ISO/IEC 27001 mukainen puuteanalyysi Keski-Suomen alueen yritykselle

Kalle Väänänen

Opinnäytetyö, AMK
Marraskuu 2021
Tekniikan ala
Insinööri , Tieto- ja viestintätekniikka

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Väänänen, Kalle

ISO/IEC 27001 mukainen puuteanalyysi Keski-Suomen alueen yritykselle

Jyväskylä: Jyväskylän ammattikorkeakoulu. Marraskuu 2021, 33 sivua

Tekniikan ala. Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Verkkojulkaisulupa myönnetty: kyllä

Tiivistelmä

ISO/IEC 27001 on johtamisen ja hallinnan standardi, jonka avulla voidaan luoda riskiperusteinen hallintajärjestelmä ja sitä kautta näyttää, että tietoturvallisuuteen liittyvät asiat on otettu organisaatiossa huomioon. Se on yksi kansainvälisesti käytetyimmistä tietoturvallisuuden hallinnan standardeista. Tällaiseen standardiin sertifioituminen voi vaikuttaa positiivisesti yrityksen imagoon, varsinkin viimeaikaisten tietoturvaskandaalien jälkeen.
Opinnäytetyössä tehtiin puuteanalyysi Keski-Suomessa sijaitsevalle yritykselle. Tavoitteena oli saada tietopohja yrityksen nykytilasta ja täten helpottaa yrityksen tulevaisuuden standardoitumisprosessin aloittamista.
Puuteanalyysiä varten selvitettiin ISO/IEC 27001 standardin vaatimukset ja luotiin niistä luettelo kysymyksiä, joihin vastausvaihtoehdot olivat OK, NOT OK ja N/A. Vastaukset kysymyksiin saatiin haastattelemalla yrityksen keskeistä henkilökuntaa. Vastausten perusteella laskettiin kokonaismäärät vaatimuskategorioittain ja lukumäärien perusteella prosenttiarvo, joka kuvaa yrityksen valmiutta kyseisessä kategoriassa.
Puuteanalyysin tulokset olivat suuntaa antavia, mutta silti arvokasta tietoa yrityksen nykytilasta ja voivat helpottaa standardin mukaisiin toimintatapoihin siirtymisessä.
Työn tavoitteisiin päästiin, sillä puuteanalyysillä voitiin kartoittaa yrityksen tietoturvallisuuden hallinnan nykytilaa ja siten saatiin tietoa, johon yritys voi pohjata tulevaisuuden ISO/IEC 27001 käyttöönottoprojektia. Työssä luotua puuteanalyysiä olisi mahdollista parantaa luomalla painoarvon jokaiselle analyysin kysymykselle. Täten saataisiin luotettavampaa ja tarkempaa tietoa mihin voitaisiin keskittää käyttöönottoprojektin resursseja.

Avainsanat (asiasanat)

ISO/IEC 27001, Tietoturva, Sertifiointi, Standardointi, Puuteanalyysi, Dokumentointi

Muut tiedot (salassa pidettävät liitteet)

jamk

Description

Väänänen, Kalle

ISO/IEC 27001 GAP Analysis for Central Finland-based company

Jyväskylä: JAMK University of Applied Sciences, November 2021, 33 pages

Information and Communication Technologies. Bachelor's Degree Programme in information and Communication Technology.

Permission for web publication: Yes

Language of publication: Finnish

Abstract

ISO/IEC 27001 is an international standard for information security management. It allows for a risk-based view into how the organization manages its information security. The standard is one of the most recognized and widely used management standards. Having a certification for ISO/IEC 27001 can positively affect the organizations image, especially after recent cyber security scandals. Showing that information security is being considered in the organization.
The thesis subject was assigned by a Central Finland-based company. The goal was to gather information about the company's current state regarding the standard and to create a basis for a certification project to get the company ISO/IEC 27001 certified in the near future.
The chosen method was to create a gap analysis, that checks each of the ISO/IEC 27001 requirements and gives it a score whether it was OK, NOT OK or N/A. The answers were gathered by interviewing relevant personnel in the company. The data was then summed up and a percentage calculated that shows how ready the company is for the requirement category in question.
Thesis goals were achieved even if the results of the gap analysis were approximate at best, but still convey the current state of the company and is a valuable asset when the company starts the project to get ISO/IEC 27001 certified.
The gap analysis can be further improved by creating a value for each of the requirement to make the data more precise. This way the results are more reliable and more valuable for the company.

Keywords/tags (subjects)

ISO/IEC 27001, Cyber security, Certification, Quality management, Gap analysis, Documentation

Miscellaneous (Confidential information)

Sisältö

Kuviot

Taulukot

Lyhenteet

ICT	Information and Communication Technology
SWOT	Strengths, Weaknesses, Opportunities, Threats
ISO	International Organization for Standardization
SESKO	sähkö- ja elektroniikka-alan kansallinen standardointijärjestö SESKO ry
IEC	International Electrotechnical Commission
ISO/IEC	ISOn ja IECn yhteistyökomitea
N/A	Not Applicable
JTC 1	Joint Technical Committee 1 “Information technology”
CIA	Confidentiality, Integrity, Availability
SFS	Suomen Standardisoimisliitto

1 Johdanto

Nykyajan kiihtyvästi kehittyvässä maailmassa tulee jatkuvasti uusia tuotteita, laitteita, protokollia ja rakennuksia. Mikähän olisi lopputulos, jos kuka vain saisi päättää miten asioita hoidetaan ilman yhteisiä sääntöjä ja sopimuksia? Laitteet ja rakennukset eivät välttämättä olisi tehty sääntöjen mukaisesti kulujen välttämiseksi, ostamasi tuote ei saata toimia koska se ei ole yhteensopiva ja protokollat eivät keskustele keskenään, koska yhteisistä pelisäännöistä niiden toteuttamiseksi ei olisi olemassa. Näitä yhteisiä pelisääntöjä kutsutaan standardeiksi. Ne voivat olla kansallisia, mutta nykypäivän globaalien toimitusketjujen kanssa ne eivät riitä. Tätä varten on perustettu organisaatioita, joiden tehtävänä on luoda kansainvälisiä standardeja ja edistää standardointia maailmanlaajuisesti. Tätä työtä tekee esimerkiksi kansainvälinen standardisointi organisaatio ISO ja Suomessa Suomen standardisoimisliitto SFS. (Lazarte 2016.)

SFS kertoo standardien hyödyistä seuraavasti: ”Standardien tavoitteena on lisätä yhteensopivuutta, laatua, sujuvuutta ja turvallisuutta. Emme useinkaan huomaa standardeja, vaikka niitä on kaikkialla.” Standardit hyödyttävät meitä kaikkia: verkkopalvelut toimivat, koska niiden taustalla toimivat protokollat on standardisoitu; sähkölaitteet ovat turvallisia käyttää, koska niiden testauksesta on sovittu; Ulkomailta hankittua laitetta voi käyttää oman maan sähköverkossa, koska laite on suunniteltu toimimaan standardisoiduissa sähköverkoissa. Standardeilla voidaan myös vaikuttaa yrityksen palvelun tai tuotteen imagoon tekemällä siitä luotettavampi. Näitä standardeja kutsutaan laatustandardeiksi ja niistä nykyään eniten käytetty on ISO 9001, laadunhallinta. (Standardeista on hyötyä meille kaikille n.d.)

Watkinsin ja Orchistonin (2016) mukaan tuotteiden ja palveluiden laadulla on ollut suuri merkitys jo ihmiskunnan historiassa. Laadukkailla tuotteilla saatettiin varmistaa niiden menekki ja vähentää mahdollisesti tarvittavia korjaustoimia huonolaatuiselle työlle. Ennen teollistumista tuotteen tekijän koulutuksella pystyi varmistamaan laadukkaampaa jälkeä, mutta teollistumisen ja tehtävien rinnakkaistamisen jälkeen pelkkä koulutus ei välttämättä ole riittävä tai kustannustehokas ratkaisu. Standardointi osoittautui tähän edullisimmaksi ja yksinkertaisimmaksi ratkaisuksi. Ensin standardointi koski aseiden ja koneiden osia, mutta se on kasvanut vaatimattomista lähtökohdista yhä merkityksellisemmäksi. Eräs ISO 9001 edeltäjistä oli Iso-Britannialainen standardi BS 5750, joka ensimmäisenä määritteli laadunhallintajärjestelmän. BS 5750 saama huomio sai myös ISOn kehittämään kansainvälisen laadunhallintastandardin ISO 9001:1987.

ISO 9001 on laadunhallinnan standardi, jonka avulla yritykset voivat lisätä asiakkaiden luottamusta tuotteen ja palvelun laatuun. Sertifikaatilla voi näyttää, että yritys on sitoutunut johdonmukaisuuteen ja jatkuvaan parantamiseen. Laadunhallintajärjestelmän tarkoitus on tuottaa laadukkaita tuotteita ja palveluita, mutta sen avulla voidaan myös selvittää organisaation päätösten seurauksia. Hyvin suunnitellun laadunhallintajärjestelmän avulla voidaan lisätä asiakastyytyväisyyttä, resurssitehokkuutta ja karsia kustannuksia. ISO 9001 standardia on käytössä yli miljoonassa työpaikassa maailmanlaajuisesti ja se onkin eniten käytössä oleva ISO standardi. Myös toinen ajankohtainen standardi löytyy tilaston kärjestä, ISO/IEC 27001. ISO/IEC 27001, kuten ISO 9001, on hallintajärjestelmästandardi. Tosin sen fokuksena on tietoturvallisuuden hallinta samoista riskiperusteisista lähtökohdista. (The ISO survey 2020; ISO 9001 Laadunhallinta n.d.; ISO 9001 – Quality management n.d.)

Tietoturvan merkitys kasvaa jatkuvasti nykypäivän verkottuneessa maailmassa. Uusia tietoturvauhkia ja -aukkoja löytyy lähes viikoittain ja uutisia tietomurroista näkyy usein. Täten myös tietoturvaan kiinnitetään enemmän huomiota ja resursseja. Yritykset voivat parantaa omien palveluidensa ja järjestelmiensä tietoturvaa koventamalla niitä tiedossa olevia uhkia vastaan sekä riskienhallinnalla.

Yksi tapa näyttää yrityksen asennetta tietoturvaa kohtaan on sertifioituminen yhteen tai useampaan tietoturvastandardiin. Eräs näistä standardeista on ISO/IEC 27001, Tietoturvallisuuden hallintajärjestelmät. Tosin Kyberturvallisuuskeskuksen mukaan:

> *ISO/IEC 27001 on tarkalleen ottaen hallinnan ja johtamisen standardi, ei tietoturvastandardi. Se antaa viitekehyksen ja riskiperusteisen näkymän siihen, että organisaatiossa hallitaan tietoturvallisuuteen kuuluvia asioita. (Luottamuksen lähteillä 2019, 9.)*

ISO/IEC 27001 mukainen hallintajärjestelmä sisältää toimintaperiaatteita, ohjeita ja toimintoja, joiden avulla yritykset voivat suojata tieto-omaisuuttaan. Sertifioidun tietoturvallisuuden hallintajärjestelmän avulla organisaatiot voivat myös ottaa paremmin huomioon niitä mahdolliset koskevat lakiasiat, kuten yleisen tietosuoja-asetuksen GDPRn. (ISO/IEC 27000 Tietoturvallisuuden standardisarja n.d.; ISO/IEC 27001 – information security management system n.d.)

