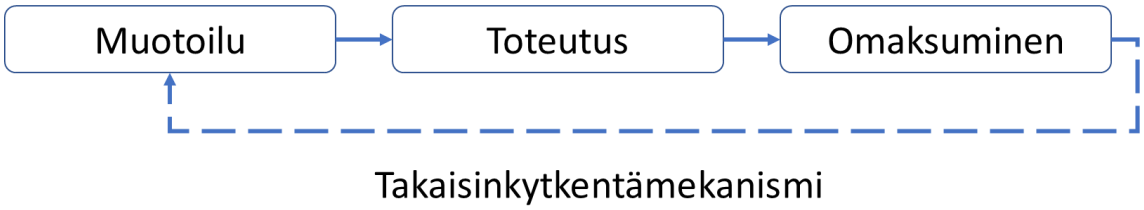
Kuten edellä mainittiin, tietoturvastandardit tarjoavat yrityksille erilaisia ohjeita tietoturvapolitiikan laatimiseen. Ensimmäiset viitekohdat, kun ryhdytään keräämään tietoa tietoturvapolitiikasta ja samalla yrityksen tietoturvapolitiikkaa aloitetaan kehittämään, ovatkin usein kansainväliset tietoturvastandardit. Kansainväliset tietoturvastandardit tunnustavatkin, että tietoturvapolitiikka on tärkeä aihe, kun käsitellään yrityksen tietoturvaa ja sen hallintaa (Höne & Eloff, 2002).

Vaikka standardit tarjoavat erilaisia ohjeita tietoturvapolitiikan laatimiseen, tulee muistaa, että turvallisuustavoitteet voivat poiketa toisistaan eri yritysten välillä, joten ei ole olemassa yksittäistä standardia tai politiikkaa, joka sopii kaikkiin yrityksiin. Tietoturvapolitiikan käyttöönotto on prosessi, joka koostuu muotoilusta (engl. formulation), toteutuksesta (engl. implementation) ja omaksumisesta (engl. adoption), kuten Kuviossa 2 on esitetty.

Tietoturvapolitiikan muotoilu tehdään politiikan suunnitteluvaiheessa, useimmissa tapauksissa osana laajempaa turvallisuussuunnitelmaa, jonka tavoitteena on tarjota riittävä suoja tietojärjestelmille ja tietovaroille erilaisten turvatoimenpiteiden ja -käytäntöjen avulla. Toteutus on prosessi, jonka aikana koottu politiikka käännetään ohjeiksi, menettelyiksi ja tehtävälistoiksi, jotka pannaan käytäntöön yrityksen työntekijöiden toimesta. Tietoturvapolitiikan omaksuminen tarkoittaa yrityksen työntekijöiden toimia, joiden avulla heidän pitäisi edellyttää politiikan onnistunutta toteutusta. Työntekijät siis muokkaavat toimintaansa sekä käyttäytymistään huomioiden tietoturvapolitiikassa olevat ohjeet. Yleensä työntekijät, jotka ottavat vastuun tietoturvapolitiikan täytäntöönpanosta, kuuluvat yrityksen informaatioteknologian osastolle. Kun uusi tietoturvapolitiikka on otettu käyttöön, se tulee tarkastaa ja arvioida säännöllisesti esimerkiksi erilaisten palautteiden tai haastatteluiden avulla (Karyda ym., 2004).

Politiikan tarkastamisella ja arvioinnilla on tärkeä osa politiikan omaksumisen edistämistä. Esimerkiksi Niemimaa ja Niemimaa (2017) huomasivat tutkimuksessaan, että uuden tietoturvapolitiikan käyttöönottaminen puutteellisilla ja epäselvillä ohjeilla sekä vähäisellä informaatiolla vaikutti merkittävästi työntekijöiden suhtautumiseen liittyen uuden tietoturvapolitiikan omaksumiseen. Epäonnistuneen käyttöönoton jälkeen työntekijöitä kuitenkin haastateltiin ja heiltä pyydettiin neuvoja, miten uuden politiikan käyttöönottoa voitaisiin yritystasolla parantaa. Tämän jälkeen politiikkaa muotoiltiin uudestaan, jonka jälkeen sitä alettiin myös toteuttaa uudestaan. Tämä johti siihen, että työntekijät alkoivat

vähitellen omaksua uutta tietoturvapolitiikkaa onnistuneesti (Niemimaa & Niemimaa, 2017).



KUVIO 2 Tietoturvapolitiikan käyttöönottoprosessi (mukaillen Karyda ym., 2004)

2.3 Tietoturvan hallintajärjestelmä (ISMS)

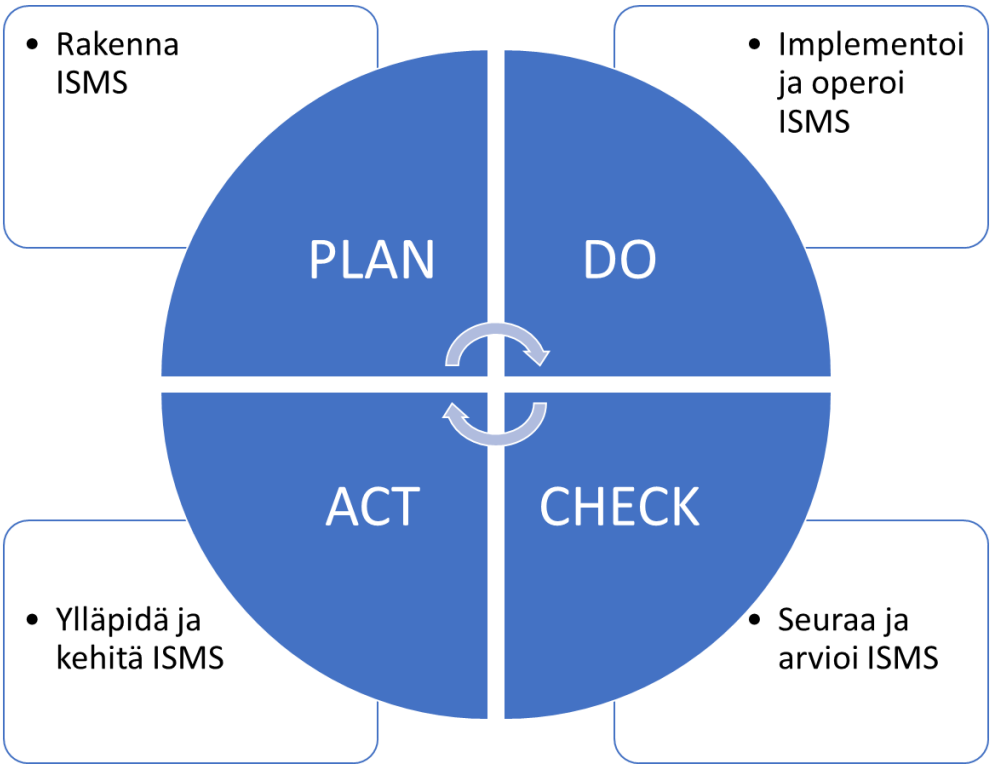
Tietoturvan hallintajärjestelmä (engl. Information Security Management System, ISMS) on tärkeä elementti, kun käsitellään ISO 27000 -standardiperhettä sekä yrityksen kykyä hallita sen tietoturvallisuutta (Nowak, 2015). Yrityksen tietoturva saavutetaan ottamalla käyttöön sopiva hallintajärjestelmä, joka sisältää käytännöt, säännöt, prosessit, menettelyt, organisaatiorakenteet sekä ohjelmisto- ja laitteistotoiminnot. Täyttääkseen erityiset turvallisuus- ja liiketoimintatavoitteensa yrityksen tulee tarvittaessa määrittää, toteuttaa, seurata, tarkistaa ja parantaa näitä valvontatoimia.

Standardissa ISO 27001 määritellyn kaltainen tietoturvan hallintajärjestelmä ottaa kokonaisvaltaisen sekä koordinoidun näkemyksen yrityksen tietoturvariskeistä voidakseen määrittää ja toteuttaa kattavan tietoturvan valvontajärjestelmän yhtenäisen hallintajärjestelmän puitteissa. Sopiva, riittävä ja tehokas tietoturvan hallintajärjestelmä takaa yrityksen johdolle ja muille asianosaisille sen, että heidän tietonsa ja muu siihen liittyvä omaisuus on turvassa ja suojattu erilaisilta uhkilta ja haitoilta, jolloin yritys voi saavuttaa asetetut liiketoiminnalliset tavoitteet (ISO, 2022b).

Tietoturvan hallintajärjestelmä on määritelty ISO 27000 -standardisarjassa osaksi yrityksen yleistä hallintajärjestelmää, joka perustuu liiketoimintariskiin perustuvaan lähestymistapaan ja jonka tarkoituksena on luoda, toteuttaa, käyttää, valvoa, tarkistaa, ylläpitää ja parantaa yrityksen tietoturvaa. Kyseinen järjestelmä sisältää yritysrakenteen, politiikat, suunnittelutoiminnot, vastuut, menettelyt, prosessit ja resurssit. Kyseessä on siis jäsennelty ja johdonmukainen tietoturvan johtamistapa, joka on suunniteltu varmistamaan tietoturvapolitiikan kolmen keskeisen osatekijän tehokasta vuorovaikutusta. Kyseiset kolme osatekijää ovat prosessi, teknologia ja käyttäjän käyttäytyminen (engl. user behaviour). Tietoturvan hallintajärjestelmä tulee kuitenkin suunnitella yksilökohtaisesti vastaamaan kunkin yrityksen omia tarpeita (Calder & Gerrard, 2013).

ISO 27001 -standardin kohdassa 4.1 todetaankin, että ”yrityksen on itse määriteltävä ulkoiset ja sisäiset asiat, jotka ovat merkityksellisiä sen tarkoituksen kannalta ja jotka vaikuttavat sen kykyyn saavuttaa tietoturvan

hallintajärjestelmänsä aiottu tulos” (ISO, 2022b). Merkittävä riski epäonnistuneeseen tietoturvan hallintajärjestelmään ovat yrityksen sisällä olevat ihmiset, jotka jättävät huomioimatta tai ohittavat kyseisen järjestelmän ohjaukset. Yrityksen ylimmän johdon on allekirjoitettava tietoturvan hallintajärjestelmän dokumentaatio sekä siihen liittyvä yrityksen tietoturvapolitiikka ja asettaa se tarvittaessa kaikkien sitä tarvitsevien saataville (Calder & Gerrard, 2013). Calder ja Gerrard (2013) toteavatkin, että tietoturvan hallintajärjestelmän suunnittelu ja perustaminen voi olla vaikeaa ilman yrityksen johdon tarjoamaa riittävää tukea ja onnistunutta ohjausta.



KUVIO 3 Tietoturvan hallintajärjestelmän toteuttaminen PDCA-mallin mukaisesti (mukaillen Susanto ym., 2011)

Tietoturvan hallintajärjestelmän idea ei perustu pelkästään järjestelmän toteuttamiseen, vaan välittömään seurantaan, järjestelmän ylläpitoon ja parantamiseen. Kuviossa 2 on esitetty tietoturvan hallintajärjestelmän toteutus standardin ISO 27001 mukaisesti PDCA-mallin avulla. Tässä jatkuvassa prosessissa keskeisessä asemassa ovat kyseisen hallintajärjestelmän suunnittelu, toiminta, tarkastaminen ja toteuttaminen. Suunnitteluvaiheeseen kuuluu tarvittavien tietoturvakäytäntöjen ja -kontrollien strategiointi. Tämä vaihe on kartoituksen kannalta ratkaiseva, koska se kartoittaa alustavan näkemyksen yrityksen halutuista tietoturvatasoista. Toimintavaihe sisältää kaikki tekniset toteutukset, jotka vaaditaan toimivan tietoturvan hallintajärjestelmän toteutukseen. Nämä edellä mainitut tekniset toteutukset suunnitellaan suunnitteluvaiheessa. Tarkastusvaihe sisältää tarvittavat tekniset arvioinnit, joiden avulla varmistetaan tietoturvan hallintajärjestelmän pitkän aikavälin

toimivuus sekä yrityksen sisällä tapahtuvat auditointimenettelyt jatkuvan turvatason varmistamiseksi. Toimintavaiheessa säilytetään laadunvarmistustason turvallisuustaso, joka perustuu tarkastusvaiheessa saatuun palautteeseen. Tietoturvan hallintajärjestelmään voidaan lisätä uusia päivityksiä tai toteutuksia uusien havaintojen, uhka- ja riskinarviointien perusteella (Qusef ym., 2018).

Edellä mainituilla keinoilla voidaan varmistaa, että käytetty tietoturvan hallintajärjestelmä suojaa tehokkaasti sekä jatkuvasti yrityksen tietovaroja. Tämän takia on tärkeää tunnistaa kyseiset tietovarat ja niiden turvallisuusvaatimukset, niihin liittyvien riskien arviointi ja hallinta, jotta voidaan parantaa kyseisen järjestelmän ohjausta yrityksen liiketoiminnan tarpeiden ja tietoturvan mukaisesti. Tämä prosessi on suoritettava ja toistettava yhä uudelleen ja uudelleen tehokkuuden varmistamiseksi tietoturvan hallintajärjestelmässä.

Tietoturvan hallintajärjestelmä koostuu siis käytännöistä, menettelyistä, ohjeista ja niihin liittyvistä resursseista sekä toiminnoista, joita yritys ja sen sisällä työskentelevät ihmiset hallinnoivat yhdessä sen tietovarojen suojelemiseksi. Tietoturvan hallintajärjestelmä on systemaattinen lähestymistapa perustaa, toteuttaa, käyttää, seurata, arvioida, ylläpitää ja parantaa yrityksen tietoturvaa saavuttaakseen liiketoiminnalle asetettuja tavoitteita. Se perustuu riskinarviointiin ja yrityksen riskien hyväksymistasoihin (Nowak, 2015).

Yrityksen riskienhallintasuunnitelma voidaan laatia, kun riskit on tunnistettu, analysoitu ja arvioitu. Riskinarviointiprosessi tulee suunnitella toimimaan yrityksen yleisen riskinkäsittelykehyksen puitteissa ja sen tulee tässä tapauksessa noudattaa ISO 27001 -standardin erityisvaatimuksia liittyen tietoturvan hallintajärjestelmään (Calder & Gerrard, 2013).

Riskienhallinnan lisäksi myös suojausvaatimusten analysointi ja asianmukaisten valvontatoimien soveltaminen tietojen suojaamiseksi edistää tietoturvan hallintajärjestelmän onnistunutta toteutusta (Nowak, 2015). Calderin ja Gerrardin (2013) mukaan tietoturvan hallintajärjestelmän käyttöönotto sisältää viisi erilaista tehtävää:

- Toteuta riskienhallintasuunnitelma ja sovellettavuusilmoituksessa yksilöidyt kontrollit.
- Määrittele, miten kaikkien valvontatoimien tehokkuutta mitataan ja arvioidaan.
- Toteuta koulutus- ja tiedotusohjelmia, jotka liittyvät ISO 27001 -standardin ohjeeseen A.7.2.2 – tietoturvatietoisuus, koulutus ja harjoittelu
- Hallitse tietoturvan hallintajärjestelmää. Kaikki toisiinsa kytkeytyvät ohjaukset ja prosessit on pidettävä toiminnassa ja uudet uhat tunnistettava, arvioitava ja tarvittaessa neutraloitava. Ihmisiä tulee rekrytoida ja kouluttaa, heidän suoriutumistaan valvoa ja heidän taitojaan kehittää liiketoiminnan muuttuvien tarpeiden mukaisesti.
- Toteuta tapaturmien havaitsemis- ja reagointimenettely, joka liittyy ISO 27001 -standardin liitteen A lausekkeeseen 16, tietoturvan hallinta.

Edellä mainitut tietoturvan hallintajärjestelmän käyttöönoton tehtävät ovat merkittävässä asemassa, jotta tietoturvan hallintajärjestelmää voidaan käyttää tehokkaasti. Mirtsch ym. (2021) toteavatkin, että tietoturvan hallintajärjestelmä on yksi tehokkaimmista riskienhallinnan työkaluista, jonka avulla voidaan torjua miljardeja yrityksiin vuosittain kohdistuvia erilaisia tietoturvahyökkäyksiä. Tämän vuoksi tärkeä osa kyseistä tietoturvan hallintaprosessia on tietoturvan hallintajärjestelmä, joka toimii yrityksessä keskeisessä roolissa ennakoiden kriittisiä tilanteita liittyen yrityksen tietoturvaan sekä kyseisten tilanteiden ratkaisemisessa (Hoffmann ym., 2016).

