Osaamista
ja oivallusta
tulevaisuuden
tekemiseen

Marko Mantere

ISO/IEC -standardin mukainen puuteanalyysi

Tapaustutkimus

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tieto- ja viestintätekniikan tutkinto-ohjelma

Insinöörityö

Tekijä Otsikko Sivumäärä Aika	Marko Mantere ISO/IEC 27001 standardin mukainen puuteanalyysi 19 sivua + 2 liitettä 7.3.2019
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	tieto- ja viestintätekniikka
Ammatillinen pääaine	ammatillisen pääaineen nimi
Ohjaajat	lehtori Erik Pätynen

Insinöörityössä kartoitettiin puuteanalyysin avulla kohdeyrityksen tietoturvan tilaa vertaamalla sitä ISO/IEC 27001 -standardin vaatimuksiin. Opinnäytetyön tavoitteena oli tuottaa puuteanalyysiraportti, josta selviäisi, millä osa-alueilla tietoturvasta löytyy puutteita ja ylätason suositukset tietoturvan tilan parantamiseksi.

Työ suoritettiin noudattamalla ISO/IEC 27001 -standardin sertifioimiskäytäntöjä eli suorittamalla yrityksen tietoturvan kannalta keskeisten dokumenttien katselmointi ja henkilöstön haastattelu. Puuteanalyysi rajattiin organisaation palvelunhallinnan ja tietoturvan kannalta kriittisimpiin osiin.

Puuteanalyysi paljasti puutteita yrityksen tietoturvassa. Standardin osa-alueista suhteellisesti eniten puutteita löytyi toimittajien hallinnasta ja jatkuvuuden hallinnasta. Myös vaatimustenmukaisuuden, käyttöturvallisuuden ja viestintäturvallisuuden osa-alueet sisälsivät merkittäviä puutteita. Näiden puutteiden korjaamiseksi tekijä suosittelee standardin mukaisen tietoturvanhallintajärjestelmän käyttöönottoa.

Lopputuloksena syntyi raportti ISO/IEC 27001 -standardin 114 tietoturvakontrollin tilasta kohdeyrityksessä. Tätä raporttia ja sen suosituksia voidaan käyttää tietoturvan kehittämiseksi lähitulevaisuudessa.

Avainsanat	ISO/IEC 27001, tietoturva, hallinta, johtaminen

Author	Marko Mantere
Title	ISO/IEC 27001 gap analysis
Number of Pages	19 pages + 2 appendices
Date	7 March 2019
Degree	Bachelor of Engineering
Degree Programme	Information and Communication Technology
Professional Major	
Instructors	Erik Pätynen, Senior Lecturer

The purpose of this thesis was to perform a gap analysis on a current state of information security in target company against the ISO/IEC 27001 information security controls in the Annex A of the standard. Its aim was to produce a gap analysis report which would list the non-conformities found and suggestions on improving information security management on a high level.

The analysis was performed following the general guidelines and methods of ISO/IEC 27001 certification body by reviewing existing documentation and performing personnel interviews. The scope of the analysis is limited to functions critical to service operations from information security perspective.

The analysis revealed short comings in the state of information security in the target company. Biggest gaps were in the areas of supplier relationships and information security aspects of business continuity management. Areas of compliance, operations security and communications security were also found to have considerable gaps. The recommendation is to implement an information security management system as described in the standard.

As a result of this work a gap analysis report was produced which lists the state of the 114 information security controls of Annex A of the standard in the target company. This report and its recommendations can be used to further improve the status of information security in the target company.

Keywords	ISO/IEC 27001, information security, governance

Sisällys

Lyhenteet

ISO	International Organization for Standardization, kansainvälinen standardointiorganisaatio
IEC	International Electrotechnical Commission, kansainvälinen sähköalan standardointiorganisaatio
CIA	Confidentiality, Integrity, Availability, Luottamuksellisuus, eheys ja saavutettavuus
ISO/IEC 27001	Standardi, joka määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset.
ISMS	Information Security Management System, tietoturvan hallintajärjestelmä

1 Johdanto

Opinnäytetyön tarkoituksena on kartoittaa kohdeyrityksen tietoturvallisuuden tason ja nykyisen tietoturvallisuuden hallintamallin kattavuus ja toimivuus vertaamalla sitä ISO/IEC 27001:2013 -standardin vaatimuksiin. Lisäksi kartoituksen perusteella luodaan toimenpidesuosituslista, jonka pohjalta voidaan tietoturvallisuuden hallintaa jatkokehittää.

Kohdeyritys pidetään opinnäytetyössä anonyyminä, jotta yrityksen toiminta ei vaarantuisi. Lisäksi tällöin päästään tässä dokumentissa paneutumaan tarkemmin havaintoihin ja niiden luonteeseen. Kohdeyrityksestä voidaan kuitenkin mainita, että kyseessä on suomalainen, keskisuuri, ohjelmisto- ja SaaS-palveluihin keskittyvä pörssiyhtiö.

Opinnäytetyössä tutustutaan ensin ISO/IEC 27000 –standardiperheeseen ja erityisesti sen tietoturvaan keskittyvään ISO/IEC 27001:2013 -standardiin. Sen jälkeen käydään läpi puuteanalyysin rajaukset ja metodologia sekä puuteanalyysiraportti ja havainnot ja suositukset.

Opinnäytetyö pyrkii vastaamaan muun muassa seuraaviin kysymyksiin:

- Kuinka tärkeänä yrityksen johto pitää tietoturvallisuutta toimialallaan?
- Millaisella tasolla on yrityksen työntekijöiden tietoturvallisuustietoisuus suhteessa olemassa olevaan tietoturvallisuuden hallintajärjestelmään ja politiikkoihin?
- Miten nykyinen tietoturvallisuuden hallintajärjestelmä ja menetelmät vastaavat ISO/IEC 27001:2013 -standardin tavoitteita ja vaatimuksia?
- Onko ISO/IEC 27001 -sertifikaatin hankkiminen perusteltua ottaen huomioon liiketoiminnan tavoitteet?

Opinnäytetyön tutkimus on luonteeltaan kvalitatiivinen, eli laadullinen. Opinnäytetyö on niin sanottu toiminnallinen opinnäytetyö, jossa tuotetaan kirjallinen raportti tutkimuksen kohteesta ja aiheesta. Menetelminä ovat dokumenttien katselmointi, henkilökohtaiset haastattelut sekä kyselyt.

Dokumenttien katselmointi

Dokumenttien katselmoinnissa käydään läpi olemassa oleva kirjoitettu aineisto tietoturvallisuudesta, kuten tietoturvallisuuden hallintajärjestelmän kuvaus, tietoturvapolitiikat ja menettelyohjeistus. Dokumenttien sisältöä verrataan standardin tavoitteisiin ja vaatimuksiin.

Henkilökohtaiset haastattelut ja kyselyt

Haastatteluilla pyritään kartoittamaan yrityksen henkilöstön suhtautuminen tietoturvallisuuteen ja tietämyksen taso olemassa olevasta tietoturvallisuuden hallintajärjestelmästä sekä tietoturvapolitiikoista.

Henkilöstölle suunnatuilla kyselyillä pyritään kartoittamaan tietoturvapolitiikkojen ja menettelyohjeistuksen tunnettuus koko organisaatiossa.

Toimipistevierailut

Toimipistevierailuilla pyritään silmämääräisesti toteamaan tietoturvapolitiikkojen toimivuus esimerkiksi fyysisen turvallisuuden osalta.