Sertifikaatilla voidaan näyttää, että yritys on ottanut huomioon palveluidensa tietoturvan ja toteuttanut niihin liittyvien riskienhallintaa tietoturvallisuuden hallintajärjestelmällä. Tähän standardiin oli sertifioitunut Suomessa vuonna 2017 72 yritystä, eniten ICT alalta (Luottamuksen lähteillä 2019, 14). Tämä luku on kasvanut Suomessa 102:een vuonna 2020, jolloin maailmanlaajuisesti tilanne oli vajaassa 45 000 (The ISO survey 2020). ISO/IEC 27001 standardin vaatimuksia voi myös sitoutua noudattamaan ilman sertifiointia. Kyberturvallisuuskeskus (2019, 9) toteaa julkaisussaan, että tällöin yritykset pitävät itse yllä tiedon CIA-mallia ja myös auditoivat itse hallintajärjestelmänsä.

1.1 Toimeksiantaja

Opinnäytetyön toimeksiantaja on Keski-Suomessa sijaitseva yritys. Yrityksessä työskentelee noin 100 henkilöä. Yritys on työssä anonymisoitu arkaluonteisen tiedon vuoksi.

1.2 Työn tavoitteet

Työ pohjataan yrityksen haluun sertifioitua ISO/IEC 27001 standardiin parin vuoden sisään. Tätä varten opinnäytetyön tavoitteena on selvittää ISO/IEC 27001 standardin vaatimukset ja verrata niitä yrityksen toimintatapoihin ja valmiuksiin. Opinnäytetyön pohjalta yritys saa tietoa sen puutteista ISO/IEC 27001 standardin viitekehyksessä ja pystyy aloittamaan itselleen valmiuden hankkimisen ISO/IEC 27001 sertifiointiin. Työn tietoperustana käytetään soveltuvia ISO/IEC 2700x standardien dokumentaatioita ja muita standardeja koskevia lähteitä.

1.3 Työn rajaus

Työssä toteutetaan ISO/IEC 27001 mukainen puuteanalyysi yrityksen Keski-Suomen toimipisteelle. Työn ulkopuolelle rajataan yrityksen muut toimipisteet ja emoyhtiön toimipisteet, sekä Keski-Suomen toimispisteen ulkopuolella sijaitsevat palvelut. Puuteanalyysissä käsitellään ISO/IEC 27001 standardin vaatimukset ja sen liitteen A mukaiset tietoturvallisuuden hallintajärjestelmän hallintatavoitteet ja -keinot. (ISO27001-puuteanalyysi 2018.)

2 Tutkimusasetelma

Toimeksiantaja haluaa tavoitella ISO/IEC 27001 sertifikaattia lähitulevaisuudessa ja toivoo saavansa pohjatietoa lähtökohdistaan sertifikaatin hankintaan. Tällaisen kohteen tutkimiseen toimii tapaustutkimus toimeksiantaja yrityksestä. Tapaustutkimuksessa on erittäin tärkeää valita tutkittava tapaus sopivasti suhteessa tavoiteltavaan tietoon. Vallin ja Aarnoksen mukaan tapauksen pitäisi vastata kysymyksiin mitä, miten ja mistä on kyse sekä selittää miksi näin on. Tässä työssä tapauksen valinta on yksinkertainen, koska kyse on yhdestä yrityksestä ja sen valmiuksista hakea kansainvälistä, hyvin määriteltyä standardia. Tutkimuskohteena on siis yrityksen nykytila, jonka suhteen pitäisi selvittää standardin vaatimukset ja verrata näitä keskenään. Tämän selvittämiseksi valittiin työn tutkimusmetodiksi puuteanalyysi. (Valli & Aarnos 2018, 161.)

2.1 Puuteanalyysi tutkimusmenetelmänä

Nykytilan vertaaminen tavoitetilaan on tehokas tapa selvittää mitä asioita pitää parantaa tai mitä toimintatapoja muuttaa, jotta tavoitetilaan on mahdollista päästä. Puuteanalyysi sopii tällaiseen selvitykseen loistavasti. Puuteanalyysillä kartoitetaan tutkittavan asian nykytila ja verrata sitä johonkin valittuun tavoitetilaan. Puuteanalyysin tuloksien perusteella voidaan selvittää keinoja päästä nykytilasta tavoitetilaan, joko suoraan tuloksista tai tekemällä loogisia ratkaisuja nykytilan ja tavoitetilan välin pienentämiseksi, kunnes lopulta tavoitetila saavutetaan. Kun puute huomataan analyysin aikana, voi olla kannattavaa kuvailla puute ja kirjoittaa siitä miksi se on puute ja mitkä asiat siihen vaikuttavat. Analyysin jälkeen jokaiselle puutteelle pitäisi selvittää millä varsinaisilla keinoilla tavoitetilaan päästään. IT-alalla erityisesti projektinpäälliköt saattavat käyttää puuteanalyysiä työkaluna selvittääkseen miten projektin resursseja kannattaisi jakaa. Samoin puuteanalyysiä voidaan käyttää selvittämään mitä jokin laki tai säännöstö vaatii ja verrata niitä käytössä oleviin käytäntöihin. Näin saadaan selville, noudatetaanko kyseistä säännöstöä. (Peltier 2010, luku 5.1; What is a Gap Analysis? N.d.)

Puuteanalyysityökaluja on paljon erilaisia ja eri tilanteisiin soveltuvia. Yleisimmin tunnettuja lienee SWOT-analyysi, jolla voidaan kartoittaa jonkin kohteen toimivuutta. SWOT analyysissä kohde voi olla jokin yrityksen tuote tai palvelu, projekti tai henkilö. SWOT-analyysillä on tarkoitus selvittää mitä vahvuuksia, heikkouksia, mahdollisuuksia ja uhkia tutkittavaan kohteeseen liittyy sekä sisäisesti että ulkoisesti. Tämän jälkeen on mahdollista pyrkiä säilyttämään kohteen vahvuudet, paikata

sen heikkouksia, käyttää saatavilla olevia mahdollisuuksia ja välttää kohteeseen vaikuttavia uhkia. (What is a Gap Analysis? n.d.; Namugenyi, Nimmagadda & Reiners 2017, 4.)

2.2 Puuteanalyysi käytännön työkaluna

Puuteanalyysi siis sopii myös jonkin asian määräystenmukaisuuden selvittämiseen (What is a Gap Analysis? n.d.). Opinnäytteen aihetta vastaavan puuteanalyysin on suorittanut Peltier (2010) kirjassaan: Information security risk analysis, jossa hän kuvaa työvaiheitaan tehdessään puuteanalyysiä yritykselle sen hakeman kansainvälisen standardin suhteen.

Peltier (2010, luku 5.2) kertookin, että puuteanalyysiä varten kannattaa ensin kerätä kaikki säädökset ja vaatimukset, joita yrityksen tulee noudattaa. Tämän jälkeen puuteanalyysin rajaus tulee määrittää ja se, selvittääkö puuteanalyysi vain vaatimusten täyttämistä, vai myös täyttämiseksi tehtävien toimien laatua. Seuraavaksi Peltier suositelee keräämään kaiken dokumentaation, jotka kuvaavat yrityksen tämänhetkisiä toimintatapoja ja järjestämään ne haettavan standardin rakenteen mukaisesti. Viimeiseksi ennen varsinaisen analyysin suorittamista Peltier kehottaa haastattelemaan yrityksen henkilökuntaa varsinaisen tietämyksen ja toimintatapojen käytön selvittämiseksi. Tämä sen takia, että luodut prosessit eivät välttämättä vastaa työntekijöiden varsinaisessa käytössä olevia toimintatapoja. Lopuksi pitää verrata nykykäytänteitä ja työskentelytapoja standardin vaatimiin. Tulosten perusteella voidaan huomata osa-alueita mitkä eivät täyty standardien valossa. Näitä puutteita voidaan sitten alkaa työstämään, jotta lopulta päästään tavoitetilaan.

Opinnäytteessä määritetään, mitä vaatimuksia yrityksen hakema standardi asettaa sitä hakeville. Puuteanalyysi rajataan yrityksen Keski-Suomen toimipisteeseen ja sen nykytilaan, jossa sillä ei ole standardin mukaisia toimintatapoja käytössä. Puuteanalyysiä varten kerätään tietoa yrityksen nykyisistä toimintatavoista haastattelujen avulla. Lopuksi arvioidaan yrityksen nykytilan ja tavoitetilan eroa standardin vaatimusten valossa. Näiden tietojen perusteella voidaan arvioida yrityksen suhteellista valmiutta hakea standardia.

3 ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmästandardisarja

ISO/IEC 27000 -sarja on kasvava IT standardien kokonaisuus, joka käsittelee pääsääntöisesti tietoturvallisuuden hallintaa ja sen eri puolia. 27000-sarjaa julkaisee yhdessä kansainvälinen standardisoimisjärjestö ISO ja kansainvälinen sähköalan standardisointijärjestö IEC, joka näkyy myös standardin nimessä. Standardisarja koskee tietoturvallisuuden hallintajärjestelmiä ja esittää niille mallin, jota voidaan hyödyntää tietoturvallisuuden hallintajärjestelmän luomisessa ja käyttämisessä. Näitä standardeja noudattamalla yritys voi toteuttaa tieto-omaisuuden suojaamisen hallinnan perusedellytykset. (SFS-EN ISO/IEC 27000, 5.) ISO ja IEC ovat muodostaneet JTC 1 työryhmän, jonka aihealueena on ICT-ala. JTC 1 tavoitteena on edistää alan standardointia, jotta voidaan: varmistaa tuotteiden toimivuus myös eri toimittajien välillä, korostaa alan rakentavaa kilpailua, ja koota parhaita työtapoja, jotta tietotekniikkaa voidaan käyttää tuottavasti ja turvallisesti. (JTC 1 Strategic Business Plan 2020, 1.) JTC 1 on tällä hetkellä suoraan vastuussa 510 ISO standardista. (ISO/IEC JTC 1. n.d.; SFS-EN ISO/IEC 27000, 4.)

3.1 ISO

ISO on maailmanlaajuinen organisaatio, jonka jäseninä toimivat kansalliset standardisointielimet ja sen tehtävänä on luoda ja julkaista kansainvälisiä standardeja (About Us - What we do n.d.). Tällä hetkellä ISO on kehittänyt 23748 standardia eri aloille (https://www.iso.org/store.html). Osaan näistä standardeista voi sertifioitua, kuten ISO 9001 laatustandardiin tai työn kohteeseen ISO/IEC 27001 Tietoturvallisuuden hallintajärjestelmät -standardiin. ISOn Suomen jäsenjärjestö on Suomen Standardisoimisliitto SFS, joka osallistuu ISO standardien kehitykseen, käyttöönottoon, ylläpitämiseen ja myymiseen kansallisella tasolla (Members n.d.).