Ympäröivien muutosten lisääntyessä yritykset alkavat havaita enemmän erityyppisiä riskejä liittyen yritystoimintaansa ja tämä lisää enemmän huomion kiinnittämistä myös turvallisuuskysymykseen, mukaan lukien tietoturvaan. Riskeihin liittyvät asiat tietoturvan hallintajärjestelmässä ovat tärkeä osa yritysten strategista johtamista ja monissa tapauksissa ne ovat elintärkeitä liiketoiminnan järkeistämisen ja toiminnan jatkumisen kannalta (Hoffmann, 2016).

Tietoturvan hallintajärjestelmän suunnitteluvaiheessa määritellään vaatimukset tietojen ja tietojärjestelmien suojaamiseksi, tunnistetaan ja arvioidaan riskit sekä kehitetään sopivat menettelyt ja toimenpiteet riskien vähentämiseksi. Kyseiset menettelytavat ja toimenpiteet toteutetaan suunniteltujen toteutuksien ja operaatioiden aikana. Toiminnan jatkuvalla seurannalla syntyneitä raportteja käytetään hyväksi erilaisten parannusten tekemiseen ja tietoturvan hallintajärjestelmän kehittämiseen edelleen (Disterer, 2013).

Beckers ym. (2013) toteavat kuitenkin artikkelissaan, että tietoturvan hallintajärjestelmän kokoaminen voi olla vaikeaa, sillä kyseisen järjestelmän kokoamiseen kuuluu useita vaikeita ja erilaisia tehtäviä. Näitä ovat esimerkiksi yrityksen arvokkaan omaisuuden (engl. asset) tunnistaminen, uhkien ja riskien analysointi sekä erilaiset turvallisuusperustelut. Tällaiset vaatimukset voivat aiheuttaa järjestelmästä huolehtiville tietoturvainsinööreille ja muille työntekijöille monialaisia haasteita.

Nowakin (2015) mukaan tietoturvan hallintajärjestelmän onnistunutta toteuttamista lisäävät kuitenkin muun muassa kattava lähestymistapa vahvistamaan tietoturvan hallintaa, tietoturvan jatkuva uudelleenarviointi ja tarvittavien muutosten tekeminen, tietoturvavastuun osoittaminen sekä yrityksen johdon sitoutuminen liittyen tietoturvaan ja tietoturvallisuuden hallintaan.

3 ISO 27000 -TIETOTURVASTANDARDISARJA

ISO (International Organisation for Standardization) on maailmanlaajuinen kansallisten standardointielinten, eli ISO-jäsenjärjestöjen liitto, jossa myös ISO 27000 -tietoturvastandardisarja on kehitetty (ISO, 2018). ISO 27000 -sarjan standardit syntyivät kehittämällä yksityiskohtaisia kuvauksia tuotteiden erityisistä ominaisuuksista tai asiantuntijoiden palveluista. Standardit edustavat yksimielisyyttä sellaisista ominaisuuksista laatua, turvallisuutta ja luotettavuutta, joiden pitäisi pysyä voimassa pitkään. Standardien kehittämisen tavoitteena on tukea varsinkin yrityksiä ja niiden tietoturvallisuuden hallintaa (Disterer, 2013).

ISO 27000 -standardisarja on tarjonnut opastusta yrityksille jo vuodesta 1980 asti. Tietoturvastandardien idea alkoi juuri 1980-luvun lopulla, kun Royall Duch/Shell -konserni lahjoitti yleisölle sisäisen tietoturvapolitiikan käsikirjan, joka tunnettiin nimellä ”British Code of Practise”, eli BS 7799. Asiakirja kuitenkin vanhentui, sillä se keskittyi pelkästään keskustietokoneiden tietoturvakäsitteisiin, joista puuttuivat käsitteet ja viittaukset Internet-teknologioihin.

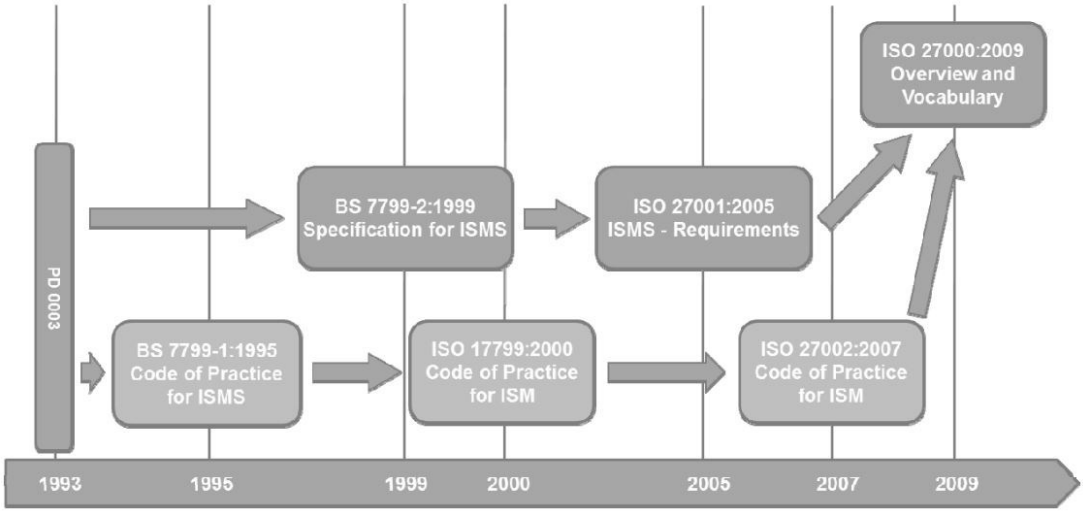
Vuonna 1998 kehitettiin uusi sertifiointistandardi osana alkuperäistä BS 7799:ää. Tämä osa tarkistettiin vuonna 1999 ja se nimettiin lopulta ISO 17799 joulukuussa vuonna 2000 kansainvälisten keskustelujen jälkeen. Vuonna 2005 ISO 17799 päivitettiin ja siihen lisättiin useita merkittäviä osia, mukaan lukien riskien ja tapausten hallintaa ja kunkin ohjausosan toteutusoppaat. Tämän jälkeen kyseinen standardi lopulta nimettiin uudelleen nimellä ISO 27000 (Nowak, 2015). Nykyään kyseinen standardisarja sisältää yli neljäkymmentä kansainvälistä standardia, mukaan lukien esimerkiksi tietoturvaohjaimet, pilviturvallisuus ja tapahtumien tutkinnan (Mirtsch ym., 2021).

Tässä tutkimuksessa käsiteltävien tietoturvastandardien ISO 27000, ISO 27001 ja ISO 27002 olemassaolo voidaan jäljittää aina vuoteen 1993 asti (Kuvio 4). Tällöin brittiläinen ammattiyhdistys, National Computing Center (NCC), julkaisi asiakirjan nimeltä "PD 0003 A Code of Practice for Information Security Management", josta nykypäivän standardit ISO 27000, ISO 27001 ja ISO 27002 ovat saaneet alkunsa. The British Standards Institute (BSI) hyväksyi tämän PD 0003 -nimisen asiakirjan ja julkaisi siitä pari vuotta myöhemmin uuden version, BS 7799-1, jonka jälkeen BSI toi sen kansalliseksi standardiksi vuonna 1995 ja sitä

päivitettiin myöhemmin lisää vuonna 2000, muun muassa uudella nimellä: ISO 17799 (Kuvio 4).

Vuonna 2007 ISO 17799 harmonisoitiin muiden standardien kanssa ja sen nimeksi tuli ISO 27002 (Kuvio 4). ISO 27002 (tällöin standardi toimi vielä nimellä BS 779) standardia täydentävä osa julkaistiin vuonna 1999 nimellä BS 7799-2 ja se antoi yrityksille mahdollisuuden sertifioida tietoturvallisuuden hallintaan liittyviä prosesseja. ISO harmonisoi myös tämän standardin muiden kanssa ja kehitti siitä uuden ISO 27001 -nimisen standardin lokakuussa 2005 (Kuvio 4). Siitä lähtien yritykset ovat voineen sertifioida prosessinsa tämän kansainvälisen standardin mukaisesti, joka käsittelee erityisesti yrityksen tietoturvan hallintajärjestelmää (Disterer, 2013).

Vuonna 2009 kehitettiin ISO 27000 -standardi (Kuvio 4), joka muodostaa yleiskatsauksen sekä yhteisen sanaston liittyen koko ISO 27000 -standardisarjaan, johon myös standardit ISO 27001 ja ISO 27002 kuuluvat. Kyseiseen sarjaan jouduttiin tekemään useita tarkistuksia ja muutoksia ajan kuluessa, sillä nopeasti muuttuvan tekniikan ja teknologian takia standardit vaativat erilaisia pienempiä sekä suurempia päivityksiä. Varsinkin vuonna 2013 ISO 27000 -sarjan standardeja tarkistettiin ja kehitettiin merkittävästi (Nowak, 2015).



KUVIO 4 Standardien ISO 27000, ISO 27001 ja ISO 27002 kehitys vuosien saatossa (Disterer, 2013).

Kuten muutkin informaatioteknologian standardit, ISO 27000 -standardisarja viittaa suoraan aikaisemmin tutkimuksessa mainittuun "Plan-Do-Check-Act" (PDCA) -sykliin (Disterer, 2013). Kyseisen PDCA-syklimallin kehitti 1950-luvulla Edwards Deming. Deming halusi, että yrityksen liiketoimintaprosesseja tulee käsitellä ikään kuin ne olisivat jatkuvassa palautesilmukassa, jotta yrityksen johtajat voivat tunnistaa ja muuttaa niitä prosessin osia, jotka kaipaavat parantamista tai kehittämistä. Prosessi tai prosessin parannus tulee ensin suunnitella, sitten toteuttaa ja mitata. Tämän jälkeen mittaustulokset tarkistetaan, jotta mahdolliset poikkeamat tai parannukset voidaan tunnistaa (Calder & Gerrard, 2013).

Kyseinen sykli korostaa tietoturvallisuuden hallinnassa tarvetta prosessilähtöisyyteen sekä toiminnan suunnittelun integrointiin ja suunnittelun mukaisen toteutuksen jatkuvaan tarkastukseen. Kyseinen sykli sisältää muun muassa turvallisuuspolitiikan määrittelyn ja täytäntöönpanon, roolien ja vastuiden määrittelyn, rekrytoinnin sekä tarvittavien henkilöstö- ja materiaaliresurssien valmistelun sekä riskienhallintapäätökset (Disterer, 2013).

Varsinkin vuonna 2005 määritelty versio ISO 27001 -standardista käytti voimakkaasti PDCA-syklimallia rakentamaan yrityksissä toimivia liiketoimintaprosesseja ja niiden hallintaa. Vuoden 2013 ISO 27001 -standardin versiossa painotettiin PDCA-syklimallin lisäksi kuitenkin myös enemmän mittaamista ja arviointia liittyen siihen, kuinka hyvin yrityksen tietoturvan hallintajärjestelmä toimii (Nowak, 2015).

ISO 27000 -standardisarjan mukaan tietoturvaan kuuluu kolme näkökohtaa, joita kyseinen sarja kutsuu dimensioiksi. Nämä kolme näkökohtaa ovat luottamuksellisuus, saatavuus ja eheys, jotka ovat merkittävässä roolissa, kun kyseessä on yrityksen tietoturva ja sen hallinta. Kyseinen standardisarja antaakin yleiskatsauksen tietoturvan hallintajärjestelmistä, määrittelee niihin liittyvät ehdot ja hahmottelee perustan kaikille tämän standardisarjan standardeille. Standardisarja esittelee ensin määritelmät ja termit, sitten hyödyt ja menettelyt ja tämän jälkeen kaikki ISO 27000 -standardit kuvauksineen. Esimerkiksi ISO 27000 -standardi on sanastostandardi, kun taas 27001 on arviointi- sekä prosessinhallintastandardi ja 27002 antaa erilaisia ohjeita tietoturvaohjaimien käyttöönotosta.

Toiset sarjan standardit ovat jakautuneita kahteen muuhun ryhmään: ohjestandardeihin sekä alakohtaisiin ohjestandardeihin. On olemassa myös erillinen ryhmä nimeltä "ohjauskohtaiset ohjestandardit", joita kutsutaan nimellä 2703x- ja 2704x -sarja. ISO 27000 -standardisarjan avulla yritykset voivat kehittää ja toteuttaa erilaisia puitteita tietovarojensa turvallisuuden hallintaan. Näitä tietovaroja ovat muun muassa taloudelliset tiedot, työntekijätiedot ja tietysti asiakkaiden tai kolmansien osapuolien uskomat tiedot (Nowak, 2015). Kyseisiä standardeja voidaan käyttää myös valmistelemaan riippumatonta arviointia edellä mainittujen tietovarojen suojaamiseen sovelletusta tietoturvan hallintajärjestelmästä (ISO, 2018).

3.1 ISO 27000

Kuviosta 4 käy ilmi, ISO 27000 -standardi julkaistiin vuonna 2009 ja sen päällimmäinen tarkoitus oli tarjota yleiskatsaus sekä yhteinen käsitteellinen perusta liittyen ISO 27000 -standardisarjaan. ISO 27000 -standardi antaa yleiskatsauksen tietoturvan hallintajärjestelmistä, määrittelee niihin liittyvät ehdot ja hahmottelee perustan kaikille tämän standardisarjan standardeille. Kyseisessä standardissa on määritelty ja eriytetty 47 erilaista turvallisuustermiä, jotka on esitelty "Käyttöehdot" -osiossa. Kyseinen standardi kehitettiin yhteistyössä IEC:in (International Electrotechnical Commission) kanssa, joka on johtava kansainvälinen

standardien liikkeeseenlaskija elektroniikkaan ja siihen liittyvien teknologioiden alalla (Disterer, 2013).

ISO 27000 viittaa kasvavaan ISO/IEC standardisarjaan, jonka yhteinen otsikko on "Information technology - Security – Information Security Management systems". Kyseinen standardi esittelee ensiksi määritelmät sekä termit ja tämän jälkeen hyödyt ja menettelyt liittyen tietoturvan hallintajärjestelmään. ISO 27000 -standardi tarjoaa yrityksille muun muassa yleiskatsauksen koko standardisarjaan sekä johdatuksen tietoturvan hallintajärjestelmiin (Nowak, 2015). ISO 27000 -standardin sisältö on seuraavanlainen:

1. Laajuus (engl. Scope)
2. Normatiiviset viittaukset (engl. Normative references)
3. Termit ja määritelmät (engl. Terms and definitions)
4. Tietoturvan hallintajärjestelmä (engl. Information security management system)
5. ISMS-standardiperhe (engl. ISMS family of standards)

Kyseisen asiakirjan tarkoituksena on siis kuvata tietoturvan hallintajärjestelmien perusteet sekä määritellä niihin liittyvät termit. Tämä standardi on julkisesti saatavilla (Nowak, 2015). Sanotaankin, että ISO 27000 -tietoturvastandardisarja on ensimmäinen askel kohti tietoturvaohjelmaa, joka suojaa yritystä kunnolla. ISO 27000 -standardisarjan yksi tärkeimmistä tarkoituksista onkin helpottaa yritystä kehittämään vankka tietoturvan hallintajärjestelmä.

3.2 ISO 27001

3.2.1 ISO 27001 kuvaus

ISO 27001 on kansainvälinen tietoturvan hallintajärjestelmien standardi. Tämä standardi yhdessä ISO 27002 kanssa voi auttaa yrityksiä ja organisaatioita saavuttamaan kaikki tietoon liittyvät säännösten noudattamista koskevat tavoitteensa ja auttaa niitä valmistautumaan uusiin sekä tuleviin säännöksiin ja asettumaan niihin. Kuviosta 2 käy ilmi, että ISO 27001 -standardi julkaistiin vuonna 2005 ja se määritettiin otsikon “Information technology—Security techniques—Information security management systems—Requirements” alle ja se korvasi samalla vanhan BS7799-2-standardin (Nowak, 2015).