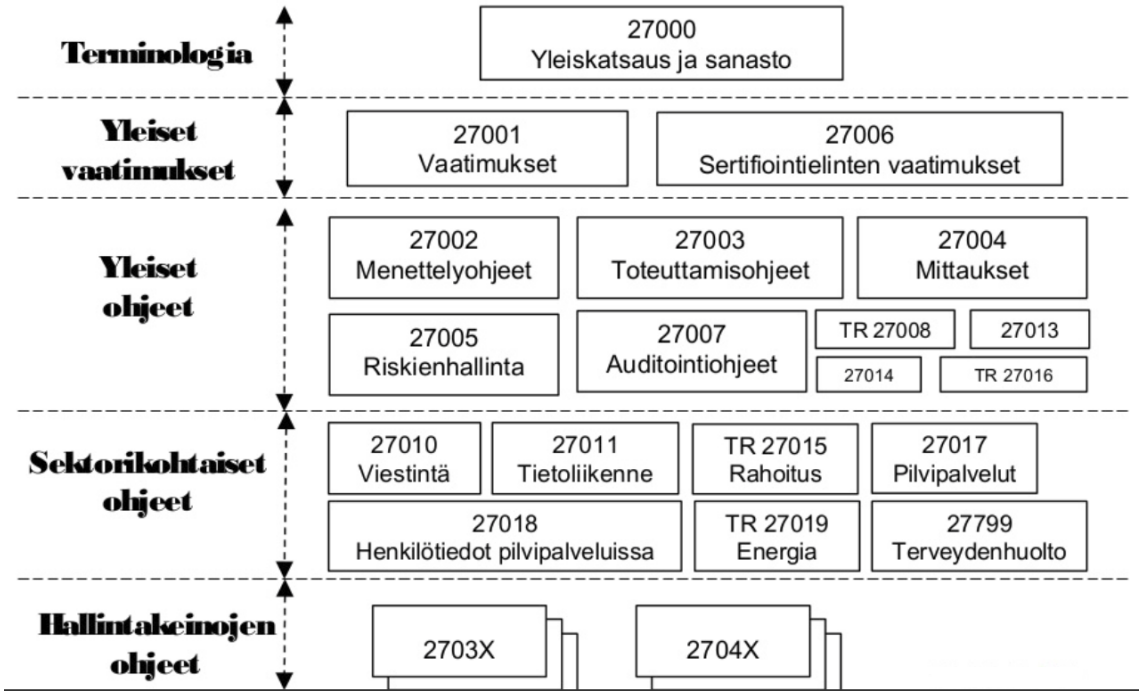
2 ISO/IEC 20000 -standardiperhe

2.1 Yleistä standardiperheestä

ISO-etuliitteelliset standardit julkaisee vuonna 1947 perustettu International Organization for Standardization -niminen kansainvälinen, riippumaton standardoimisjärjestö. Tämän kattojärjestön jäseniä ovat kansalliset standardoimisjärjestöt, joita kirjoitushetkellä on 162 (1). Suomea järjestössä edustaa Suomen Standardisoimisliitto SFS ry. ISO-organisaatio ei ole viranomainen, eikä sillä ole valtuuksia määrätä asioista, joten ISO:n standardeja tulee pitää suosituksina. Nämä suositukset ovat kuitenkin laajalti arvostettuja, ja siksi ISO:n julkaisemilla standardeilla on suuri käyttäjäkunta ja painoarvo.

ISO:n julkaisemista standardeista standardit ISO/IEC 27000 – 27050 käsittelevät tietoturvaa ja tietoturvallisuuden hallintaa. Näiden standardien yhteinen suomenkielinen otsikko on ”Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät”. IEC tulee sanoista International Electrotechnical Commission, joka on kansainvälinen sähköalan standardointiorganisaatio, joka yhteistyössä ISO:n kanssa määrittelee tietotekniikka-alan standardit. Näiden kahden muodostama yhteistyöelin on nimeltään JTC1, eli Joint Technical Committee 1. Yli 2.600 julkaistulla standardilla JTC1 on merkittävä informaatioteknologia-alan vaikuttaja. (2.)

Standardiperhe, joka on kuvattu kuvassa 1., jakautuu karkeasti viiteen osa-alueeseen, joita ovat terminologia, yleiset vaatimukset, yleiset ohjeet, sektorikohtaiset ohjeet sekä hallintakeinojen ohjeet. Standardeista ISO/IEC 27000 ”Yleiskatsaus ja sanasto” määrittelee standardeissa käytetyn terminologian. ISO/IEC 27001 ”Vaatimukset” asettaa tietoturvalle ja tietoturvallisuuden hallintajärjestelmälle yleiset tavoitteet ja vaatimukset. ISO/IEC 27002 ”Menettelyohjeet” määrittelee malliesimerkit ISO/IEC 27001:n täyttävistä tietoturvakontrolleista. Muita ohjeistuksia ovat mm. sektorikohtaiset rahoituksen ja energia-alan ohjeistukset (3).



Kuva 1. ISO/IEC 27000 -standardiperheen rakenne (3).

2.2 ISO/IEC 27001:2013 -standardi

2.2.1 Yleistä ISO/IEC 27001:2013 -standardista

ISO/IEC 27001:2013 on tietoturvastandardi, jonka viimeisin versio on julkaistu vuonna 2013. Standardi määrittelee tietoturvallisuuden hallintajärjestelmän (information security management system, ISMS) ja vaatimukset hallintajärjestelmälle. Organisaatiot voivat halutessaan hakea ISO/IEC 27001 -sertifikaattia, joka osoittaa, että organisaation tietoturvallisuuden hallinta on järjestetty standardin mukaisesti.

ISO/IEC 27001 -standardin taustalla on Ison-Britannian kauppa- ja teollisuusministeriön vuonna 1995 julkaisema BS 7799, joka määritteli tietoturvallisuuden hallinnan parhaat käytännöt. BS 7799 -standardin ensimmäinen osa otettiin vuonna 2000 ISO/IEC -standardiksi 17799. ISO/IEC 17799 päivitettiin vuonna 2005, jolloin se siirrettiin ISO/IEC 27000 -standardiperheeseen nimellä ISO/IEC 27002. BS 7799 standardin toinen osa, joka julkaistiin vuonna 1999, otettiin ISO/IEC -standardiksi 27001 vuonna 2005. Sekä ISO/IEC 27001 että 27002 päivitettiin vuonna 2013, jolloin julkaistiin standardien toistaiseksi uusin versio (4).

2.2.2 Rakenne ja tavoitteet

ISO/IEC 27001:2013 on hallinnointistandardi, joka keskittyy teknisten yksityiskohtien sijaan liiketoimintaprosesseihin. Standardi kuvaa tietoturvallisuuden kannalta keskeisten prosessien tavoitteet ja vaatimukset sekä tietoturvallisuuden hallintajärjestelmän, mutta ei määritä yksityiskohtaisia vaatimuksia itse tietoturvallisuuden hallintajärjestelmälle. Tavoitteena standardilla on suojata tietoa tietoturvallisuuden luottamuksellisuus, eheys ja saatavuus analysointimallin, eli ns. CIA-mallin, mukaisesti (Confidentiality, Integrity, Availability). Standardi lähestyy tavoitettaan riskienhallinnan näkökulmasta eli pyrkii kartoittamaan tärkeään tietoon kohdistuvat riskit, joille etsitään riskienhallintatoimenpiteet riskien minimoimiseksi (6).

Standardin rakenne väliotsikoineen on seuraavanlainen:

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

Väliotsikoista numerot 0–3 sisältävät standardille yleisiä määritelmiä ja rajauksia, jotka ovat yhteisiä kaikille ISO/IEC 27000 -perheen standardeille. Väliotsikot numeroilla 4–10 sisältävät tietoturvan hallintajärjestelmän vaatimukset ja tavoitteet. Standardissa on liite A (Annex A), joka sisältää standardin vaatimusten mukaisten tietoturvakontrollien esimerkkitoteutukset.

Seuraavaksi käydään läpi mitä kukin väliotsikko käsittelee, jotta voidaan saada jonkinlainen kuva standardin sisällöstä. Otsikot 0–3 jätetään käymättä läpi niiden yleisluontoisuuden vuoksi.