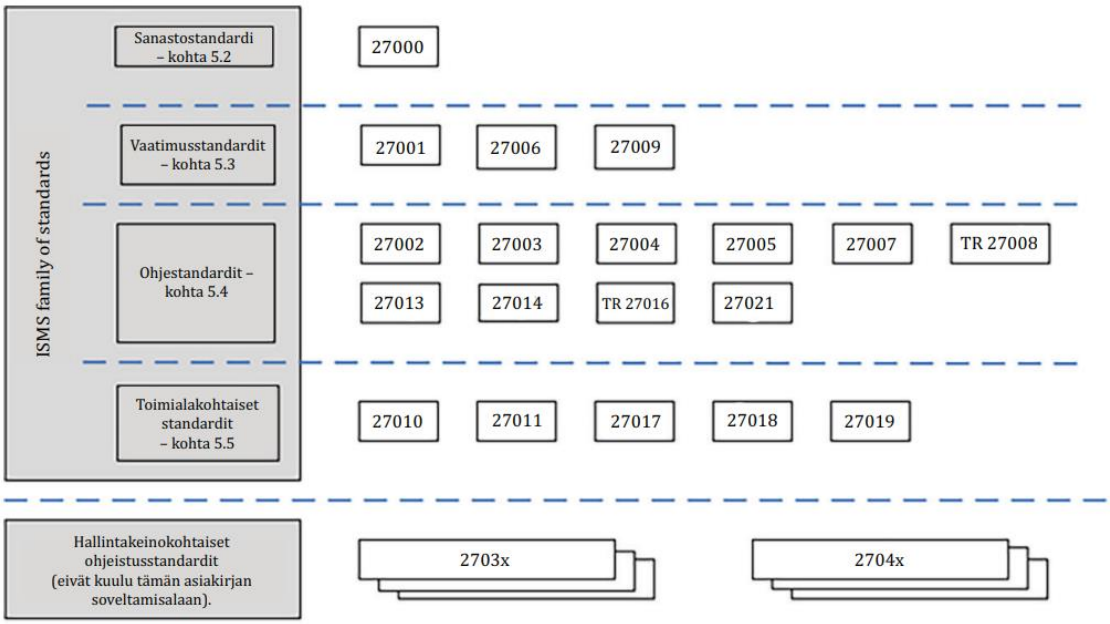
3.2 IEC

IEC on maailmanlaajuinen voittoa tavoittelematon järjestö, joka työllään edistää laadukasta infrastruktuuria ja sähkölaitteiden kansainvälistä kauppaa. IEC myös osallistuu kansainväliseen standardisointiin, varsinkin sähkölaitteiden ja teknisten alojen suhteen (What we do n.d.). Kokonaisuudessaan IEC on ollut osallisena yli 10 000 standardin kehittämisessä, pääasiassa sähköalalle. IECssä Suomea edustaa sähkö- ja elektroniikka-alan kansallinen standardointijärjestö SESKO ry, joka on IECssä täysi jäsen. IECn täytenä jäsenenä organisaatiolla on mahdollista lähettää asiantuntijoita vaikuttamaan standardien kehittämiseen IECn eri komiteoiden tai alikomiteoiden kautta. SESKO ry

on myös SFSn jäsenjärjestö ja vastaa Suomen sähkötekniikan standardisoinnista. (SESKO ry n.d.; National Committees. N.d.)

3.3 ISO/IEC 2700x standardeista

ISO/IEC 27000 standardisarja käsittelee tietoturvallisuuden hallintajärjestelmiä. Sarjan keskeisimpiä standardeja ovat 27000–27005. 27000 on sarjan sanastostandardi, 27001 on sarjan ”varsinainen osa” eli vaatimusstandardi, 27002–27005 ovat ohjestandardeja, jotka tukevat organisaatioita ISO/IEC 27001 mukaisen hallintajärjestelmän toteuttamisessa. Kuviossa 1 nähdään standardisarjan rakenne ja eri standardien sisältö standardityypin mukaan.



Kuvio 1. ISO/IEC 27000 standardisarja (SFS-EN ISO/IEC 27000:2020, 24).

ISO/IEC 27000 sisältää yleiskatsauksen ja sanaston 2700x -sarjalle. Standardissa määritellään standardisarjaa koskevat keskeiset käsitteet, sekä määritellään tietoturvallisuuden hallintajärjestelmä. Standardissa kerrotaan myös tarkemmin tietoturvallisuuden hallintajärjestelmästandardisarjasta ja sen rakenteesta. (SFS-EN ISO/IEC 27000:2020, 5, 16, 23.)

ISO/IEC 27001 sisältää hallintajärjestelmiä koskevat vaatimukset. Nämä vaatimukset koskevat tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja sen jatkuvaa kehittä-

mistä. Standardissa myös kuvataan riskienhallinnan arvioinnin ja käsittelyn vaatimuksia, sekä esitetään hallintakeinoja, joilla riskejä voi käsitellä. (SFS-EN ISO/IEC 27000:2020, 25; SFS-EN ISO/IEC 27001:2017, 5.)

ISO/IEC 27002 on ohjestandardi, jossa luetellaan hallintatavoitteita ja hallintakeinoja. Standardissa esitellyt hallintakeinot ovat yleisesti hyväksyttyjä ja noudattavat toteutuksen parhaita käytäntöjä. Standardi on suunniteltu hallintajärjestelmän toteuttamisprosessissa käytettäväksi. (SFS-EN ISO/IEC 27000:2020, 25; SFS-EN ISO/IEC 27002:2017, 6.)

ISO/IEC 27003 standardissa avataan ISO/IEC 27001 standardia tarkemmin ja kerrotaan, miten sen mukainen hallintajärjestelmä voidaan toteuttaa onnistuneesti (SFS-EN ISO/IEC 27000:2020, 26).

ISO/IEC 27004 ohjestandardissa määritetään keinot, joiden avulla tietoturvallisuuden hallintajärjestelmän vaikuttavuutta ja tietoturvan tasoa voidaan mitata ja arvioida. Seurannan tuloksia voidaan siten käyttää hallintajärjestelmän parantamiseen. (SFS-EN ISO/IEC 27000:2020, 26; SFS-EN ISO/IEC 27004:2016, 5.)

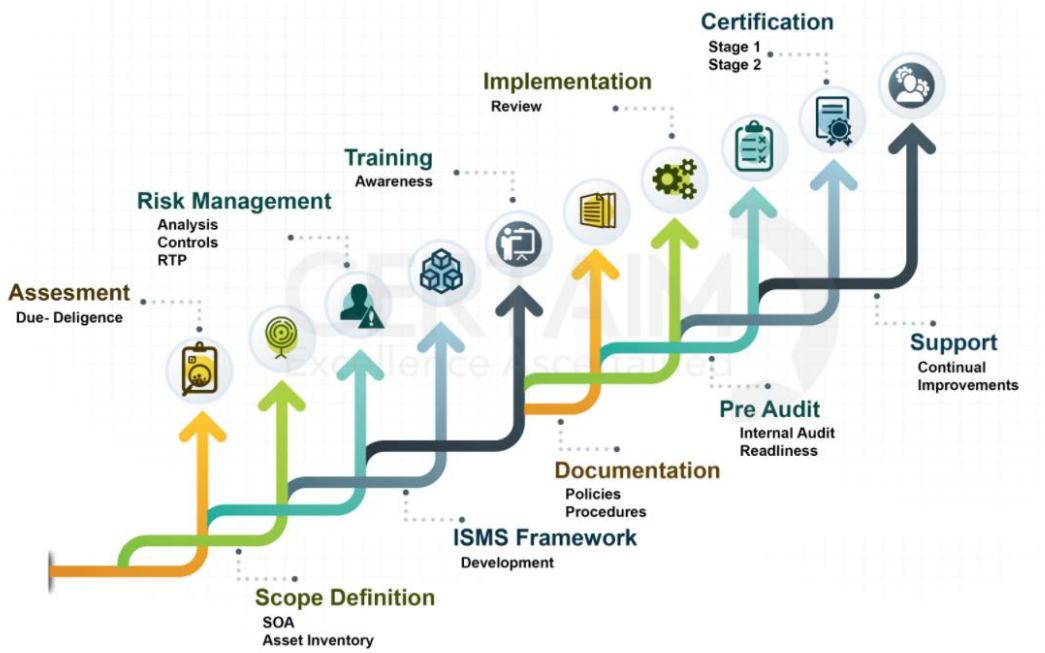
ISO/IEC 27005 standardissa annetaan ohjeistusta tietoturvariskien hallinnasta. Standardin mukaisen riskienhallinnan toteuttaminen voi helpottaa ISO/IEC 27001 asetettujen vaatimusten täyttämistä. (SFS-EN ISO/IEC 27000:2020, 26; SFS-EN ISO/IEC 27005:2018, 5.)

3.4 Sertifiointi yleisesti

Yksinkertaistettuna ISO/IEC 27001 sertifikaatin hankinta seuraa alla kuvattuja kohtia:

1. Päätös sertifikaatin hankinnasta
2. Soveltamisalan määrittäminen
3. Vaatimusten mukaisten asioiden dokumentointi
4. Dokumentoinnin mukainen toteutus
5. Sisäinen auditointi
6. Sertifiointi auditointi
7. Sertifioinnin ylläpito

Ensimmäinen askel on päätös hankkia sertifikaatti ylipäätään. Tämän päätöksen pitää tulla yrityksen ylimmältä johdolta, ainakin ISO/IEC 27001 kohdalla, sillä johdon sitouttaminen on yksi standardin vaatimuksista. Tämän jälkeen pitää määritellä mitä kaikkea sertifikaatti koskee eli sen soveltamisala. Koskeeko standardi jotain tiettyä toimipistettä, yrityksen koko toimintaa, vai kenties vain jotain tiettyä palvelua? Sen jälkeen pitää luoda standardin vaatimusten mukaiset dokumentit, prosessit ja ohjeet. Seuraava askel on implementoida nämä yrityksen toimintaan. Lopuksi kannattaa suorittaa ensin yrityksen sisäinen auditointi ennen varsinaista ulkoisen sertifioijan auditointia. Mikäli sisäisessä auditoinnissa vielä löytyy puutteita, niin yrityksen ei tarvitse maksaa ulkoisen auditoinnin kustannuksia useaan kertaan. Viimeinen ja jatkuva askel on sertifioinnin ylläpito, mikä sisältää: hallintajärjestelmän jatkuvan parantamisen, sertifioinnin seuranta-arvioinnit ja sertifioinnin jatkaminen uudella auditoinnilla. Näitä kohtia on havainnollistettu kuviossa 2. (ISO/IEC 27001 Certification Process n.d.; Pournader 2018.)



Kuvio 2 ISO/IEC 27001 sertifiointikaavio (ISO IEC 27001 Implementation & certification n.d.)