ISO/IEC jäsenorganisaatioiden kanssa käydyn laajennetun kuulemisen jälkeen ISO 27001 -standardin seuraavaksi uusin versio julkaistiin lokakuussa 2013. Kyseinen versio siirsi painopisteen yritykseen ja sen prosesseja täydentävän tietoturvan hallintajärjestelmän luomiseen samalla vähentäen spesifikaatioiden ja hallintalaitteiden redundanssia (Calder & Gerrard, 2013). Viimeisin tarkastus tähän kyseiseen standardiin on tehty vuonna 2019 (Mirtsch ym., 2021).

ISO 27001 -standardi on siis yksi ISO 27000 -sarjan standardeista, joka on hyväksytty lukuisissa maissa ja lukuisissa eri toimialoilla. Standardissa kuvataan

vaatimukset, jotka tietoturvan hallintajärjestelmän on täytettävä sertifioinnin saavuttamiseksi. Kyseinen standardi on prosessin hallinta- ja arviointistandardi, joka tarjoaa tietoturvan hallintajärjestelmän eritelmät. ISO 27001 -standardin ydin on vaatimus prosessilähtöisen tietoturvan hallintajärjestelmän suunnitteluun, toteutukseen, käyttöön ja jatkuvaan seurantaan sekä parantamiseen. Lähestymistavan tulee olla linjassa tutkimuksessa aikaisemmin mainitun PDCA-syklin kanssa (Disterer, 2013).

ISO 27001 -standardi koostuu kahdesta osasta. Ensimmäisessä osassa eritellään vaatimukset tietoturvan hallintajärjestelmälle, jotta se voidaan ottaa käyttöön ja sitä voidaan ylläpitää. Toinen osa on nimeltään liite A, jossa määritellään valvontalaitteet ja erilaiset turvatarkastukset (Hamdi ym., 2019).

Liitteessä A on lueteltu ja nimenomaisesti määrätty yhteensä 39 valvontatavoitetta ja 114 turvallisuuden hallinnan toimenpidettä, jotka on edelleen jaettu neljääntoista eri kategoriaan (Disterer, 2013). ISO 27001 -standardin sisältö on seuraavanlainen:

1. Johdanto (engl. Introduction)
2. Laajuus (engl. Scope)
3. Normatiiviset viittaukset (engl. Normative references)
4. Termit ja määritelmät (engl. Terms and definitions)
5. Organisaation konteksti (engl. Context of the organisation)
6. Johtajuus (engl. Leadership)
7. Suunnittelu (engl. Planning)
8. Tuki (engl. Support)
9. Toiminta (engl. Operation)
10. Suorituskyvyn arviointi (engl. Performance evaluation)
11. Parantaminen (engl. Improvement)

    Liite A: Tietoturvallisuuden valvontalaitteet (engl. Annex A: Information security controls)

ISO 27001 sisältää siis normatiiviset vaatimukset laitteiston kehittämiselle ja tietoturvan hallintajärjestelmän toiminnalle. Kuten edellä mainittiin, kyseinen standardi sisältää vaatimukset myös joukolle valvontalaitteita, joilla voidaan hallita ja vähentää riskejä liittyen tietovaroihin, joita yritys pyrkii suojelemaan käyttämällä tietoturvan hallintajärjestelmää (Nowak, 2015).

Kyseisen standardin avulla yritykset voivat saada tietoturvan hallintajärjestelmän sertifioinnin kolmannen osapuolen organisaatiolta ja siten näyttää asiakkailleen todisteita tietoturvaansa liittyvistä hallintatoimista (Disterer, 2013).

ISO 27001 -standardi on toimittajaneutraali ja teknologiasta riippumaton. Se on tarkoitettu sovellettavaksi kaikkiin yrityksiin ja organisaatioihin tyypistä, koosta tai luonteesta riippumatta kaikilla aloilla kaikkialla maailmassa (Calder & Gerrard, 2013).

ISO 27001 -tietoturvastandardi onkin osoittanut viime vuosina nopeaa kasvua yritysmaailmassa (Mirtsch ym., 2021). Mirtsch ym. (2021) toteavat tutkimuksessaan, että varsinkin digitalisaation on odotettu vauhdittavan kyseisen standardin käyttöönottoa yritysmaailmassa. Koska yritykset varastoivat sekä

tallentavat tietovarojaan yhä enemmän tieto- ja viestintätekniikan avulla, yhä useammat ulkopuoliset toimijat vaativat yrityksiltä riittävän tietoturvan varmistamista. Tämä on johtanut siihen, että myös muiden yritysten liiketoiminta-alat informaatioteknologian lisäksi haluavat ja ovat ottaneet ISO 27001 -standardin käyttöön ja hankkineet yritykselleen sitä koskevan sertifioinnin (Mirtsch ym., 2021).

3.2.2 ISO 27001 -sertifikaatti ja sen hakuprosessi

ISO 27001 -standardin vaatimus on, että kunkin yrityksen tarpeet sekä tavoitteet, käytetyt organisaatioprosessit sekä yrityksen koko ja rakenne vaikuttavat suoraan tietoturvan hallintajärjestelmän suunnitteluun ja toteutukseen. ISO 27001 -yhteensopiva tietoturvan hallintajärjestelmä tarjoaakin systemaattisen lähestymistavan yrityksen tietojen sekä sen tietojärjestelmien saatavuuden, luottamuksellisuuden ja eheyden varmistamiseen.

Yritys, joka ottaa käyttöön tietoturvan hallintajärjestelmän ja haluaa arvioida sen ISO 27001 -standardin mukaisesti, on noudatettava kyseisen standardin eritelmiä. ISO 27001 -standardi vaatii erityisesti tietoturvan hallintajärjestelmän dokumentointia. Esimerkiksi kyseisen standardin liitteen A kohta 12.1.1 vaatii nimenomaisesti, että turvamenettelyt dokumentoidaan, ylläpidetään ja asetetaan kaikkien niitä tarvitsevien käyttäjien saataville (Calder & Gerrard, 2013).

Tietoturvan hallintajärjestelmän ja sen ISO 27001 -standardin mukaisuuden sekä vaatimusten tarkistamisen edellytyksenä on se, että yrityksen on läpäistävä sertifiointimenettely, jota ohjaa valtuutettu kolmannen osapuolen sertifiointiorganisaatio. Kyseisellä sertifiointiorganisaatiolla on valtuudet käsitellä yrityksen jättämä sertifikaattihakemus ja myöntää sertifikaatti onnistuneiden testauksien sekä auditointien jälkeen (Nowak, 2015).

Yrityksen ISO 27001 -sertifiointiprosessi alkaa, kun yritys tekee päätöksen hakea sertifikaattia. Tämä edellyttää yrityksen johdon sitoutumista ja vastuun määrittämistä liittyen kyseiseen hankkeeseen. Tämän jälkeen yrityksen tulee määritellä, mitkä yrityksen osat kuuluvat tietoturvan hallintajärjestelmän piiriin. Tyypillisesti määritellään esimerkiksi sijainti, voimavarat ja teknologia (Nowak, 2015).

Kuviossa 5 on kuvattu koko sertifiointiprosessi aikajanallisesti, missä prosessin vaiheet koostuvat riskin arvioinnista, tietoturvallisuuden suunnittelusta, turvallisuuden testaamisesta sekä arvioinnista ja sertifikaatin saavuttamisesta. Riskinarviointi on pakollinen prosessi liittyen riskinhallintaan ja se toimii myös perustana muille vaiheille. Riskinarvioinnin tarkoituksena on auttaa yritystä tunnistamaan esimerkiksi tietojärjestelmien heikkouksia, jotta voidaan tehdä päätöksiä liittyen turvavalvontaan ja korjaavien toimenpiteiden toteuttamiseen. Riskinarviointi edistää johdonmukaista lähestymistapaa riskien mittaamiseen ja sen avulla voidaan asettaa arvoja mahdollisille tappioille. Tämä vaihe sisältää itsessään esimerkiksi laajuuden määrittelyn, arvokkaan omaisuuden tunnistamisen, vaikutusten arvioinnin sekä uhkien, haavoittuvuuksien ja riskien tunnistamisen (Talib ym., 2012).

Suunnitteluvaiheen tavoitteena on suojata yrityksen tietoja riskeiltä ja mahdollisilta vahingoilta, kuten esimerkiksi luvaton pääsy tietoihin, tietojen menetys, tietojen luvaton käyttö tai muuttaminen. Kyseessä on tärkeä vaihe, sillä se auttaa käsittelemään riskejä, jotka on tunnistettu edellisessä vaiheessa. Tämä vaihe auttaa myös säätimien valinnassa, jotka käsittelevät turvallisuusriskejä. Suunnitteluvaihe on jatkuva prosessi, sillä turvallisuusasioita on käsiteltävä jatkuvasti (Talib ym., 2012).

Turvallisuuden testaamis- ja arviointivaihe suoritetaan turvavalvonnan validoimiseksi ja sen varmistamiseksi, että ne on toteutettu suunnitteluvaiheessa dokumentoidulla tavalla. Tämän vaiheen tavoitteena on varmistaa, että kaikki turvatarkastukset on toteutettu ja että ne toimivat oikein sekä odotetulla tavalla. Kyseinen vaihe suoritetaan myös silloin, kun lisätään uusia turvakontrolleja tai vanhoja on muutettu (Talib ym., 2012).

Näiden vaiheiden jälkeen itse sertifiointiprosessi voidaan aloittaa valitsemalla kolmannen osapuolen sertifiointiorganisaatio, jonka jälkeen alustavassa tutkimuksessa määritellään se, että missä määrin ISO 27001 -standardin ominaisuudet ovat yrityksessä jo olemassa ja mitä toimia tarvitsee lisätä onnistuneen sertifioinnin takaamiseksi.

KUVIO 5 ISO 27001 -sertifiointiprosessi (mukaillen Talib ym., 2012)

Sertifiointikoe koostuu kaikkien asiakirjojen tarkastuksesta sekä yksityiskohtaisista auditoinneista sekä tarkastuksista yrityksessä paikan päällä. Käynti sisältää muun muassa haastatteluja yrityksen vastuuhenkilöiden kanssa, jossa he selittävät ymmärryksensä turvallisuuspolitiikasta, kuvaavat prosesseja sekä esittävät yksityiskohtia ja ominaisuuksia liittyen yrityksen prosessidokumentaatioon (Disterer, 2013).

Tämän lisäksi sertifiointiorganisaatio vaatii yritykseltä pitkän luettelon tietoturvan hallintajärjestelmän dokumentoiduista tiedoista, mukaan lukien sen laajuus, tietoturvapolitiikka, riskien arviointi- ja käsittelyprosessit, toiminnan suunnittelu ja valvonta. Dokumentaatiossa voidaan vaatia myös esimerkiksi erilaisia käytäntöjä ja asiaankuuluvia lakeja, määräyksiä ja sopimusvelvoitteita sekä niihin liittyviä vaatimustenmukaisuusmenettelyjä (Nowak, 2015).

Tämän jälkeen sertifiointiorganisaatio laatii raportin, jossa selvitetään auditoinnin tulokset ja luetellaan parannustoimenpiteet, jotka on toteutettava ennen seuraavaa auditointia. Mikäli kokonaisuus on sertifiointiorganisaation mielestä positiivinen, yritys saa virallisen sertifikaatin, joka todistaa, että yrityksen tietoturvan hallintajärjestelmä on standardin ISO 27001 mukainen. Sertifikaatti on voimassa kolme vuotta, jonka jälkeen uudelleensertifiointia voidaan hakea hieman vähemmällä vaivalla, kuin edellistä.

ISO 27001 -standardin vaatimusten noudattamista sekä tietoturvan hallintajärjestelmän jatkuvaa parantamista varmistetaan ja seurataan vuosittaisten seurantatarkastuksien avulla. Kyseiset tarkastukset suorittaa kolmannen osapuolen sertifiointiorganisaatio. Mikäli seurantatarkastuksen aikana huomataan poikkeamia liittyen standardin vaatimuksiin, sertifiointiorganisaatio voi keskeyttää tai jopa peruuttaa sertifikaatin, kunnes poikkeamat on korjattu (Disterer, 2013). Monimutkaisesta sertifiointimenettelystä huolimatta ISO 27001 -standardin sertifikaatilla varusteltujen yritysten määrä kasvaa maailmanlaajuisesti koko ajan yhä enemmän. Kyseinen sertifikaatti tuo yrityksille väistämättä kurinalaisuutta ja muodollisuutta tietoturvan hallintajärjestelmän toteutusprosessiin, mikä tarkoittaa yrityksen tietoturvan merkittävää parantamista (Nowak, 2015).

3.3 ISO 27002

ISO 27001 -standardin kodifoituja vaatimuksia laajennetaan ja selitetään standardissa ISO 27002 ”Code of practice for information security controls” ohjeen muodossa. ISO 27002 -standardin ensimmäinen käsikirja julkaistiin vuonna 2000, jolloin se nimettiin nimellä ISO 17799. Vuonna 2007 kyseinen standardi tarkistettiin sekä yhdenmukaistettiin ja sen nimeksi muutettiin ISO 27002. Kyseisen standardin kehittämisen myötä yrityksille tarjottiin yhteisiä käytäntöjä ja menetelmiä, joiden avulla yritykset voisivat mukauttaa standardia liittyen yritysten erityisvaatimuksiin (Disterer, 2013).

ISO 27002 -standardi tarjoaa erilaisia ohjeita tietoturvaohjaimien käyttöönotosta ja antaa erityisiä täytäntöönpanoneuvoja sekä ohjausta tukevia parhaita käytäntöjä koskevia ohjeita liittyen standardoinnin määrittelyyn. Kyseinen standardi määrittelee myös ohjeita sekä yleisiä periaatteita yrityksen tietoturvahallinnan käynnistämiselle, toteuttamiselle, ylläpidolle ja parantamiselle (Nowak, 2015).

Tämä standardi on tarkoitettu kaiken tyyppisille ja kokoisille yrityksille. Sitä on tarkoitus käyttää viitteenä määritettäessä ja toteutettaessa valvontatoimenpiteitä tietoturvariskien käsittelyä varten ISO 27001 -standardiin perustuvassa tietoturvan hallintajärjestelmässä. Sitä voidaan myös käyttää ohjeasiakirjana yrityksille, jotka määrittävät ja toteuttavat yleisesti hyväksyttyä tietoturvan valvontaa. Lisäksi tämä kyseinen standardi on tarkoitettu käytettäväksi toimiala- ja yrityskohtaisten tietoturvallisuuden hallinnan ohjeiden kehittämisessä ottaen huomioon niiden erityiset tietoturvariskiympäristöt (ISO, 2022b). ISO 27002 -standardin sisältö on seuraavanlainen:

1. Johdanto (engl. Introduction)
2. Laajuus (engl. Scope)
3. Normatiiviset viittaukset (engl. Normative references)
4. Termit ja määritelmät (engl. Terms and definitions)
5. Tämän standardin rakenne (engl. Structure of this standard)

6. Tietoturvapolitiikka (engl. Information security policy)
7. Tietoturvan järjestäminen (engl. Organisation of information security)
8. Henkilöresurssien turvallisuus (engl. Human resource security)
9. Vahvuuksien hallinta (engl. Asset management)
10. Kulunvalvonta (engl. Access control)
11. Kryptografia (engl. Cryptography)
12. Fyysinen- ja ympäristön turvallisuus (engl. Physical and environmental security)
13. Toiminnan turvallisuus (engl. Operations security)
14. Viestinnän turvallisuus (engl. Communications security)
15. Järjestelmien hankinta, kehittäminen ja ylläpito (engl. System acquisition, development and maintenance)
16. Toimittajasuhteet (engl. Supplier relationships)
17. Tietoturvaloukkausten hallinta (engl. Information security incident management)
18. Liiketoiminnan jatkuvuuden hallinnan tietoturvanäkökohdat (engl. Information security aspects of business continuity management)
19. Noudattaminen (engl. Compliance)

ISO 27002 -standardin sisällön kohdat viidestä kahdeksaantoista, sisältävät ISO 27001 -standardin liitteessä A määritellyt hallintalaitteet. Kyseiset kohdat sisältävät myös 35 erilaista turvaluokkaa. Jokainen turvaluokka sisältää ohjaustavoitteen, joka ilmoittaa, mitä on saavutettava ja yhden tai useamman hallinnan, joita voidaan käyttää mainitun tavoitteen saavuttamiseksi (Calder & Gerrard, 2013).