Organisaation toimintaympäristö

Standardi vaatii, että organisaation on ymmärrettävä oma toimintaympäristönsä ja määritettävä yritykseen vaikuttavien sidosryhmien vaatimukset tietoturvallisuuden kannalta sekä laadittava nämä vaatimukset täyttävä tietoturvan hallintajärjestelmä ISO/IEC 27001 -standardin mukaisesti. Tällaisia sidosryhmiä ovat muun muassa kansalliset ja ylikansalliset viranomaiset, asiakkaat ja toimittajat.

Johtajuus

Yrityksen johdon on osoitettava johtajuutta ja sitoutumista tietoturvallisuuden ylläpitoon, kehittämiseen ja sen hallintajärjestelmään varmistamalla riittävät resurssit, määrittämällä roolit, vastuut ja valtuudet sekä laatimalla tietoturvapolitiikan ja sitä tukevat toimenpideohjeet ja muut vastaavat dokumentit. Yrityksen johdon on varmistettava, että tietoturvan hallintajärjestelmä saavuttaa sille asetetut tavoitteet.

Suunnittelu

Organisaation on hallittava tietoturvallisuuteen kohdistuvia riskejä suunnitelmallisesti ja dokumentoidusti siten, että riskien vaikuttavuus, omistajuus sekä hallintakeinot ovat selvillä ja että niitä katselmoidaan säännöllisesti. Organisaation on asetettava tietoturvapolitiikan mukaiset tietoturvatavoitteet organisaation eri funktioille ja tasoille, joiden on hyvä olla mitattavissa ja joiden toteutumista seurataan säännöllisesti.

Tukitoiminnot

Organisaation on määritettävä ja varattava tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen tarvittavat resurssit. Organisaation on määritettävä millaista tietoturvallisuuden hallintajärjestelmän kannalta oleellista sisäistä ja ulkoista viestintää tarvitaan, ja huolehdittava sen toteutumisesta. Organisaation on määritettävä tietotuvallisuuden hallintajärjestelmän kannalta oleellinen dokumentoitu tieto ja hallittava dokumentoitua tietoa vaatimusten mukaisesti.

Toiminta

Organisaation on suunniteltava ja toteutettava prosessit, joita tarvitaan tietoturvavaatimusten täyttämiseen, sekä ohjattava niitä. Organisaation on dokumentoitava prosessit ja valvottava prosessien tietoturvallisuuden tavoitteiden täyttymistä. Ulkoistettujen prosessien tavoitteet määritetään ja niitä valvotaan. Organisaation on tehtävä tietoturvariskien arviointia suunnitelluin aikavälein, tai kun merkittäviä muutoksia ehdotetaan, tai kun niitä tapahtuu.

Suorituskyvyn arviointi

Organisaation on arvioitava tietoturvan tasoa ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta määrittämällä mitä tulee seurata ja mitata, millä seuranta- ja arviointimenetelmillä vaikuttavuutta mitataan, ketkä toteuttavat mittaamisen ja ketkä analysoivat ja arvioivat tulokset. Organisaation on tehtävä sisäisiä tietoturvallisuuden auditointeja suunnitelluin aikavälein. Organisaation ylimmän johdon on katselmoitava tietoturvallisuuden hallintajärjestelmä suunnitelluin aikavälein, jotta voidaan varmistua sen ajantasaisuudesta ja asianmukaisuudesta.

Parantaminen

Organisaation on reagoitava havaittuihin poikkeamiin ja ryhdyttävä toimiin niiden hallitsemiseksi ja korjaamiseksi sekä arvioitava, tarvitaanko toimenpiteitä, joilla poistetaan poikkeaman juurisyyt, jotta poikkeama ei toistu tai esiinny muualla. Organisaation on parannettava jatkuvasti tietoturvallisuuden hallintajärjestelmän soveltuvuutta, riittävyyttä ja vaikuttavuutta. (6.)

2.3 Sertifiointiprosessi

Suoritettuaan standardin mukaisten tietoturvapolitiikkojen ja kontrollien määrittelyn, toteutuksen ja jalkauttamisen yritys voi halutessaan aloittaa sertifiointiprosessin ISO/IEC 27001 -standardille akkreditoidun sertifiointielimen kanssa. Hyväksytysti myönnetty sertifikaatti osoittaa yrityksen sidosryhmille ja muille ulkopuolisille tahoille yrityksen tietoturvan hyvien tietoturvakäytäntöjen ja standardin mukaisen tason.

Sertifiointiprosessi ja toimintatavat määritellään ISO/IEC -standardeissa ISO/IEC 17021 ja ISO/IEC 27006, joista ensimmäinen kuvaa yleiset vaatimukset ja toimintatavat ja jälkimmäinen tietoturvanhallintajärjestelmän sertifiointiprosessin vaatimukset ja toimintatavat.

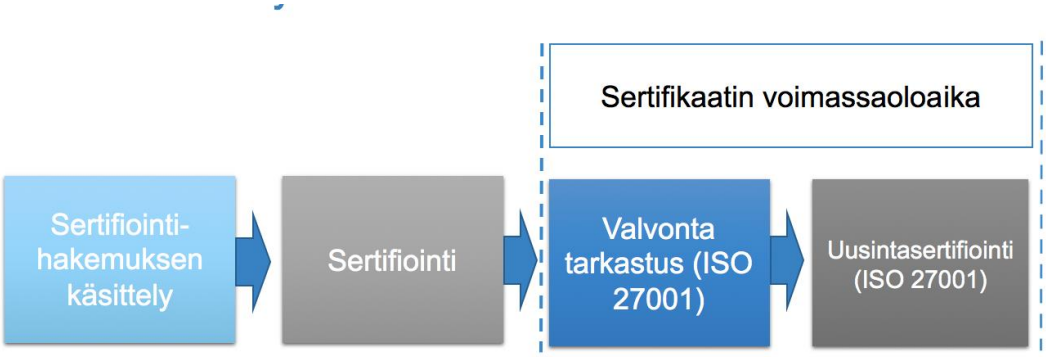
Sertifioinnin elinkaari jakautuu yleisellä tasolla neljään osaan, mikä on kuvattu kuvassa 2. Osat ovat seuraavat:

1. Sertifiointihakemuksen käsittely – jonka aikana alustavasti varmistetaan, että sertifioinnin vaatimukset voivat ylipäätänsä täyttyä.

2. Sertifiointi – jonka aikana suoritetaan tietoturvanhallintajärjestelmän katselmointi, sekä sen soveltuvuuden, riittävyyden ja vaikuttavuuden arviointi sovitulta kattavuudeltaan (scope).

3. Valvontatarkastus – joita suoritetaan sertifikaatin voimassaoloaikana kerran vuodessa, joiden aikana arvioidaan standardin vaatimusten toteutumista eri funktioissa ja yksiköissä, sertifikaatin kattavuuden sisällä.

4. Uusintasertifiointi – jonka aikana vaatimusten arviointi suoritetaan uudelleen standardin koko laajuudessa ja kattavuudessa.



Kuva 2. Sertifiointiprosessi (5).

Osa 1. Sertifiointia tavoitteleva taho lähettää akkreditoidulle sertifiointielimelle hakemuksen sertifiointiprosessin aloittamisesta. Sertifiointielin katselmoi tässä vaiheessa sertifioinnin tavoitellun soveltamisalan, sertifiointiin tarvittavan aikajänteen ja valitsee henkilöstöstään ne henkilöt, joilla on riittävä kompetenssi kyseisen toimialan ja laajuuden puitteissa auditoida asiakasta.

Osa 2 jakautuu itsessään kahteen vaiheeseen. Vaihe 1 tehdään yleensä yrityksessä paikan päällä. Vaiheessa 1 käydään läpi kohdeyrityksen dokumentaatio, vahvistetaan sertifioinnin soveltamisala, kerätään tietoa yritykseen kohdistuvista lakisääteisistä vaatimuksista ja niiden toteutumisesta, käydään läpi sisäisen valvontasuunnitelman ja johdon

katselmoinnin tulokset, sovitaan vaiheeseen 2 tarvittavat resurssit ja aikataulutus sekä arvioidaan yleistä valmiutta vaiheeseen 2. Vaihetta 1 voi edeltää valinnainen ns. esiauditointi, jossa käydään läpi kaikki ISO/IEC 27001 -standardin vaatimukset ja jonka tarkoituksena on valmistaa yritystä varsinaiseen auditointiin.