4 ISO/IEC 27001 standardin vaatimukset

ISO/IEC 27001 standardin vaatimuksiin kuuluu siinä määritettyjen dokumenttien olemassaolo tai dokumentoitua tietoa seuraavista asioista. Nämä dokumentit ovat:

1. Tietoturvallisuuden hallintajärjestelmän soveltamisala
2. Tietoturvapolitiikka
3. Tietoturvariskien arviointi- ja käsittelyprosessi ja niiden tulosten dokumentaatio
4. Tietoturvatavoitteet
5. Näyttöä tietoturvan tasoon vaikuttavien työntekijöiden pätevyydestä
6. Tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämätön tieto
7. Tietoturvavaatimusten täyttämiseen suunnitellut prosessit ja dokumentoitua tietoa niiden toteuttamisesta suunnitellusti
8. Tietoturvan tason ja hallintajärjestelmän vaikuttavuuden seurannan ja mittauksen tulokset
9. Sisäinen auditointiohjelma ja sisäisten auditointien tulokset
10. Dokumentoitua tietoa johdon katselmusten tuloksista
11. Dokumentoitua tietoa tietoturvapoikkeamista, poikkeamien johdosta tehdyistä toimenpiteistä, sekä korjaavien toimenpiteiden tuloksista (SFS-EN ISO/IEC 27001:2017, 6–14.)

Vaadituista dokumenteista tarkemmin

Organisaation tulee rajata hallintajärjestelmän soveltamisala. Tämä tarkoittaa hallintajärjestelmän laajuuden rajaamista organisaation määritettyyn osaan. Tämä voi olla esimerkiksi jokin tietty palvelu, toimipiste tai vaikka koko organisaatio. Soveltamisalan määrittämisessä tulee ottaa huomioon organisaation toiminnan kannalta olennaiset sisäiset ja ulkoiset asiat, jotka vaikuttavat tietoturvallisuuden hallintajärjestelmän kykyyn saavuttaa sille määritetyt tulokset. Tämän lisäksi pitää määritellä hallintajärjestelmän kannalta olennaiset sidosryhmät ja niiden vaatimukset tietoturvalle. (SFS-EN ISO/IEC 27001:2017, 6.)

Standardin hankkimisessa organisaation johdon sitouttamisen tärkeyttä on korostettu, sillä heillä on mahdollisuudet varmistaa hallintajärjestelmän tarvittavat resurssit ja että hallintajärjestelmä on yhdenmukainen organisaation strategian kanssa. Ylimmän johdon on laadittava tietoturvapolitiikka, joka soveltuu yritykselle ja tukee sen toiminta-ajatusta. Tietoturvapolitiikan tulee sisältää tietoturvatavoitteet tai perustan niiden määrittämiselle. (SFS-EN ISO/IEC 27001:2017, 7, 9.)

Erilaiset tietoturvariskit tulee arvioida ja käsitellä. Arviointiprosessissa riskit tulee tunnistaa ja antaa niille niiden todennäköisyyden ja mahdollisten seurausten mukainen riskitaso. Tunnistettuja riskejä pitää sitten verrata riskikriteereihin ja priorisoida hyväksymättömät riskit käsittelyprosessia varten. Käsittelyprosessissa riskeille pitää määrittää kaikki hallintakeinot, joita sitten verrataan ISO/IEC 27001 Liite A:n luetteloon hallintatavoista ja hallintakeinoista. Vertailun jälkeen luodaan soveltuvuuslausunto, jossa kerrotaan kyseisen riskin hallintakeinot ja perustelut niiden käyttämiselle tai käyttämättä jättämiselle. (SFS-EN ISO/IEC 27001:2017, 9.)

Organisaation tulee määrittää tietoturvan tasoon vaikuttavien henkilöiden pätevyyden taso. Näiden henkilöiden pätevyys pitää varmistaa koulutuksen, harjoittelun, tai kokemuksen kautta. (SFS-EN ISO/IEC 27001:2017, 10.)

Organisaation määrittämä tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämätön tieto, voi tarkoittaa vähimmillään vain standardin vaatimaa dokumentoitua tietoa tai hyvinkin paljon erilaisia dokumentteja, sillä siihen vaikuttaa organisaation koko, sen toimiala ja tarjottavat palvelut, organisaation prosessit, jne. (SFS-EN ISO/IEC 27001:2017, 11.)

Organisaation tietoturvavaatimukset täyttävät prosessit on suunniteltava ja toteutettava siten, että voidaan luottaa niiden toteutuneen suunnitelmien mukaisesti. Mikäli prosesseja on ulkoistettu, organisaation tulee varmistaa, että ne on määritetty ja että niitä valvotaan. (SFS-EN ISO/IEC 27001:2017, 12.)

Organisaation tulee määrittää mitä hallintajärjestelmästä tulee seurata ja mitata. Tähän sisältyy menetelmät, jolla saadaan tyydyttäviä ja toistettavia tuloksia, aikaväli ja tuloksien analysointi. (SFS-EN ISO/IEC 27001:2017, 12.)

Standardin vaatimuksissa pysymisen kannalta on tärkeää luoda ja toteuttaa sisäinen auditointi säännöllisin väliajoin. Täten organisaatio voi itse seurata onko hallintajärjestelmä organisaation tietoturvavaatimusten mukainen, täyttääkö se ISO/IEC 27001 vaatimukset ja onko sitä ylläpidetty vaikuttavasti. Sisäisten auditointien lisäksi organisaation ylimmän johdon tulee katselmoida tietoturvallisuuden hallintajärjestelmä, jotta se pysyy organisaatiolle tarkoitukseen sopivana ja vaikuttavana. (SFS-EN ISO/IEC 27001:2017, 13.)

Viimeisenä mainittuna dokumentoituna tietona standardissa vaaditaan tietoturvapoikkeamien havainnointi, reagointi, arviointi, ja poikkeaman korjaavat toimenpiteet. Tämän lisäksi organisaation on arvioitava korjaavien toimenpiteiden vaikuttavuus ja dokumentoida poikkeamat ja niiden hallintaan valittujen toimenpiteiden tulokset. (SFS-EN ISO/IEC 27001:2017, 14.)

5 Puuteanalyysi

Puuteanalyysillä voidaan selvittää nykytilan ja tavoitetilan välistä eroa. Täten voidaan kartoittaa mitä osa-alueita tarvitsee kehittää ja mitkä mahdollisesti ovat tavoitetasolla. Puuteanalyysin tulosten perusteella voidaan luoda projektisuunnitelma standardiin sertifioitumiselle.

5.1 Puuteanalyysin valmistelu

Puuteanalyysissä käydään läpi ISO/IEC 27001 vaatimuksiin kuuluvat dokumentoidun tiedon dokumentit, sekä ISO/IEC 27001 Liite A:n tietoturvatavoitteiden ja tietoturvakontrollien lista ja verrataan näitä yrityksen nykytilaan. Vaikka yrityksellä ei tällä hetkellä olekaan virallista tietoturvanhallintajärjestelmää, puuteanalyysiä voidaan silti käyttää tunnistamaan standardin vaatimusten mukaisia puutteita (ISO27001-puuteanalyysi 2018). Näiden vaatimusten pohjalta luotiin Excel taulukko, jossa standardin vaatimukset on eritelty kolmeen kategoriaan: Liite A:n vaatimukset, Standardin vaatimukset, ja Standardin vaatimat dokumentoidun tiedon dokumentit. Näistä standardin vaatimukset ja vaaditut dokumentoidut tiedot menevät osittain päällekkäin, mutta niitä korostettiin niitä erillisinä vaatimuksina, sillä tietyt standardin vaatimat asiat pitää olla saatavina dokumentoituna tietona.

Puuteanalyysissä sisältää kokonaisuudessaan 230 käsiteltävää vaatimusta, ne on kirjoitettu vain otsikko tasolla näkyviin, mutta kyseisen solun kommentiksi on kirjattu vaatimuksen tai hallintakeinon tarkempi tekstikuvaus. Puuteanalyysin kolme isompaa kategoriaa on vielä tarvittaessa jaettu standardin mukaisesti alaotsikoihin. Jokaiselle vaatimukselle annetaan arvoksi: OK jos vaatimus täyttyy, NOT OK, jos vaatimus ei täyty, tai N/A jos kyseinen vaatimus tai hallintakeino ei koske yrityksen hallintajärjestelmän rajausta. Vastaukset on koottu jokaiselle otsikko tasolle taulukon selkeyttämiseksi.

Excel taulukko laskee annetuista arvoista prosenttiarvon täyttyneiden arvojen, N/A arvojen ja kyseisen vaatimusotsikon vaatimusten kokonaismäärän perusteella yhtälön 1 mukaisesti. Tämän prosenttiarvon avulla voidaan arvioida, kuinka valmis yritys on kyseisessä aihealueessa ja siten kyseisessä standardin aihealueessa (mitä lähempänä 100 % sitä parempi). Puuteanalyysi löytyy työn liitteinä 1–4.

$$X = \frac{A+C}{N} \quad (1)$$

missä X = prosenttiarvo valmiudesta
A = täyttyneiden vaatimusten lukumäärä
C = N/A arvon saaneiden vaatimusten lukumäärä
N = Kyseisen alakohdan vaatimusten kokonaismäärä

5.2 Puuteanalyysin toteutus

Puuteanalyysi toteutetaan haastattelemalla yrityksen tietoturvatiimin jäseniä, sekä muita oleellisia henkilöitä ja käymällä läpi kaikki standardin vaatimukset luodun Excel taulukon avulla. Haastattelun ja vastausten perusteella jokaiseen kohtaan annetaan arvo (OK, NOT OK, N/A). Kun taulukko on käsitelty kokonaan, saadaan yleiskuva yrityksen tilasta ISO/IEC27001 vaatimuksia vastaan.

6 Tulokset ja yhteenveto

Puuteanalyysin tulokset koottiin Excel taulukkoon omalle sivulleen pääotsikoittain ja vielä kokonaisuutena, josta saatiin suuntaa antava prosenttiluku yrityksen valmiudesta ISO/IEC 27001 sertifiointiin. Ymmärrettävästi näitä lukuja ei voi seurata sokeasti, vaan kaikki nämä kohdat on käytävä uudelleen läpi, jos ja kun yritys aloittaa ISO/IEC 27001 sertifioitumisprosessin. Ylätason aiheet ja niiden kootut tulokset on esitetty taulukoissa 1.–3., yllättävästi monet ISO/IEC 27001 Liite A:n hallintakeinot olivat jo jossain määrin käytössä yrityksen toiminnassa, vaikka kyseisiä toimia ei ole otettu käyttöön standardia mielessä pitäen.

6.1 Puuteanalyysin tulokset

Taulukossa 1 näkyvät standardin liitteen A hallintatavoitteiden ja hallintakeinojen luettelon mukaiset tulokset yläotsikoittain koottuna. Standardia käyttöönotettaessa liite A:n luettelon jokainen kohta tulee käydä läpi ja perustella hallintakeinon käyttö tai käyttämättä jättäminen. Standardissa kehotetaan käyttämään Liite A:n luetteloa standardin käyttäjille, jotta tarvittavia hallintatavoitteita tai hallintakeinoja jätetä huomiotta. (SFS-EN ISO/IEC 27001:2017, 9.) Näiden tulosten mukaan yritys olisi suhteellisen valmis Liite A:n hallintakeinojen osalta prosenttiarvolla 73 %. Tämä tulos on todennäköisesti korkeampi kuin mitä yrityksen varsinainen valmius standardin mukaiseen toteutukseen, sillä hallintakeinoja ei ole otettu keskitetysti ja hallitusti käyttöön, vaan ne ovat toteutettu irrallisina toisistaan.

