LAB University of Applied Sciences

ISO27001-sertifikaattiprojekti

Sertifikaatin hankkiminen toimeksi antavalle yritykselle

LAB-ammattikorkeakoulu
Tradenomi (AMK)
2024
Roope Pellinen

Tiivistelmä

Tekijä(t)	Julkaisun laji	Valmistumisaika
Roope Pellinen	Opinnäytetyö, AMK	2024
	Sivumäärä	
	24	

Työn nimi

ISO27001-sertifikaattiprojekti

Sertifikaatin hankkiminen toimeksi antavalle yritykselle

Tutkinto ja koulutusala

Tradenomi (AMK), Tietojenkäsittelyn koulutus

Toimeksiantajaorganisaatio (jos opinnäytetyöllä on toimeksiantaja)

Toimeksi antava yritys

Tiivistelmä

Opinnäytetyön tarkoitus on saavuttaa ISO27001-standardi toimeksi antavalle yritykselle. Opinnäytetyössä valotetaan prosessia ja vaiheita, jotka johtivat haluttuun lopputulokseen sekä käydään läpi tietoturvan ja siihen liittyvien standardien tärkeyttä yritysten päivittäisessä toiminnassa. Opinnäytetyöstä saa kattavan käsityksen, mitä standardoituminen voi yritykseltä vaatia ja mitä osa-alueita siihen liittyy.

Asiasanat

Tietoturva, ISO/IEC 27001, tietoturvastandardi

Abstract

Author(s)	Type of Publication	Published
Roope Pellinen	Thesis, UAS	2024
	Number of Pages	
	24	

Title of Publication

ISO/IEC 27001 certification project

Certification project for a mandator company

Degree, Field of Study

Bachelor's Degree Programme in Business (UAS), Information Technology

Organisation of the client (if the thesis work is commissioned by another party)

Mandator company

Abstract

This Thesis describes how it is possible to achieve ISO/IEC 27001-certification for a mandator company. Thesis describes the process and the iterations which lead to the results. Thesis looks over importance of information security and information security standards in companies' daily actions. The reader gets comprehensive picture about what certification process requires and which sections are related to it.

Keywords

Information security, ISO/IEC 27001, information security standard

Sisällys

1 Johdanto

Tässä opinnäytetyössä kuvataan, miten tämän opinnäytetyön toimeksi antava yrityksen on mahdollista saavuttaa ISO/IEC 27001-standardi (myöhemmin ISO27001) ja mitä yrityksen tulee ottaa huomioon projektin aikana. Keskiössä ovat toimeksi antavan yrityksen sertifioitumisprosessin aikana tehdyt havainnot ja niistä tehdyt päätelmät. Tavoitteena on myös analysoida seikkoja, jotka voivat olla yritykselle haasteellisia prosessin aikana ja kuinka kehittää toimintaa jatkossa niiden osalta.

Opinnäytetyön aiheen valintaan vaikuttaa vahvasti se, että tietoturvan tärkeys kasvaa koko ajan ja se myös kiinnostaa monien yritysten asiakkaita entistä enemmän. Tietoturva, sekä siihen liittyvät tietoturvaloukkaukset ja muut ongelmat, ovat myös jatkuvasti esillä mediassa erityisesti silloin, kun tietoturvaonnettomuudet ovat jo tapahtuneet. Tästä hyvänä esimerkkinä Vastaamon tietomurto, jota on paljon käsitelty mediassa.

Vastauksia edellä mainittuihin opinnäytetyön tavoitteisiin selvitetään osallistumalla ISO27001-standardointi projektiin toimeksi antavalle yritykselle. Tämä tehdään työllistymällä toimeksi antavaan yritykseen perustettuun ISO27001-työryhmään. Työ tehtiin sisäisenä auditointina syksyn 2022 ja alkukevään 2023 aikana. Ulkopuolinen auditoija tekee ulkoisen auditoinnin keväällä 2023. Tässä opinnäytetyössä paneudutaan aiheeseen ja opinnäytetyön tavoitteisiin sekä sisäisten ja ulkoisten auditointien osalta, jotka tapahtuvat syksyn 2022 ja jatkuvat kesän 2023 loppuun saakka. Menetelmänä työssäni käytän toiminnallista menetelmää, sillä kyseessä on toimeksianto yritykseltä. Työssä ei myöskään oteta huomioon yksityisihmisten tietoturvaa, vaan aihetta käsitellään vain toimeksi antavan yrityksen näkökulmasta.

Opinnäytetyön teoriaosuudessa perehdytään myös siihen, mihin tietoturvaa tarvitaan jokapäiväisessä työskentelyssä ja siihen, miksi yrityksen hyvin toteutettu ja toimiva tietoturva sekä siihen liittyvät käytänteet ovat yhä tärkeämpi osa yritysten turvallista ja vastuullista toimintaa. Nämä asiat luovat perustan oikeastaan minkäänlaisten tietoturva standardien olemassaololle ja niiden käytölle yrityksissä.

Tässä opinnäytetyössä käydään läpi myös tietoturvan peruskäsitteistöä, siltä osin kuin se on relevanttia ja liittyy tässä opinnäytetyössä rajattuun aiheeseen ja tavoitteisiin. Osaltaan käydään läpi myös syitä, miksi tietoturvastandardeja ylipäätään on ja mitä hyötyä yritykset niistä saavat sisäisesti sekä yritysten välisesti.

Opinnäytetyössä ei käsitellä yksityiskohtaisia tietoja koskien toimeksi antavan yrityksen tietoturva ratkaisuista, kuten käytössä olevat tietojärjestelmät, asiakkaat jne. Asiat ja vaiheet, joita tuon auditoinnista esille, esitellään yleisellä tasolla, jottei toimeksi antavan yrityksen

tietoturva vaarannu. Opinnäytetyössä ei myöskään esitellä lopullista tuotosta raporteista, jotka käytännön projektissa toimeksiantajalle syntyvät ulkoisen auditoinnin yhteydessä. Yrityksen sisäistä dokumentaatiota ei tulla myöskään esittelemään sen tarkemmin.

Toimeksi antavana yrityksenä toimii suomalainen IT-alan yritys, joka tarjoaa IT-alan ratkaisuja pienille ja keskisuurille yrityksille usealla toimipisteellä ympäri Suomea. Yrityksen palvelutarjontaan kuuluu myös pilvi- ja tietoturvapalveluja sekä käyttäjätukea huomioiden asiakkaan tarpeet kokonaisvaltaisesti mukaan lukien tarvittavat ohjelmistot sekä niiden ylläpito. Yrityksen palveluihin lukeutuvat niin ikään laitteiden myynti asiakkaille sekä tarpeen arviointi näiden osalta.

Lähteinä opinnäytetyölle käytetään sekä tieteellisiä lähteitä (kirjat, artikkelit ja julkaisut) että alan asiantuntija lähteitä ja oppaita. Perusteluna asiantuntija lähteille voidaan lukea muun muassa se, että tietoturva sekä tietoturvallinen toiminta on enemmän käytännönläheistä kuin teoreettista ja siksi aiheesta on saatavilla enemmän käytäntöön nojaavia lähteitä kuin tieteellistä tutkimusta. Se on oikea ratkaisu opinnäytetyön aiheenvalinnan ja rajauksen näkökulmasta.

Opinnäytetyö tehtiin toiminnallisella tutkimusmenetelmällä toimeksi antavan yrityksen projektin luonteen vuoksi. Projekti sisälsi laajasti yrityksen sisäisten käytänteiden nykytilan selvitystä uudelleen määrittelyä ja dokumentointia. Myös auditoinnit ja niihin liittyvät toiminnot olivat iso osa projektia, joten toiminnallinen tutkimus valikoitui siten luonnollisesti tämän opinnäytetyön menetelmäksi.

2 Tietoturva

2.1 Tietoturvan määritelmä

Liikenne- ja viestintävirasto kertoo kyberturvallisuuden verkkosivuillaan tietoturvan kattavan ne tekniset ja hallinnolliset ratkaisut, joilla taataan välitettävän ja säilytettävän datan eli tiedon kolme keskeistä osa-aluetta. Nämä osa-alueet ovat seuraavat ja tämä kolmen osan jako on yleisesti hyväksytty ja esitetty muissakin lähteissä seuraavasti: Tiedon luottamuksellisuus, tiedon eheys sekä tiedon käytettävyys (kyberturvallisuuskeskus.fi, 2022). On olemassa myös muutamia muita tapoja määritellä tietoturvan osa-alueet, mutta tämä on luultavasti yleisin ja laajemmalti hyväksytty tapa.

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat käytettävissä (eli tarkasteltavissa tai luettavissa) vain niillä, keillä on siihen oikeus. Tiedon eheys puolestaan tarkoittaa sitä, että tietoja voivat muokata ainoastaan sellaiset henkilöt, jotka ovat siihen oikeutettuja. Tiedon käytettävyydellä taas tarkoitetaan sitä, että tietojärjestelmiä ja niissä säilytettävää tietoa pääsevät hyödyntämään vain sellaiset henkilöt, joille on määritelty oikeus niitä hyödyntää (kyberturvallisuuskeskus.fi, 2022).

