LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

ISO/IEC 27001 -standardi ja tietoturvallisuu-teen sitoutuminen

Salonen, Arto

2016 Laurea

Laurea-ammattikorkeakoulu

ISO/IEC 27001 -standardi ja tietoturvallisuuteen sitoutuminen

Salonen Arto
Tietojenkäsittely
Opinnäytetyö
Syyskuu, 2016

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittely
Tradenomi (AMK)

Arto Salonen

ISO/IEC 27001 -standardi ja tietoturvallisuuteen sitoutuminen

Vuosi 2016 Sivumäärä 32

Tämän opinnäytetyön tarkoituksena oli koota yhteen ISO/IEC 27001 vaatimuskokoelma. Ajatus työstä lähti toimeksiantaja yritykseltä, joka on Suomalainen kansainvälisesti toimiva rahalaitos. Yritys haluaa selvitettävän ISO/IEC 27001 tietoturvasertifikaatin hankkimiseen liittyviä hyötyjä sekä siihen sitoutumiseen vaatimia resursseja. Tässä opinnäytetyössä käydään läpi sertifikaatin saamiseen liittyvää prosessia sekä muita tietoturvallisuuden hallintajärjestelmiä.

Teoreettisen viitekehyksen lisäksi haastateltiin Inspecta Sertifiointi Oy:n pääarvioija Jyrki Lahnalahtea sekä suppeana kyselytutkimuksena kahdeksan eri yrityksen tietoturvasertifikaatista vastuussa olevia henkilöä. Haastatteluiden avulla haettiin kokemuksia sekä mahdollisia ongelmakohtia ja toisaalta myös onnistumisia, joita yritykset kohtasivat sertifiointiprosessissa. Yksi tavoite oli myös selvittää sertifikaatin etuja kehittäessä yrityksen tietoturvallisuutta, yrityksen imagon kohottamisessa ja asiakashankinnoissa. Työssä käydään läpi standardin hyödyllisyyttä yritykselle, joka ei myy it-palveluita, mutta jolla tietotekniikka ja tietoturva ovat erittäin suuressa roolissa. Toimiva ja ajanmukainen tietoturva on tärkeä osa yrityksen toimintaa ja siihen myös pyritään panostamaan toimeksiantaja yrityksessä.

Asiasanat: Tietoturvallisuuden hallintajärjestelmä, ISO/IEC 27001

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Information Technology
Bachelor's Thesis

Arto Salonen

ISO/IEC 27001 -standard and committing to information security

Year 2016 Pages 32

The purpose of this thesis is to go through the ISO/IEC 27001 information security management system. Motive for the thesis originates from a Finnish assignment company that operates internationally in the monetary sector. Assignment company seeks to investigate the pros and cons of ISO/IEC 27001 information security certificate and the resources needed if committed to the process. This thesis will go through the process involved in acquiring the ISO/IEC 27001 information security certificate as well as other similar information security management systems.

In addition to the theoretical framework the head evaluator from Inspecta Certification Jyrki Lahnalahti was interviewed. In addition, eight different companies with the ISO/IEC 27001 certificate were also interviewed. The interview was targeted to the person responsible for the information security certificates. The purpose of the interviews was to acquire information and details regarding the certification process and to discover how different companies succeeded in the process. Target was to find out about the benefits of the certificate when developing information security, how to improve the image of the company and gain advantage attaining new clients. Goal is to study how the ISO/IEC 27001 information security standard benefits a company that does not function in the it-sector but where technology and information security play a big role. Well-functioning and up-to-date information security is a vital component in the organizations daily operations and the assignment company has invested in it heavily.

Keywords: Information Security Management System, ISO/IEC 27001

Sisällys

LYHENTEET

Auditointi Jonkin asian puolueeton arviointi ja tarkastelu joka voidaan suorittaa ulkoisen- tai sisäisen tarkastajan avulla.

IEC International Electrotechnical Commission, kansainvälinen sähkö-teknisen alan standardisointiorganisaatio.

ISO International Organization for Standardization, kansainvälinen standardoimisorganisaatio.

ISO/IEC 27001 on sertifikaatti, joka määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset.

ISO 9001 Kansainvälinen standardi joka määrittelee laadunhallintajärjestelmien vaatimukset.

ISO/IEC 20000-1 Kansainvälinen standardi joka määrittelee it-palvelunhallintajärjestelmien vaatimukset

Katakri Kansallinen turvallisuusauditointikriteeristö

Sertifikaatti Menettely, jolla tunnistettu, riippumaton ja puolueeton kolmas osapuoli antaa kirjallisen varmistuksen siitä, että tuote, menetelmä tai palvelu on määriteltyjen vaatimusten mukainen

Tietoturvallisuuden hallintajärjestelmä kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet

Vaatimuskokoelma Standardista laadittu kirjallinen dokumentti

1 Johdanto

Nykypäivänä yrityksen tietoturvallisuus on yksi liiketoiminnan tärkeistä osa-alue, jonka pettäessä koko yritystoiminta voi vaarantua ja näin ollen tietoturvallisuus toimii yrityksen selkärankana. Tietoturvallisuuteen liittyvien haavoittuvuuksien paikantaminen yleensä vaatii koko organisaation toimintaketjun perusteellista läpikäymistä, johon erinomaisena työkaluna toimii eri vaatimuskokoelmat eli standardit.