Taulukko 1. ISO/IEC 27001 Liite A: tulokset (SFS-EN ISO/IEC 27001:2017, 2).

ID	OTSIKKO	OK	NOT OK	N/A	YHTEENSÄ	%
5	TIETOTURVAPOLITIIKAT	1	1	0	2	50 %
6	TIETOTURVALLISUUDEN ORGANISOINTI	4	2	1	7	71 %
7	HENKILÖSTÖTURVALLISUUS	4	0	2	6	100 %
8	SUOJATTAVAN OMAISUUDEN HALLINTA	5	4	1	10	60 %
9	PÄÄSYNHALLINTA	7	4	3	14	71 %
10	SALAUS	0	2	0	2	0 %
11	FYYSINEN TURVALLISUUS JA YMPÄRISTÖN TURVALLISUUS	11	2	2	15	87 %
12	KÄYTTÖTURVALLISUUS	9	4	1	14	71 %
13	VIESTINTÄTURVALLISUUS	5	1	1	7	86 %
14	JÄRJESTELMIEN HANKKIMINEN, KEHITTÄMINEN JA YLLÄPITO	7	4	2	13	69 %
15	SUHTEET TOIMITTAJIIN	1	1	3	5	80 %
16	TIETOTURVAHÄIRIÖIDEN HALLINTA	6	1	0	7	86 %
17	LIIKETOIMINNAN JATKUVUUDEN HALLINTAAN LIITTYVIÄ TIETOTURVANÄKÖKOHTIA	1	2	1	4	50 %
18	VAATIMUSTENMUKAISUUS	4	3	1	8	63 %
	Liite A koonti	**65**	**31**	**18**	**114**	**73 %**

Toisena kokonaisuutena oli standardin eksplisiittiset vaatimukset, jotka pitää olla määritelty tai toteutettu, jotta standardiin voi sertifioitua. Tässä kategoriassa tuli jo selvästi pienempi tulos, 27 % ja useammasta alakohdasta 0 %. Tulos oli odotettavissa, sillä yritys ei ole vielä aloittanut standardin käyttöönottoa ja monet tämän kategorian vaatimuksista on standardiin liittyvien asioiden määrittämistä. Kyseisiä asioita ei välttämättä tule erikseen määriteltyä yrityksissä, jotka eivät yritä noudattaa tätä tai muita standardeja. Standardin vaatimusten tulokset esitetään taulukossa 2.

Taulukko 2. Standardin vaatimukset: tulokset

ID	OTSIKKO	OK	NOT OK	N/A	YHTEENSÄ	%
4	ORGANISAATION TOIMINTAYMPÄRISTÖ	0	5	0	5	0 %
5	JOHTAJUUS	10	7	0	17	59 %
6	SUUNNITTELU	7	16	3	26	38 %
7	TUKITOIMINNOT	2	22	0	24	8 %
8	TOIMINTA	0	3	0	3	0 %
9	SUORITUSKYVYN ARVIOINTI	0	19	0	19	0 %
10	PARANTAMINEN	5	2	1	8	75 %
	Vaatimukset koonti	**24**	**74**	**4**	**102**	**27 %**

Viimeisenä kokonaisuutena oli standardin vaatiman dokumentoidun tiedon vaatimukset. Yhteensä standardissa mainitaan 14 asiaa mitkä pitää löytyä dokumentoituna tietona. Taulukossa 3 esitetään koonti dokumentoidun tiedon tuloksista.

Taulukko 3. Dokumentoitu tieto: tulokset

OTSIKKO	OK	NOT OK	N/A	YHTEENSÄ	%
DOKUMENTOITU TIETO	3	11	0	14	21 %

6.2 Tulosten yhteenveto

Kaikkiaan puuteanalyysissä käsiteltiin 230 erillistä kohtaa. Kaikkien kategorioiden koonti esitetään taulukossa 4. Lopulliseksi prosenttiarvoksi yritys sai 50 %, mikä on yllättävän korkea arvo ottaen huomioon, ettei yrityksellä ole ollut laatustandardia käytössä ennen puuteanalyysin toteutusta. Tulokseen tosin vaikuttaa taulukon 1. tulosten arvioitu liian korkea tulos, sillä sitä koskevia hallintakeinoja ei ole otettu keskitetysti käyttöön.

Taulukko 4. Puuteanalyysin tulokset koottuna

ID	OTSIKKO	OK	NOT OK	N/A	YHTEENSÄ	%
A	Liite A	65	31	18	114	73 %
B	Vaatimukset	24	74	4	102	27 %
C	Dokumentoitu tieto	3	11	0	14	21 %
	Kaikkien koonti	**92**	**116**	**22**	**230**	**50 %**

Näiden tulosten pohjalta yritys voi arvioida mihin alueisiin pitää keskittää enemmän resursseja, kun ISO/IEC 27001 käyttöönottoa aletaan toteuttaa. Vaikka tulokset ovat suuntaa antavia, ne ovat arvokasta tietoa käyttöönottoa suunnitellessa.

7 Pohdinta

Opinnäytetyössä toteutettiin puuteanalyysi kohdeyritykselle, joka aikoo aloittaa ISO/IEC 27001 standardiin sertifioitumisen lähitulevaisuudessa. Työn tavoitteena oli luoda tietoperustaa yritykselle sen nykytilasta, jotta standardin mukaiseen toteutukseen siirtyminen ja sitä kautta standardiin sertifioituminen olisi helpompaa. Puuteanalyysissä käsiteltiin kaikki ISO/IEC 27001 standardin vaatimukset, sen liitteen A mukaiset hallintatavoitteet ja -keinot, sekä vielä erikseen vaadittu dokumentoitu tieto. Tuloksena saatiin jokaiselle vaatimukselle arvo OK / NOT OK / N/A ja alakohdittain prosenttiarvo, joka laskettiin yhtälön 1 mukaisesti.

Työssä onnistuttiin kartoittamaan yrityksen nykytila ja saamaan siitä tuloksia, joita yritys voi käyttää tulevassa standardin käyttöönottoprojektissa. Tulokset koottiin kategorioittain ja kaikki yhteensä, josta lopulliseksi prosenttiarvoksi saatiin 50 %. Tämä tulos yllättävän korkea, sillä yrityksellä ei ole aiemmin ollut käytössä laatustandardia.

Puuteanalyysiä on käytetty standardisoimis- tarkoitukseen esimerkiksi ICT-alalla, kuten Peltier (2010) toteaa kirjassaan. Siinä hän kertoo käyttäneensä puuteanalyysiä juuri ISO 27001 sertifioinnin pohjana. Vastaavasti puuteanalyysiä voitaisiin varmasti käyttää myös ISO 9001 sertifiointiin valmistautumisen apuvälineenä. Opinnäytteessä oli myös tavoitteena saada riittävät pohjatiedot ISO/IEC 27001 standardiin ja sen taustoihin, jotta sitä voidaan verrata yrityksen nykytilaan. Opinnäytetyössä on käsitelty kattavasti ISO/IEC 27000 standardisarjaa ja myös tarkemmin sen eri osia, tärkeimpänä ISO/IEC 27001.

7.1 Luotettavuusanalyysi

Työn tutkimusosuudessa valmisteltu puuteanalyysi, joka toimi käytännössä pitkänä kyselynä, onko kyseinen vaatimus yrityksessä kunnossa vai ei. Vastaukset näihin saatiin haastattelemalla kysymykselle oleellista henkilökuntaa, keillä on tietoa yrityksen tilasta kyseisen vaatimuksen tilasta. Tarvittaessa vaatimuksen tekstiä ja merkitystä avattiin haastateltaville, jotta kysymyksen merkitys oli selvä. Tämä lisää tutkimustulosten luotettavuutta, sillä se vähentää väärinkäsitysten ja sitä kautta virheellisten määrää. Jotta puuteanalyysin tulokset olisivat mahdollisimman tarkkoja ja kuvaavia, pitäisi näiden ihmisten olla täysin varmoja vaatimuksen nykytilasta, mutta tämä ei tietysti ihmisten kohdalla aina pidä paikkaansa. Ihmiset saattavat kaunistella asioita tai antaa tiettyä suuntaa puoltavan vastauksen, jolloin tulokset vääristyvät. Kuitenkin haastatellut olivat työssä nimettömiä, joten heillä ei pitäisi olla syytä vääristellä totuutta, mikä lisää tutkimuksen luotettavuutta. Tätä on kuitenkin lähes mahdotonta mitata, joten se on pitänyt jättää konkreettisten tulosten ulkopuolelle, mutta silti tärkeää pitää mielessä.

Puuteanalyysin tuloksen korkeuteen vaikuttaa myös se, ettei yksittäisen vaatimuksen toteuttamisen työläyttä ole otettu huomioon. Esimerkiksi yksittäinen hallintakeino ja tietoturvariskikriteerien luominen eivät ole toteutuksen tasolla yhtä työläitä, mutta ne arvioidaan puuteanalyysissä samalla asteikolla ja vaikuttavat lopputulokseen saman verran. Toisaalta osa vaatimuksista olettaa, että hallintajärjestelmä on jo luotu, näiden kohdalla on valittu arvo N/A, joka samalla vääristää tuloksia.

Tämä korostaa sitä lähestymistä, että tulokset ovat suuntaa antavia, eivätkä suora totuus yrityksen nykytilasta standardia ajatellen.

Puuteanalyysin toteutus on kuitenkin onnistunut, sillä sekä puuteanalyysiä että sen tuloksia voidaan käyttää tietoperustana, kun yritys aloittaa standardin mukaisiin toimintatapoihin ja vaatimuksiin siirtymisen. Tulosten perusteella yrityksen on mahdollista arvioida standardin käyttöönoton vaativuutta ja mihin aihealueisiin tulee erityisesti keskittää resursseja. Puuteanalyysiä olisi mahdollista kehittää luomalla vaatimuksille painoarvot niiden tärkeyden tai toteutuksen työläyden perusteella. Täten tulokset tarkentuisivat ja vastaisivat paremmin yrityksen valmiutta standardin vaatimuksiin.

7.2 Eettisyys

Työssä on huomioitu hyvät eettiset periaatteet ja tieteellinen käytäntö. Työn toimeksiantaja on tekstissä anonymisoitu. Haastateltavilta ei ole kerätty nimi- tai muita henkilötietoja, sillä heiltä tarvittiin vain vastaus vaatimuksen tilaan yrityksessä. Hyvää tieteellistä käytäntöä on noudatettu lähteiden käyttämisellä ja merkitsemisellä, sekä tekstiviitteiden käytöllä.