Tämä tietoturvan määritelmän jako kolmeen osaan ei rajoitu ainoastaan tiedon säilyttämiseen ja sen tarkasteluun, vaan se määrittää oleellisesti myös sitä, kuinka tietoa siirretään järjestelmästä toiseen. Käytännön esimerkkinä voidaan ottaa vaikka tilanne, jossa sairaanhoitaja hakee tietoa potilaasta sairaalan potilastietokannasta, jolloin tiedon siirto tulee toteuttaa siten, että potilaan tietojen siirtyessä tietokannasta sitä hakevan sairaanhoitajan työaseman näyttöpäätteelle ei tietoa pysty kukaan kaappaamaan siten, että joku tietoihin oikeudeton voisi lukea potilaan terveystietoja (luottamuksellisuus) tai muokata niitä (eheys) taikka hyödyntää omiin vihamielisiin tarkoitusperiinsä (käytettävyys). Tietosuojavaltuutetun sivustolla todetaan seuraavasti:

> *Henkilötietojen käsittelyn on oltava luottamuksellista ja turvallista. Rekisterinpitäjän on arvioitava mahdollisia riskejä, organisaation tietosuoja- ja tietoturvaohjeistuksen tasoa sekä henkilötietojen teknistä suojausta. Suojatoimien riittävyyttä on punnittava suhteessa olosuhteisiin ja riskeihin. Suojatoimien tarkoituksena on varmistaa järjestelmien, palvelujen ja tietojen luottamuksellisuus, eheys ja saatavuus (tietosuoja.fi).*

2.2 Tietoturvan osa-alueet

Tietoturva voidaan jakaa, riippuen määrittelijästä, useaan eri osa-alueeseen, mutta niiden pääpiirteet ja sisällöt ovat määrittelijästä riippumatta suunnilleen samat. Seuraavissa kappaleissa käydään läpi yleisimpiä tietoturvan osa-alueita.

2.2.1 Yhteiset tietoturvakäytännöt

Yhteinen suunnitelma siitä, miten tietoturva organisaatiossa hoidetaan, muodostavat organisaation tietoturvakäytännön. Siihen sisältyvät yhteiset käytännöt, suunnitelmat ja ohjeet, jotka ovat kirjallisessa muodossa. Tästä näkökulmasta tietoturvaa tulee ajatella kokonaisuutena, joka kehittyy ja muuntuu jatkuvasti läpi koko organisaation elinkaaren. Lähtökohta on se, että oma IT-järjestelmä tunnetaan läpikotaisin sisältäen laitteet ja järjestelmät sekä käyttäjien oikeudet ja velvollisuudet sekä näihin liittyvät riskit ja uhat. Riskeihin ja uhkiin liittyy myös oleellisesti se, että niiden realisoituminen pyritään estämään tai ainakin rajaamaan niin pieneksi kuin on järkevää edellyttää (Frendy Oy, 2022).

2.2.2 Tietoturvakoulutus käyttäjille

Edellisessä alaluvussa käsitellyt toimet eivät yksin riitä. Veigan ym. (Veiga, A Da. Eloff, J H P, 2007) mukaan usein onkin sanottu, että käyttäjä on tietoturvan pahin vihollinen. Organisaatiossa on siis pidettävä huolta käyttäjien ajan tasalla pitämisestä kouluttamalla heitä tietoturvakoulutuksissa. Tärkeintä kouluttamisessa on se, että kouluttamisen tulokset jalkautetaan yrityksen jokapäiväiseen toimintaan.

Koulutus ei saada jäädä vain teoreettiseksi osaamiseksi (Frendy Oy, 2022). Jotta koulutus ei jää vain teoreettiseksi osaamiseksi, on sen jalkautusta hyvä seurata erilaisin menetelmin. Yksi menetelmä voi olla sisäinen tai ulkoinen auditointi tai tietoturvaan liittyvät testit henkilöstölle. Henkilöstö voi aluksi suhtautua vastustaen testeihin, mutta ne on hyvä tehdä arkipäiväiseksi osaksi yrityskulttuuria. Se voi kuitenkin vaatia paljon aikaa ja resursseja, niin kuin tietoturva ja muutokset yleisesti usein tarvitsevat toteutettuna huolellisesti.

2.2.3 Laitteiden suojaaminen teknisesti sekä fyysisesti

Seuraava askel tietoturvalliseen toimintaan on laitteiston suojaaminen ulkoisilta uhilta. Tavalliset työntekijät usein mieltävät, että tietoturvaa on ainoastaan se, että työaseman viruksentorjunta on päällä. Yrityksellä on todellisuudessa usein käytössä suuri määrä muita laitteita, jotka ovat myös alttiina tietoturvaloukkauksille. Näitä ovat esimerkiksi matkapuhelimet, tablettitietokoneet, verkkotulostimet ja oikeastaan kaikki sellaiset laitteet, jotka ovat tavalla tai toisella yhteydessä yrityksen IT-infrastruktuuriin. Näin ollen kaikki nämä pitää myös suojata tilanteen mukaan joko teknisesti tai fyysisesti ja useimmissa tapauksissa myös molemmilla (Frendy Oy, 2022).

Tekninen suojaaminen tarkoittaa Leijona Securityn mukaan seuraavaa:

> *Teknisen tietoturvan osa-alueet ovat työasema-, palvelin-, ja verkon tietoturva. Kokonaisuutena tekninen tietoturva on järjestelmien hallintaa, jolla pyritään yleisen tietoturvan tavoitteisiin.* (Leijona Security, 2022)

Tämä tarkoittaa käytännössä kaikkia niitä tietoturvan toimia, jotka ovat toteutettu ohjelmallisesti kuten viruksen torjunta, palomuurit, järjestelmien käyttöoikeudet, kaksivaiheinen tunnistautuminen järjestelmien ja laitteistojen ylläpito ja päivittäminen. Tämä tekninen osuus on yksi niistä osa-alueista, jotka peruskäyttäjä mielellään mieltää ainoaksi osaksi tietoturvaa, sillä näitä teknisiä kokonaisuuksia käyttävät nimenomaan ihmiset (kyberturvallisuuskeskus.fi, 2023).

Tämä ei kuitenkaan usein riitä vaan on otettava huomioon myös laitteiden ja IT-ratkaisujen fyysinen suojaaminen (kyberturvallisuuskeskus.fi, 2020). Fyysisen suojaaminen on harvoin mielletty osaksi tietoturvallista toimintaa, mutta se on yhtä tärkeää, ellei tietyissä tilanteissa jopa tärkeämpää kuin tekniset ratkaisut. Fyysinen suojaaminen kattaa tilanteesta ja organisaation koosta ja tyypistä riippuen valtavan määrän asioita alkaen kulunvalvonnasta aina jopa ilkivallan tekoon asti. Se sisältää myös asiakirjojen ja esimerkiksi lisenssitietojen yms. turvallisen säilyttämisen. Yksi esimerkki fyysisestä tietoturvasta on esimerkiksi se, kuinka näyttöpäätteet on suojattu ulkopuolisten katseilta, onko käytössä tietosuojakalvoja ovatko näytöt sijoitettu niin, ettei niiden takana ole esimerkiksi avoimia ikkunoita sellaiseen suuntaan, jossa asiaankuulumattomien henkilöiden on mahdollista nähdä arkaluontoista dataa.

2.2.4 Tietoturvastrategia ja hallinnollinen tietoturva

Yritykset voivat määritellä tietoturvastrategian. Tietoturvastrategiassa määritellään yrityksen sekä lyhyen- että pitkänaikavälin sisäinen tietoturvasuunnitelma. Tässä suunnitelmassa määritellään esimerkiksi tietoturvaan liittyvät roolit ja vastuut yrityksessä (Veiga ym. 2007). Tietyn tietoturvaroolin ja -vastuun saanut yrityksen työntekijä on vastuussa oman osa-alueensa toteuttamisesta, kehittämisestä ja raportoinnista esimerkiksi yrityksen tietoturvapäällikölle.

Nykyään puhutaan myös hallinnollisesta tietoturvasta, jolla on selkeä yhteys kaikkiin tietoturvaosa-alueisiin. Eniten se kuitenkin kulkee käsikädessä käyttäjien koulutuksen kanssa. Hallinnollinen tietoturva onkin vähemmän teknistä ja siinä keskitytään ennemminkin käyttäjien toiminnan suuntaamiseen koulutusten, kunnollisen ohjeistuksen sekä vaatimustason esillä pidon näkökulmista. Useimmilla organisaatioilla on nykyään käytössä monia isoja tietokantoja ja -järjestelmiä, ja ne asettavat myös mukanaan korkeita vaatimuksia tietoturvalle. Ne tuovat vaatimuksia esimerkiksi tiedonluokittelulle (esimerkiksi julkinen, sisäinen ja salassa pidettävä) tai fyysiselle turvallisuudelle. (2ns.fi, 2022).

Hallinnollisessa tietoturvassa määritellään myös paljon samoja asioita, jotka sisältyvät yrityksen tietoturvakäytänteisiin ja nämä käsitteet voidaankin nähdä osittain päällekkäisinä ja toisiinsa rinnastettavina käsitteinä. Hallinnolliselle tietoturvalle syntyy usein tarve vasta, kun yrityksen teknisiä tietoturvaratkaisuja on niin paljon, että niiden hallinointiin tarvitaan keskitettyjä toimintoja (2ns.fi, 2022).