Organisaatioiden päivittäinen toiminta nojaa täydellisesti eri tietoteknisiin järjestelmiin toimialasta riippumatta, eikä palveluiden ulkoistaminen poista riskejä, joita tiedon käsittely ja varastointi aiheuttavat. Opinnäytetyön tehtävänä on toimia apuvälineenä suomalaiselle kansainvälisesti toimivalle rahalaitokselle, joka selvittää ISO/IEC 27001 -tietoturvasertifikaatin hankintaa sen hyöty- ja haittanäkökulmasta. It on yritykselle tärkeä osa toimivaa kokonaisuutta, jossa erityisesti tietoturva tulee huomioida. Tilaajayrityksen näkökulmasta ongelma oli epävarmuus ISO/IEC 27001 -sertifikaatin vaatimasta ajasta ja resurssien sitomisesta määrittämättömäksi ajaksi. Sertifiointiprosessi vaatii resursseja ja sitoutumista useiksi kuukausiksi ilman, että päivittäinen yritystoiminta keskeytyy. Työn tarkoituksena on vastata kysymyksiin, joita sertifikaattia harkitsevalle toimeksiantajayritykselle syntyi mietittäessä eri keinoja ja työkaluja tietoturvan kehittämiseen sitoutumisessa.

Tietoturvallisuuden hallintaan tulee panostaa organisaatiossa huolimatta sen koosta, tyypistä tai toiminta-alueesta. Opinnäytetyön tehtävä on tarjota lukijalle läpileikkaus ISO/IEC 27001 -vaatimuskokoelmaan, sen hyötyihin tietoturvallisuuden kehittämisessä ja niihin sitoutumisessa. Opinnäytetyötä varten suoritettiin sähköpostikyselyjä eri it-alan yrityksille. Lisäksi henkilöhaastattelun avulla pyrittiin saamaan luotettava kokonaiskuva sertifiointiprosessista ja siihen sitoutumisesta. Näin ollen sertifikaattia harkitseva yritys pystyy tekemään päätöksen prosessiin sitoutumisesta. Henkilöhaastatteluna haastateltiin sertifikaatteja myöntävän Inspecta Sertifiointi Oy:n pääarvioija Jyrki Lahnalahtea, ja tällä pyrittiin selvittämään sertifiointiprosessia ja kokemuksia auditoijan näkökulmasta. Lisäksi haastattelun avulla pyrittiin selvittämään sertifikaatin hyötyjä organisaatioiden tietoturvallisuuden ja yrityskuvan edistämisessä sekä näiden vaikuttavuudesta asiakashankinnoissa. Jyrki Lahnalahden haastattelussa pyrittiin myös selvittämään prosessin vaatimaa työmäärää sekä resurssien sitomista pitkäkestoiseen projektiin.

Opinnäytetyössä selvitetään ISO/IEC 27001 -standardin vaatimuksia ja yrityksen johdon tarvetta sitoutua tietoturvan kehittämiseen. Vaatimuskokoelman tehtävänä on toimia apuvälineenä, kun organisaatio suunnittelee ja kehittää tietoturvallisuuden hallintajärjestelmäänsä. Opinnäytetyö rajattiin koskemaan ISO/IEC 27001 tietoturvan hallintajärjestelmää sekä valmis-

tautumista sertifiointiprosessiin. Opinnäytetyön teoreettinen viitekehys pohjautuu alan kirjallisuuteen pääpainon ollessa digitaalisissa lähteissä niiden ajantasaisuuden takia, painettujen lähteiden ollessa vanhentuneita jo muutaman vuoden jälkeen. Digitaalisista lähteistä, artikkeleista ja julkaisuista on saatavilla viimeisintä tietoa yrityksen tietoturvallisuuden kehittämisestä ja yritysten turvallisuutta uhkaavista trendeistä. Digitaaliset verkkojulkaisut toimivat myös tietohallinnosta vastaavalle taholle tavan pysyä ajan hermoilla sekä verkostoitua muiden ammattilaisten kanssa.

Sertifikaatit ovat osoitus yrityksen sitoutumisesta toimintaan ja yritys osoittaa asiakkailleen ja sidosryhmilleen, että jatkuva kehittäminen ja parantaminen ovat keskeinen osa yrityksen toimintaa. Toimintajärjestelmät ja niiden sertifioinnit ovat yhä usein edellytyksenä asiakkaan valitessa toimittajia tai kumppaneita. Opinnäytetyössä pyritään eri keinoin selvittämään konkreettisia etuja sertifioinnista asiakashankinnoissa sekä tietoturvaan sitoutumisessa. Sertifiointiprosessissa käytetyt auditoinnit eli arvioinnit, ovat oleellinen osa tietoturvallisuuden hallintajärjestelmän toimintamallia ja ne muodostavat osaltaan toiminnalle mittareita.