ISO 27002 -standardin kontrollit perustuvat yrityksen tietovarastoon kohdistuvien mahdollisten riskien koko kirjon tunnistamiseen sekä torjumiseen. ISO 27002 tarjoaa myös merkittäviä käyttöönotto-ohjeita siitä, kuinka yksittäisiä ohjaimia tulisi lähestyä. Jokaisen yrityksen, joka ottaa käyttöön ISO 27001 -standardin mukaisen tietoturvan hallintajärjestelmän, on hankittava ja tutkittava kopiot sekä ISO 27001:sta että ISO 27002:sta.

ISO 27002 eroaa muista standardeista siten, että se on käytännesääntö, ei erittely. Siinä käytetään sanoja kuten "pitäisi" sekä "saattaa" ja kyseessä onkin neuvoa antava asiakirja, eikä suositus. Kyseistä standardia voidaan kuitenkin pitää lähtökohtana yrityskohtaisten ohjeiden kehittämiselle (Calder & Gerrard, 2013). Yrityksiä kehotetaankin tunnistamaan ja arvioimaan omat tietoturvariskinsä sekä valitsemaan ja soveltamaan sopivia tietoturvatoimia ei-hyväksyttävien riskien vähentämiseksi kyseisen standardin sekä muiden asiaankuuluvien standardien ja ohjeiden kanssa (ISO, 2022b).

4 TIEDONKERUUMENETELMÄ

Tässä tutkimuksessa tiedonkeruumenetelmän välineenä käytettiin sähköistä kyselylomaketta (Liite 1), joka toteutettiin Webropol-nimisen kyselylomaketyökalun avulla. Kysely toimitettiin yrityksille sähköisesti. Sähköisen kyselyn tarkoituksena ei ollut selvittää yrityksistä mitään kriittisiä tietoja, kuten auditointeja tai raportteja, liittyen heidän tietoturvallisuuteensa tai tietoturvallisuuden hallintaansa. Tarkoituksena oli kerätä riittävä ja laadukas aineisto sekä saada yleinen käsitys siitä, miten tutkimukseen osallistuneissa yrityksissä huolehditaan tietoturvallisuudesta ISO 27001 -sertifikaatin sekä standardien ISO 27000, ISO 27001 ja ISO 27002 avulla.

Vaikka tutkimuksessa selvitettiin yritysten tietoturvallisuuteen ja tietoturvallisuuden hallintaan liittyviä seikkoja yleisellä tasolla, tutkimuksen tekijä halusi pitää tutkimusta tehdessä yllä riittävää luotettavuutta sekä eettisyyttä, sillä kyseinen aihe voi olla varsinkin yritysten näkökulmasta erittäin arka sekä kriittinen. Tämän takia kyselyyn vastanneiden yritysten vastauksia ei voi yhdistää tässä tutkimuksessa spesifioidusti mihinkään yritykseen. Tutkimukseen osallistuneille yrityksille annettiin myös mahdollisuus pitää yrityksen nimi salassa ja kyseisistä yrityksistä tässä tutkimuksessa käytetään nimeä ”yritys X”.

4.1 Tiedonkeruumenetelmän valinta ja toteutus

Tähän tutkimukseen tiedonkeruumenetelmäksi valikoitui kyselytutkimus sen takia, että kvalitatiiviset kyselyt ovat joustava menetelmä kerätä aineistoa ja jolla on monia sovelluksia ja etuja sekä tutkijalle että osallistujille. Laadulliset kyselytutkimukset koostuvat joukosta kysymyksiä, jotka tutkija on laatinut ja jotka keskittyvät tiettyyn asiaan tai aiheeseen (Braun ym., 2021).

Myös tämän tutkimuksen kysely rakennettiin joukosta erilaisia kysymyksiä, jotka liittyivät keskeisesti tämän tutkimuksen aiheeseen sekä tutkimuskysymykseen ja joihin kyselyyn vastanneet yritykset saivat itse henkilökohtaisesti vastata

heille sopivien aikataulujen mukaisesti. Kyseisen tiedonkeruumenetelmä tähän tutkimukseen valittiin juuri sen joustavuuden ja sujuvuuden takia.

Braun ym. (2021) toteavat, että kvalitatiivisten kyselylomakkeiden avulla pystytään priorisoimaan laadulliset tutkimusarvot ja hyödyntämään datan rikas potentiaali. Braun ym. (2021) toteavat myös, että kvalitatiivisten online-kyselyjen keskeinen etu on avoimuus ja joustavuus käsitellä monenlaisia kiinnostavia tutkimuskysymyksiä, sillä menetelmä mahdollistaa pääsyn tietoihin, jotka vaihtelevat riippuen ihmisten kokemuksista, näkemyksistä tai käytännöistä. Kyseiset tekijät olivat merkittävässä asemassa valittaessa tämän tutkimuksen tiedonkeruumenetelmää. Myös se, että sähköisen kyselylomakkeen tekeminen alusta saakka itse oli joutuisaa, oli positiivinen tekijä valittaessa tiedonkeruumenetelmää.

Kuten edellä mainittiin, kysely tehtiin Webropol-työkalun avulla ja kysely toimitettiin sähköisesti kaikille neljälle eri yritykselle ja heidän edustajilleen. Kysely kohdistettiin tutkimukseen osallistuvien yritysten sellaisille edustajille, jotka eritoten vastaavat yrityksen tietoturvallisuudesta, tietoturvan hallintajärjestelmästä sekä tietoturvallisuuden yleisestä hallinnasta tai työskentelevät vahvasti kyseisten aiheiden parissa.

Kysely sisälsi yhteensä 12 erilaista kysymystä, joista kymmenessä keskityttiin yritysten tietoturvallisuuden hallintaan standardien ISO 27000, ISO 27001 ja ISO 27002 avulla. Näihin edellä mainittuihin kymmeneen kysymykseen sisältyi myös kysymykset liittyen yritysten hankkimaan ISO 27001 -sertifikaattiin ja sen hakuprosessiin. Jäljelle jääneissä kysymyksissä selvitettiin yritysten halua osallistua tutkimukseen nimettömänä sekä kyselyyn vastanneiden yrityksien edustajien työnimikkeitä. Kyselyyn vastaaminen kesti noin 5–10 minuuttia ja yrityksen edustajilla oli aikaa vastata kyselyyn yksi viikko. Kysely sisälsi alussa myös ohjeet siitä, kuinka kyselyyn vastataan ja miten kysely etenee.

4.2 Keskeiset haasteet ja riskit

Hirsjärven ym. (2009) mukaan kyselytutkimuksessa haasteita voivat olla esimerkiksi vastausvaihtoehtojen onnistuminen, aihealueen selkeys, varmistuminen osallistujien suhtautumisesta kyselyyn sekä osallistujien vastaamattomuus. Tässä kyselyssä tärkeää oli olla selvittämättä yrityksistä mitään kriittisiä tietoja liittyen heidän tietoturvallisuuteensa tai sen hallintaan. Tämä riski huomioitiin kyselyn suunnitteluvaiheessa, kun yritysten huoli liittyen vastausten mahdolliseen arkuuteen ilmeni. Kysymysten muodostaminen ja asettelu loi haasteita, sillä jokaista kysymystä muodostettaessa oli otettava huomioon osallistuvien yritysten vastauksien mahdollinen kriittisyys ja arkuus. Vastausten laatu, sisältö ja määrä ei kuitenkaan saanut kärsiä esimerkiksi tämän tutkimuksen tutkimuskysymyksen kannalta. Haasteiden ja riskien päihittämisessä tärkeintä on huolellinen kyselylomakkeen suunnittelu (Hirsjärvi ym., 2009, s. 202–203).

Kuten edellä mainittiin, osallistujien vastaamattomuus voi muodostua haasteeksi kyselytutkimuksessa. Tähän tutkimukseen osallistuneilla yrityksillä oli yksi viikko aikaa vastata kyselyyn. Ainoastaan yksi yritys neljästä vastasi

kyselyyn myöhässä, mutta myöhästyminen ei ollut merkittävää tämän tutkimuksen edistymisen kannalta.

4.3 Aineiston analyysi ja luotettavuus

Tässä tutkimuksessa on käytetty laadullista tutkimusmenetelmää ja aineistonkeruumenetelmänä toimi sähköinen kyselylomake. Tämän tutkimuksen aineisto koostuu neljälle yritykselle suunnatuista kyselylomakkeen avulla kerätystä datasta. Kyselylomake oli mahdollista täyttää internetissä ja osa kysymyksistä oli asetettu pakollisiksi. Kaikki tutkimukseen osallistuneet yritykset vastasivat jokaiseen kysymykseen, joten aineistoa oli mahdollista analysoida tasapuolisesti kaikkien yritysten näkökulmasta.

Tutkimuksessa kerättyä aineistoa on analysoitu oman pohdinnan sekä kirjallisuuden avulla. Kyselytutkimuksesta saatujen vastausten analysoinnissa käytettiin apuna teemoittelua. Vastaukset jaettiin analysoinnissa kolmeen eri teemaan: ISO 27000 -standardi, ISO 27002 -standardi ja ISO 27001 -sertifikaatti.

Kyselytutkimukseen vastanneita yrityksiä oli neljä kappaletta. Kvalitatiivisen tutkimuksen näkökulmasta otanta on pieni, eikä aineiston perusteella voi tehdä yleistäviä päätelmiä nykypäivän yritysten tietoturvallisuuden hallinnasta ISO 27000 -standardisarjan avulla. Kerätyn aineiston avulla voidaan kuitenkin tarjota yleislaatuinen katsaus tutkimukseen osallistuneiden yritysten tietoturvallisuuden hallinnasta kyseisen aiheen näkökulmasta. Pieni otanta ei myöskään sulje sitä vaihtoehtoa, etteikö tämän tutkimuksen aineiston ja sen analyysia voisi käyttää pohjana muiden saman aihepiirin tutkimusten aineistojen analyysissa.

Koska tutkimus käsittelee yrityksen tietoturvallisuutta ja sen hallintaa, kyselyyn vastaavien yritysten edustajien valinta oli olennaista, jotta kerätty aineisto on kerätty sellaisilta henkilöiltä, joilla on relevanttia tietoa kyseisestä aiheesta. Tällä tavoin pyrittiin varmistamaan kerätyn aineiston luotettavuus.

5 TUTKIMUSTULOKSET

Tutkimukseen osallistui neljä Suomessa toimivaa eri liiketoiminta-alan yritystä. Tutkimuksen kyselylomake toimitettiin sähköisesti kaikille osallistuville yrityksille ja siihen vastasi jokaisesta yrityksestä yksi yrityksen edustaja. Vastaukset yrityksiltä tähän kyselylomakkeeseen saatiin kerättyä yhdeksässä päivässä.

5.1 Vastaajien taustatiedot

Tutkimukseen osallistui neljä eri yritystä. Kyselyn alussa yhdessä kysymyksessä yrityksille annettiin mahdollisuus käyttää tässä tutkimuksessa yrityksestään nimeä muuttuja X, jotta kerättyä aineistoa sekä vastauksia ei voi spesifisti yhdistää mihinkään kyselyyn vastanneeseen yritykseen. Kolme neljästä yrityksestä antoi luvan kertoa tässä tutkimuksessa johdanto-osiossa yrityksensä nimen, mutta yksi yritys neljästä halusi pitää yrityksensä nimen tässä tutkimuksessa anonyymina.

Tutkimukseen vastasi neljä henkilöä neljästä eri yrityksestä. Kyselylomakkeen yhdessä kysymyksessä selvitettiin kyselyyn vastanneiden yritysten edustajien työnimikkeet, jolla he työskentelevät yrityksessä. Kysymyksen avulla selvitettiin, että kyselyyn vastasi neljästä yrityksestä kaksi tietoturvapäällikköä, yksi toimitusjohtaja ja yksi CISO (engl. chief information security officer).

5.2 Yritykset ja ISO 27000 -standardi

Tutkimuksessa haluttiin selvittää ISO 27000 -standardin käyttöä yrityksissä, liittyen yritysten tietoturvan hallintaan sekä sen ohjaamiseen. Kolme neljästä yrityksestä ilmoitti, että yrityksen tietoturvallisuuden hallinnassa käytetään standardia ISO 27000 jollain tasolla. Ainoastaan yksi neljästä yrityksestä ilmoitti, että ISO 27000 -standardia ei käytetä yrityksen tietoturvallisuuden hallinnassa jollain tasolla.

Yrityksiltä kysyttiin myös, että ohjaako ISO 27000 -standardi yrityksen tietoturvallisuuden hallintaa jollain tasolla. Kysymykseen vastaamiseen käytettiin Likert-asteikkoa, jossa asteikko asetettiin numeroiden 1-5 välille: 1 = Täysin eri mieltä, 2 = Eri mieltä, 3 = Ei samaa eikä eri mieltä, 4 = Samaa mieltä, 5 = Täysin samaa mieltä. Kolme neljästä yrityksestä ilmoitti olevansa samaa mieltä siitä, että ISO 27000 -standardi ohjaa jollain tasolla yrityksen tietoturvallisuuden hallintaa. Yksi neljästä yrityksestä ilmoitti olevansa täysin eri mieltä siitä, että ISO 27000 -standardi ohjaa jollain tasolla yrityksen tietoturvan hallintaa.

5.3 Yritykset ja ISO 27002 -standardi

Tutkimuksessa haluttiin selvittää myös standardin ISO 27002 käyttöä yrityksissä, liittyen heidän tietoturvansa hallintaan sekä tietoturvan hallinnan ohjaamiseen kyseisen standardin avulla. Yrityksiltä kysyttiin, että käytetäänkö yrityksen tietoturvan hallinnassa jollain tasolla standardia ISO 27002. Kolme neljästä yrityksestä ilmoitti, että standardia ISO 27002 käytetään jollain tasolla heidän tietoturvansa hallinnassa. Ainoastaan yksi yritys neljästä ilmoitti, ettei kyseistä standardia käytetä heidän yrityksen tietoturvan hallinnassa.

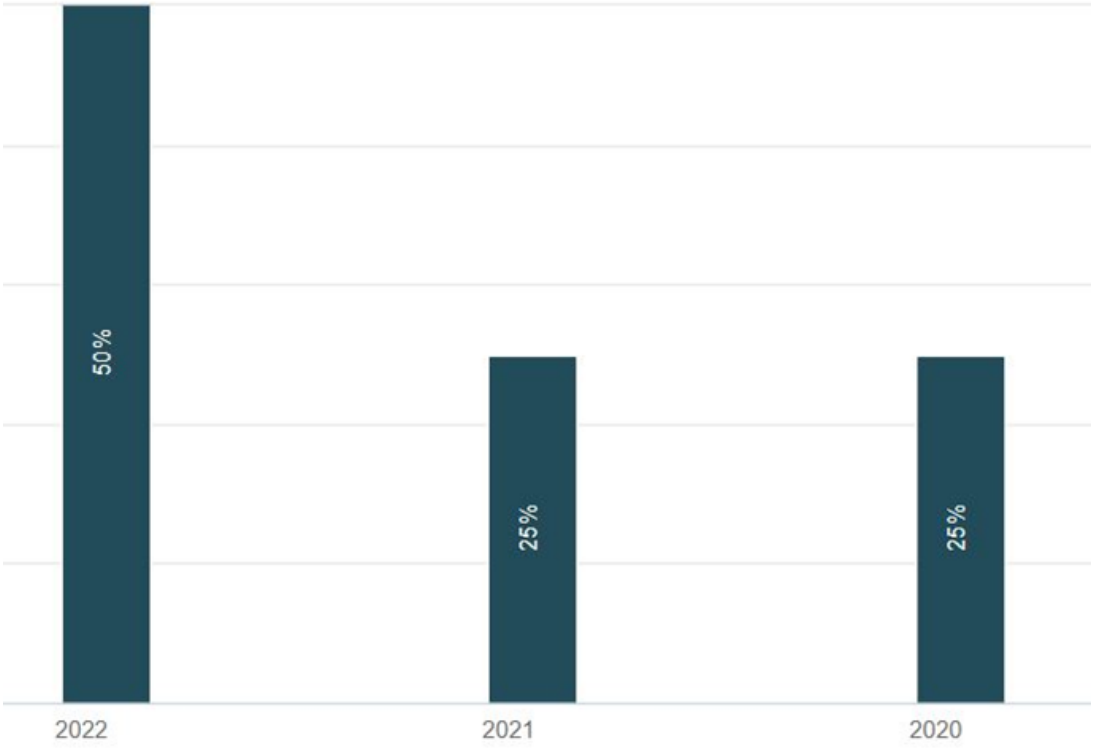
Yrityksiltä kysyttiin myös, että että ohjaako ISO 27002 -standardi yrityksen tietoturvan hallintaa jollain tasolla. Tähän kysymykseen vastaamiseen käytettiin myös Likert-asteikkoa, jossa asteikko asetettiin myös numeroiden 1-5 välille: 1 = Täysin eri mieltä, 2 = Eri mieltä, 3 = Ei samaa eikä eri mieltä, 4 = Samaa mieltä, 5 = Täysin samaa mieltä.