2.3 Tietoturvallisen toiminnan hyödyt

2.3.1 Tietoturva ja viranomaismääräykset

Erilaisten IT-palveluita tarjoavien organisaatioiden ja yritysten tietoturvan tasoa säännellään viranomaisten määrittämillä oikeuksilla ja velvollisuuksilla. Liikenne- ja viestintävirasto kertoo Kyberturvallisuuskeskuksen verkkosivuillaan, että useille erityyppisille toimijoille on säädetty asetuksia, joiden puitteissa kyseisten toimijoiden on velvollisuus huolehtia verkkojen ja palveluiden tietoturvasta siltä osin kuin toimijat niitä tarjoavat. Toimijoille on määritetty myös tiettyjä oikeuksia velvollisuuksien lisäksi, jotta velvollisuudet voidaan täyttää. Nämä asetukset koskevat kyberturvallisuuskeskuksen mukaan laajaa joukkoa erilaisia IT-toimijoita, kuten esimerkiksi digitaalisia palveluita, toisin sanoen pilvipalveluita tarjoavia toimijoita. Saman sääntelyn alle menevät myös muun muassa hakukoneet, viestinnän välittäjät sekä teleyritykset (Kyberturvallisuuskeskus.fi, 2022).

2.3.2 Tietoturva yrityksen oman toiminnan turvaamiseksi

Tietoturvallinen toiminta on ennen kaikkea oman toiminnan suojaamista ja yritykseltä olisi erittäin lyhytnäköistä toimintaa olla investoimatta ja toteuttamatta tietoturvallista liiketoimintaa. Monilla yrityksillä ei kuitenkaan ole tarvittavaa osaamista yrityksen sisällä toteuttaakseen laadukasta tietoturvaa (yrittajat.fi). Yritysten tulee myös vastata lain velvoittamiin vaateisiin sekä kaikista sen ulkopuolelle jäävistä tietoturvan osista, jotka on myös tärkeää ottaa huomioon tietoturvaa suunnitellessa. Tämän vuoksi monet yritykset ulkoistavat ainakin teknisen suojaamisen ja ostavat myös ulkopuolisilta asiantuntijoilta ja palveluntarjoajilta koulutuksia käyttäjilleen. Kuten mainittua jo laki ja kansainväliset asetukset vaativat tietyn tyyppisiltä yrityksiltä tietyn tasoista toimintaa tietoturvan takaamiseksi.

Tietoturva ei siten suinkaan toteudu ilmaiseksi, vaan vaatii yrityksen johdolta selkeää tahtotilaa investoida laadukkaaseen tietoturvaan. Tietoturvaan investoiminen onkin nykyisessä tietojärjestelmiin perustuvassa länsimaisessa yhteiskunnassa välttämätöntä. Lyhyellä tähtäimellä yrityksen hyöty tästä investoinnista on yrityksen jokapäiväisen toiminnan suojaaminen ulkoisilta uhilta ja tietoturvahyökkäyksiltä ja -onnettomuuksilta. Pahimmillaan koko yrityksen toiminta voi halvaantua pitkäksi aikaa, jos tietoturva on toteutettu alimitoitetusti.

Pitkällä tähtäimellä laadukkaasti toteutettu tietoturva ja erityisesti hallinnollinen tietoturva säästää myös yrityksen varoja. Se ohjaa toimintaa kustannustehokkaaksi, kun tietoturvaan tehdyt toimenpiteet kohdennetaan oikein ja käytetyt resurssit eivät mene hukkaan. Toinen iso yrityksen saama hyöty on yrityksen tietoturvantason mukanaan tuoma kypsyystaso tai sertifikaatti, joka taas on suuri etu esimerkiksi kilpailutustilanteissa kolmansille osapuolille. Monesti kilpailutuksissa toimivat osapuolet nimittäin haluavat toimia sellaisten organisaatioiden kanssa, jotka toimivat tietoturvan suhteen vastuullisesti. Nykyään tämä on usein jo ehto monille sopimuksille eri organisaatioiden välillä (2ns.fi, 2022).

2.3.3 Tietoturva yrityksen asiakkaan näkökulmasta

Edellisessä alaluvussa viitattiin nykyisen sopimus- ja kilpailutusilmapiirin muutoksesta. Nykyään asiakkaat eivät välttämättä valitse yhteistyökumppaneikseen sellaisia yrityksiä, joiden hallussa ollessaan heidän tietonsa ja ostamansa palvelut eivät ole turvassa. Joissain tapauksissa esimerkiksi julkisella sektorilla (kuten julkiset terveyspalvelut) ovat tietyt tietoturvalliset toimintatavat edellytyksiä ja vaatimuksia sopimusten solmimiseen (finlex.fi, 2022). Myös Euroopan Unionin Yleinen tietosuoja-asetus (GDPR) tuo omat vaatimustasonsa tietoturvan toteuttamiselle, mutta kuitenkin vain siitä näkökulmasta, että mitä seuraamuksia yritykselle asetetaan, jos asiakkaiden tiedot onnistutaan varastamaan esimerkiksi asiakasrekisteristä tai joku yrityksen sisältä pääsee niihin käsiksi ilman oikeutusta (europa.eu, 2022). Laadukkaasti toteutettu tietoturva myös lisää osapuolten välistä luottamusta.

2.4 Tietoturvan nykyisiä standardeja

Tietoturvan standardoimisessa käytetään yleisesti hyväksyttyjä kansainvälisiä standardeja. Standardin tehtävä on osoittaa, että sen haltija toimii kyseisen standardin vaatimusten mukaisesti. Standardi on joukko sääntöjä, jotka yhtä aikaa toteutuessaan luovat kokonaisuuden, jonka mukaan on sitouduttu toimimaan. Tietoturvastandardeista tunnetuimmat ovat ISO- ja NIST-standardi perheet. ISO-standardeista yksi tunnetuimmista on ISO/IEC 27001, joka käsittää lähinnä yrityksen sisäisiä toimintoja ja niiden toteuttamista tietoturvallisesti. Standardien vaatimuksia päivittävät ja ylläpitävät muuttuvaa toimintaympäristöä vastaaviksi kansainväliset standardointijärjestöt.

2.4.1 Tietoturvastandardien hyödyt yleisesti

Kuten tutkittua, tuovat standardit yleensä (sfs.fi), kuten myös tietoturvastandardit mukavaan monia etuja. Ne helpottavat yritysten kanssakäymistä keskenään ja vähentävät tiettyjen selvitysten ja paperityön määrää. Yritykset voivat tietyillä sertifikaateilla osoittaa toisilleen jo ennen yhteistyön solmimista tai neuvotteluvaiheessa noudattavansa tiettyjä tietoturva asetuksia ja toimia. Sertifikaatteja on luotu moniin eri tarkoituksiin. Osa kuvaa yrityksen sisäistä toimintaa ja toiset kertovat yritysten asiakkailleen tuottamien palveluiden laadusta. Näin yritykset varmistavat lakisääteisten ja sopimusluontoisten vaatimusten noudattamisen ikään kuin automaattisesti. Tietystikään standardien hyödyt eivät rajoitu vain sopimusten laatimiseen, vaan niistä on suora hyöty myös yritysten tietoturvaan ja ydintoimintojen jatkumiseen mahdollisista poikkeusoloista huolimatta. Standardit ovat myös osa yritysten vastuullisuutta yhteiskunnassa. Niiden mukaisesti toimiminen vähentää laajoja tietovuotoja sekä jopa ulkoisen ja tahallisen sabotaasin aiheuttamista. Nykyisessä muuttuneessa kansainvälisessä tilanteessa ei voida liioitella, kun todetaan, että standardien noudattaminen estää jopa valtioiden välistä vakoilua, sillä jopa yksityishenkilöiden, puhumattakaan yrityksistä, laitteita voidaan käyttää välikappaleina vakoilulle ja esimerkiksi palvelunestohyökkäysten kohdentamiseen yksityisiin ja valtiollisiin toimijoihin.

2.4.2 ISO/IEC 27001

ISO27000-standardiperhe on määritelty vuonna 2005 ja on sittemmin tullut laajalti tietoon sekä käyttöön. Standardeja on päivitettyä vuosien varrella useasti vastaan muuttuviin olosuhteisiin. ISO27001-standardi sisältyy tähän perheeseen. ISO-standardit tarjoavat maailmanlaajuisesti tunnustetun viitekehyksen parhaille mahdollisille tietoturva käytänteille. ISO27000-standardiperhe lähtee liikkeelle siitä, että se ei ole riippuvainen toimittajista tai myyjistä eikä organisaation käytössä olevista teknologioista. Sen on myös tarkoitus olla toiminnallinen kaikenlaisille organisaatioille riippumatta niiden koosta, alasta tai luonteesta. Sitä voidaan käyttää niin julkisella kuin yksityisellä sektorilla. ISO27000-perheen standardit eivät määrittele käytettäviä teknologioita tai niiden kriteerejä vaan ovat ennemminkin toiminnanohjaus metodeja. Nämä standardit eivät rajoitu maantieteellisesti rajattuihin sijainteihin, vaan ne ovat käytettävissä ympärimaailmaa. Huolimatta siitä, että ISO-perhe sisältää monia eri standardeja, ne ovat suunniteltu siten, että ne ovat yhdisteltävissä eivätkä ole ristiriidassa keskenään (Calder A, 2013).

ISO27001-standardissa määritellään suuri määrä erilaisia tilanteita, joihin standardin täyttävän yrityksen on vastattava kirjallisesti ja kuvailtava seikkaperäisesti, miten kyseiset

tilanteet ja tietoturvan osa-alueet on yrityksessä huomioitu tai miten niihin on varauduttu. Standardin mukaisia osa-alueita voivat olla esimerkiksi tietoturvaorganisaation määrittely, turva-alueidin määrittely, kulku- ja pääsyoikeuksien hallinta, ennalta määrätyt toimintamallit tietoturvauhan realisoituessa ja niin edelleen. Yrityksellä tulee olla olemassa näihin vaatimuksiin huolelliset dokumentaatiot sillä ne vaikuttavat sekä yrityksen toimintaan että standardin myöntämiseen.