Vaiheessa 2 arvioidaan tietoturvan hallintajärjestelmän jalkauttamista ja vaikuttavuutta yrityksessä. Vaiheessa 2 käydään läpi, miten yritys on toteuttanut tietoturvariskienhallinnan, miten tietoturvan tavoitteet ja kontrollit on valittu riskianalyysin perusteella, miten kontrollien jalkautus on toteutettu, miten yritys mittaa ja valvoo tietoturvan hallintajärjestelmän toimivuutta, miten toimivuuden raportointi on toteutettu sekä miten tietoturvan hallintajärjestelmä kattaa ja täyttää lakisääteiset vaatimukset.

Jos vaiheissa 1 tai 2 havaitaan tietoturvan hallintajärjestelmässä tai sen toteutuksessa puutteita, ne raportoidaan sertifikaattia hakevalle yritykselle, jonka kanssa sovitaan aikataulu havaintojen korjaamisesta ja uudelleenkatselmoinnista.

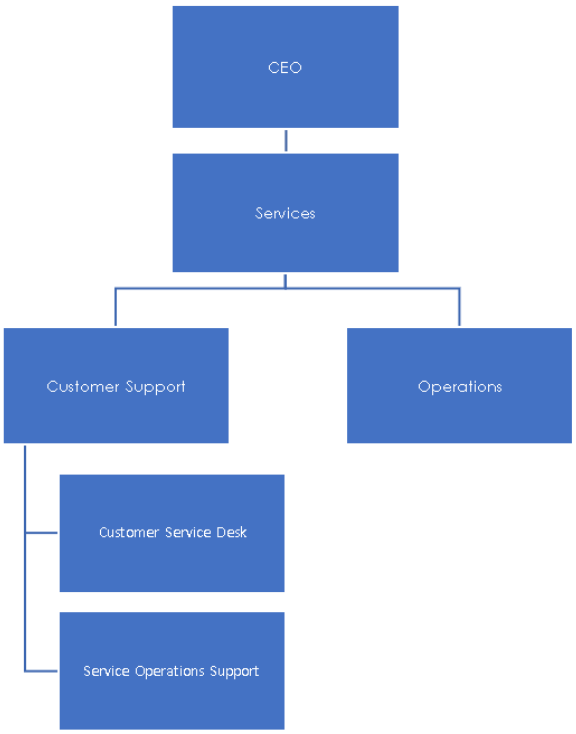
Jos puutteita ei havaita, sertifiointielin tekee vaiheiden 1 ja 2 tulosten pohjalta päätöksen sertifikaatin myöntämisestä. Tästä alkaa sertifikaatin kolmivuotinen elinkaari, jonka aikana tehdään vuotuisia valvontatarkistuksia kohdistaen tarkistukset johonkin standardin osa-alueeseen siten, että kolmen vuoden aikana tulevat katettua koko standardin vaatimukset. Valvontatarkastuksiksi voidaan hyväksyä myös yrityksen itsensä tekemät, standardin vaatiman sisäisen valvontasuunnitelman mukaiset tarkastukset.

Uusintasertifiointi siihen liittyvine katselmointeineen ja tarkastuksineen suoritetaan riittävän ajoissa ennen sertifikaatin vanhenemista siten, että mahdolliset havainnot voidaan korjata ennen sertifikaatin viimeistä voimassaolopäivää. Hyväksytty uusintasertifiointi aloittaa uuden kolmivuotisen jakson, jonka aikana jälleen suoritetaan valvontatarkistuksia. (8.)

3 Puuteanalyysi

3.1 Rajaukset

Insinöörityössä tehdyn puuteanalyysin kohteena kohdeyrityksessä olivat operatiivista työtä tekevät organisaation osat. Näiden osien toimintaa voidaan kuvata esimerkiksi nimillä customer service desk, service operations support ja operations. Organisaatiorakenne on kuvattu kuvassa 3. Näillä organisaation osilla on kohdeyrityksessä laajimmat pääsyoikeudet palveluntuotannon kannalta kriittisiin infrastruktuurikomponentteihin, järjestelmiin sekä informaatioon, joten yrityksen tietoturvallisuuden kannalta näiden organisaation osien hyvä tietoturvallisuuden hallinto on keskeistä. Vastaavasti sellaiset organisaation osat, jotka eivät suoraan osallistu palveluntuotantoon, kuten henkilöstö-, markkinointi- ja taloushallinto, ovat puuteanalyysin ulkopuolella.



Kuva 3. Kohteena olevan yrityksen puuteanalyysin rajauksen sisälle jäävät organisaation osat

3.2 Metodologia

Puuteanalyysin metodologia pyrkii noudattamaan virallisen ISO/IEC27001 -auditoinnin metodeja, joihin kuuluvat dokumenttien katselmointi, yrityksen henkilöstön haastattelut sekä toimipistevierailut. Normaalista auditoinnista, jotka aina ovat laajuudeltaan rajattuja, poiketen opinnäytetyön tekijän päivätyö kohdeyrityksessä mahdollisti syvemmän ja laajemman tutustumisen kohdeyrityksen tietoturvallisuuden tasoon. Auditoinnin toteuttamisen keskeiset vaatimukset, käytännöt ja ohjeet on määritelty ISO/IEC 27007 -standardissa.

3.2.1 Dokumenttien katselmointi

ISO/IEC27001 -standardi vaatii tiettyjen dokumenttien tai sisällöltään tietyntyyppisten dokumenttien olemassaoloa. Nämä dokumentit, tai niiden sisällöt, ovat

- tietoturvallisuuden hallintajärjestelmän soveltamisala
- tietoturvallisuuden hallintajärjestelmän kuvaus
- tietoturvapolitiikka ja tietoturvatavoitteet
- tietoturvariskien käsittelyprosessi
- dokumentoitu tieto, jonka organisaatio on määrittänyt tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämättömäksi
- tietoturvavaatimusten täyttämiseen tarvittavat prosessit, sekä niihin liittyvä muu dokumentaatio, jonka avulla voidaan varmistua, että prosessit toimivat
- tietoturvariskien käsittelyn tulokset
- tietoturvallisuuden tason ja tietoturvallisuuden hallintajärjestelmän vaikuttavuuden seurannan ja mittaamisen tulokset

- sisäisen tietoturvallisuuden hallintajärjestelmän auditointiohjelma ja sen tulokset
- tieto tietoturvallisuuden hallintajärjestelmän katselmoinneista ja niiden tuloksista
- tieto tietoturvapoikkeamien luonteesta ja niiden perusteella tehdyistä toimenpiteistä ja toimenpiteiden tuloksista.

Dokumenttien katselmoinnissa käydään läpi olemassa oleva tietoturvallisuuteen liittyvä dokumentaatio ja arvioidaan, täyttääkö se ISO/IEC27001 -määritellyt vaatimukset ja tavoitteet. Arvio on arvioijan subjektiivinen näkemys vaatimusten ja tavoitteiden täyttymisestä.

Tätä opinnäytetyötä varten katselmoitiin yrityksen olemassa oleva tietoturvadokumentaatio ja siihen liittyvät dokumentit kuten esimerkiksi häiriönhallintaprosessin kuvaus.

3.2.2 Haastattelut ja kyselyt

Dokumenttien katselmoinnin lisäksi tietoturvallisuuden hallintajärjestelmän vaikuttavuutta, ajantasaisuutta ja jalkautusta arvioidaan henkilöstön haastatteluilla. Haastatteluilla pyritään saamaan näkemys siitä, miten hyvin tietoturvallisuuden hallintajärjestelmän tavoitteet toteutuvat henkilöstön toiminnassa.