Yksi yritys neljästä ilmoitti olevansa täysin samaa mieltä siitä, että standardi ISO 27002 ohjaa yrityksen tietoturvan hallinta jollain tasolla. Kaksi yritystä neljästä ilmoitti olevansa samaa mieltä siitä, että standardi ISO 27002 ohjaa yrityksen tietoturvan hallinta jollain tasolla. Ainoastaan yksi yritys neljästä ilmoitti olevansa täysin eri mieltä siitä, että standardi ISO 27002 ohjaa yrityksen tietoturvan hallinta jollain tasolla.

5.4 Yritykset ja ISO 27001 -sertifikaatti

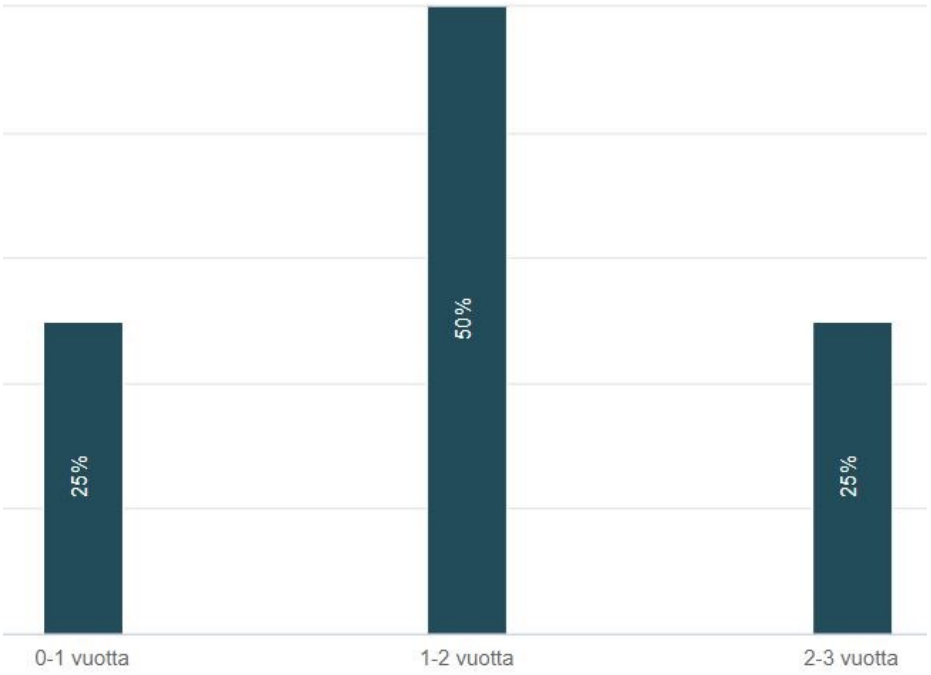
Kyselytutkimuksessa selvitettiin, minä vuonna tutkimukseen osallistuvat yritykset ovat saavuttaneet ISO 27001 -sertifikaatin (Taulukko 1). Vastausvaihtoehtoina olivat vuodet 2018, 2019, 2020, 2021 ja 2022. Kaksi neljästä yrityksestä ilmoitti saavuttaneensa ISO 27001 -sertifikaatin vuonna 2022. Yksi yritys neljästä ilmoitti saavuttaneensa kyseisen sertifikaatin vuonna 2021. Toinen yksi yritys neljästä ilmoitti saavuttaneensa kyseisen sertifikaatin vuonna 2020.

TAULUKKO 1 Yritysten ISO 27001 -sertifikaatin saavuttamisvuosi



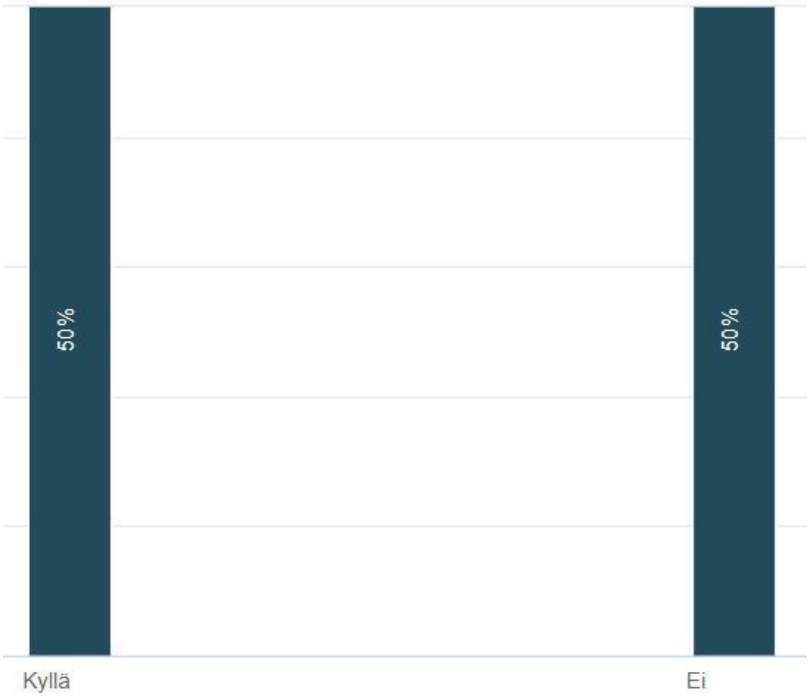
Kyselyn avulla yrityksiltä selvitettiin, kuinka kauan ISO 27001- sertifikaatin hakuprosessi kesti kokonaisuudessaan prosessin käynnistymisestä aina sertifikaatin saamiseen asti (Taulukko 2). Vastausvaihtoehdot olivat 0- vuotta, 1–2 vuotta, 2–3 vuotta, 3–4 vuotta ja 4–5 vuotta. Kaksi neljästä yrityksestä ilmoitti hakuprosessin kestäneen kokonaisuudessaan 1–2 vuotta. Yksi neljästä yrityksestä ilmoitti hakuprosessin kestäneen 0–1 vuotta ja toinen yksi neljästä yrityksestä ilmoitti hakuprosessin kestäneen 2–3 vuotta.

TAULUKKO 2 Yritysten ISO 27001 -sertifikaatin hakuprosessin kesto



Yrityksiltä haluttiin myös selvittää, koettiinko ISO 27001 -sertifikaattiin liittyvä hakuprosessi haastavaksi (Taulukko 3). Kaksi neljästä yrityksestä koki kyseisen sertifikaatin hakuprosessin haastavaksi, mutta toiset kaksi yritystä neljästä eivät kokeneet hakuprosessia haastavaksi.

TAULUKKO 3 Yritysten kokemus ISO 27001 -sertifikaatin hakuprosessin haastavuudesta



Yrityksiltä haluttiin myös selvittää tärkeimpiä tekijöitä, mitkä vaikuttivat heidän mielestänsä merkittävimmin päätökseen hakea yritykselle ISO 27001 -sertifikaattia (Taulukko 4). Kysymyksen vastausvaihtoehdoiksi annettiin valmiita ennalta mietittyjä vaihtoehtoja, joista yritykset saivat valita heidän sertifikaatin hakupäätökseensä vaikuttaneet merkittävimmät tekijät. Yrityksille annettiin myös yhtenä vaihtoehtona mahdollisuus valita kaikki kysymyksessä olleet vastausvaihtoehdot.

Kolme neljästä yrityksestä piti tärkeänä tekijänä tietoturvaosaamisen jatkuvuuden sekä -käytäntöjen saavuttamista sekä ylläpitoa. Ainoastaan yksi yritys neljästä piti tärkeänä yrityksen toiminnan läpinäkyvyyden lisäämistä. Kolme neljästä yrityksestä ilmoitti tärkeäksi tekijäksi sen, että sertifikaatti on osoitus siitä, että yrityksellä on käytössään alan parhaat ja viimeisimmät toimintatavat. Kolme neljästä yrityksestä piti tärkeänä myös sitä, että sertifikaatin avulla yritys pystyy vahvistamaan asiakkaiden, yrityskumppanien sekä viranomaisten mielipidettä liittyen yrityksen tietoturvallisuuden panostamiseen. Kolme yritystä neljästä ilmoitti tärkeäksi tekijäksi myös tietoturvallisuuden kehittämisen. Yksi yritys neljästä ilmoitti tärkeäksi tekijäksi halun toimia yleisten standardien mukaisesti sekä halun toimia tietoturvallisuuden johtamisen mahdollistajana. Kyselyyn vastanneista yrityksistä ainoastaan yksi piti tärkeänä tekijänä yrityksen työntekijöiden tietoturvallisuustietoisuuden kasvattamista.

Kaksi yritystä neljästä ilmoitti pitävänsä halua kehittää tietoturvan hallintajärjestelmää sellaiseen tilaan, jota nykypäivän yritykseltä vaaditaan, tärkeänä tekijänä. Yksi yritys neljästä piti tärkeänä tekijänä sertifikaatin hakemiselle tunnistettujen turvallisuusriskien hallitsemista. Kaksi neljästä yrityksestä piti tärkeänä tekijänä myös sitä, että kilpaileva saman liiketoiminta-alan yritys oli saavuttanut kyseisen sertifikaatin ennen heitä. Yrityksille annettiin mahdollisuus myös vastata itse, mitkä tekijät olivat tärkeitä, kun sertifikaattia päätettiin hakea. Yksi yritys neljästä vastasi ainoastaan tähän kysymykseen seuraavasti: “Halu osoittaa, että hallinnollisen puolen ollessa kunnossa, myös tekninen tietoturva on hallittua”.

TAULUKKO 4 Yritysten kokemat tärkeimmät tekijät, jotka vaikuttivat ISO 27001 -sertifikaatin hakupäätökseen

	n	Prosentti
Tietoturvaosaamisen jatkuvuuden sekä -käytäntöjen saavuttaminen sekä ylläpito	2	50,0%
Yrityksen toiminnan läpinäkyvyyden lisääminen	0	0,0%
Osoitus siitä, että yrityksellä on käytössä alan parhaat ja viimeisimmät toimintatavat	2	50,0%
Asiakkaiden, yrityskumppanien sekä viranomaisten mielipiteen vahvistaminen liittyen yrityksen tietoturvallisuuden panostamiseen	2	50,0%
Tietoturvallisuuden kehittäminen	2	50,0%
Halu toimia yleisten standardien mukaisesti	0	0,0%
Yrityksen halu toimia tietoturvallisuden johtamisen mahdollistajana	0	0,0%
Yrityksen työntekjöiden tietoturvallisuustietoisuuden kasvattaminen	0	0,0%
Halu kehittää tietoturvan hallintajärjestelmä sellaiseen tilaan, jota nykypäivän yritykseltä vaaditaan	1	25,0%
Tunnistettujen turvallisuusriskien hallitseminen	0	0,0%
Saman liiketoiminta-alan kilpaileva yritys saavutti sertifikaatin	1	25,0%
Kaikki ylläolevat vaihtoehdot	1	25,0%
Muita tekijöitä, mitä?	1	25,0%

Viimeisenä kysymyksenä, joka liittyi ISO 27001 -sertifikaattiin, yrityksiltä kysyttiin, että onko sertifikaatin saamisesta koettu olevan hyötyä yrityksen toiminnassa. Kaikki tutkimukseen osallistuneet neljä yritystä vastasivat, että sertifikaatista on ollut hyötyä yrityksen toiminnalle sen saavuttamisen jälkeen.

6 POHDINTA JA JOHTOPÄÄTÖKSET

6.1 Tutkimuksen analyysiä

Tutkimustulokset osoittavat, että yritysten antamat vastaukset tukevat tutkimuksessa käytettyä kirjallisuutta, mutta tuloksissa on myös havaittavissa mielenkiintoisia yksityiskohtia. Kuten tutkimustuloksissa mainittiin, tähän tutkimukseen liittyvään kyselylomakkeeseen vastasi kaksi tietoturvapäällikköä, yksi CISO ja yksi toimitusjohtaja. Yrityksille annettiin mahdollisuus valita yrityksistään henkilö, joka vastaa kyselyyn.

Tutkimuksen aiheen takia on loogista, että kyselyyn vastasi yritysten tietoturvapäälliköt sekä CISO, sillä kyseiset henkilöt ovat varmasti tekemisissä yrityksensä tietoturvallisuuden ja tietoturvallisuuden hallinnan parissa päivittäin. Onkin mielenkiintoista, että kyselyyn vastasi myös yksi toimitusjohtaja. Helposti voisi ajatella, että yrityksen toimitusjohtaja ei välttämättä ole täysin perillä yrityksensä tietoturvallisuudesta sekä sen hallinnasta ainakaan teknisellä tasolla. Tämän tutkimuksen kyselylomakkeeseen vastaaminen kuitenkin osoittaa sen, että kyseisellä toimitusjohtajalla on tietoa liittyen yrityksensä tietoturvallisuuteen sekä sen hallintaan ja halu vastata kyselyyn esimerkiksi yrityksen tietoturvapäällikön puolesta on perusteltua.

Kuten tässä tutkimuksessa on aikaisemmin mainittu, myös yrityksen johdolla on merkittävä rooli, kun kyseessä on yrityksen tietoturvallisuus ja sen hallinta. Esimerkiksi tietoturvapolitiikan käyttöönotto sekä ISO 27001 -sertifikaattiin liittyvä prosessi lähtee aina yrityksen johdon sitoutumisesta sekä vastuun määrittämisestä liittyen kyseisiin hankkeisiin. Nowakin (2015) mukaan yrityksen johdon sitoutuminen tietoturvaan ja tietoturvallisuuden hallintaan lisää tietoturvan hallintajärjestelmän onnistunutta toteuttamista, joka on keskeinen osa sertifikaattia. Tämän takia myös johdolla on oltava runsaasti tietoa oman yrityksensä tietoturvallisuudestaan sekä sen hallinnasta.

Tutkimustulokset antoivat myös informaatiota liittyen yritysten ISO 27001 -sertifikaatin hakuprosessiin. Kuten tässä tutkimuksessa todettiin aikaisemmin, ISO 27001 -standardiin liittyvä sertifiointiprosessi voi olla monimutkainen ja haastava, mutta kaksi neljästä tähän tutkimukseen osallistuneesta yrityksestä ilmoitti, ettei sertifikaatin hakuprosessia koettu heidän yrityksessään lainkaan haastavaksi.

Kyseiseen vastaukseen liittyviä tekijöitä voi olla useita. Esimerkiksi hyvä ennakointi ja perinpohjaiset valmistelut ennen hakuprosessin aloittamista voivat edesauttaa merkittävästi ajatusmallia siitä, että kyseinen prosessi ei ollut haastava. Edellä mainitut ennakointi sekä valmistelut ovat voineet kattaa yrityksen riskinarvioinnin ja -alttiuden sekä sen, että mitkä yrityksen osat kuuluvat tietoturvan hallintajärjestelmän piiriin. Nämä ovat merkittävimpiä vaatimuksia, joiden tulee olla kunnossa, jotta sertifiointiprosessi voidaan edes aloittaa. Myös prosessin aikana tehdyt kolmannen osapuolen auditoinnit sekä vaaditut dokumentoinnit ovat mitä ilmeisimmin sujuneet ongelmitta, mikä on edistänyt mielipidettä siitä, ettei prosessi ollut haastava.