2.5 Organisaatioiden haasteita tietoturvan toteutuksessa

Tietoturva Pro kertoo (Tietoturva Pro, 2019) kertoo yritysten olevan edelleen heikosti varautuneita tietoturva uhkiin. Tietoturva Pro viittaa Vakuutusyhtiö If:n vuonna 2017 julkaisemaan kyselytutkimukseen. Kyselyn tuloksista ilmenee, että 29 prosenttia pienistä- ja keskisuurista yrityksistä on joutunut rikoksen merkit täyttävän tietoturva yrityksen kohteeksi ja niistä reilu viidesosa on jopa onnistunut. Samasta tutkimuksesta ilmenee myös, että heidän yrityksensä ei ole varautunut riittävällä laajuudella tietoturvauhkia vastaan. Näin myönsi peräti kolmasosa kyselyyn vastanneista yrityksistä. Tämä tutkimus kattoi 100 pk-yritystä ja siihen vastasivat yritysten tietoturvavastaavat.

Edelleen tästä kyselystä selviää myös se, että tuolloin (elokuussa 2017), eivät kyselyyn vastanneet yritykset olleet varautuneet millään asteella myöhemmin toukokuussa 2018 voimaan astuvaan EU:n tietosuoja-asetukseen.

Usein sanotaan, että käyttäjä on tietoturvan heikoin lenkki. Tämä johtuu suurimmalta osin tiedon ja tietoturvakoulutuksen puutteesta. Oikeanlaisella kouluttamisella monet inhimillisistä virheistä johtuneet tietoturvarikkeet ja -onnettomuudet olisi voitu ehkäistä. Tätä koulutusta valitettavasti aina ole käyttäjän saatavilla johtuen yrityksen huonoista tietoturvakäytänteistä, sillä vaikka jopa yrityksen johto olisi motivoitunut toimimaan tietoturvallisesti ei heilläkään ole välttämättä tarvittavaa osaamista tai keinoja sekä resursseja korjata ongelmaa. Työntekijöiden koulutus ja tietoturvan korostaminen arjen rutiineissa ovat siis ensimmäinen askel tietoturvassa onnistumiseen.

Aina pelkkä koulutuskaan ei riitä. Yrityksen koosta ja luonteesta riippuen tietoturvan toteuttamiseen saatetaan tarvita myös suuria taloudellisia investointeja ja niitä ei ole aina mahdollista tehdä, vaikka yritys voi joutua maksamaan näistä laiminlyönneistä mittavan hinnan sekä suorasti että välillisesti tietoturvauhkien realisoituessa. Näitä taloudellisia investointeja voivat olla virustorjunta ohjelmistot, palomuurit ynnä muut tekniset ratkaisut, mutta kuten aiemmin mainittua tietoturva ei ole vain tietoteknisiä ratkaisuja. Myös toimitilat on suojattava asianmukaisesti kuten fyysisen tietoturvan käsitteestä käy ilmi.

2.5.1 Tietoisuus tietoturvallisesta toiminnasta

Osa yrityksistä herää tietoturvan tarpeellisuuteen vasta, kun yritys on kasvanut riittävän suureksi ja viranomaisten asettamat velvoitteet sekä asetukset alkavat vaatia tietyn tasoista toimintaa. Vaatimukset voivat tulla joko valtakunnalliselta tai kansainväliseltä tasolta, kuten EU:lta. Toki tietoturvaan liittyvät ongelmat ovat olleet viime aikoina laajemmin osana julkista keskustelua, ja yritykset ovat heränneet tietoturvan tarpeeseen myös sitä kautta (kauppakamari.fi). Myös yrityksen asiakkaat tai yhteistyökumppanit saattavat vaatia tiettyjä standardeja, jotta voivat solmia sopimuksia eri toimijoiden kanssa. Tallaisia voivat olla esimerkiksi valtiolliset toimijat tai terveydenhuollon toimialoilla työskentelevät yritykset, joita viranomaiset velvoittavat käyttämään vain tietyn standardin omaavia kumppaneita.

2.5.2 Yrityksen resurssit

Yrityksen haasteet tietoturvan laadukkaaseen toteuttamiseen ei rajaudu aina vain tietoisuuden puutteeseen. Vaikka yrityksellä olisikin tietoisuus tietoturvan tarpeellisuudesta, ei sillä välttämättä ole osaamista tai riittäviä henkilöresursseja toteuttaa laadukasta tietoturvaa puhumattakaan standardien hankkimisesta, johon liittyy pelkästään jo paljon dokumentaatiota sekä ISMS:n (tietoturvan hallintajärjestelmä) ylläpitoa sekä poikkeamien korjaamista, joita standardin myöntämiseksi vaadituissa auditoinneissa havaitaan.

Tällaisissa tilanteissa yritykset monesti pyrkivät ulkoistamaan tietoturvan toteutuksen tai standardeja hankkiessaan turvautuvat konsultaatioon. Ulkoisten toimijoiden hyödyntäminen ei ole itsestään selvää, sillä sekin vaatii yritykseltä tahtotilaa priorisoida budjettiaan ulkoisen toimijan käyttämiseen.

3 Projektin toteutus

3.1 Projektin suunnittelu ja projekti kokonaisuutena

3.1.1 Projektin osa-alueet

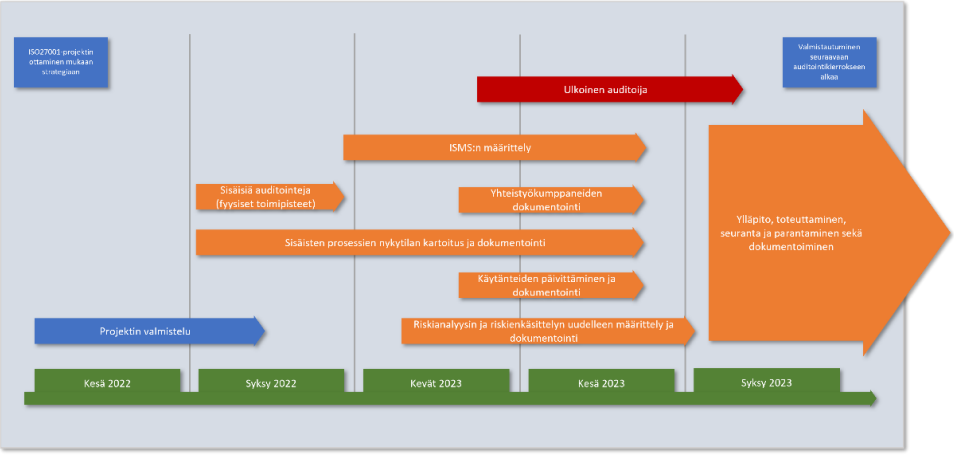
Opinnäytetyö toteutettiin projektina toimeksi antavalle yritykselle, jonka tavoite oli saada ISO27001-sertifikaatti. Projekti alkoi syksyllä 2022 ja päättyi syksyllä 2023, jolloin toimeksi antavalle yritykselle myönnettiin tavoiteltu sertifikaatti. Tämän opinnäytetyön kirjoittaja osallistui vahvasti projektin lähes kaikkiin vaiheisiin sekä suunnitellen että toteuttaen projektia yhdessä siihen perustetun työryhmän sekä muiden tiimien kanssa.

Projektin toteuttamista voidaan jossain määrin luonnehtia iteratiivikseksi eli vaiheittaiseksi, johtuen sertifikaatin auditointisykleistä. Toteutuksen aikana projektiin valittu työryhmä teki parannuksia edellisiin projektin vaiheisiin auditoijalta saadun palautteen mukaisesti. Myös yrityksen sisäinen prosessi kehittyi iteraation myötä.

Seuraavissa kappaleissa kuvaillaan projektin keskeisimpiä osa-alueita ja määritellään tarkemmin tiettyä terminologiaa, joka liittyy oleellisesti ISO27001-standardiin sekä tietoturvaan. Osa-alueet eivät ole täysin kronologisessa järjestyksessä eivätkä tärkeys järjestyksessä. Kriittisten osa-alueiden prioriteettia on korostettu erikseen sitä käsittelevässä kappaleessa.

3.1.2 Projekti aikajanalla

Projekti alkoi kesällä 2022 ottamalla sertifioituminen ISO27001-standardin mukaisesti osaksi yrityksen strategiaa. Kuviossa 1 näkyvälle aikajanalle on sijoitettu projektin eri vaiheet.



Kuvio 1. Projektin vaiheet aikajanalla

Oranssilla pohjalla olevat tehtävät ovat yrityksen sisäistä käytännön toteutusta. Sinisellä pohjalla olevat merkinnät kertovat hallinnollisesta työskentelystä yrityksen sisällä. Ulkoisen auditoinnin osuus on merkitty punaisella pohjalla.

3.1.3 Projektin aloitus

Projekti aloitettiin toimeksi antavan yrityksen johdon halusta saavuttaa ISO27001-standardin mukaiset vaatimukset sekä näin sertifioitua ISO27001-standardin mukaiseksi. Sertifioitumisella haluttiin saavuttaa hyötyä yrityksen kasvussa asiakashankinnan kautta. Se myös mahdollistaisi ISO27001-markkinointimateriaalin hyödyntämisen. Sertifikaatin saaminen kasvattaa myös uskottavuutta.