7.3 Jatko

Seuraavaksi yrityksen tulisi luoda projektiryhmä suunnittelemaan ja aloittamaan standardiin siirtymisen prosessia. ISO/IEC 27001 on suuri kokonaisuus ja sen käyttöönottoon tulee sitouttaa erityisesti yrityksen johto, jotta projektille voidaan varmistaa riittävät resurssit. Tämän lisäksi yrityksen johdon kautta standardin mukaiset prosessit ja toimintamallit on mahdollista ottaa käyttöön koko yrityksen laajuisesti. Vaihtoehtoisesti ISO 9001 laadunhallinta standardi voisi sopia yrityksen tarpeisiin, sillä molemmilla standardeilla on runsaasti päällekkäisyyttä. Molemmat ovat prosessilähtöisiä, riskiperustaisia hallintajärjestelmästandardeja, joiden avulla voidaan parantaa sekä asiakastyytyväisyyttä että palveluiden ja tuotteiden luotettavuutta. Tosin, koska työssä ei tarkemmin paneuduttu ISO 9001 standardiin, on sitä vaikeampi suositella ISO/IEC 27001 sijasta, jota toimeksiantaja erikseen pyysi selvittämään.

Molempien standardien kohdalla ensimmäiseksi yrityksen tulee hankkia standarditeksti ja tutustua siihen ja sitä tukeviin dokumentteihin huolella. Tätä seuraisi projektiryhmän luominen ja valitun

standardin toteutuksen aloitus. Yrityksen kannattaa myös harkita konsulttipalveluita standardin hankintaa varten.

Lähteet

About Us - What we do. N.d. Artikkeli iso.org www-sivuilla. Viitattu 20.10.2020. https://www.iso.org/what-we-do.html.

ISO27001-puuteanalyysi. 2018. Artikkeli Insta Group Oy:n www-sivuilla. Julkaistu 2.8.2018. Viitattu 14.7.2021 https://www.insta.fi/nakemyksia/tietoturvapalvelut/iso27001-puuteanalyysi.

ISO/IEC 27001 Certification Process. N.d. Blogi julkaisu pivotpointsecurity.com www-sivuilla. Viitattu 23.05.2021. https://www.pivotpointsecurity.com/iso-27001/iso-27001-certification-process/.

ISO/IEC 27000 Tietoturvallisuuden standardisarja. N.d. Verkkojulkaisu sfs.fi www-sivuilla. Viitattu 19.11.2021. https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-iec-27000-tietoturvallisuuden-standardisarja/.

ISO/IEC 27001 – information security management system. N.d. Verkkojulkaisu dnv.com www-sivuilla. Viitattu 19.11.2021. https://www.dnv.com/services/iso-iec-27001-information-security-management-system-3327.

ISO/IEC JTC 1. N.d. Verkkojulkaisu iso.org www-sivuilla. Viitattu 13.10.2021. https://www.iso.org/committee/45020.html.

ISO 9001 Laadunhallinta. N.d. Verkkojulkaisu sfs.fi www-sivuilla. Viitattu 19.11.2021 https://sfs.fi/standardeista/tutustu-standardeihin/suositut-standardit/iso-9001-laadunhallinta/.

ISO 9001 – Quality management. N.d. Verkkojulkaisu dnv.com www-sivuilla. Viitattu 19.11.2021. https://www.dnv.com/services/iso-9001-quality-management-3283.

ISO IEC 27001 Implementation & certification. N.d. Artikkeli Certaim.com www-sivuilla. Viitattu 15.11.2020. https://certaim.com/isoiec-27001-certification/.

JTC 1 Strategic Business Plan. 2020. Verkkojulkaisu iso.org verkkosivuilla. Julkaistu 11.2020. Viitattu 14.10.2021. https://www.iso.org/files/live/sites/isoorg/files/developing_standards/who_develops_standards/docs/JTC%201%20Strategic%20Business%20Plan%20November%202020.pdf.

Lazarte, M. 2016. No trust in world without standards. Artikkeli iso.org www-sivuilla. Viitattu 19.11.2021. https://www.iso.org/news/2016/10/Ref2128.html.

Luottamuksen lähteillä. 2019. Verkkojulkaisu Kyberturvallisuuskeskuksen www-sivuilla. Viitattu 11.02.2021. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Luottamuksen_lahteilla.pdf.

Members. N.d. Artikkeli iso.org www-sivuilla. Viitattu 22.10.2020. https://www.iso.org/members.html.

Namugenyi, C., Nimmagadda, S.L. & Reiners, T. 2017. Design of a SWOT Analysis Model and its Evaluation in Diverse Digital Business Ecosystem Contexts. Artikkeli dspacedirect.org www-sivuilla. Julkaistu 11.08.2017. Viitattu 19.10.2021. https://demo.dspacedirect.org/handle/10673/792.

National Committees. N.d. Artikkeli iec.ch www-sivuilla. Viitattu 14.10.2021. https://www.iec.ch/national-committees.

Peltier, T. R. 2010. Information security risk analysis. 3rd ed. Boca Raton, Fla.: Auerbach Publications.

Pournader, B. 2018. 6 Steps to get ISO 27000. Verkkojulkaisu medium.com www-sivuilla. Julkaistu 11.04.2018. Viitattu 13.05.2021. https://benpournader.medium.com/6-steps-to-get-iso-27000-9a85dfee2633.

SESKO ry. N.d. Verkkojulkaisu sesko.fi www-sivuilla. Viitattu 14.10.2021. https://www.sesko.fi/sesko_ry.

SFS-EN ISO/IEC 27000:2020. Yleiskuvaus ja sanasto. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.02.2020. Viitattu 10.10.2020. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27001:2017. Vaatimukset. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 02.06.2017. Viitattu 15.10.2021. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27002:2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Aihealueet: Informaatioteknologia, turvallisuustekniikat. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 03.03.2017. Viitattu 24.11.2020. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27003:2017. Ohjeistusta. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 10.11.2017. Viitattu 16.02.2021. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27004:2016. Seuranta, mittaus, analysointi ja arviointi. Aihealueet: Informaatioteknologia, turvallisuustekniikat, tietoturvallisuuden hallintajärjestelmät. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 30.12.2017. Viitattu 10.10.2020. https://janet.finna.fi, SFS Online.

SFS-EN ISO/IEC 27005:2018. Tietoturvariskien hallinta. Aihealueet: Informaatioteknologia, turvallisuustekniikat. Helsinki: Suomen Standardisoimisliitto SFS. Vahvistettu 28.12.2018. Viitattu 18.10.2020. https://janet.finna.fi, SFS Online.

Standardeista on hyötyä meille kaikille. N.d. Artikkeli sfs.fi www-sivuilla. Viitattu 19.11.2021. https://sfs.fi/standardeista/standardien-hyodyt/.

The ISO survey. 2020. Verkkojulkaisu iso.org www-sivuilla. Viitattu 19.11.2021. https://www.iso.org/the-iso-survey.html.

Valli, R. & Aarnos, E. 2018. Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle. 5., uudistettu painos. Jyväskylä: PS-kustannus.

Watkins, S. & Orchiston, N. 2016. ISO 9001: 2015 : a pocket guide. Cambridgeshire: IT Governance Publishing.

What is a Gap Analysis? N.d. Artikkeli techtarget.com www-sivuilla. Viitattu 19.10.2021 https://searchcio.techtarget.com/definition/gap-analysis.

What we do. N.d. Artikkeli iec.ch www-sivuilla Viitattu 29.10.2020. https://www.iec.ch/what-we-do.

Liitteet

Liite 1. Puuteanalyysin tulosten koonti

Liite A:n tietoturvakontrollien tulokset						
ID	Otsikko	OK	NOT OK	N/A	Yhteensä	%
A.5	TIETOTURVAPOLITIIKAT	1	1	0	2	50 %
A.6	TIETOTURVALLISUUDEN ORGANISOINTI	4	2	1	7	71 %
A.7	HENKILÖSTÖTURVALLISUUS	4	0	2	6	100 %
A.8	SUOJATTAVAN OMAISUUDEN HALLINTA	5	4	1	10	60 %
A.9	PÄÄSYNHALLINTA	7	4	3	14	71 %
A.10	SALAUS	0	2	0	2	0 %
A.11	FYYSINEN TURVALLISUUS JA YMPÄRISTÖN TURVALLISUUS	11	2	2	15	87 %
A.12	KÄYTTÖTURVALLISUUS	9	4	1	14	71 %
A.13	VIESTINTÄTURVALLISUUS	5	1	1	7	86 %
A.14	JÄRJESTELMIEN HANKKIMINEN, KEHITTÄMINEN JA YLLÄPITO	7	4	2	13	69 %
A.15	SUHTEET TOIMITTAJIIN	1	1	3	5	80 %
A.16	TIETOTURVAHÄIRIÖIDEN HALLINTA	6	1	0	7	86 %
A.17	LIIKETOIMINNAN JATKUVUUDEN HALLINTAAN LIITTYVIÄ TIETOTURVANÄKÖKOHTIA	1	2	1	4	50 %
A.18	VAATIMUSTENMUKAISUUS	4	3	1	8	63 %
A	**Liite A koonti**	**65**	**31**	**18**	**114**	**73 %**

ISO/IEC 27001 vaatimusten tulokset						
ID	Otsikko	OK	NOT OK	N/A	Yhteensä	%
4	ORGANISAATION TOIMINTAYMPÄRISTÖ	0	5	0	5	0 %
5	JOHTAJUUS	10	7	0	17	59 %
6	SUUNNITTELU	7	16	3	26	38 %
7	TUKITOIMINNOT	2	22	0	24	8 %
8	TOIMINTA	0	3	0	3	0 %
9	SUORITUSKYVYN ARVIOINTI	0	19	0	19	0 %
10	PARANTAMINEN	5	2	1	8	75 %
B	**Vaatimukset koonti**	**24**	**74**	**4**	**102**	**27 %**

Dokumentoidun tiedon tulokset						
ID	Otsikko	OK	NOT OK	N/A	Yhteensä	%
C	**Dokumentoitu tieto**	**3**	**11**	**0**	**14**	**21 %**

Kaikkien koonti						
ID	Otsikko	OK	NOT OK	N/A	Yhteensä	%
A	Liite A koonti	65	31	18	114	73 %
B	Vaatimukset koonti	24	74	4	102	27 %
C	Dokumentoitu tieto	3	11	0	14	21 %
	Kaikkien koonti	**92**	**116**	**22**	**230**	**50 %**