Toiset kaksi yritystä neljästä kuitenkin ilmoittivat kokeneensa sertifikaatin hakuprosessin haastavaksi. Kyseiseen mielipiteeseen vaikuttavia tekijöitä voivat olla esimerkiksi hakuprosessin pitkä kesto kokonaisuudessaan sekä suuri ja täsmällinen työmäärä, jota vaaditaan koko prosessin ajan yrityksen johdolta sekä jokaiselta työntekijältä keskeytyksettä. Myös yrityksen koolla voi olla merkitystä hakuprosessin kokonaiskestossa. Mikäli yritys on suuri, on huomioitava paljon enemmän erilaisia tietoturvallisuuteen liittyviä käytäntöjä ja menettelytapoja sekä otettava myös huomioon työtehtävät, joihin liittyy paljon yrityksen työntekijöitä (Legalesign, 2021). Kyseisten yritysten mielipide prosessin haastavuudesta ei kuitenkaan tarkoita sitä, etteikö näissä yrityksissä olisi välttämättä myös valmistauduttu hyvin alkavaan hakuprosessiin sekä tehty ennakoivia toimenpiteitä.

Tähän tutkimukseen käytetyn kirjallisuuden perusteella hakuprosessin kesto kokonaisuudessaan on merkittävin tekijä, mikäli prosessi on koettu yrityksessä haastavaksi. Tutkimustuloksissa käy ilmi, että yhdellä yrityksellä neljästä sertifikaatin hakuprosessi kesti vain 0–1 vuotta, kahdella yrityksellä neljästä hakuprosessi aina käynnistymisestä sertifikaatin saamiseen saakka kesti 1–2 vuotta ja yhdellä yrityksellä neljästä sertifiointiprosessi ilmoitettiin kestäneen 2–3 vuotta.

IT Governance (2023) kirjoittaa blogikirjoituksessaan, että keskiarvollinen aika yrityksellä ISO 27001 -sertifikaatin saamiseen kestää noin 6–12 kuukautta. Tämän perusteella voidaan päätellä, että tähän tutkimukseen osallistuneista yrityksistä yksi pysyi keskiarvollisessa ajassa liittyen sertifikaatin hakuprosessiin. Kolmella yrityksellä neljästä hakuprosessi kesti pidempään. Hakuprosessiin käytetyllä kokonaisajalla ei kuitenkaan välttämättä ole suurta merkitystä yrityksille. Luultavasti tärkeintä on se, että kyseinen sertifikaatti saadaan hankittua, riippumatta siihen käytetystä ajasta.

ISO 27001 -sertifikaatilla varusteltujen yritysten määrä maailmalla kasvaa koko ajan ja kaikki neljä tähän tutkimukseen osallistunutta yritystä on saavuttanut kyseisen sertifikaatin viimeisen kolmen vuoden sisällä. Tämä kertoo siitä,

että kyseinen sertifikaatti on nostanut huomattavasti suosiotaan yritysten keskuudessa viime vuosina.

Esimerkiksi ISO teetti vuonna 2021 tutkimuksen, jonka tuloksista kävi ilmi, että ISO 27001 -sertifioitujen yritysten määrä kasvoi 19 % vuodesta 2020 (ISO, 2022b). On mahdollista, että yritykset maailmalla ovat huomanneet digitalisaation vauhdittavan kyseisen sertifikaatin positiivista käyttöönottoa sekä yritykset ovat esimerkiksi huomanneet sertifikaatin vaikuttavan myös positiivisesti yrityksen liiketoimintaan. Tätä ajatusta tukee myös se, että kyselyyn vastanneista yrityksistä kaikki neljä olivat sitä mieltä, että ISO 27001 -sertifikaatin saamisesta on ollut hyötyä yrityksen toiminnassa.

Kyselyyn vastanneiden yritysten mielipidettä tukee myös tutkimukseen käytetty kirjallisuus, sillä esimerkiksi ISO:n (ISO, 2022b) mukaan kyseisen sertifikaatin avulla yritykset voivat saavuttaa asianmukaisen, tehokkaan sekä pätevän tietoturvan hallintajärjestelmän, joka takaa sen, että yrityksillä on mahdollisuus saavuttaa niille asetetut liiketoiminnalliset tavoitteet. Mikäli yritys pystyy saavuttamaan sille ennalta asetettuja liiketoiminnallisia tavoitteita, yrityksen toiminta on onnistunutta. Sertifikaatin saaminen voi myös vaikuttaa yrityksen maineeseen myönteisesti, jolloin kyseinen sertifikaatti vaikuttaa myös toisella näkökulmalla positiivisesti yrityksen toimintaan.

Tutkimustulokset antoivat myös dataa liittyen tutkimukseen osallistuvien yritysten merkittävimmistä tekijöistä, jotka vaikuttivat ISO 27001 -sertifikaatin hakemiseen. Tärkeimmät tekijät yritysten mielestä olivat

- Tietoturvaosaamisen jatkuvuuden sekä -käytäntöjen saavuttaminen sekä ylläpito
- Osoitus siitä, että yrityksellä on käytössä alan parhaat ja viimeisimmät toimintatavat
- Asiakkaiden, yrityskumppanien sekä viranomaisten mielipiteen vahvistaminen liittyen yrityksen tietoturvallisuuden panostamiseen
- Tietoturvallisuuden kehittäminen

Kolme neljästä yrityksestä ilmoitti edellä mainitut tekijät tärkeimmiksi. Tästä voidaan päätellä, että yrityksille on tärkeää kehittää, saavuttaa sekä ylläpitää tietyn tasoista tietoturvallisuutta samalla hallinnoiden sitä käyttäen alan parhaimpia ja viimeisimpiä toimintatapoja. ISO 27001 -sertifikaatin avulla kyseiset asiat ovat mahdollista saavuttaa, sillä kyseisen sertifikaatin mukaan toteutettu tietoturvan hallintajärjestelmä auttaa luomaan yrityksille kokonaisvaltaisen ja koordinoidun näkökulman yrityksen tietoturvariskeistä samalla kattaen jäsennellyt sekä johdonmukaiset tietoturvan johtamis- ja toimintatavat.

Nämä osatekijät myös edesauttavat yrityksen liiketoimintaa positiivisella tavalla. Kuten edellä on mainittu, sertifikaatin saavuttaminen voi vaikuttaa positiivisesti myös yrityksen maineeseen. Tätä väitettä tukee myös se, että tutkimukseen osallistuvien yritysten mielestä sertifikaatin hankkiminen on tärkeää heidän asiakkaiden, yrityskumppanien sekä viranomaisten mielipiteen

vahvistamisen takia liittyen yrityksen tietoturvallisuuden panostamiseen. Myös se, että yritykset haluavat sertifikaatin avulla osoittaa, että yrityksellä on käytössä alan parhaat ja viimeisimmät toimintatavat, tukee kyseistä väitettä.

Vähemmän tärkeitä tekijöitä yritysten mielestä olivat:

- Halu kehittää tietoturvan hallintajärjestelmä sellaiseen tilaan, jota nykypäivän yritykseltä vaaditaan
- Saman liiketoiminta-alan kilpaileva yritys saavutti sertifikaatin

Vaikka nykypäivänä yrityksiltä vaaditaan paljon liittyen heidän tietovarojen luottamuksellisuuden, eheyden ja saatavuuden takaamiseksi, on mielenkiintoista, että vain kaksi yritystä neljästä piti tärkeänä tekijänä sitä, että tietoturvan hallintajärjestelmä kehitettäisiin sellaiseen tilaan, mitä yrityksiltä nykypäivänä vaaditaan. Varsinkin digitalisaation kehittyminen sekä tietotekniikan merkityksen kasvaminen nykypäivänä vaatii yrityksiltä valtavia ponnisteluita liittyen riittäviin turvatoimiin. Informaatioteknologia on tullut olennaiseksi osaksi nykypäivän yritysmaailmaa ja siitä on tulossa jatkuvasti suurempi tekijä (von Solms, 1999).

Yrityksillä voi olla kuitenkin erilaisia tavoitteita sekä malleja liittyen omaan tietoturvan hallintajärjestelmään ja kyseisiin osatekijöihin ei välttämättä liity muualla yritysmaailmassa vaikuttavat odotetut vaatimukset. Tämän takia edellä mainittua tekijää ei välttämättä pidetä tutkimukseen osallistuneiden yritysten mielestä kovin merkittävänä. Kaksi neljästä yrityksestä ilmoitti tärkeäksi tekijäksi sen, että saman liiketoiminta-alan kilpaileva yritys saavutti sertifikaatin ennen heitä. Tämä on osoitus siitä, että kilpailu saman liiketoiminta-alan yritysten välillä on kovaa, mutta osoitus myös siitä, että yritykset haluavat olla lähtökohtaisesti samalla viivalla kilpailijoidensa kanssa. Tällä voi olla myös vaikutusta esimerkiksi asiakkaiden sekä yhteistyökumppanien hankintaan.

Vähiten merkittävimpiä tekijöitä yritysten mielestä olivat

- Yrityksen toiminnan läpinäkyvyyden lisääminen
- Halu toimia yleisten standardien mukaisesti
- Yrityksen halu toimia tietoturvallisuuden johtamisen mahdollistajana
- Yrityksen työntekijöiden tietoturvallisuustietoisuuden kasvattaminen
- Tunnistettujen turvallisuusriskien hallitseminen

Ainoastaan yksi yritys neljästä piti edellä mainittuja tekijöitä tärkeänä. Tähän tutkimukseen osallistuneet yritykset eivät pitäneet tärkeänä tekijänä yrityksen liiketoiminnan läpinäkyvyyden lisäämistä. Yrityksen liiketoiminnan läpinäkyvyydellä tarkoitetaan sitä, kun yritys jakaa tietoa, luo oppimismahdollisuuksia sekä kommunikoi avoimesti.

Parris ym. (2016) toteavat artikkelissaan, että avoimuuden puute voi lisätä sidosryhmien skeptisyyttä samalla vähentäen luottamusta siihen, että yritykset toimivat sosiaalisten, eettisten ja ympäristöllisten standardien puitteissa. Avoimuuden tulisi toimia perustavanlaatuisena välineenä sidosryhmien

kanssakäymisen parissa ja yrityksen vastuullisen johtamisen käytäntöjen parantamisessa (Parris ym., 2016).

Tähän tutkimukseen osallistuneet yritykset eivät kuitenkaan pitäneet yrityksen toiminnan läpinäkyvyyttä merkittävänä tekijänä ISO 27001 -sertifikaattia hakiessa. Liiketoiminnan läpinäkyvyyden määritelmät kuitenkin vaihtelevat suuresti ja niissä on hyvin vähän johdonmukaisuutta ja ne ovat tyypillisesti epätarkkoja (Parris ym., 2016). Tämän takia yritykset eivät välttämättä pidä liiketoimintansa läpinäkyvyyttä juuri tässä asiayhteydessä kovinkaan tärkeänä. Tutkimukseen osallistuneiden yritysten mielestä halu toimia yleisten standardien mukaisesti ei ollut merkittävä tekijä sertifikaatin hakuprosessiin liittyen.

Yleisten tietoturvallisuuden hallinnan ohjeiden noudattaminen on nykypäivän yrityksissä välttämätöntä, mutta esimerkiksi Siponen ja Willison (2009) toteavat tutkimuksessaan, että tietoturvallisuuden hallintastandardeissa on kaksi ongelmaa: ne ovat laajuudeltaan yleisiä, eikä niitä ole validoitu. Nämä väittämät puoltavat sitä, ettei yritysten halu toimia yleisten standardien mukaisesti ollut merkittävä tekijä tässä tutkimuksessa. Vaikka tietoturvan hallintastandardit tarjoavat yrityksille ohjeita ja menettelytapoja liittyen tietoturvallisuuden hallintaan, ne sisältävät vahvistamattoman sekä laajan ohjeskaalan, eikä niitä ole kokonaisuudessaan kuitenkaan välttämätöntä käyttää.

Kyseisiä standardeja on myös erilaisia (esimerkiksi NIST), joten yhden yleisen standardin käyttö liittyen tietoturvan hallintajärjestelmään ei välttämättä tarkoita halua käyttää niitä kaikkia yrityksen toiminnassa. Halua toimia tietoturvallisuuden johtamisen mahdollistajana ei myöskään pidetty kovin tärkeänä tekijänä haettaessa ISO 27001 -sertifikaattia. Kyseinen sertifikaatti on itsessään jo osoitus siitä, että yrityksellä on käytössään standardoidut toimintatavat liittyen tietoturvan hallintajärjestelmään. Tämä voi puoltaa sitä, ettei halua toimia tietoturvallisuuden johtamisen mahdollistajana haluta erikseen nostaa esille tai pitää tärkeänä tekijänä, kun sertifikaattia on päätetty hakea. On kiinnostavaa, että tutkimukseen osallistuvien yritysten mielestä työntekijöiden tietoturvallisuustietoisuuden kasvattamista ei pidetty tärkeänä tekijänä. Nowak (2015) toteaa tutkimuksessaan, että yritykset voivat kehittää ja toteuttaa erilaisia puitteita liittyen tietoturvallisuuden hallintaansa yritysten työntekijöiden tietojen ansiosta.

Myös Karyda ym. (2004) toteavat, että esimerkiksi yrityksen onnistunut tietoturvapolitiikka on lähtöisin yrityksen työntekijöistä. Yritysten työntekijöillä on merkittävä vaikutus tietoturvallisuuteen sekä sen hallintaan, joten on mielenkiintoista, ettei yritykset pitäneet työntekijöiden tietoturvallisuustietoisuuden kasvattamista kovinkaan tärkeänä tekijänä haettaessa sertifikaattia. Sertifikaatin hakuprosessi kuitenkin edistää myös työntekijöiden tietoisuutta liittyen yrityksen tietoturvallisuuteen ja sen hallintaan.

Koska sertifiointiprosessi itsessään lisää automaattisesti työntekijöiden tietoturvallisuustietoisuutta, yritykset eivät välttämättä pidä sitä tärkeänä tekijänä haettaessa sertifikaattia tai työntekijöiden tietoturvallisuustietoisuutta

pidetään yrityksissä itsestään selvänä asiana. Tunnistettujen turvallisuusriskien hallitsemista ei myöskään pidetty tärkeänä tekijänä haettaessa sertifikaattia. ISO 27001 -sertifikaatin yksi merkittävimmistä osa-alueista ovat riskinarviointi, riskien hyväksymistasot sekä riskienhallintasuunnitelma, joita myös kolmannen osapuolen sertifiointiorganisaatio vaatii sertifiointiprosessissa. On mielenkiintoista, etteivät yritykset pitäneet tunnettujen turvallisuusriskien hallitsemista tärkeänä tekijänä, kun sertifikaatin hakuprosessi on haluttu käynnistää.

Tämä voi myös tarkoittaa sitä, että yritykset olivat jo kerenneet tunnistaa heidän liiketoimintansa kannalta merkittävimmät sekä tunnetuimmat turvallisuusriskit, eikä täten riskien uudelleen tunnistamista ja hallitsemista pidetty olennaisena, kun sertifiointiprosessi on haluttu käynnistää. Yksi yritys neljästä vastasi avoimeen kommenttikenttään, liittyen tärkeimpiin tekijöihin. Kyseinen yritys ilmoitti tärkeäksi tekijäksi halun osoittaa, että hallinnollisen puolen ollessa kunnossa, myös tekninen tietoturva on hallittua. Tästä voidaan päätellä, että ISO 27001 -sertifikaatti edesauttaa laadukkaan tietoturvan hallintajärjestelmän toteutumisen lisäksi myös yrityksen laitteistojen, ohjelmistojen ja tietojärjestelmien tietoturvallisuutta.

Tutkimustuloksissa kävi ilmi, että kolme neljästä yrityksestä käyttää yrityksensä tietoturvallisuuden hallinnassa jollain tasolla standardia ISO 27000. Kuten tässä tutkimuksessa on aikaisemmin mainittu, ISO 27000 -standardi esittelee määritelmät sekä termit ja tämän jälkeen hyödyt ja menettelyt liittyen tietoturvan hallintajärjestelmään.