Projektia aloittamista oli suunniteltu aiemmin vuonna 2022 ja projekti aloitettiin syksyllä 2023. Tiettyjä osia standardin saavuttamiseksi oli ollut olemassa jo aiemmin johtuen toimeksi antavan yrityksen historiasta, mutta kyseiset osiot tuli saattaa yrityksen nykymuotoa vastaavaksi. Kyseisten osa-alueiden päivitystarpeen kartoitukseen käytettiin paljon aikaa syys-marraskuussa 2022 sekä niiden saattamista käytössä oleviin tietojärjestelmiin sekä dokumentaatioon. Osa aiemmin käytössä olleesta datasta oli tallessa poistuvissa tietojärjestelmissä ja oli siirrettävä helpommin käytettävissä oleviin paikkoihin.

Projektin toteuttavaan työryhmään kuuluivat projektipäällikkö sekä projektityöntekijä. Lisäresursseja ja tukea he saivat konsultoimalla muita tiimejä yrityksen sisäisesti.

3.1.4 Tietoturvan hallintajärjestelmä (ISMS)

Sertifioitumisprosessissa tulee määrittää tietoturvanhallintajärjestelmä (ISMS, Information Security Management System). ISMS tarkoittaa tapaa, jolla yrityksen tietoturvaa hallinnoidaan. Siihen liittyy myös dokumentaation säilyttäminen. Muita ISMS:n tehtäviä on esimerkiksi tietoturvaohjeistuksen jalkautushenkilöstölle. ISMS:ään myös kirjataan havaitut poikkeamat sekä niiden käsittelyn ja korjaamisen tila. Käytännössä kaikki, mikä liittyy tavalla tai toisella yrityksen tietoturvaan, tulisi löytyä jotenkin linkitettynä ISMS:ään. ISMS voi olla toteutettu esimerkiksi paperisena dokumentaationa tai joukkona sähköisiä tiedostoja, jotka säilytetään esimerkiksi yrityksen verkossa. Kehittyneempi tapa on ostaa kolmannen osapuolen tarjoama ohjelmisto, jonka avulla ylläpidetään yrityksen tietoturvaa. Toimeksi antavassa yrityksessä siirryttiin kolmannen osapuolen tarjoamaan ISMS-järjestelmään. Käytössä on edelleen jonkin verran kyseisen ohjelmiston ulkopuolella olevaa dokumentaatiota, sillä sitä ei ole vielä tarkoituksen mukaista siirtää käytössä olevaan ISMS-järjestelmään. Käyttöön onkin tällä hetkellä otettu hybridimalli, jossa suurin osa esimerkiksi dokumentaatiosta on varsinaisessa ISMS-järjestelmässä, mutta osa dokumentaatiosta on nähty

tarpeelliseksi säilyttää erijärjestelmissä. Dokumentaation säilytyspaikkoja arvioidaan tulevaisuudessa uudelleen.

Toimeksi antavan yrityksen ISMS-järjestelmä valittiin seuraavin kriteerein: tietoturvallinen järjestelmä, joka integroituu helposti osaksi yrityksen nykyisiä järjestelmiä. ISMS:n on kevyt ylläpitää ja ottaa käyttöön. Varsinainen järjestelmä ei saa aiheuttaa tarpeetonta vaivaa järjestelmänä.

Hinta-laatu-suhteeltaan täydellistä järjestelmää ei ole olemassa, ja siksi toimeksi antavassa yrityksessä käytetään myös osittain ISMS-pääjärjestelmän ulkopuolisia säilytyspaikkoja dokumentaatiolla ja ohjeistukselle. Ohjeistus tullaan jalkauttamaan täysin ISMS:n pääjärjestelmällä lähitulevaisuudessa.

3.1.5 Hyväksi havaitut työvälineet ja käytännöt projektin aikana

Auditointia varten ISO27001-työryhmä oli saanut käyttöönsä normaaleiden työvälineiden lisäksi mahdollisuuden kartoittaa tehokkaamman ISMS:n hankkimiseksi. Kun uusi ISMS-järjestelmä hankittiin ulkoiselta järjestelmäkehittäjältä, työ sertifioinnin saavuttamiseksi tehostui huomattavasti. Edelleen ohella käytettiin myös alkuperäisiä dokumentaatioita, jotka olivat esimerkiksi Excel-, PowerPoint- sekä Word-tiedostoja, joita säilytettiin toimeksi antavan yrityksen järjestelmissä. Niitä päivitettiin, mutta hybridimalli nähtiin toistaiseksi hyväksi ratkaisuksi, vaikka ulkoinen ISMS-järjestelmä olikin hankittu. Ulkoisessa ISMS-järjestelmässä on tiettyjä puutteita, jonka vuoksi kaikkea dokumentaatiota sinne ei haluttu viedä. Puutteista on viestitty ISMS:n järjestelmäkehittäjälle, ja he ovatkin jo kehittäneet palveluaan toivottuun suuntaan.

Hyväksi työmenetelmäksi havaittiin nopeasti ryhmätyöskentely ISO27001-työryhmässä. Työryhmä oli projektin työmäärän nähden verrattain pieni, kaksi työntekijää. Työryhmän projektipäälliköllä oli hoidettavanaan myös muita toimeksi antavan yrityksen sisäisiä tehtäviä ja työryhmän toinen työntekijä edisti projektia syksyllä 2022 osa-aikaisesti, kunnes huomattiin tarve suuremmalle panokselle, jonka jälkeen keväällä 2023 tämä työsti projekti lähes kokoaikaisesti, joskin hän hoiti samaan aikaan myös toimeksi antavan yrityksen sisäisiä mobiililiittymiä. ISO27001-projektin kanssa työskentely oli siitä huolimatta päivittäistä. Käytännön työtä tehtiin siis paljon projektityöntekijän ja projektipäällikön välillä Teamsin kautta ryhmätyöskentelynä. Kummallakaan ei ollut aikaisempaa kokemusta sertifioinneista, joten aikaa ja resursseja käytettiin paljon uuden opetteluun. Erityisesti dokumentointia toteutettiin ryhmätyöskentelynä.

Jonkin verran tehtiin myös yhteistyötä ISMS:n kehittäjän kanssa. Heiltä saatiin arvokasta tietoa muun muassa webinaarien ja ohjepankkien kautta. Ohjeistukset eivät liittyneet

ainoastaan ISMS:n käyttöön vaan niissä otettiin myös laajasti näkökulmia auditointeihin valmistautumiseen ja tärkeisiin seikkoihin sertifioinnissa painotettaviin kohtiin.

Toimeksi antavalla yrityksellä oli jonkin verran aiempaa kokemusta ISO27001-sertifioitumisesta, ja näitä tahoja hyödynnettiin yrityksen sisäisesti tarvittaessa.

3.2 Sisäiset ja ulkoiset auditoinnit

3.2.1 Fyysisten toimipisteiden kartoitus

Yrityksen fyysinen turvallisuus arvioidaan myös sertifioitumisprosessissa. Teimme toimeksi antavan yrityksen sisäisen auditoinnin koskien toimipisteiden fyysistä turvallisuutta syksyllä 2022. Tulokset ja havainnot parannusehdotuksineen kerättiin ISMS:ään ja ne lisättiin myös riskiarviointiin. Auditoinneissa havaitut puutteet arvioitiin ja niistä saatiin todennäköisyys-vaikutus-suhdeluku. Tämän suhdeluvun perusteella tehtiin arvio puutteen korjaamisen tavasta ja kiireellisyydestä. Toimipisteillä havaittiin puutteita, joskaan niistä yhdessäkään ei ollut kyse kriittisestä haavoittuvuudesta.

3.2.2 Yhteistyökumppaneiden kartoitus

Toimeksi antavan yrityksen yhteistyökumppaneista, kuten tavarantoimittajat, järjestelmätoimittajat, laitoshuolto, viranomaiset, oli olemassa dokumentaatiota, mutta se tuli päivittää. Dokumentaatiota päivitettiin loppukeväästä ja alkukesästä 2023. Dokumentaatio oli tässä kohtaa osittain yleisluontoista, mutta kriittiseksi luokitelluista kumppaneista on olemassa tarkempi kartoitus. Yhteistyökumppanit luokiteltiinkin myös kriittisyysasteikolla. Kriittisten toimijoiden kanssa järjestetään toistuva turvallisuus arviointia ja heidän sitoutumistaan toimeksi antavan yrityksen tietoturvakäytänteisiin tullaan seuraamaan säännöllisesti yhteistyöpalavereissa heidän edustajiensa kanssa. Osa yhteistyökumppaneista on globaaleja suuryrityksiä, jolloin heidän kanssaan on haastavaa järjestää seurantaa, jolloin palveluiden tietoturvallinen toteutus jää toimeksi antavan yrityksen vastuulle. Tällöin on seurattava tarkasta yhteistyökumppanin toimintaa ja tiedotusta esimerkiksi heidän toimittamistaan järjestelmäpäivityksistä tai havaitsemistaan tietoturvahaavoittuvuuksista toimittamissaan järjestelmissä.

3.2.3 Sisäiset auditoinnit

Toimeksi antavan yrityksen kanssa on laadittu myös sisäisten auditointien vuosikello. Tämä sisältää muun muassa sisäisiä toimipisteauditointeja sekä auditointeja käytössä oleviin

järjestelmiin sekä liiketoimintoihin. Sisäiseen auditointiin ei oteta mukaan ulkoista auditoijaa. Sisäisten auditointien tehtävä on ylläpitää ja parantaa tehtyjen havaintojen perusteella yrityksen tietoturvaa ulkoisten auditointien välillä. Sisäiset auditoinnit ovat sertifioinnin kannalta pakollisia, mutta ovat muutenkin osa yrityksen vastuullista tietoturvaa.