Tätä opinnäytetyötä varten haastateltiin sähköpostitse suppeana kyselytutkimuksena neljäätoista kohdeorganisaation asiakasrajapinnassa ja operoinnissa toimivaa henkilöä, jotka toimivat opinnäytetyön puuteanalyysin rajauksien mukaisissa tehtävissä yrityksen palvelutuotannossa. Kyselyn tarkoituksena oli kartoittaa, minkälainen käsitys henkilöstöllä on yrityksen tietoturvapolitiikoista ja ohjeistuksesta.

Lisäksi tehtiin sähköpostitse suppea kysely yrityksen johtaville avainhenkilöille, jotka vastaavat puuteanalyysin rajauksen mukaisista toiminnoista. Kyselyn tarkoituksena oli kartoittaa kuinka tärkeänä yrityksen johto pitää tietoturvallisuutta yrityksen toimialalla yleisesti ja yrityksen liiketoiminnan kannalta.

3.2.3 Toimipistevierailut

Dokumenttien katselmoinnin ja haastattelujen lisäksi yleensä suoritetaan toimipistevierailu vähintään yhdessä yrityksen toimipisteessä. Toimipistevierailulla voidaan silmämääräisesti todeta yrityksen tietoturvapolitiikan toimivuus esimerkiksi fyysisen turvallisuuden osalta. Lisäksi toimipistevierailu saattaa paljastaa muuten huomiotta jääviä asioita henkilöstön toiminnasta, kuten vaikka miten tulosteita ja massamuisteja kohdellaan yrityksen tiloissa.

Tätä opinnäytetyötä varten katselmoitiin yrityksen Suomen toimipisteistä pääkaupunkiseudulla sijaitsevaa pääkonttoria, jossa suurin osa yrityksen henkilöstöstä työskentelee. Yrityksellä on Suomessa ja muissa Euroopan maissa myös muita toimipisteitä, mutta niissä ei rajallisen ajan vuoksi päästy käymään.

3.3 Havainnot ja suositukset

3.3.1 Kyselytutkimuksen tulokset

Puuteanalyysiä varten järjestettiin yrityksessä kaksi eri kyselyä, yksi puuteanalyysin rajauksen mukaisten funktioiden johtajille ja yksi näissä funktioissa työskenteleville työntekijöille. Kyselyt pyrkivät kartoittamaan, millainen on henkilöstön tietämys nykyisestä tietoturvan hallinnasta sekä millainen näkemys johtajilla on tietoturvan tärkeydestä toimialalla yleensä ja yrityksen liiketoiminnassa.

Johtajille lähetetyt kysymykset olivat seuraavanlaiset:

1. Kuinka tärkeää tietoturva on mielestäsi yrityksen toimialalla yleensä (SaaS)?

2. Kuinka tärkeää tietoturva on mielestäsi yrityksen liiketoiminnan kannalta?

3. Tiedätkö, missä yrityksen tietoturvapolitiikka ja muut tietoturvaan liittyvät dokumentit sijaitsevat?

4. Oletko lukenut yrityksen tietoturvapolitiikan?

5. Tiedätkö miten toimia, jos epäilet tietoturvaloukkausta?

Kysely lähetettiin neljälle johtavassa asemassa työskentelevälle henkilölle. Vastaukset kysymyksiin saatiin kaikilta neljältä, joten vastausprosentti on kiitettävä 100. Kysymyksiä 1 ja 2 arvotettiin asteikolla 0-5, jossa suurempi luku on parempi, eli 0 ”ei lainkaan tärkeää” ja 5 ”erittäin tärkeää”. Kysymykset 3–5 arvotettiin 1 ”Kyllä” ja 2 ”Ei”. Kyselyn tulokset taulukossa 1.

Taulukko 1. Johtajille lähetetyn kyselyn tulokset.

Vastaaja	**Kysymys 1**	**Kysymys 2**	**Kysymys 3**	**Kysymys 4**	**Kysymys 5**	
-						
Vastaaja1	5	5	1	1	1	
Vastaaja2	5	5	2	2	1	
Vastaaja3	5	5	2	1	1	
Vastaaja4	5	5	2	2	1	
	5	5				Ka.
			25 %	50 %	100 %	Kyllä %

1 = 1 2 = 2 3 = 3 4 = 4 5 = 5	1 = 1 2 = 2 3 = 3 4 = 4 5 = 5	1 = Kyllä 2 = En	1 = Kyllä 2 = En	1 = Kyllä 2 = En

Kaikki vastaajat pitivät tietoturvaa liiketoiminnan ja SaaS-toimialan kannalta erittäin tärkeänä, mikä on hyvä tulos tietoturvan kannalta. Vastausten perusteella tietoturvapolitiikkojen jalkauttamista ei ole toteutettu kunnolla, sillä dokumentaation sijainnin ja sisällön sisäistämisessä oli puutteita.

Työntekijöille lähetetyt kysymykset olivat seuraavanlaiset:

1. Tiedätkö, missä yrityksen tietoturvapolitiikka ja muut tietoturvaan liittyvät dokumentit sijaitsevat?

2. Oletko lukenut yrityksen tietoturvapolitiikan?

3. Tiedätkö, miten toimit, jos epäilet tietoturvaloukkausta?

Taulukko 2. Työntekijöille lähetetyn kyselyn tulokset.

Vastaaja	Kysymys 1	Kysymys 2	Kysymys 3	
-				
Vastaaja1	1	1	1	
Vastaaja2	2	2	1	
Vastaaja3	1	1	1	
Vastaaja4	2	2	1	
Vastaaja5	1	2	1	
Vastaaja6	1	1	1	
Vastaaja7	1	1	1	
	71 %	57 %	100 %	Kyllä %
	1 = Kyllä	1 = Kyllä	1 = Kyllä	
	2 = En	2 = En	2 = En	

Kysely lähetettiin 14 henkilölle, joista 7 vastasi kyselyyn, eli vastausprosentti on välttävät 50. Työntekijöiden parissa tietoturvapolitiikan sijainti oli paremmin tiedossa: 71 % vastaajista tiesi mistä dokumentit löytyvät. Vain hieman yli puolet vastaajista oli lukenut kyseiset dokumentit.

Huomionarvoista on, että molemmat ryhmät kokevat tietävänsä, miten toimia epäillessään tietoturvaloukkausta, mitä voidaan pitää kiitettävänä tuloksena.

3.3.2 Puuteanalyysin havainnot

Yksityiskohtainen tietoturvan hallintajärjestelmän puuteanalyysi suoritettiin käymällä läpi kaikki ISO/IEC 27001 -standardin 114 referenssitietoturvakontrollia standardin liitteestä A ”Hallintatavoitteiden ja -keinojen viiteluettelo” (Annex A) ja vertaamalla yrityksen tietoturvan hallintajärjestelmää, olemassa olevia dokumentteja ja käytäntöjä sekä tietoja yrityksen prosessien toiminnasta kontrollien vaatimuksia vasten. Nämä tavoitteet ja keinot on määritelty siten, että standardin kappaleissa 4–10 kuvatut tavoitteet ja henki toteutuvat standardin mukaisesti, jos tavoitteet ja keinot on toteutettu sertifioinnin rajausten sisällä oleviin funktioihin. (6.)

Vaatimusten toteutuminen kirjattiin yksinkertaisesti seuraavanlaisella luokittelulla:

- OK – vaatimuksille, jotka toteutuvat sellaisinaan

- NOT OK – vaatimuksille, joiden toteutumisessa on puutteita

- NOT APPLICABLE – niille vaatimuksille, joiden voidaan katsoa olevan sertifikaatin rajausten mukaisten funktioiden toimivallan tai vastuun ulkopuolella tai muuten rajausten ulkopuolella.