Nowakin (2015) mukaan ISO 27000 -standardi on ensimmäinen askel kohti hyvin tehtyä tietoturvan hallintajärjestelmää. Tämä osoittaa sen, että tähän tutkimukseen osallistuneet kolme yritystä neljästä pitävät kyseistä standardia hyödyllisenä liittyen heidän tietoturvallisuutensa hallintaan ja haluavat käyttää sitä. Yksi yritys neljästä ilmoitti, ettei käytä kyseistä standardia yrityksensä tietoturvallisuuden hallinnassa. Tämä ei ole kuitenkaan huomiota herättävää, sillä ISO 27000 -standardi ei ole yritykselle pakollinen, vaikka ISO 27001 -sertifikaatti yrityksestä löytyisikin.

Yrityksiltä haluttiin myös kysyä, että ohjaako ISO 27000 -standardi yrityksen tietoturvallisuuden hallintaa jollain tasolla. Kysymykseen vastaamiseen käytettiin Likert-asteikkoa ja kolme neljästä yrityksestä vastasi olevansa täysin samaa mieltä ja yksi yritys neljästä vastasi olevansa täysin eri mieltä. Tämän perusteella voidaan olettaa, että ne yritykset, jotka ilmoittivat käyttävänsä ISO 27000 -standardia yrityksensä tietoturvallisuuden hallinnassa, ovat myös sitä mieltä, että kyseinen standardi myös ohjaa heidän tietoturvallisuutensa hallintaa. Voidaan myös olettaa, että yritys, joka ilmoitti, ettei ISO 27000 -standardia käytetä heidän tietoturvallisuutensa hallinnassa, ei myöskään käytä kyseistä standardia ohjaamaan yrityksensä tietoturvallisuuden hallintaa.

Tutkimustulokset kertovat, että kolme yritystä neljästä käyttävät standardia ISO 27002 jollain tasolla heidän yrityksen tietoturvallisuuden hallinnassa ja yksi yritys neljästä ei käytä. Calder ja Gerrard (2013) toteavat, että

jokaisen yrityksen, joka ottaa käyttöön ISO 27001 -standardin mukaisen tietoturvan hallintajärjestelmän, on hankittava ja tutkittava kopiot myös ISO 27002 -standardista. ISO 27002 -standardia on tarkoitus käyttää viitteenä määritettäessä ja toteutettaessa valvontatoimenpiteitä tietoturvariskien käsittelyä varten ISO 27001 -standardiin perustuvassa tietoturvan hallintajärjestelmässä (Calder & Gerrard, 2013).

Jokainen tähän tutkimukseen osallistunut yritys on saavuttanut ISO 27001 -sertifikaatin liittyen ISO 27001 -standardiin, joten on mielenkiintoista, että yksi tähän tutkimukseen osallistuneesta yrityksestä ilmoitti, ettei käytä ISO 27002 -standardia yrityksensä tietoturvallisuuden hallinnassa jollain tasolla. On mahdollista, että yritys on käyttänyt kyseistä standardia joissain määrin aikaisemmin yrityksen liiketoiminnan aikana, mutta ei välttämättä koe tänä päivänä enää kyseisen standardin sisältöä itselleen tärkeäksi ISO 27001 -sertifikaatin saamisen jälkeen.

Tutkimukseen osallistuvilta yrityksiltä kysyttiin myös, että ohjaako ISO 27002 -standardi yrityksen tietoturvallisuuden hallintaa jollain tasolla. Myös tähän kysymykseen vastattiin Likert-asteikon avulla. Yksi yritys ilmoitti olevansa täysin samaa mieltä, kaksi yritystä ilmoitti olevansa samaa mieltä ja yksi yritys ilmoitti olevansa täysin eri mieltä. Myös näistä vastauksista voidaan päätellä, että yritys, joka ei käytä ISO 27002 -standardia yrityksen tietoturvallisuuden hallinnassa on myös täysin eri mieltä siitä, että kyseinen standardi ohjaisi heidän tietoturvallisuuden hallintaansa. Kolme yritystä neljästä ilmoitti, käyttävänsä ISO 27002 -standardia tietoturvallisuuden hallinnassa jollain tasolla, joten voidaan olettaa, että kyseiset yritykset myös ilmoittivat olevansa täysin samaa mieltä ja samaa mieltä siitä, että ISO 27002 -standardi ohjaa yrityksien tietoturvallisuuden hallintaa jollain tasolla.

6.2 Johtopäätökset

Tässä tutkimuksessa on tarkasteltu neljän eri Suomessa toimivan yrityksen tietoturvallisuuden hallintaa kolmen eri tietoturvastandardin avulla. Tarkoituksena oli selvittää, että käytetäänkö yrityksissä standardeja ISO 27000 ja ISO 27002 heidän tietoturvallisuutensa hallinnassa ja ohjaavatko kyseiset standardit hallintaa jollain tasolla. Tarkoituksena oli myös selvittää ISO 27001 -standardiin liittyvän sertifikaatin hakuprosessiin liittyviä kysymyksiä sekä tärkeimpiä tekijöitä, jotka edesauttoivat yrityksiä hakemaan kyseistä sertifikaattia.

Tämän tutkimuksen tutkimuskysymys kuului seuraavasti:

Miten ISO 27000 -standardisarja ja erityisesti standardit ISO 27000, ISO 27001 ja ISO 27002 ovat osana tietoturvallisuuden hallintaa tutkimukseen osallistuvien nykypäivän yrityksissä.

Tässä tutkimuksessa tarkasteltavat tietoturvastandardit olivat joko kaikki tai yksittäin käytössä tutkimukseen osallistuvien yritysten tietoturvallisuuden hallinnassa. Kolme yritystä neljästä käyttää ISO 27000 -tietoturvastandardia jollain

tasolla yrityksen tietoturvallisuuden hallinnassa sekä kyseinen standardi myös ohjaa heidän yrityksen tietoturvallisuuden hallintaa jollain tasolla. Yksi yritys neljästä ei käytä kyseistä standardia yrityksensä tietoturvallisuuden hallinnassa eikä se myöskään ohjaa sitä, joten enemmistö tähän tutkimukseen osallistuneista yrityksistä käyttää ISO 27000 -standardia tietoturvallisuuden hallinnassa ja sen ohjaamisessa.

Kolme yritystä neljästä ilmoitti käyttävänsä myös ISO 27002 -tietoturvastandardia jollain tasolla yrityksen tietoturvallisuuden hallinnassa. Samat yritykset myös ilmoittivat kyseisen standardin ohjaavan heidän yrityksen tietoturvallisuuden hallintaa jollain tasolla. Yksi yritys ilmoitti, ettei käytä ISO 27002 -standardia yrityksensä tietoturvallisuuden hallinnassa. Sama yritys ilmoitti myös, ettei käytä kyseistä standardia yrityksensä tietoturvallisuuden hallinnan ohjaamiseen, joten enemmistö tähän tutkimukseen osallistuneista yrityksistä käyttää ISO 27002 -standardia tietoturvallisuuden hallinnassa ja sen ohjaamisessa.

Tutkimuksessa tarkasteltiin standardia ISO 27001 yritysten hankkiman ISO 27001 -sertifikaatin kautta. Sertifikaattiin liittyvää hakuprosessia tarkasteltiin saavutusvuoden, keston sekä haastavuuden näkökulmista. Kaikki tutkimukseen osallistuneet yritykset ovat saavuttaneet ISO 27001 -sertifikaatin viimeisen kolmen vuoden aikana. Yritysten sertifikaatin hakuprosessi vaihteli yrityksien kesken 1–3 vuoden välillä ja he kokivat sertifikaatin hakuprosessin sekä haastavaksi että ei haastavaksi, joten hakuprosessi oli kaikissa yrityksissä erilainen.

Tärkeimpiä tekijöitä sertifikaatin hakemispäätökseen olivat asiakkaiden, yrityskumppanien sekä viranomaisten mielipiteen vahvistaminen liittyen yrityksen tietoturvallisuuden panostamiseen, joten yrityksille oli tärkeää sertifikaatin tuoma positiivinen mainehyöty. Yksi tärkeä tekijä oli yrityksen tietoturvallisuuden ja tietoturvaosaamisen kehittäminen sekä ylläpito, joten yritykset kokevat sertifikaatin edistävän ja vahvistavan yritysten jo olemassa olevaa tietoturvallisuutta entisestään.

Vähemmän tärkeitä tekijöitä olivat kilpailevan yrityksen sertifikaatin saavuttaminen ja halu kehittää yrityksen tietoturvan hallintajärjestelmä sellaiseen tilaan, jota nykypäivän yrityksiltä vaaditaan, joten osa yrityksistä ei näe vertailua toisiin yrityksiin sertifikaatin näkökulmasta merkittävänä. Vähiten tärkeitä tekijöitä olivat työntekijöiden tietoturvallisuustietoisuuden kasvattaminen, yrityksen toiminnan läpinäkyvyyden lisääminen, halu toimia yleisten standardien mukaisesti, halu toimia tietoturvallisuuden johtamisen mahdollistajana ja tunnistettujen turvallisuusriskien hallitseminen. Toisin sanoen suurin osa yrityksistä ei näe tarpeelliseksi edistää työntekijöidensä tietoturvallisuuskäyttäytymistä sertifikaatin avulla, eivätkä koe sertifikaattia tärkeänä, kun halutaan hallita jo tunnistettuja riskejä, toimia yleisten tunnettujen ohjeiden mukaan tai käsiteltäessä yrityksen liiketoiminnan avoimuutta.

6.3 Tutkimuksen vahvuudet ja rajoitteet

Tutkimuksen avulla saavutettiin yleiskatsaus siitä, miten ISO 27000 -tietoturvastandardi on osana neljän eri Suomessa toimivan yrityksen tietoturvallisuuden hallintaa. Otanta oli kuitenkin verrattain pieni, joten yleistyksiä nykypäivän yritysten tietoturvallisuuden hallinnasta ei voi tehdä. Tutkimuksen aineisto kerättiin sekä tutkijan että vastaajien kannalta joustavalla kyselylomakkeella ja kyselyyn vastasivat yrityksistä sellaiset henkilöt, jotka ovat päivittäin tekemisissä yrityksensä tietoturvallisuuden ja sen hallinnan kanssa. Tämän takia kerättyä aineistoa voidaan pitää validina ja täten tutkimuksessa saatiin selvitettyä yritysten tietoturvallisuuden hallintaan liittyviä asioita aidosti, unohtamatta kuitenkaan kerätyn aineiston arkuutta ja kriittisyyttä. Tutkimuksen aineisto saatiin kerättyä nopeasti, joten myös itse tutkimuksella oli mahdollisuus edetä nopeasti. Tutkimuksen rajoitteeksi oli muodostua tutkimukseen osallistuvien yritysten määrä, sillä ISO 27001 -sertifikaatin omaavia yrityksiä oli verrattain vaikea löytää.

Tulevaisuudessa samankaltaisessa tutkimuksessa otantaa tulisi kasvattaa merkittävästi. Mikäli osallistuvien yritysten määrää saataisiin kasvatettua esimerkiksi viiteenkymmeneen, olisi yleistysten tekeminen Suomessa toimivien yritysten kesken mahdollista. Myös yritysten mahdollisia eroavaisuuksia liittyen ISO 27000 -standardien käyttöön voitaisiin havaita enemmän. Tässä tutkimuksessa yrityksiä ei rajattu spesifisti osallistumisen suhteen esimerkiksi liiketoiminta-alan perusteella. Tulevaisuuden tutkimuksessa yrityksiä voisi myös rajata eri liiketoiminta-alojen perusteella, jolloin voitaisiin tarkastella isompana kokonaisuutena myös eri liiketoiminta-alojen yritysten välisiä eroja. Myös kyselyyn vastaavia yrityksien edustajia voitaisiin rajata heidän työnimikkeensä perusteella tarkemmin, jotta saataisiin vaihtelevia havaintoja eri työnimikkeellä toimivien henkilöiden kokemuksista liittyen yrityksen tietoturvaan ja sen hallintaan.

Tähän tutkimukseen liittyvässä kyselylomakkeessa olleet vaihtoehdot liittyen merkittävimpiin tekijöihin ISO 27001 -sertifikaattia haettaessa annettiin yrityksille valmiiksi. Tulevaisuuden tutkimuksessa olisi mielenkiintoista nähdä, jos osallistuvat yritykset pohtisivat ja kirjoittaisivat merkittävimmät tekijät itse. Tällä tavoin voitaisiin saavuttaa paljon erilaisia näkemyksiä merkittävimmistä tekijöistä haettaessa sertifikaattia, mutta samalla voitaisiin tehdä havaintoja myös tekijöistä, jotka yhdistävät yrityksiä. Tämän tutkimuksen tutkimuskysymyksen ja näkökulmien avulla voitaisiin suorittaa myös laajempi tutkimus Suomen ulkopuolella toimiviin yrityksiin jollain tietyllä liiketoiminta-alalla.

7 YHTEENVETO

Tämän tutkielman tarkoituksena oli selvittää, kuinka nykypäivän yritykset käyttävät ISO 27000 -tietoturvastandardisarjaa heidän tietoturvallisuutensa hallinnassa. Tavoitteena oli selvittää, kuinka tähän tutkimukseen osallistuneet yritykset käyttävät ISO 27000 -standardisarjan standardeja ISO 27000, ISO 27001 sekä ISO 27002 tietoturvallisuutensa hallinnassa ja miten kyseiset standardit ohjaavat kyseistä tietoturvallisuuden hallintaa. Tutkimukseen osallistuvilta yrityksiltä selvitettiin myös heidän kokemuksiansa ISO 27001 -standardiin liittyvään sertifikaattiin sekä sen hakuprosessiin.

Tämän tutkielman kirjallisuuskatsauksessa tutustuttiin yritysten tietoturvallisuuden hallintaan tietoturvapolitiikan sekä tietoturvan hallintajärjestelmän avulla. Kirjallisuuskatsauksessa perehdyttiin myös ISO 27000 -tietoturvastandardisarjaan, sekä sen historiaan ja kehitykseen. Päähuomio tässä tutkimuksessa keskittyi standardeihin ISO 27000, ISO 27001 sekä ISO 27002.

Yritykset käsittelevät nykypäivänä valtavia määriä erilaista dataa samalla käyttäen erilaisia tietojärjestelmiä, mikä johtaa siihen, että yritykset sekä heidän liiketoimintansa ovat nykyään myös entistä riippuvaisempia informaatioteknologiasta kuin aikaisemmin. Tämän takia nykypäivän yritysten on tärkeää huolehtia tietoturvallisuutensa hallinnasta riittävän tehokkain keinoin. ISO 27000 -tietoturvastandardisarja tarjoaa yrityksille erilaisia ohjeita ja menettelytapoja, joiden avulla he voivat suunnitella, toteuttaa, ylläpitää sekä parantaa tietoturvallisuuden hallintaa. Kyseinen standardisarja tarjoaa myös suuntaviivoja yrityksen tietoturvapolitiikalle sekä tietoturvan hallintajärjestelmälle ja niiden käyttöönotolle. Esimerkiksi onnistuneen tietoturvan hallintajärjestelmän avulla yrityksillä on mahdollisuus hakea kolmannen osapuolen myöntämä ISO 27001 – sertifikaatti, joka on osoitus siitä, että yrityksessä toimitaan ISO 27001 -standardin mukaisella tavalla.

Tietoturvallisuus kasvaa yrityksissä jatkuvasti kohti laajempaa kokonaisuutta ja siitä on muodostunut tärkeä osa eri liiketoiminta-alojen liiketoimintaprosesseja sekä yrityskokonaisuutta. Hyvän tietoturvallisuuden hallinnan tarkoituksena on huolehtia yrityksen tietovarojen luottamuksellisuudesta,

eheydestä ja saatavuudesta, samalla kun yrityksessä pyritään keskittymään myös riskien hallitsemiseen koko ajan muuttuvassa uhkaympäristössä.