Sisäisten auditointien suorittamiseen on merkitty omistaja ja hän vastaa auditoinnin toteuttamisesta vuosikellon mukaisesti. Sisäiseen auditointiin on tehty dokumentaatio, josta ilmenee tarkastettavat asiat. Omistaja nimeää etukäteen muut sisäiseen auditointiin liittyvät työntekijät ja asiantuntijat. Esimerkiksi sisäisessä toimipiste auditoinnissa kyseisen toimipisteen toimistovastaava osallistuu auditointiin. Sisäisestä auditoinnista tehdään dokumentaatio ISMS:ään. Dokumentaatioon kirjataan muun muassa havaitut puutteet korjausehdotuksineen. Sisäistä auditointia seuraa aina myös jälkiauditointi, jossa tarkistetaan mm. varsinaisessa auditoinnissa havaittujen puutteiden korjaustoimenpiteiden edistyminen. Lopulta sisäisen auditoinnin omistaja hyväksyy auditoinnin erivaiheineen valmiiksi. Dokumentaatiot sisäisistä auditoinneista esitellään toimeksi antavan yrityksen johdolle säännöllisissä johdon katselmoineissa.

3.2.4 Ulkoinen auditointi, poikkeamat ja sertifikaatin myöntäminen

Ulkoinen auditointi on viimeinen työvaihe sertifioinnissa. Ennen lopullista sertifiointia ulkoinen auditoija hyväksyttää saamansa tulokset organisaatiollaan, joka hakee vielä hyväksynnän standardin kansainväliseltä katto-organisaatiolta.

Ulkoisessa auditoinnissa auditoijalle ilmoitettiin kaikki toimipisteet, jotka toimeksi antava yritys halusi sertifikaatin piiriin. Näistä valittiin auditoinnin ensimmäiselle kierrokselle tietyt toimipisteet syvempään tarkasteluun ja ne kierrettiin myös fyysisen tietoturvan näkökulmasta toukokuun 2023 aikana yhdessä auditoijan kanssa. Ulkoinen auditoija kirjasi ylös havaitsemiaan poikkeamia, joista saimme kehotukset korjauksiin sekä aikataulun niiden toteuttamiselle. Ensimmäisessä deadlinessa tuli esitellä suunnitelmat poikkeamien korjaamiseksi ja seuraavassa tuli esitellä kuinka poikkeamien korjaaminen oli aloitettu sisäisesti laaditun suunnitelman mukaisesti.

Ulkoinen auditointi ei rajoittunut ainoastaan fyysisten toimipisteiden auditointiin, vaan toimeksi antava yritys esitteli myös muita kokonaisuuksia, kuten ISMS:n käyttöä, prosessikuvauksia kriittisistä toiminnoista, tietoturvaohjeistuksien jalkautusta, riskien analysointia sekä niiden käsittelyä. Ensimmäisen kierroksen pääauditointi oli kattava läpileikkaus toimeksi antavan yrityksen tietoturvakäytäntöihin sekä -ratkaisuihin. Se antoi myös yritykselle hyvän mielikuvan nykytilanteesta, sen puutteista ja vahvuuksista. Ensimmäisellä

auditointikierroksella painotettiin vahvasti dokumentaation tärkeyttä ja sen tila paranikin huomattavasti ensimmäisten toimipiste auditointien välillä, sillä auditoija antoi hyvissä ajoin parannuskohteita ja niihin ehdittiin reagoida tehokkaasti jo ensimmäisen kierroksen aikana.

Kesän 2023 loppupuolella varsinaista auditointia seurasivat niin kutsuttua seuranta-auditointia ja myöhemmin tarkastusauditointi. Seuranta-auditoinnissa käytiin yhdessä auditoijan kanssa läpi, onko toimeksi antava yritys lähtenyt tekemään korjaustoimenpiteitä ilmoitetuista poikkeamista haluttuun suuntaan. Myöhemmässä tarkastusauditoinnissa käytiin läpi lopulliset kriteerit liittyen toukokuussa 2023 ilmoitettuihin poikkeamiin. Toimeksi antavan yrityksen ISO27001-työryhmä oli saanut poikkeamat pääosin korjattua ja ulkoinen auditoija lähetti auditointi esityksensä kotimaan organisaation kautta kansainväliselle katto-organisaatiolle, joka myönsi ISO27001-sertifikaatin toimeksi antavalle yritykselle. Toimeksi antava yritys sai sekä sähköiset että fyysisen version sertifikaatista sekä viralliset ISO27001-markkinointimateriaalit käyttöohjeineen käytettäväkseen.

Lisäksi tulee mainita, että osa ulkoisista auditoinneista voitiin hoitaa etäyhteydellä. Kriittisimmät toimipisteet auditointiin luonnollisesti paikan päällä. Toimeksi antavan yrityksen ISO27001-työryhmä vastasi auditointien sujuvasta kulusta niiden aikana ja järjesti paikalle kulloinkin käsiteltävästä aiheesta asiantuntivimmat työntekijät, jotta auditoijalle saatiin kattava kokonaiskuva nykytilasta. Auditoinnin aikana suoritettiin myös työntekijöiden haastatteluja, joissa he kertoivat työstään tietoturvan näkökulmasta ja vastasivat auditoijan esittämiin tarkentaviin kysymyksiin.

Toimeksi antavassa yrityksessä oli entuudestaan tehty riskianalyysiä, mutta yrityksen luonteen muuttuessa sitä oli päivitettävä. Riskianalyysi on tehty kattavaksi yhdessä Tietoturvatiimin kanssa ja sitä tarkastellaan ja päivitetään säännöllisesti sekä tiettyjen kriteerien täyttyessä jo ennen vuosikellon ajankohtia. Riskianalyysi johtaa väistämättä myös riskien käsittelyyn ja siihen on määriteltävä prosessi. Prosessissa kuvataan esimerkiksi, kuinka toimeksi antava yritys puuttuu havaittuihin riskeihin. Tätä arviointia tehdään esimerkiksi aiemmin mainitun todennäköisyys-vaikuttavuus-suhdeluvun avulla. Riskien käsittelyyn on määritelty myös prosessi, kuinka yrityksen työntekijät ilmoittavat havaitsemistaan poikkeamista ja tietoturvahäiriöistä. ISMS:n pääkäyttäjät ja tietoturvatiimi yhdessä toteuttavat riskianalyysin ylläpitoa sekä riskien käsittelyä ja ottavat mukaan sisäisesti määritellyn prosessin mukaisesti muiden tiimien asiantuntijoita.

3.3 Prosessit ja dokumentaatio

3.3.1 Dokumentaatio

Dokumentaatio on erittäin suuressa roolissa ISO27001-standardoitumista. Dokumentaation tulee olla tarkoitukseen nähden varsin kattavaa ja sitä tulee ylläpitää säännöllisesti. Dokumentaation tulee olla myös saatavilla (vain) asiaankuuluville työntekijöille helposti, mutta kuitenkin siten, ettei dokumentaation turvallisuus vaarannu. Dokumentaatiota voidaan tehdä esimerkiksi käytössä olevista järjestelmistä tai toimintamuodoista ja prosesseista. Näin tehtiin myös toimeksi antavan yrityksen projektissa.

Dokumentaation kattavuuteen vaikuttaa erityisesti sen käyttötarkoitus. Kun dokumentaatiota laadittiin eri osa-aluille, tuli ottaa huomioon dokumentoitavan kokonaisuuden tarkoitus ja tärkeys yrityksen toiminnoille. Dokumentaation tärkeyttä voidaan arvioida kriittisyysasteikolla esimerkiksi matala – normaali – tärkeä – kriittinen. Kriittiset kokonaisuudet dokumentoitiin yksityiskohtaisemmin, kun taas matalan prioriteetin kokonaisuudet dokumentoitiin huomattavasti kevyemmin tai ei ollenkaan – tarkastellaan tarvittaessa -periaatteella.

Kullekin dokumentaatiolle määriteltiin omistaja. Omistajalla tarkoitetaan työntekijää, joka on vastuussa kyseisen dokumentaation paikkansapitävyydestä sekä ylläpidosta. Dokumentaation omistajan ei tule välttämättä olla dokumentaatiota vastaavan aihealueen paras asiantuntija yrityksessä, mutta hänen vastuullaan on varmistaa, että aihealueen paremmin tuntevat työntekijät pitävät dokumentaatiota yllä. Dokumentaatiota ja sen ajantasaisuutta tulee tarkastella ja arvioida omistajan johdolla säännöllisesti. Säännöllisyys voi tarkoittaa esimerkiksi vuosittaista dokumentaation läpikäynti palaveria, johon osallistuvat omistajan koolle kutsumat yrityksen asiantuntijat. Jos dokumentaatio on luokiteltu kriittiseksi tai se on luonteeltaan altis muutoksille, on tällöin arviointia toteutettava tiheämmällä syklillä, esimerkiksi 3 tai 6 kuukauden välein. Dokumentaation ajantasaisuuden arviointi merkittiin tietoturvanhallintajärjestelmän (ISMS, Information Security Management System) vuosikelloon, joka automaattisesti muistuttaa dokumentaation omistajaa tarkastusajankohta lähestyessä.

Dokumentaatiota säilytettiin projektivaiheessa DRAFT-tiedostoina projekti kansiossa ja sitä mukaa kun dokumentaatiota valmistui, sitä siirrettiin saataville asianmukaiselle henkilöstölle. Kaikki dokumentaatio ole ollut avointa koko henkilöstölle ja osa dokumentaatiosta (varsinkin kriittiseksi luokiteltu dokumentaatio) onkin käyttöoikeuksien takana.