Varsinainen ISO/IEC 27001 -sertifiointi käyttää erilaista luokittelua, jossa tässä käytetty ”NOT OK” on jaettu kolmeen eri vakavuusasteeseen havaintojen määrän ja vakavuuden suhteen. Nämä luokittelut ovat opportunity for improvement, minor nonconformity ja major noncorformity. Tässä opinnäytetyössä tehdyn puuteanalyysin luokittelu eroaa sertifioinnin käyttämästä, koska tämän työn puitteissa moniportaisen luokittelun käyttäminen ei tuo lisäarvoa.

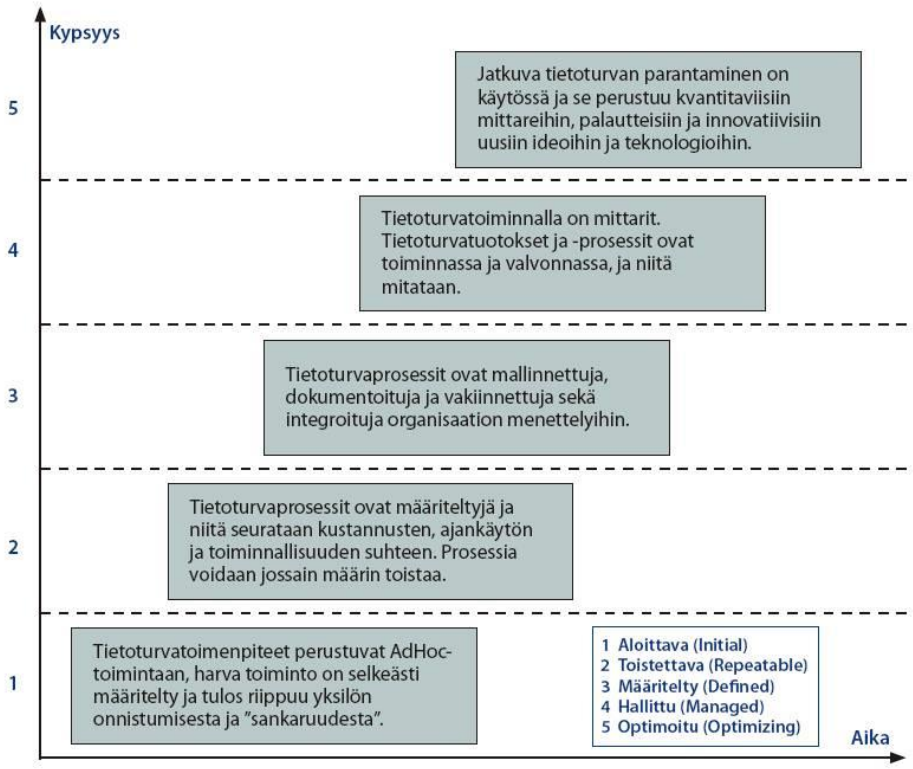
Taulukko 3. Puuteanalyysin havainnot ISO/IEC 27001 liitteen A yläotsikoittain

ID	Otsikko	OK	NOT OK	NOT APP.	TOTAL	OK+N.A. %
A.5	Tietoturvapolitiikat	1	1		2	50 %
A.6	Tietoturvallisuuden organisointi	2	3	2	7	57 %
A.7	Henkilöstöturvallisuus	3	3		6	50 %
A.8	Suojattavan omaisuuden hallinta	7	3		10	70 %
A.9	Pääsynhallinta	8	5	1	14	64 %
A.10	Salaus			2	2	100 %
A.11	Fyysinen turvallisuus ja ympäristön turvallisuus	12	2	1	15	87 %
A.12	Käyttöturvallisuus	6	8		14	43 %
A.13	Viestintäturvallisuus	2	4	1	7	43 %
A.14	Järjestelmien hankkiminen, ylläpito ja kehitys	2	1	10	13	92 %
A.15	Suhteet toimittajiin		5		5	0 %
A.16	Tietoturvahäiriöiden hallinta	5	2		7	71 %
A.17	Liiketoiminnan jatkuvuuteen liittyviä tietoturvanäkökohtia		4		4	0 %
A.18	Vaatimustenmukaisuus	2	5	1	8	38 %
	Summa:	50	46	18	114	60 %

Eri tietoturvakontrollien tilan arviointi työn rajausten sisällä perustuu täysin opinnäytetyön tekijän omaan osaamiseen, kokemuksiin ja tietotaitoon. Koska tekijällä ei ole täydellistä tietoa kohdeyrityksen toiminnoista, jokin näistä kontrolleista saattaa saada eri

luokittelun eri henkilön tekemänä. Tämä toisaalta kuvastaa hyvin myös auditoijan työn hankaluutta: koska auditoijalla ei koskaan voi olla täyttä tietoa kohdeyrityksestä, muutamassa päivässä tehty auditointi perustuu aina epätäydellisiin tietoihin.

Kyselytutkimuksen ja puuteanalyysin perusteella yrityksen tietoturvan tila suhteessa ISO/IEC 27001 -standardissa määriteltyihin vaatimuksiin on puutteellinen. Tietoturvadokumentaatio sisältää muutamalta osa-alueelta tietoturvapolitiikkoja ja toimintaohjeita. Näiden dokumentoitujen tietoturvaan liittyvien politiikkojen jalkauttaminen organisaatioon on tehty puutteellisesti, sillä kaikilla kyselytutkimukseen osallistuneilla ei ollut tietoa siitä, missä dokumentaatio sijaitsee tai mitä se sisältää. Yrityksestä puuttuu määritelty, systemaattinen, tietoturvan hallintamalli, jolla pyrittäisiin ennakoimaan ja hallitsemaan yrityksen liiketoimintaan vaikuttavia riskejä kuten standardissa määritellään. Yrityksen tietoturvallisuus perustuu yrityksen työntekijöiden tietotaitoon ja ulkopuolisten järjestelmä- ja palvelutoimittajien tietoturvaan. Jälkimmäinen siitä huolimatta, että voimassa olevissa palvelusopimuksissa ei välttämättä viitata tietoturvaan lainkaan.



Kuva 4. Tietoturvallisuuden kypsyysmalli (7).

Vahti-ohjeistuksesta löytyvällä tietoturvan kypsyysmallilla, kuva 4, arvioituna yrityksen tietoturvan taso liikkuu välillä 1–2, eli tietoturvaan liittyviä politiikkoja, prosesseja ja käytäntöjä on määritelty ja dokumentoitu, mutta ei standardin edellyttämällä laajuudella ja syvyydellä. Lisäksi on syytä varmistaa olemassa olevan ja tulevan tietoturvadokumentaation osalta, että dokumentaation jalkauttaminen etenee työntekijäportaalle saakka, jotta kaikki olisivat tietoisia omista vastuista ja velvollisuuksistaan tietoturvan suhteen ja miten tietoturvan hallinta yrityksessä toimii.

3.3.3 Suositukset

Tässä työssä esille tulleiden havaintojen perusteella opinnäytetyön tekijä suosittelee, että yrityksessä otetaan käyttöön ISO/IEC 27001 -standardissa kuvattu tietoturvan hallintajärjestelmä tai muu vastaavanlainen järjestelmä yrityksen koko laajuudessa. Tämän tavoitteen saavuttaakseen yrityksen pitää käyttää aikaa ja resursseja saattaakseen ajan tasalle, laajentaakseen ja syventääkseen olemassa olevan tietoturvadokumentaation vastaamaan standardin vaatimuksia. Keskeiset tietoturvaan liittyvät prosessit kuten tietoturvariskien hallinta, poikkeamien hallinta, muutoksenhallinta ja pääsynhallinta tulee määrittää ja jalkauttaa sekä seurata näiden prosessien tietoturvatavoitteiden täyttymistä.