Tässä tutkimuksessa tutkimusmenetelmänä käytettiin laadullista tutkimusmenetelmää ja aineistonkeruumenetelmänä toimi sähköinen kyselylomake. Tutkimukseen osallistui neljä Suomessa toimivaa eri liiketoiminta-alan yritystä. Tutkimustuloksista voidaan päätellä, että enemmistö tutkimukseen osallistuneista yrityksistä käyttää sekä standardia ISO 27000 ja ISO 27002 jollain tasolla heidän yrityksensä tietoturvallisuuden hallinnassa sekä sen ohjaamisessa.

Tulokset osoittavat, että ISO 27001 -sertifikaatin hakuprosessia pidettiin osallistuvien yritysten kesken sekä haastavana että ei haastavana ja ainoastaan yksi yritys pysyi kestoltaan hakuprosessin keskiarvollisessa ajassa. Tuloksista kävi ilmi, että tärkeimpiä tekijöitä haettaessa ISO 27001 -sertifikaattia olivat sen tuoma positiivinen mainehyöty sekä yrityksen tietoturvallisuuden kehittäminen. Vähemmän tärkeä tekijä oli yrityksen toiminnan vertailu muihin kilpaileviin yrityksiin. Vähiten tärkeitä tekijöitä olivat yritysten työntekijöiden tietoturvallisuustietoisuuden kasvattaminen, yrityksen liiketoiminnan läpinäkyvyyden lisääminen, halu toimia yleisten standardien mukaisesti, halu toimia tietoturvallisuuden johtamisen mahdollistajana ja tunnistettujen turvallisuusriskien hallitseminen.

Tämän tutkimuksen otanta oli yritysmäärältään verrattain pieni, joten yleistäviä päätelmiä liittyen nykypäivän Suomessa toimivien yritysten tietoturvallisuuden hallintaan ei ole mahdollista tehdä. Tutkimustulokset kuitenkin tarjoavat yleiskatsauksen juuri tähän tutkimukseen osallistuneiden yritysten tietoturvallisuuden hallinnasta ISO 27000 -tietoturvastandardisarjan avulla.

Tämän tutkielman tutkimustulosten pohjalta nousi esiin kuitenkin myös mahdollisia jatkotutkimusaiheita. Tulevaisuudentutkimuksessa yritysmäärää voitaisiin kasvattaa merkittävästi ja esimerkiksi osallistuvia yrityksiä voisi rajata niiden liiketoiminta-alan perusteella. Tämä mahdollistaisi suuremman määrän aineistoa tutkittavaksi ja samalla voitaisiin tarkastella saman liiketoiminta-alojen yritysten yhtäläisyyksiä sekä eroavaisuuksia liittyen heidän tietoturvallisuutensa hallintaan ja sen ohjaamiseen.

LÄHTEET

Alexei, A., & Alexei, A. (2023). The Difference Between Cyber Security vs. Information Security. *Journal of Engineering Science*, 29(4), 72-83. https://doi.org/10.52326/jes.utm.2022.29(4).08

Alhabeeb, M., Almuhaideb, A., Le, P. D. & Srinivasan, B. (2010). Information Security Threats Classification Pyramid, *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, Perth, WA, Australia, 2010, pp. 208-213, doi: 10.1109/WAINA.2010.39.

Ashenden, D. (2008). Information Security management: A human challenge? *Information security technical report*, 13(4), 195-201.

Beckers, K., Côté, I., Faßbender, S., Heisel, M. & Hofbauer, S. (2013). A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance. *Requirements engineering, 18*(4), 343-395. https://doi.org/10.1007/s00766-013-0174-7

Braun, V., Clarke, V., Boulton, E., Davey, L., & McEvoy, C. (2021). The online survey as a qualitative research tool. *International Journal of Social Research Methodology*, 24(6), 641-654.

Calder, A. & Gerrard, L. (2013). *ISO27001 / ISO27002: A Pocket Guide*. IT Governance Ltd.

Colwill, C. (2009). Human factors in information security: The insider threat–Who can you trust these days? *Information security technical report*, 14(4), 186-196.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, *4*(2).

DVV. (2023). Mitä on digiturva? https://dvv.fi/mita-on-digiturva, viitattu 10.2.2023.

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.

Fingrid Oyj. Esittely. URL https://www.fingrid.fi/sivut/yhtio/esittely/, viitattu 21.01.2023.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & security*, 61, 169-183.

Fossey, E., Harvey, C., McDermott, F., & Davidson, L. (2002). Understanding and evaluating qualitative research. *Australian & New Zealand journal of psychiatry*, 36(6), 717-732.

Gerić, S., & Hutinski, Ž. (2007). Information system security threats classifications. *Journal of Information and organizational sciences*, 31(1), 51-61.

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *TQM journal, 23*(4), 367-376. https://doi.org/10.1108/17542731111139455

Gofore. Mitä teemme. URL https://gofore.com/mita-teemme/, viitattu 12.01.2023

Goodman, S., Straub, D. W., & Baskerville, R. (2008). *Information Security: Policy, Processes, and Practices*.

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of management information systems*, 28(2), 203-236.

Hamdi, Z., Anir Norman, A., Nuha Abdul Molok, N. & Hassandoust, F. (2019). A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors. *Journal of physics.* Conference series, *1339*(1), 12103. https://doi.org/10.1088/1742-6596/1339/1/012103

Hirsjärvi, S., Remes, P., Sajavaara, P., & Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.

Hoffmann, R., Kiedrowicz, M. & Stanik, J. (2016). Risk management system as the basic paradigm of the information security management system in an organization. https://doi.org/10.1051/matecconf/20167604010

Hong Kong Veritas. *ISO 27001 Information Security Management System.* http://www.hkveritas.com/index.php/hkvcertification/information-security-management-system-iso-27001-2013.php

Hytönen, J., & Sipilä, O. (1987). *Tietoturvallisuus yrityksessä*.

Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say? *Computers & security*, *21*(5), 402-409.

Ilvonen, I. (2006). Tietoturvallisuus pirkanmaalaisissa tietointensiivisissä pk-yrityksissä. Tampere University of Technology: University of Tampere : distribution: eBRC.

Irwin L., (2023). IT Governance: ISO 27001 Certification: 10 Easy Steps. URL https://www.itgovernanceusa.com/blog/iso-27001-registrationcertification-in-ten-easy-steps, viitattu 22.01.2023

ISO (2022). The ISO Survey. URL https://www.iso.org/the-iso-survey.html, viitattu 23.01.2023

ISO (2018). *ISO/IEC 27000:2018(en)* Information technology — Security techniques — Information security management systems — Overview and vocabulary. *https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en*

ISO (2022a). ISO/IEC 27001:2022(en) Information security, cybersecurity and privacy protection — Information security management systems — Requirements. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

ISO (2022b). *ISO/IEC 27002:2022(en)* Information security, cybersecurity and privacy protection — Information security controls. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32, 489-496.

Karyda, M., Kiountouzis, E., & Kokolakis, S. (2005). Information systems security policies: A contextual perspective. *Computers & security*, 24(3), 246-260. https://doi.org/10.1016/j.cose.2004.08.011

Legalesign (2021). Is ISO 27001 Certification worth it? URL https://legalesign.com/blog/is-ISO27001-certification-worth-it/, viitattu 23.01.2023

Magic Cloud. Tarinamme. URL https://magiccloud.fi/magic-cloud/tarinamme/, viitattu 12.01.2023

Meriah, I. & Arfa Rabai, L. B. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Computer Science*, 160, 85-92. https://doi.org/10.1016/j.procs.2019.09.447

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE transactions on engineering management, 68*(1), 87-100. https://doi.org/10.1109/TEM.2020.2977815

Ngo, F. T., Agarwal, A., Govindu, R., & MacDonald, C. (2020). Malicious software threats. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 793-813.

Niemimaa, E., & Niemimaa, M. (2017). Information systems security policy implementation in practice: From best practices to situated practices. *European journal of information systems*, 26(1), 1-20. https://doi.org/10.1057/s41303-016-0025-y

Nowak, G. J. (2015). Information Security Management with accordance to ISO27000 Standards: Characteristics, implementations, benefits in global Supply Chains. *Logistyka*, *2*, 639-654.

Parris, D. L., Dapko, J. L., Arnold, R. W., & Arnold, D. (2016). Exploring transparency: a new framework for responsible business management. *Management Decision*.

Porvari, P. (2012). Tietoturvallisuus liiketoiminnan johtamisessa, prosesseissa ja henkilöiden toiminnassa. Aalto-yliopisto, Sähkötekniikan korkeakoulu, Elektroniikan laitos. *Aalto University publication series Doctoral Dissertations, 131/2012*

Qusef, A., Arafat, M., & Al-Taher, S. (2018). Organizational management role in information security management system. https://doi.org/10.1145/3231053.3231064

Rocha Flores, W., Antonsen, E., & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & security*, *43*, 90-110. https://doi.org/10.1016/j.cose.2014.03.004

Singh, A. N., Gupta, M. P., & Ojha, A. (2014). Identifying factors of 'organizational information security management'. *Journal of enterprise information management*, 27(5), 644-667. https://doi.org/10.1108/JEIM-07-2013-0052

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & management*, 46(5), 267-270. https://doi.org/10.1016/j.im.2008.12.007

Sofaer, S. (1999). Qualitative methods: what are they and why use them? *Health services research*, 34(5 Pt 2), 1101.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, 11(5), 23-29.

von Solms, R. (1999). Information security management: Why standards are important. *Information management & computer security*, 7(1), 50-58. https://doi.org/10.1108/09685229910255223

von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Talib, M. A., El Barachi, M., Khelifi, A., & Ormandjieva, O. (2012). Guide to ISO 27001: UAE case study. *Issues in Informing Science and Information Technology*, 7, 331-349.

Taherdoost, H. (2022). Cybersecurity vs. Information Security. *Procedia computer science*, 215, 483-487. https://doi.org/10.1016/j.procs.2022.12.050

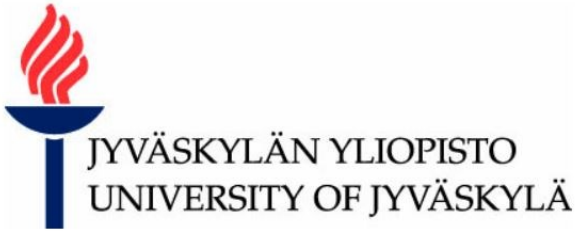
Wang, C., & Tsai, D. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. https://doi.org/10.1109/CCST.2009.5335527

Zafar, H. (2013). Human resource information systems: Information security concerns for organizations. *Human resource management review*, 23(1), 105-113. https://doi.org/10.1016/j.hrmr.2012.06.010

LIITE 1 KYSELYTUTKIMUS

ISO 27000 -standardisarja osana nykypäivän yritysten tietoturvallisuuden hallintaa - Eeva Mäki-Maukola, Pro Gradu -tutkielman kyselylomake

Pakolliset kysymykset merkitty tähdellä (*)



Kiitos tutkimukseen osallistumisesta!

Tämä kysely lähetetään teille sen takia, että yrityksenne on lupautunut osallistua Eeva Mäki-Maukolan Pro -Gradu -tutkielmaan, jonka aiheena on "ISO 27000 -standardisarja osana nykypäivän yritysten tietoturvallisuuden hallintaa". Kysely sisältää yhteensä 12 kysymystä, jotka ovat pääosin pakollisia monivalintakysymyksiä. Muutama kysymys voi vaatia myös kirjoittamista.

Tämän kyseisen Pro Gradu -tutkielman johdanto-osiossa on tarkoitus esitellä tutkimukseen osallistuvat yritykset lyhyiden kuvauksien kera. Mikäli ette halua, että yrityksenne nimi mainitaan tutkimuksen johdannossa, yrityksestänne voidaan käyttää muuttujaa X (kysymys 1).

Aineisto tätä edellä mainittua Pro Gradu -tutkielmaa varten kerätään tämän kyseisen kyselylomakkeen avulla. Aineistoa tullaan käsittelemään niin, ettei vastauksia voi yhdistää spesifioidusti kyselyyn vastanneeseen yritykseen, vaan vastauksia käsitellään yhtenä kokonaisuutena: esimerkiksi "kolme neljästä yrityksestä saavutti sertifikaatin vuonna 2021". Mikäli kyselylomake herättää kysymyksiä, minuun voi olla yhteydessä sähköpostitse matalalla kynnyksellä (eeva.makimaukola@gmail.com).

Kyselyyn vastaaminen kestää noin 5-10 minuuttia. Vastaathan kyselyyn viimeistään perjantaihin 13.1.2023 klo 16.00 mennessä. Huomioi, että kyselyyn voi vastata vain kerran!

1. Haluan, että yrityksestäni käytetään tutkimuksen johdanto-osiossa muuttujaa X *

- ◯ Kyllä
- ◯ Ei

2. Kyselyyn osallistuvan yrityksen nimi. Vastaa tähän, mikäli vastasit edelliseen kysymykseen "Ei".

3. Minä vuonna yrityksenne saavutti ISO 27001 -sertifikaatin? *

- ◯ 2022
- ◯ 2021
- ◯ 2020
- ◯ 2019
- ◯ 2018

4. Kuinka kauan sertifikaatin hakuprosessi kesti kokonaisuudessaan prosessin käynnistymisestä sertifikaatin saamiseen? *

- ◯ 0-1 vuotta
- ◯ 1-2 vuotta
- ◯ 2-3 vuotta
- ◯ 3-4 vuotta
- ◯ 4-5 vuotta

5. Koettiinko sertifikaatin hakuprosessi haastavaksi? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

6. Mitkä tekijät olivat yrityksellenne tärkeimmät haettaessa sertifikaattia? *

- ☐ Tietoturvaosaamisen jatkuvuuden sekä -käytäntöjen saavuttaminen sekä ylläpito
- ☐ Yrityksen toiminnan läpinäkyvyyden lisääminen
- ☐ Osoitus siitä, että yrityksellä on käytössä alan parhaat ja viimeisimmät toimintatavat
- ☐ Asiakkaiden, yrityskumppanien sekä viranomaisten mielipiteen vahvistaminen liittyen yrityksen tietoturvallisuuden panostamiseen
- ☐ Tietoturvallisuuden kehittäminen
- ☐ Halu toimia yleisten standardien mukaisesti
- ☐ Yrityksen halu toimia tietoturvallisuden johtamisen mahdollistajana
- ☐ Yrityksen työntekjöiden tietoturvallisuustietoisuuden kasvattaminen
- ☐ Halu kehittää tietoturvan hallintajärjestelmä sellaiseen tilaan, jota nykypäivän yritykseltä vaaditaan
- ☐ Tunnistettujen turvallisuusriskien hallitseminen
- ☐ Saman liiketoiminta-alan kilpaileva yritys saavutti sertifikaatin
- ☐ Kaikki ylläolevat vaihtoehdot
- ☐ Muita tekijöitä, mitä? _____

7. Onko sertifikaatin saamisesta koettu olevan hyötyä yrityksenne toiminnassa? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

8. Käytetäänkö yrityksenne tietoturvallisuuden hallinnassa jollain tasolla standardia ISO 27000? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

9. Ohjaako ISO 27000 -standardi yrityksenne tietoturvallisuuden hallintaa jollain tasolla? Anna arviosi asteikolla 1-5. *

- ◯ 5 = Täysin samaa mieltä
- ◯ 4 = Samaa mieltä
- ◯ 3 = Ei samaa eikä eri mieltä
- ◯ 2 = Eri mieltä
- ◯ 1 = Täysin eri mieltä

10. Käytetäänkö yrityksenne tietoturvallisuuden hallinnassa jollain tasolla standardia ISO 27002? *

- ◯ Kyllä
- ◯ Ei
- ◯ En osaa sanoa

11. Ohjaako ISO 27002 -standardi yrityksenne tietoturvallisuuden hallintaa jollain tasolla? Anna arviosi asteikolla 1-5. *

- ◯ 5 = Täysin samaa mieltä
- ◯ 4 = Samaa mieltä
- ◯ 3 = Ei samaa eikä eri mieltä
- ◯ 2 = Eri mieltä
- ◯ 1 = Täysin eri mieltä

12. Tämän kyselyyn vastanneen yrityksen edustajan työnimike (esimerkiksi tietoturvapäällikkö). Mikäli et halua vastata, jätä tämä kohta tyhjäksi.

Lähetä