Kuten aiemmin todettu, on dokumentaatio todella tärkeässä roolissa ISO27001-sertifioinnissa. Ulkoinen auditoija, joka myöntää sertifikaatin, kiinnittää erityistä huomiota dokumentaation laajuuteen kolmevuotisen auditointi kierroksen ensimmäisessä vaiheessa. Tämän

vuoksi dokumentaatio on tehtävä erityisen huolellisesti ja siihen panostettiin toimeksi antavan yrityksen sertifioitumisessa erityistä huomiota.

3.3.2 Sisäisten prosessien kuvaaminen

Sisäset prosessikuvaukset määriteltiin olemassa olevien prosessikuvausten perusteella nykyistä yritysmuotoa vastaaviksi syksyn 2022 ja kesän 2023 välillä. Prosessilla tarkoitetaan jonkin toiminnon säännönmukaisuutta yrityksessä ja tapaa hoitaa tietyt toiminnot (esimerkiksi liittymänavaus uudelle työntekijälle tai sen sulkeminen työntekijän poistuessa yrityksen palveluksesta). Prosessikuvaus taas tarkoittaa kirjallista tai kuvallista dokumentaatiota prosessista. Prosesseja myös linkitettiin toisiinsa periaatteella, jossa toinen prosessi aktivoi toisen prosessin tietyssä vaiheessa. Esimerkiksi uuden työntekijän rekrytointi aiheuttaa jossain kohtaa prosessiaan tunnusten-luontiprosessin järjestelmiin rekrytoidulle työntekijälle.

Prosessit olivat pääosin olemassa, mutta niiden kuvaukset olivat vanhentuneita tai puutteellisia, joten ne tuli päivittää. Pääosin prosessikuvaukset toteutettiin tekstiä ja kaavioita yhdistelevinä PowerPoint -tiedostoina. Prosessikuvaukset ovat saatavilla niitä tarvitseville henkilöille tarvittavien pääsyoikeuksien takana.

3.3.3 Riskianalyysi ja sisäinen riskien käsittelyn prosessi

Sertifiointi, kuten myös laadukkaan tietoturvan toteuttaminen, lähtee perusteellisesti tehdystä riskianalyysista. Riskianalyysissä tunnistetaan yleisesti toimialaan vaikuttavia tietoturvariskejä, mutta erityisesti niitä riskejä, jotka vaikuttavat yrityksen toimintaympäristössä. Koska yritysten toimintaympäristöt (erityisesti IT-ala huomioon ottaen) ovat alati jatkuvassa muutoksessa, on riskianalyysiä tarkasteltava ja päivitettävä säännöllisesti. Riskianalyysin ylläpidon laiminlyönti johtaa väistämättä suuriin haasteisiin laadukkaan tietoturvan toteuttamisessa. Riskeistä voidaan olla tietoisia, mutta niistä tulee olla myös kirjallinen dokumentaatio sertifioituessa ISO27001:n mukaisesti. Myöhemmissä vaiheessa sertifikaation ylläpitoauditoinneissa, tulee ulkoiselle auditoijalle esittää evidenssiä riskianalyysin ja riskien käsittelyn ylläpidosta ulkoisten auditointien välissä eli noin vuoden ajalta. Tätä evidenssiä voidaan esittää laadukkaan ja jatkuvasti ylläpidetyn dokumentaation avulla.

3.3.4 Jatkuvuussuunnitelmat

Jatkuvuussuunnitelmalla tarkoitetaan kirjallista suunnitelmaa, jolla yrityksen ydintoiminnot ylläpidetään poikkeavissa tilanteissa. Jatkuvuussuunnitelma voidaan esimerkiksi toteuttaa tietyn toimipisteen tai liiketoiminnon (myynti, asiakastuki, markkinointi jne) kohdalla. Vesivahinko toimitiloissa voi olla esimerkki poikkeustilanteesta, jossa yrityksen toiminnot voivat

vaarantua ja tilanteeseen tulee reagoida. Jatkuvuussuunnitelmien luontia lähestytään riskilähtöisesti. Tämä tarkoittaa sitä, että kun olemassa oleva riski tunnistetaan riittävän todennäköiseksi ja sen vaikutukset ovat myös suuria, tehdään sen aktualisoitumisen varalle jatkuvuussuunnitelma. Jatkuvuussuunnitelmassa on määritelty vastuunhenkilöt sekä ohjeet toimintojen ylläpitämiseksi poikkeustilanteessa. Ohjeita voi olla määritelty myös eri aikajänteille, jos poikkeava tilanne kestää pitkään.

Olemassa olevia jatkuvuussuunnitelmia ja niiden tilaa on kartoitettu projektin aikana toimeksi antavan yrityksen kohdalla. Alkuvuodesta 2023 on tehty suunnitelma, jonka avulla jatkuvuussuunnitelmat päivitetään yrityksen nykytilaa vastaaviksi.

3.3.5 Velvoitteiden tunnistaminen

Toimeksi antavan yrityksen kanssa tehtiin myös velvoitteiden tunnistamista. Tällä tarkoitetaan niitä asetuksia ja lakeja, joita yrityksen toimialalla on otettava huomioon. Toinen huomioon otettava muuttuja on myös asiakkaiden ja heidän toimialojensa mukanaan tuomat velvoitteet tietoturvassa. Yleisellä tasolla velvoitteiden tunnistaminen on melko helppoa, mutta tässä projektissa turvauduttiin myös lakitoimiston palveluihin. Laadimme dokumentaation yleisellä tasolla yhteistyökumppaneistamme ja asiakkaittemme toimialoista. Dokumentaatio toimitattiin keskisuurelle suomalaiselle lakitoimistolle ja he tekivät arvion toimeksi antavaa yritystä koskevista kansallisista ja kansainvälisistä laeista ja asetuksista, jotka otetaan huomioon tietoturvakäytänteitä laadittaessa ja ylläpidettäessä. Edellä kuvatulle toimenpiteelle on merkitty omistaja ja hän tekee tarvittavan arvion lakeihin ja asetuksiin säännöllisesti vuosikellon mukaisesti. Tarvittaessa omistaja konsultoi lakitoimistoa uudelleen. Prosessissa havaitut velvoitteet ja niitä seuranneet toimenpiteet dokumentoitiin tietoturvanhallintajärjestelmään.

3.4 Projektin reflektointi ja jatkotoimenpiteet

3.4.1 Vastoinkäymiset projektissa ja mitä niistä opittiin

Isoin vastoinkäyminen oli projektin liian tiukka aikataulu ja lopulta aikataulua lykättiin kahteen kertaan. Aikataulu oli alun perin ollut liian optimistinen eikä siinä ollut tarvittavaa virheen sietoa. Aikataulua saatiin silti lykättyä melko vaivattomasti vetoamalla olosuhteisiin, sillä yrityksen johto oli myös havainnut aikatauluun liittyvät haasteet.

Näin isoon projektiin ryhdyttäessä, olisi annettava riittävästi aikaa projektin toteuttamiselle ja otettava huomioon myös yrityksessä käynnissä olevat muut muutokset. Toimeksi antavalla yrityksellä oli samaan aikaan käynnissä useampi suuri muutosprojekti, jolloin

ISO27001-työryhmä ei saanut aina tarvitsemiaan resursseja projektin edistämiseen muista tiimeistä, koska myös niissä oli korkean prioriteetin työskentelyä vaativia tehtäviä työnalla.

Toimeksi antavalla yrityksellä oli vahva tahtotila sertifioitumiseen, mutta ajankohta oli haastava. Sertifioituminen saatiin silti vietyä läpi, siitä huolimatta, että alkuperäisessä aikataulussa ei pysytty.

Toinen tärkeä huomio oli se, että dokumentaatiota tulee pitää yllä tarkasti ja säännöllisesti. Jos dokumentaatiota laiminlyödään, niin seuraavalla kerralla edessä voi olla tilanne, jossa aiemmasta dokumentaatiosta ei ole enää mitään hyötyä vaan päivittämisen sijaan on helpompaa laatia dokumentaatio täysin uudelleen vastaamaan yrityksen nykytilannetta.

Myös dokumentaation tekemiseen on syytä varata reilusti aikaa. Koska ISO27001-työryhmä ei todennäköisesti ole asiantuntija kaikissa yrityksen osa-alueissa, on tärkeää varata yrityksen muille työryhmille riittävästi työaikaa dokumentointiin yhdessä varsinaisen työryhmän kanssa. Työryhmän on hyvä myös tehdä dokumentointi avustaville tiimeille mahdollisimman helpoksi, esimerkiksi tekemällä aikataulutus ja täytettävä dokumentti pohjat mahdollisimman valmiiksi ja yksiselitteisiksi. Kommunikaatio hyvissä ajoin etukäteen muiden tiimien kanssa on yhteisymmärryksen sekä aikataulussa pysymisen edellytys.

3.4.2 Seuraavat vaiheet ja sertifikaatin ylläpito

Sertifikaatin ensimmäisen kierroksen jälkeen alkaa toisen auditointi kierroksen valmistelu. Sen aikana päivitetään ja ylläpidetään dokumentaatiota ja puututaan poikkeamiin, jotka ovat saaneet runsaammin korjaamisen aikaa ensimmäisten auditointien aikana. Tärkeitä seikkoja, joihin tulee kiinnittää huomiota ennen toista auditointi kierrosta ovat esimerkiksi riskien käsittelyn dokumentointi sekä riskianalyysin tarkastelu. Myös sisäisiä auditointeja tulee toteuttaa ja dokumentoida. Sisäisiä auditointeja voidaan tehdä tänä aikana myös ulkopuolisten konsulttien toimesta, jotka esimerkiksi testaavat ja arvioivat järjestelmien tietoturvaa testiympäristöissä, jotka vastaavat mahdollisimman paljon tuotantoympäristöä.