Täytettyään standardissa kuvatut vaatimukset yrityksen tulee harkita ISO/IEC 27001 -sertifioinnin hakemista yrityksen strategian ja liiketoiminnan tavoitteiden pohjalta. Sertifiointi ja sen saavuttamiseksi ja ylläpitämiseksi tarvittava työmäärä ja resurssit ovat tämän työn rajauksen laajuudessa opinnäytetyön tekijän arvioimana merkittäviä suhteessa liiketoiminnan kokoon ja saavutettuihin hyötyihin nähden, joten päätös standardin käyttöönotosta ja mahdollisesta sertifioinnin hakemisesta pitää tehdä painavin liiketoimintaperustein.

Joka tapauksessa tietoturvan hallinnan ja johtamisen määrittäminen, systematisointi ja säännöllistäminen on suositeltava tavoite, vaikka sertifikaattia ei lähdettäisikään hakemaan.

4 Yhteenveto

Tässä insinöörityössä perehdyttiin ISO/IEC 27000 -standardiperheeseen ja erityisesti standardiin ISO/IEC 27001. Työssä tehtiin tietoturvallisuuden puuteanalyysi ISO/IEC 27001 -standardin pohjalta kohdeyrityksen tällä hetkellä käytössä olevaa tietoturvan hallintaa vasten. Puuteanalyysin perusteella laadittiin ylätason suositukset tietoturvan hallinnan jatkokehittämisestä.

Työssä päästiin sille asetettuihin tavoitteisiin. Kyselytutkimukset ja puuteanalyysi saatiin tehtyä aikataulu- ja resurssipaineista huolimatta. Erityisesti tekijän henkilökohtaiset tavoitteet standardin osaamisen ja sisäistämisen syventämisestä toteutuivat täysin.

Opinnäytetyössä aloitettua työtä voi jatkaa laatimalla standardin aihealueittain toimenpidelistan, jonka tavoitteena on standardin vaatimusten täyttäminen. Tämän toimenpidelistan perusteella voidaan arvioida tarvittavien resurssien ja toteuttamiseen menevän ajan määrä, jolloin saadaan realistinen arvio koko projektin kustannuksista. Jos aikataulu olisi antanut myöden, toimenpidelista olisi tuotettu ja liitetty jo tähän opinnäytetyöhön. Valitettavasti tätä ei päästy työn yhteydessä tekemään. Toisaalta toimenpidelistan laatiminen vaatii myös jo osittaista ongelmanratkaisua, kun pyritään määrittelemään, miten organisaatiossa voidaan ratkaista standardin vaatimukset, joten se ei välttämättä ole perusteltua vielä tässä vaiheessa tietoturvan kehitystä.

Työ opetti myös sen, että tietoturvan hallintajärjestelmän auditointi ulkopuolisena on hankalaa, koska siihen on käytettävissä aina vain hyvin rajallinen aika ja puutteelliset lähtötiedot. Jopa tilanteessa, jossa sisäinen auditoija työskentelee samassa organisaatiossa, kuin auditoitavat tahot, ei ole itsestään selvää, että auditoija saa selkeän ja oikean kuvan organisaation toimintatavoista.

Haluan kiittää tässä yhteydessä nyt nimettömäksi jäävää työnantajaani, joka salli opinnäytetyön tekemisen työaikana, vaimoa ja lapsiani, jotka uhrasivat omaa aikaansa, jotta sain kirjoittaa opinnäytetyötä, sekä lukuisia entisiä ja nykyisiä kollegoja, joiden kanssa aihetta on sparrattu. Ilman kaikkien näiden tahojen tukea tämä työ olisi jäänyt tekemättä.

Lähteet

1 All about ISO. Verkkojulkaisu. International Organization for Standardization. <https://www.iso.org/members.html> Luettu 5.1.2019.

2 ISO/IEC 27000 Tietoturvallisuuden hallintajärjestelmä. Verkkojulkaisu. Suomen Standardisoimisliitto SFS ry. <https://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_iec_27000_tietoturvallisuuden_hallinta> Luettu 5.1.2019.

3 Vision, Mission and Principles 2014. Verkkojulkaisu. ISO/IEC JTC 1. <https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/jtc1_mission_brochure_2014_final.pdf> Luettu 5.1.2019

4 ISO/IEC 27001. Verkkojulkaisu. Wikipedia. <https://en.wikipedia.org/wiki/ISO/IEC_27001> Luettu 5.1.2019.

5 Nixu Certification Oy. Verkkojulkaisu. <https://www.nixu.com/fi/nixu-certification-oy> Luettu 5.1.2019.

6 SFS-EN ISO/IEC 27001:2017 "Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset". Suomen Standardisoimisliitto SFS ry.

7 Vahti-ohje. 2009. Verkkojulkaisu. <https://www.vahtiohje.fi/web/guest/13> Luettu 7.1.2019.

8 Information Security Management Systems Auditor/Lead Auditor (IRCA 2016/PR320). 2016. Julkaisematon koulutusmateriaali. Bureau Veritas.

ISO/IEC 27001 Liite A:n 114 tietoturvakontrollia ja puuteanalyysin tulokset

ID	Topic	Status	OK	NOT OK	NOT APP.	TOTAL	OK+N.A. %
A.5	**INFORMATION SECURITY POLICIES**		1	1		2	50 %
A.5.1	**Management direction of information security**						
A.5.1.1	Policies for Information Security	OK					
A.5.1.2	Review of the policies for information security	NOT OK					
A.6	**ORGANIZATION OF INFORMATION SECURITY**		2	3	2	7	57 %
A.6.1	**Internal organization**						
A.6.1.1	Information Security Roles and Responsibilities	OK					
A.6.1.2	Segregation of duties	NOT OK					
A.6.1.3	Contact with Authorities	NOT APPLICABLE					
A.6.1.4	Contact with special interest groups	OK					
A.6.1.5	Information security in project management	NOT APPLICABLE					
A.6.2	**Mobile devices and teleworking**						
A.6.2.1	Mobile device policy	NOT OK					
A.6.2.2	Teleworking	NOT OK					
A.7	**HUMAN RESOURCE SECURITY**		3	3		6	50 %
A.7.1	**Prior to Employment**						
A.7.1.1	Screening	OK					
A.7.1.2	Terms and conditions of employment	OK					
A.7.2	**During employment**						
A.7.2.1	Management responsibilities	NOT OK					
A.7.2.2	Information security awareness, education and training	NOT OK					
A.7.2.3	Disciplinary process	NOT OK					
A.7.3	**Termination and change of employment**						
A.7.3.1	Termination or change of employment responsibilities	OK					
A.8	**ASSET MANAGEMENT**		7	3		10	70 %
A.8.1	**Responsibility for assets**						
A.8.1.1	Inventory of assets	OK					
A.8.1.2	Ownership of assets	OK					
A.8.1.3	Acceptable use of assets	OK					
A.8.1.4	Return of assets	OK					
A.8.2	**Information classification**						
A.8.2.1	Classification of information	OK					
A.8.2.2	Labeling of information	NOT OK					
A.8.2.3	Handling of assets	NOT OK					
A.8.3	**Media handling**						
A.8.3.1	Management of removable media	NOT OK					
A.8.3.2	Disposal of media	OK					
A.8.3.3	Physical media transfer	OK					
A.9	**ACCESS CONTROL**		8	5	1	14	64 %
A.9.1	**Business requirements of access control**						
A.9.1.1	Access control policy	OK					
A.9.1.2	Access of networks and network services	NOT OK					
A.9.2	**User access management**						
A.9.2.1	User registration and de-registration	OK					
A.9.2.2	User access provisioning	OK					
A.9.2.3	Management of privileged access right	NOT OK					
A.9.2.4	Management of secret authentication information of users	NOT OK					