Liite 2. Liite A:n hallintakeinot ja tulokset

ID	Otsikko	Tila	OK	NOT OK	N/A	Yhteensä	%
A.5	**TIETOTURVAPOLITIIKAT**		**1**	**1**	**0**	**2**	**50 %**
A.5.1	**Johdon ohjaus tietoturvallisuutta koskevissa asioissa**						
A.5.1.1	Tietoturvapolitiikat	OK					
A.5.1.2	Tietoturvapolitiikkojen katselmointi	NOT OK					
A.6	**TIETOTURVALLISUUDEN ORGANISOINTI**		**4**	**2**	**1**	**7**	**71 %**
A.6.1	**Sisäinen organisaatio**		4	0	1	5	100 %
A.6.1.1	Tietoturvaroolit ja -vastuut	OK					
A.6.1.2	Tehtävien eriyttäminen	N/A					
A.6.1.3	Yhteydet viranomaisiin	OK					
A.6.1.4	Yhteydet osaamisyhteisöihin	OK					
A.6.1.5	Tietoturvallisuus projektinhallinnassa	OK					
A.6.2	**Mobiililaitteet ja etätyö**		0	2	0	2	0 %
A.6.2.1	Mobiililaitteita koskeva politiikka	NOT OK					
A.6.2.2	Etätyö	NOT OK					
A.7	**HENKILÖSTÖTURVALLISUUS**		**4**	**0**	**2**	**6**	**100 %**
A.7.1	**Ennen työsuhteen alkua**		2	0	0	2	100 %
A.7.1.1	Taustatarkistus	OK					
A.7.1.2	Työsopimuksen ehdot	OK					
A.7.2	**Työsuhteen aikana**		2	0	1	3	100 %
A.7.2.1	Johdon vastuut	OK					
A.7.2.2	Tietoturvatietoisuus, -opastus ja -koulutus	OK					
A.7.2.3	Kurinpitoprosessi	N/A					
A.7.3	**Työsuhteen päättyminen tai muuttuminen**		0	0	1	1	100 %
A.7.3.1	Työsuhteen päättyminen tai vastuiden muuttuminen	N/A					
A.8	**SUOJATTAVAN OMAISUUDEN HALLINTA**		**5**	**4**	**1**	**10**	**60 %**
A.8.1	**Vastuu suojattavasta omaisuudesta**		2	1	1	4	75 %
A.8.1.1	Suojattavan omaisuuden luetteloiminen	OK					
A.8.1.2	Suojattavan omaisuuden omistajuus	NOT OK					
A.8.1.3	Suojattavan omaisuuden hyväksyttävä käyttö	N/A					
A.8.1.4	Suojattavan omaisuuden palauttaminen	OK					
A.8.2	**Tietojen luokittelu**		0	3	0	3	0 %
A.8.2.1	Tiedon luokittelu	NOT OK					
A.8.2.2	Tiedon merkintä	NOT OK					
A.8.2.3	Suojattavan omaisuuden käsittely	NOT OK					
A.8.3	**Tietovälineiden käsittely**		3	0	0	3	100 %
A.8.3.1	Siirrettävien tietovälineiden hallinta	OK					
A.8.3.2	Tietovälineiden hävittäminen	OK					
A.8.3.3	Fyysisten tietovälineiden siirtäminen	OK					
A.9	**PÄÄSYNHALLINTA**		**7**	**4**	**3**	**14**	**71 %**
A.9.1	**Pääsynhallinnan liiketoiminnalliset vaatimukset**		1	1	0	2	50 %
A.9.1.1	Pääsynhallintapolitiikka	NOT OK					
A.9.1.2	Pääsy verkkoihin ja verkkopalveluihin	OK					
A.9.2	**Pääsyoikeuksien hallinta**		3	2	1	6	67 %
A.9.2.1	Käyttäjien rekisteröinti ja poistaminen	NOT OK					
A.9.2.2	Pääsyoikeuksien jakaminen	OK					
A.9.2.3	Ylläpito-oikeuksien hallinta	OK					
A.9.2.4	Käyttäjien tunnistautumistietojen hallinta	N/A					
A.9.2.5	Pääsyoikeuksien uudelleenarviointi	NOT OK					
A.9.2.6	Pääsyoikeuksien poistaminen tai muuttaminen	OK					
A.9.3	**Käyttäjän vastuut**		1	0	0	1	100 %
A.9.3.1	Tunnistautumistietojen käyttö	OK					
A.9.4	**Järjestelmien ja sovellusten pääsynhallinta**		2	1	2	5	80 %
A.9.4.1	Tietoihin pääsyn rajoittaminen	NOT OK					
A.9.4.2	Turvallinen kirjautuminen	OK					
A.9.4.3	Salasanojen hallintajärjestelmä	OK					
A.9.4.4	Ylläpito- ja hallintasovellukset	N/A					
A.9.4.5	Lähdekoodin suojaaminen pääsynvalvonnalla	N/A					
A.10	**SALAUS**		**0**	**2**	**0**	**2**	**0 %**
A.10.1	**Salauksen hallinta**						
A.10.1.1	Salauksen käytön periaatteet	NOT OK					
A.10.1.2	Salausavainten hallinta	NOT OK					
A.11	**FYYSINEN TURVALLISUUS JA YMPÄRISTÖN TURVALLISUUS**		**11**	**2**	**2**	**15**	**87 %**
A.11.1	**Turva-alueet**		5	0	1	6	100 %
A.11.1.1	Fyysinen turva-alue	OK					
A.11.1.2	Kulunvalvonta	OK					
A.11.1.3	Toimistojen, tilojen ja laitteistojen suojaus	OK					
A.11.1.4	Suojaus ulkoisia ja ympäristön aiheuttamia uhkia vastaan	OK					
A.11.1.5	Turva-alueilla työskentely	N/A					
A.11.1.6	Toimitus- ja kuormausalueet	OK					
A.11.2	**Laitteet**		6	2	1	9	78 %
A.11.2.1	Laitteiden sijoitus ja suojaus	OK					
A.11.2.2	Peruspalvelut	OK					
A.11.2.3	Kaapeloinnin turvallisuus	N/A					
A.11.2.4	Laitteiden huolto	OK					

A.11.2.5	Suojattavan omaisuuden poistaminen	NOT OK					
A.11.2.6	Toimitilojen ulkopuolelle vietyjen laitteiden ja suojattavan omaisuuden turvallisuus	OK					
A.11.2.7	Laitteiden turvallinen käytöstä poistaminen ja kierrättäminen	OK					
A.11.2.8	Ilman valvontaa jäävät laitteet	OK					
A.11.2.9	Puhtaan pöydän ja puhtaan näytön periaate	NOT OK					
A.12	**KÄYTTÖTURVALLISUUS**		**9**	**4**	**1**	**14**	**71 %**
A.12.1	**Toimintaohjeet ja velvollisuudet**		3	1	0	4	75 %
A.12.1.1	Dokumentoidut toimintaohjeet	OK					
A.12.1.2	Muutoksenhallinta	NOT OK					
A.12.1.3	Kapasiteetinhallinta	OK					
A.12.1.4	Kehitys-, testaus- ja tuotantoympäristöjen erottaminen	OK					
A.12.2	**Haittaohjelmilta suojautuminen**		1	0	0	1	100 %
A.12.2.1	Haittaohjelmilta suojautuminen	OK					
A.12.3	**Varmuuskopiointi**		1	0	0	1	100 %
A.12.3.1	Tietojen varmuuskopiointi	OK					
A.12.4	**Kirjaaminen ja seuranta**		2	1	1	4	75 %
A.12.4.1	Tapahtumien kirjaaminen	OK					
A.12.4.2	Lokitietojen suojaaminen	NOT OK					
A.12.4.3	Pääkäyttäjä- ja operaattorilokit	OK					
A.12.4.4	Kellojen synkronointi	N/A					
A.12.5	**Tuotantokäytössä olevien ohjelmistojen hallinta**		1	0	0	1	100 %
A.12.5.1	Ohjelmistojen asentaminen tuotantokäytössä oleviin järjestelmiin	OK					
A.12.6	**Teknisten haavoittuvuuksien hallinta**		1	1	0	2	50 %
A.12.6.1	Teknisten haavoittuvuuksien hallinta	OK					
A.12.6.2	Ohjelmien asentamisen rajoittaminen	NOT OK					
A.12.7	**Tietojärjestelmien auditointinäkökohtia**		0	1	0	1	0 %
A.12.7.1	Tietojärjestelmien auditointimekanismit	NOT OK					
A.13	**VIESTINTÄTURVALLISUUS**		**5**	**1**	**1**	**7**	**86 %**
A.13.1	**Verkon turvallisuuden hallinta**		3	0	0	3	100 %
A.13.1.1	Verkon hallinta	OK					
A.13.1.2	Verkkopalvelujen turvaaminen	OK					
A.13.1.3	Ryhmien eriyttäminen verkossa	OK					
A.13.2	**Tietojen siirtäminen**		2	1	1	4	75 %
A.13.2.1	Tiedonsiirtopolitiikat ja -menettelyt	NOT OK					
A.13.2.2	Tiedonsiirtoa koskevat sopimukset	N/A					
A.13.2.3	Sähköinen viestintä	OK					
A.13.2.4	Salassapito- ja vaitiolositoumukset	OK					
A.14	**JÄRJESTELMIEN HANKKIMINEN, KEHITTÄMINEN JA YLLÄPITO**		**7**	**4**	**2**	**13**	**69 %**
A.14.1	**Tietojärjestelmiä koskevat turvallisuusvaatimukset**		3	0	0	3	100 %
A.14.1.1	Tietoturvavaatimusten analysointi ja määrittely	OK					
A.14.1.2	Sovelluspalveluiden suojaaminen julkisissa verkoissa	OK					
A.14.1.3	Sovelluspalvelutapahtumien suojaaminen	OK					
A.14.2	**Kehitys- ja tukiprosessien turvallisuus**		4	3	2	9	67 %
A.14.2.1	Turvallisen kehittämisen politiikka	OK					
A.14.2.2	Järjestelmään tehtävien muutosten hallintamenettelyt	OK					
A.14.2.3	Sovellusten tekninen katselmointi käyttöalustan muutosten jälkeen	NOT OK					
A.14.2.4	Ohjelmistopakettien muutoksia koskevat rajoitukset	N/A					
A.14.2.5	Turvallisen järjestelmäsuunnittelun periaatteet	NOT OK					
A.14.2.6	Turvallinen kehitysympäristö	OK					
A.14.2.7	Ulkoistettu kehittäminen	N/A					
A.14.2.8	Järjestelmän turvallisuustestaus	OK					
A.14.2.9	Järjestelmän hyväksymistestaus	NOT OK					
A.14.3	**Testiaineisto**		0	1	0	1	0 %
A.14.3.1	Testiaineiston suojaaminen	NOT OK					
A.15	**SUHTEET TOIMITTAJIIN**		**1**	**1**	**3**	**5**	**80 %**
A.15.1	**Tietoturvallisuus toimittajasuhteissa**		1	0	2	3	100 %
A.15.1.1	Toimittajasuhteiden tietoturvapolitiikka	N/A					
A.15.1.2	Toimittajasopimusten turvallisuus	N/A					
A.15.1.3	Tieto- ja viestintäteknikan toimitusketju	OK					
A.15.2	**Toimittajien palveluiden hallinta**		0	1	1	2	50 %
A.15.2.1	Toimittajien palvelujen seuranta ja katselmointi	NOT OK					
A.15.2.2	Toimittajan palveluihin tulevien muutosten hallinta	N/A					
A.16	**TIETOTURVAHÄIRIÖIDEN HALLINTA**		**6**	**1**	**0**	**7**	**86 %**
A.16.1	**Tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta**						
A.16.1.1	Vastuut ja menettelyt	OK					
A.16.1.2	Tietoturvatapahtumien raportointi	OK					
A.16.1.3	Tietoturvaheikkouksien raportointi	OK					
A.16.1.4	Tietoturvatapahtumien arviointi ja niitä koskevien päätösten tekeminen	OK					
A.16.1.5	Tietoturvahäiriöihin vastaaminen	OK					
A.16.1.6	Tietoturvahäiriöistä oppiminen	OK					
A.16.1.7	Todisteiden kokoaminen	NOT OK					
A.17	**LIIKETOIMINNAN JATKUVUUDEN HALLINTAAN LIITTYVIÄ TIETOTURVANÄKÖKOHTIA**		**1**	**2**	**1**	**4**	**50 %**
A.17.1	**Tietoturvallisuuden jatkuvuus**		0	2	1	3	33 %
A.17.1.1	Tietoturvallisuuden jatkuvuuden suunnittelu	NOT OK					
A.17.1.2	Tietoturvallisuuden jatkuvuuden toteuttaminen	NOT OK					