Toisen kierroksen jälkeen seuraa vielä kolmas kierros, jonka jälkeen sertifikaatin kolmivuotinen sykli päättyy. Sertifiointi kestää siis myöntämisestä kolme vuotta, mutta työ sertifioinnin ylläpitämiseksi on jatkuvaa väliauditointien takia. Sertifiointi voidaan siis ulkoisen auditoijan toimesta evätä, jos kriteerit eivät enää myöhempien auditointien aikana toteudu eikä niissä esitettyjen poikkeamien korjaamiseen ryhdytä aikataulussa tai ollenkaan. Näin ollen työryhmän on edelleen työskenneltävä projektin parissa. Erityisesti lisää työtä voivat tuottaa yrityskaupat tai uusien toimipisteiden ja liiketoimintojen perustaminen.

4 Yhteenveto ja pohdinta

Toimiksi antavan yrityksen sertifiointi projekti onnistui ja toimeksi antava yritys saavutti virallisen ISO/IEC 27001 -sertifikaatin alkusyksystä 2023 tämän projektin seurauksena. Projekti ei edennyt alkuperäisen aikataulun mukaisesti, johtuen yllättävistä haasteista projektin aikana, mutta niistä opittiin tulevaisuutta varten ja ne otetaan jatkossa huomioon vastaavissa projekteissa.

Kaiken kaikkiin voidaan todeta, että vaikka ISO27001-sertifikaatti on tarkoitettu toteutuskelpoiseksi yrityksen toimialasta ja koosta riippumatta, voi sen toteuttaminen olla ilman tietoturvan perustaitoja hyvin haasteellista. Toimeksi antavan yrityksen toimialan takia, oli työryhmän koulutukseen ja työelämässä vaadittuihin taitoihin kuulunut tietoturvan ymmärtämistä, toteuttamista ja tietoturvan nostamista korkealle prioriteetille. Vaikka työryhmällä olikin nämä perustason valmiudet olemassa, kohdattiin projektin aikana ajoittain isompiakin haasteita, sillä aiempaa kokemusta tietoturvassa sertifikaatin hankkimisesta ei ollut. Resursoiminen serfioitumiseen voi kuitenkin olla suuressa määrin hyödyllistä ja joskus jopa pakollista yrityksen toimialasta riippumatta, sillä vaikka yritys tekisi arjessaan aivan jotain muuta kuin tieto- ja viestintätekniikan tehtäviä, voi se olla alihankkijana jollekin yritykselle, joka vaatii tietyn sertifikaatin alihankkijaltaan.

Sertifikaatin hankkiminen ei kuitenkaan ole mahdotonta. Monesta sertifikaatin vaatimuksesta selvitään jo pelkällä maalaisjärjellä, varsinkin jos yrityksen ydintoiminnat eivät sisällä esimerkiksi laajaa tietokantojen ylläpitoa asiakastiedoista tai yrityksessä ei muuten käytetä tietotekniikkaa kuin mitä sen ydintoiminnot vähintään vaativat. Lopulta kysytään ainoastaan yrityksen tahtotilaa ja priorisointia kyseiseen projektin budjetoimiselle taloussuunnitelmassa. Henkilöstöä voidaan kouluttaa esimerkiksi webinaareilla ja ulkopuolisia konsultteja voidaan hyödyntää vaativissa teknisissä tehtävissä esimerkiksi palvelinpuolella. ISO27001-standardin keskiössä on ymmärrys tietoturvan tärkeydestä ja halu tehdä muutoksia yritysten nykyisiin käytänteisiin. Kuitenkin on muistettava, että sertifiointi maksaa ja aiheuttaa huomattavia kustannuksia yritykselle, joten aina ennen vastaavaan projektiin ryhtymistä on arvioitava, mitkä ovat sertifioitumisen hyödyt yritykselle rahallisesti eli saako yritys riittävästi vastinetta investoinnilleen. Toki täytyy muistaa, että esimerkiksi ulkoisen auditoijan palkkio on pienempi yrityksissä, joissa on vähemmän auditoitavia kohteita. ISO27001-sertifioitusen hinta vaihtelee yrityksen koosta ja käytetyistä työvälineistä riippuen 10 000–30 000 euron välillä (vuosittain toistuva maksu). Hintaan vaikuttaa moni muukin tekijä ja esimerkiksi konsulttien käyttäminen voi nostaa hintaa huomattavasti. Kokonaishintaan on löydettävissä monia suuntaa antavia laskureita ja taulukoita internetistä alaan liittyviltä toimijoilta. Näissä laskureissa ja taulukoissa otetaan huomioon esimerkiksi yrityksen koko, toimiala, itse

tehdyn työn määrä, konsulttien käyttö ja toteuttamiseen valitut sovellukset. Lopputulokset ovat kuitenkin karkeita arvioita ja projektiin ryhtyessä on varauduttava yllättävästi nouseviin kustannuksiin.

Standardeihin liittyvästä kokemuksesta ja osaamisesta voi olla tulevaisuudessa paljon hyötyä nimittäin Euroopan parlamentti on hyväksynyt verkko- ja tietoturvadirektiivin uuden version (NIS2) marraskuussa 2022. Aikaa standardin mukaiseen toimintaan siirtymiseen on annettu 21 kuukautta. Suomessa kaavaillaan sen tulevan osaksi kansallista lainsäädäntöä syksyllä 2024. Tämä standardi ei ole kaikille vapaaehtoinen, vaan tietyt kriteerit täyttävien toimijoiden tulee toimia standardin mukaisesti, ja sitä tulevat valvomaan valvonta viranomaiset (Bureau Veritas, 2023). Näin ollen voidaan ennustaa, että standardeihin liittyvälle osaamiselle tulee olemaan suurta kysyntää lähitulevaisuudessa ja näin tapahtuessa voidaan myös olettaa koulutuksen sekä työpaikkojen lisääntyvän aiheen ympärillä.

Lähteet

2ns.fi, 2022, Hallinnollinen tietoturva – Mitä se on? 2NS. Viitattu 17.11.2022. Saatavissa https://www.2ns.fi/hallinnollinen-tietoturva-mita-se-on/

Bureauveritas.fi, 2023, NIS2-DIREKTIIVI, Bureau Veritas. Viitattu 24.10. Saatavissa https://www.bureauveritas.fi/tietoturva/nis2-direktiivi

Calder, A. 2013. IT Governance Ltd, 2013, Iso27001/iso27002:2013 : A Pocket Guide. Viitattu 23.11.2022.

Europa.eu, 2022, Yleinen tietosuoja-asetus. Your Europe. Viitattu 17.11.2022. Saatavissa https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm

Finlex.fi, 2022, Laki julkisen hallinnon tiedonhallinnasta. Finlex. Viitattu 17.11.2022. Saatavissa https://www.finlex.fi/fi/laki/alkup/2019/20190906

Frendy.fi, 2022, Yrityksen tietoturva, mitä jokaisen yrityksen tulee tietää. Frendy Oy. Viitattu 17.11.2022. Saatavissa https://frendy.fi/tietoturva

Kauppakamari.fi. Tietoturvaopas yrityksille. Keskuskauppakamari. Viitattu 4.3.2024. Saatavissa https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

Kyberturvallisuuskeskus.fi, 2020. Digitaalinen ja fyysinen turvallisuus paiskaavat kättä Fortumissa. Traficom. Viitattu 4.3.2024. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/digitaalinen-ja-fyysinen-turvallisuus-paiskaavat-katta-fortumissa

Kyberturvallisuuskeskus.fi, 2023. Tietoturva on koko organisaation asia - vinkkejä henkilöstön tietoturvakoulutuksen suunnitteluun. Traficom. Viitattu 4.3.2024. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/tietoturva-koko-organisaation-asia-vinkkeja-henkiloston

Leijonasecurity.fi, 2022, Tietoturvan osa-alueet. Leijona Security. Viitattu 17.11.2022. Saatavissa https://www.leijonasecurity.fi/tietoturvan-osa-alueet/

Sfs.fi. Tutkittua tietoa standardeista. SFS Suomen Standardit. Viitattu 4.3.2024. Saatavissa https://sfs.fi/standardeista/standardien-hyodyt/tutkittua/

Tietosuoja.fi, Luottamuksellisuus ja turvallisuus. Tietosuojavaltuutetun toimisto. Viitattu 4.3.2024. Saatavissa https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus

Tietoturvapro.fi, 2019, Ajantasaiset laitteet ja ohjelmistot eivät riitä, vaan tietoturvasta on tehtävä tapa toimia, Tietoturva Pro. Viitattu 24.11. Saatavissa https://www.tietoturva.pro/

Traficom.fi, 2022, Tietoturva. Liikenne- ja viestintävirasto, Kyberturvallisuuskeskus. Viitattu 15.11.2022. Saatavissa https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva

Veiga, A Da. Eloff, J H P, 2007, An Information Security Governance Framework, Viitattu 19.11.2023.

Yrittajat.fi. Miten suojata yrityksen arkaluontoiset tiedot? Mitä tietoturva maksaa? Lue asiantuntijoiden neuvot – ”Tärkeintä olla kiinnostunut”. Yrittäjät. Viitattu 4.3.2024. Saatavissa https://www.yrittajat.fi/uutiset/miten-suojata-yrityksen-arkaluontoiset-tiedot-mita-tietoturva-maksaa-lue-asiantuntijoiden-neuvot-tarkeinta-olla-kiinnostunut/