ID	Topic	Status	OK	NOT OK	NOT APP.	TOTAL	OK+N.A. %
A.9.2.5	Review of user access rights	NOT OK					
A.9.2.6	Removal or adjustment of access rights	NOT OK					
A.9.3	**User responsibilities**						
A.9.3.1	Use of Secret Authentication Information	OK					
A.9.4	**System and application access control**						
A.9.4.1	Information access restriction	OK					
A.9.4.2	Secure log-on Procedures	OK					
A.9.4.3	Password management system	OK					
A.9.4.4	Use of privileged utility programs	OK					
A.9.4.5	Access control to program source code	NOT APPLICABLE					
A.10	**CRYPTOGRAPHY**				2	2	100 %
A.10.1	**Cryptographic controls**						
A.10.1.1	Policy on the use of cryptographic controls	NOT APPLICABLE					
A.10.1.2	Key management	NOT APPLICABLE					
A.11	**PHYSICAL AND ENVIRONMENTAL SECURITY**		12	2	1	15	87 %
A.11.1	**Secure areas**						
A.11.1.1	Physical security perimeter	OK					
A.11.1.2	Physical entry controls	OK					
A.11.1.3	Securing offices, rooms and facilities	OK					
A.11.1.4	Protecting against external and environmental threats	OK					
A.11.1.5	Working in secure areas	OK					
A.11.1.6	Delivery and loading areas	NOT APPLICABLE					
A.11.2	**Equipment**						
A.11.2.1	Equipment siting and protection	OK					
A.11.2.2	Supporting utilities	OK					
A.11.2.3	Cabling security	OK					
A.11.2.4	Equipment maintenance	OK					
A.11.2.5	Removal of assets	NOT OK					
A.11.2.6	Security of equipment and assets off-premises	OK					
A.11.2.7	Secure disposal or re-use of equipment	NOT OK					
A.11.2.8	Unattended user equipment	OK					
A.11.2.9	Clear desk and clear screen policy	OK					
A.12	**OPERATIONS SECURITY**		6	8		14	43 %
A.12.1	**Operational procedures and responsibilities**						
A.12.1.1	Documented operating procedures	NOT OK					
A.12.1.2	Change management	NOT OK					
A.12.1.3	Capacity management	OK					
A.12.1.4	Separation of development, testing and operational environments	OK					
A.12.2	**Protection from malware**						
A.12.2.1	Controls against malware	OK					
A.12.3	**Backup**						
A.12.3.1	Information backup	NOT OK					

ID	Topic	Status	OK	NOT OK	NOT APP.	TOTAL	OK+N.A. %
A.12.3	**Backup**						
A.12.3.1	Information backup	NOT OK					
A.12.4	**Logging and monitoring**						
A.12.4.1	Event logging	NOT OK					
A.12.4.2	Protection of log information	OK					
A.12.4.3	Administrator and operator logs	NOT OK					
A.12.4.4	Clock synchronization	NOT OK					
A.12.5	**Control of operational software**						
A.12.5.1	Installation of software on operational systems	NOT OK					
A.12.6	**Technical vulnerability management**						
A.12.6.1	Management of technical vulnerabilities	OK					
A.12.6.2	Restrictions on software installation	NOT OK					
A.12.7	**Information systems audit considerations**						
A.12.7.1	Information systems audit controls	OK					
A.13	**COMMUNICATIONS SECURITY**		2	4	1	7	43 %
A.13.1	**Network Security Management**						
A.13.1.1	Network controls	OK					
A.13.1.2	Security of network services	NOT OK					
A.13.1.3	Segregation in networks	OK					
A.13.2	**Information Transfer**						
A.13.2.1	Information transfer policies and procedures	NOT OK					
A.13.2.2	Agreements on information transfer	NOT OK					
A.13.2.3	Electronic messaging	NOT APPLICABLE					
A.13.2.4	Confidentiality or non-disclosure agreements	NOT OK					
A.14	**SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE**		2	1	10	13	92 %
A.14.1	**Security requirements of information systems**						
A.14.1.1	Information security requirements analysis and specification	NOT OK					
A.14.1.2	Securing application services on public networks	OK					
A.14.1.3	Protecting application services transactions	OK					
A.14.2	**Security in development and support processes**						
A.14.2.1	Secure development policy	NOT APPLICABLE					
A.14.2.2	System changes control procedures	NOT APPLICABLE					
A.14.2.3	Technical review of applications after operating platform changes	NOT APPLICABLE					
A.14.2.4	Restrictions on changes to software packages	NOT APPLICABLE					
A.14.2.5	Secure system engineering principles	NOT APPLICABLE					
A.14.2.6	Secure development environment	NOT APPLICABLE					

ID	Topic	Status	OK	NOT OK	NOT APP.	TOTAL	OK+N.A. %
A.14.2.7	Outsourced development	NOT APPLICABLE					
A.14.2.8	System security testing	NOT APPLICABLE					
A.14.2.9	System acceptance testing	NOT APPLICABLE					
A.14.3	**Test data**						
A.14.3.1	Protection of test data	NOT APPLICABLE					
A.15	**SUPPLIER RELATIONSHIPS**			5		5	0 %
A.15.1	**Information security policy for supplier relationships**						
A.15.1.1	Information security policy for supplier relationships	NOT OK					
A.15.1.2	Addressing security within supplier agreements	NOT OK					
A.15.1.3	Information and communications technology supply chain	NOT OK					
A.15.2	**Supplier service delivery management**						
A.15.2.1	Monitoring and review of supplier services	NOT OK					
A.15.2.2	Managing changes to supplier services	NOT OK					
A.16	**INFORMATION SECURITY INCIDENT MANAGEMENT**		5	2		7	71 %
A.16.1	**Management of information security incidents and improvements**						
A.16.1.1	Responsibilities and procedures	OK					
A.16.1.2	Reporting information security events	OK					
A.16.1.3	Reporting information security weaknesses	NOT OK					
A.16.1.4	Assessment of and decision on information security events	OK					
A.16.1.5	Response to information security incidents	OK					
A.16.1.6	Learning from information security incidents	OK					
A.16.1.7	Collection of evidence	NOT OK					
A.17	**INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT**			4		4	0 %
A.17.1	**Information security continuity**						
A.17.1.1	Planning information security continuity	NOT OK					
A.17.1.2	Implementing information security continuity	NOT OK					
A.17.1.3	Verify, review and evaluate information security continuity	NOT OK					
A.17.2	**Redundancies**						
A.17.2.1	Availability of information processing facilities	NOT OK					
A.18	**COMPLIANCE**		2	5	1	8	38 %
A.18.1	**Compliance with legal and contractual requirements**						
A.18.1.1	Identification of applicable legislation and contractual requirements	NOT OK					
A.18.1.2	Intellectual property rights	NOT OK					
A.18.1.3	Protection of records	NOT APPLICABLE					
A.18.1.4	Privacy and protection of personally identifiable information	OK					
A.18.1.5	Regulation of cryptographic controls	OK					
A.18.2	**Information security reviews**						
A.18.2.1	Independent review of information security	NOT OK					
A.18.2.2	Compliance with security policies and standards	NOT OK					
A.18.2.3	Technical compliance review	NOT OK					
			50	46	18	114	60 %

ISO/IEC 27001 standardin vaatimat dokumentit ja niiden vaadittu tietosisältö

- Tietoturvallisuuden hallintajärjestelmän soveltamisala
- Tietoturvallisuuden hallintajärjestelmän kuvaus
- Tietoturvapolitiikka ja tietoturvatavoitteet
- Tietoturvariskien käsittelyprosessi
- Dokumentoitu tieto, jonka organisaatio on määrittänyt tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämättömäksi
- Tietoturvavaatimusten täyttämiseen tarvittavat prosessit, sekä niihin liittyvä muu dokumentaatio, jonka avulla voidaan varmistua, että prosessit toimivat
- Tietoturvariskien käsittelyn tulokset
- Tietoturvallisuuden tason ja tietoturvallisuuden hallintajärjestelmän vaikuttavuuden seurannan ja mittaamisen tulokset
- Sisäisen tietoturvallisuuden hallintajärjestelmän auditointiohjelma ja sen tulokset
- Tieto tietoturvallisuuden hallintajärjestelmän katselmoinneista ja sen tuloksista
- Tieto tietoturvapoikkeamien luonteesta ja niiden perusteella tehdyistä toimenpiteistä ja toimenpiteiden tuloksista