A.17.1.3	Tietoturvallisuuden jatkuvuuden todentaminen, katselmointi ja arviointi	N/A				
A.17.2	**Vikasietoisuus**		1	0	1	100 %
A.17.2.1	Tietojenkäsittelypalvelujen saatavuus	OK				
A.18	**VAATIMUSTENMUKAISUUS**		**4**	**3**	**8**	**63 %**
A.18.1	**Lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen**		4	1	5	80 %
A.18.1.1	Sovellettavien lakisääteisten ja sopimuksellisten vaatimusten yksilöiminen	NOT OK				
A.18.1.2	Immateriaalioikeudet	OK				
A.18.1.3	Tallenteiden suojaaminen	OK				
A.18.1.4	Tietosuoja ja henkilötietojen suojaaminen	OK				
A.18.1.5	Salaustekniikan hallintaa koskevat säädökset	OK				
A.18.2	**Tietoturvallisuuden katselmoinnit**		0	2	3	33 %
A.18.2.1	Tietoturvallisuuden riippumaton katselmointi	NOT OK				
A.18.2.2	Turvallisuuspolitiikkojen ja -standardien noudattaminen	N/A				
A.18.2.3	Teknisen vaatimustenmukaisuuden katselmointi	NOT OK				

Liite 3. Standardin vaatimusten tulokset

ID	Otsikko	Tila	OK	NOT OK	N/A	Yhteensä	%
4	**ORGANISAATION TOIMINTAYMPÄRISTÖ**		**0**	**5**	**0**	**5**	**0 %**
4.1	Organisaation ja sen toimintaympäristön ymmärtäminen	NOT OK					
4.2.a	Sidosryhmien tarpeiden ja odotusten ymmärtäminen	NOT OK					
4.2.b	Sidosryhmien tarpeiden ja odotusten ymmärtäminen	NOT OK					
4.3	Tietoturvallisuuden hallintajärjestelmän soveltamisalan määrittäminen	NOT OK					
4.4	Tietoturvallisuuden hallintajärjestelmä	NOT OK					
5	**JOHTAJUUS**		**10**	**7**	**0**	**17**	**59 %**
5.1.a	Johtajuus ja sitoutuminen	OK					
5.1.b	Johtajuus ja sitoutuminen	NOT OK					
5.1.c	Johtajuus ja sitoutuminen	NOT OK					
5.1.d	Johtajuus ja sitoutuminen	NOT OK					
5.1.e	Johtajuus ja sitoutuminen	NOT OK					
5.1.f	Johtajuus ja sitoutuminen	NOT OK					
5.1.g	Johtajuus ja sitoutuminen	NOT OK					
5.1.h	Johtajuus ja sitoutuminen	OK					
5.2.a	Tietoturvapolitiikka	OK					
5.2.b	Tietoturvapolitiikka	OK					
5.2.c	Tietoturvapolitiikka	OK					
5.2.d	Tietoturvapolitiikka	NOT OK					
5.2.e	Tietoturvapolitiikka	OK					
5.2.f	Tietoturvapolitiikka	OK					
5.2.g	Tietoturvapolitiikka	OK					
5.3.a	Organisaation roolit, vastuut ja valtuudet	OK					
5.3.b	Organisaation roolit, vastuut ja valtuudet	OK					
6	**SUUNNITTELU**		**7**	**16**	**3**	**26**	**38 %**
6.1	**Riskien ja mahdollisuuksien käsittely**						
6.1.1.a	Yleistä	NOT OK					
6.1.1.b	Yleistä	OK					
6.1.1.c	Yleistä	OK					
6.1.1.d	Yleistä	OK					
6.1.1.e	Yleistä	OK					
6.1.2.a	Tietoturvariskien arviointi	NOT OK					
6.1.2.b	Tietoturvariskien arviointi	NOT OK					
6.1.2.c	Tietoturvariskien arviointi	OK					
6.1.2.d	Tietoturvariskien arviointi	NOT OK					
6.1.2.e	Tietoturvariskien arviointi	NOT OK					
6.1.3.a	Tietoturvariskien käsittely	NOT OK					
6.1.3.b	Tietoturvariskien käsittely	NOT OK					
6.1.3.c	Tietoturvariskien käsittely	N/A					
6.1.3.d	Tietoturvariskien käsittely	NOT OK					
6.1.3.e	Tietoturvariskien käsittely	NOT OK					
6.1.3.f	Tietoturvariskien käsittely	NOT OK					
6.2.a	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	OK					
6.2.b	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	N/A					
6.2.c	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	N/A					
6.2.d	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	NOT OK					
6.2.e	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	OK					
6.2.f	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	NOT OK					
6.2.g	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	NOT OK					
6.2.h	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	NOT OK					
6.2.i	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	NOT OK					
6.2.j	Tietoturvatavoitteet ja niiden saavuttamiseen tarvittavien toimien suunnittelu	NOT OK					
7	**TUKITOIMINNOT**		**2**	**22**	**0**	**24**	**8 %**
7.1	Resurssit	NOT OK					
7.2.a	Pätevyys	NOT OK					
7.2.b	Pätevyys	OK					
7.2.c	Pätevyys	OK					
7.2.d	Pätevyys	NOT OK					
7.3.a	Tietoisuus	NOT OK					
7.3.b	Tietoisuus	NOT OK					
7.3.c	Tietoisuus	NOT OK					
7.4.a	Viestintä	NOT OK					
7.4.b	Viestintä	NOT OK					
7.4.c	Viestintä	NOT OK					

7.4.d	Viestintä	NOT OK					
7.4.e	Viestintä	NOT OK					
7.5	**Dokumentoitu tieto**						
7.5.1.a	Yleistä	NOT OK					
7.5.1.b	Yleistä	NOT OK					
7.5.2.a	Dokumentoidun tiedon luominen ja päivittäminen	NOT OK					
7.5.2.b	Dokumentoidun tiedon luominen ja päivittäminen	NOT OK					
7.5.2.c	Dokumentoidun tiedon luominen ja päivittäminen	NOT OK					
7.5.3.a	Dokumentoidun tiedon hallinta	NOT OK					
7.5.3.b	Dokumentoidun tiedon hallinta	NOT OK					
7.5.3.c	Dokumentoidun tiedon hallinta	NOT OK					
7.5.3.d	Dokumentoidun tiedon hallinta	NOT OK					
7.5.3.e	Dokumentoidun tiedon hallinta	NOT OK					
7.5.3.f	Dokumentoidun tiedon hallinta	NOT OK					
8	**TOIMINTA**		**0**	**3**	**0**	**3**	**0 %**
8.1	Toiminnan suunnittelu ja ohjaus	NOT OK					
8.2	Tietoturvariskien arviointi	NOT OK					
8.3	Tietoturvariskien käsittely	NOT OK					
9	**SUORITUSKYVYN ARVIOINTI**		**0**	**19**	**0**	**19**	**0 %**
9.1.a	Seuranta, mittaus, analysointi ja arviointi	NOT OK					
9.1.b	Seuranta, mittaus, analysointi ja arviointi	NOT OK					
9.1.c	Seuranta, mittaus, analysointi ja arviointi	NOT OK					
9.1.d	Seuranta, mittaus, analysointi ja arviointi	NOT OK					
9.1.f	Seuranta, mittaus, analysointi ja arviointi	NOT OK					
9.1.e	Seuranta, mittaus, analysointi ja arviointi	NOT OK					
9.2.a	Sisäinen auditointi	NOT OK					
9.2.b	Sisäinen auditointi	NOT OK					
9.2.c	Sisäinen auditointi	NOT OK					
9.2.d	Sisäinen auditointi	NOT OK					
9.2.e	Sisäinen auditointi	NOT OK					
9.2.f	Sisäinen auditointi	NOT OK					
9.2.g	Sisäinen auditointi	NOT OK					
9.3.a	Johdon katselmus	NOT OK					
9.3.b	Johdon katselmus	NOT OK					
9.3.c	Johdon katselmus	NOT OK					
9.3.d	Johdon katselmus	NOT OK					
9.3.e	Johdon katselmus	NOT OK					
9.3.f	Johdon katselmus	NOT OK					
10	**PARANTAMINEN**		**5**	**2**	**1**	**8**	**75 %**
10.1.a	Poikkeamat ja korjaavat toimenpiteet	OK					
10.1.b	Poikkeamat ja korjaavat toimenpiteet	OK					
10.1.c	Poikkeamat ja korjaavat toimenpiteet	OK					
10.1.d	Poikkeamat ja korjaavat toimenpiteet	NOT OK					
10.1.e	Poikkeamat ja korjaavat toimenpiteet	N/A					
10.1.f	Poikkeamat ja korjaavat toimenpiteet	OK					
10.1.g	Poikkeamat ja korjaavat toimenpiteet	OK					
10.2	Jatkuva parantaminen	NOT OK					

Liite 4. Dokumentoidun tiedon tulokset

ID	Otsikko	Tila	OK	NOT OK	N/A	Yhteensä	%
C	**Dokumentoitu tieto**		**3**	**11**	**0**	**14**	**21 %**
4.3	Hallintajärjestelmän soveltamisala on oltava saatavilla dokumentoituna tietona	NOT OK					
5.2	Tietoturvapolitiikan on oltava saatavilla dokumentoituna tietona	OK					
6.1.2	Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien arviointiprosessista.	NOT OK					
6.1.3	Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien käsittelyprosessista.	NOT OK					
6.2	Organisaation on säilytettävä dokumentoitua tietoa tietoturvatavoitteista.	OK					
7.2	Organisaation on säilytettävä asianmukaista dokumentoitua tietoa näyttönä työntekijöiden pätevyydestä.	NOT OK					
7.5.1	dokumentoitu tieto, jonka organisaatio on määrittänyt tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämättömäksi.	NOT OK					
8.1	Organisaation on säilytettävä riittävästi dokumentoitua tietoa voidakseen luottaa siihen, että prosessit on toteutettu suunnitelmien mukaisesti.	NOT OK					
8.2	Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien arviointien tuloksista	NOT OK					
8.3	Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien käsittelyn tuloksista.	NOT OK					
9.1	Organisaation on säilytettävä asianmukaista dokumentoitua tietoa todisteena seurannan ja mittaamisen tuloksista.	NOT OK					
9.2	säilytettävä dokumentoitua tietoa todisteena auditointiohjelmasta ja auditointien tuloksista.	NOT OK					
9.3	Organisaation on säilytettävä dokumentoitua tietoa todisteena johdon katselmusten tuloksista.	NOT OK					
10.1	Organisaation on säilytettävä dokumentoitua tietoa todisteena poikkeamien luonteesta sekä niiden johdosta tehdyistä toimenpiteistä ja tehtyjen korjaavien toimenpiteiden tuloksista.	OK					