Opinnäytetyön lopuksi käydään läpi haastattelukyselyiden tuloksia sekä niistä saatavia johtopäätöksiä. Tavoitteena on saada mahdollisimman kattava käsitys ISO/IEC 27001 tietoturvan hallintajärjestelmän sertifikaatista, sen hyödyistä yrityksen turvallisuudelle ja mitä resursseja siihen tulee sitouttaa onnistuneen lopputuloksen saavuttamiseksi.

2 Työn lähtökohdat

Lähtökohtana oli tarve selvittää opinnäytetyön toimeksiantajayritykselle ISO/IEC 27001 -tietoturvastandardin sertifiointiprosessiin lähtemisen sekä itse sertifikaatin kannattavuutta esimerkiksi asiakashankintojen kannalta. Tarkoituksena oli saada selville todellisia hyötyjä yritykselle sertifikaatista suhteessa prosessiin sidottuihin resursseihin, kuten aikaan ja työmäärään. Sertifiointiprossin kestoon oli tärkeä saada selvyyttä ja raportin perusteella yritys pyrkii hahmottamaan prosessin ajallista ja työmäärällistä kestoa oman organisaation kokoon suhteutettuna.

Tutkimusongelmaksi muodostui aiempien empiiristen eli kokemusperäisten tutkimusten puuttuminen. Varsinaista tutkimusta ISO/IEC 27001 -tietoturvasertifikaatin konkreettisista eduista yritysten liiketoiminnalle tai tietoturvan tason kehittymiselle ei ole tehty tai sitä ei ainakaan julkisesti ole saatavilla. Opinnäytetyössä päädyttiin tuottamamaan henkilöhaastattelulla sekä sähköpostikyselyillä tutkimusmateriaalia, johon johtopäätökset pohjautuvat. ISO/IEC 27001 on maailmanlaajuinen standardi ja sen vaatimukset ovat samalla tavalla sitovia kaikkialla maailmassa.

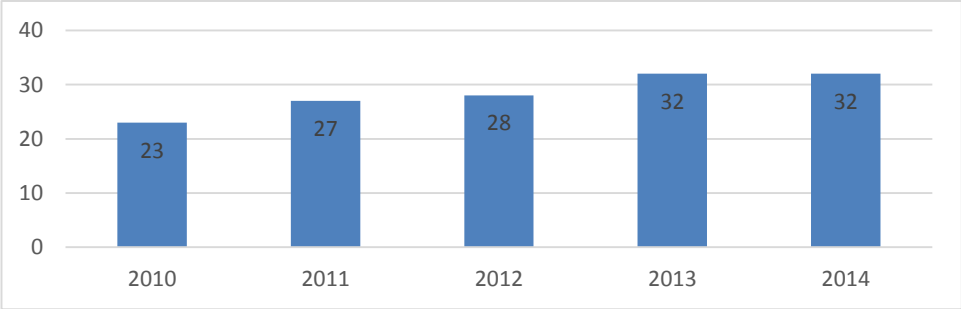
Jotta pystyttiin käsittelemään ylipäänsä ISO/IEC 27001 -sertifikaatin vaatimuksia, oli ensin tutustuttava sertifikaatin dokumenttiin eli vaatimuskokoelmaan. Vasta tämän jälkeen pystyttiin keskittymään varsinaiseen tutkimukseen ja muodostamaan esimerkiksi henkilöhaastattelun ja sähköpostikyselyn kysymykset. Vaatimuskokoelman tulkitseminen vaatii ajallista panostusta sekä syvällistä ymmärtämistä tekstin haasteellisuuden vuoksi.

3 ISO/IEC 27001 -STANDARDI

ISO/IEC 27001 on kansainvälisten ISO- ja IEC- standardisointiorganisaatioiden luoma standardi eli vaatimuskokoelma, tietoturvallisuuden hallinnalle organisaatiossa. ISO/IEC 27001 on osa isoa standardiperhettä, jonka tehtävänä on tarjota vaatimuskokoelma eri tietoturvallisuuden tarpeeseen. ISO/IEC 27000 standardiperheen yhteinen otsikko on: ”Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät”.

ISO/IEC 27001 -standardin uusin versio on vuodelta 2013, joka korvasi edellisen version vuodelta 2005. Päivitetyssä versiossa on otettu paremmin huomioon myös sovelluspohjaiset infrastruktuurit, kuten muun muassa pilvipalvelut. 2013 versiossa myös pääpaino on organisaation tietoturvan johtamisjärjestelmän suorituskyvyn arvioinnissa ja mittaamisessa, eikä prosessimaisessa toimintamallissa, kuten vuoden 2005 versiossa. (The ISO 27000 Directory 2013.)

Vuonna 2014 ISO/IEC 27001 -sertifikaatteja oli myönnetty Suomessa 32 eri yritykselle. Seuraavassa kuvassa (kuvio 1) on esitelty ISO/IEC 27001 sertifioitujen yritysten määrä ja kehitys Suomessa vuodesta 2010. Vuodesta 2010 vuoteen 2014 ISO/IEC 27001 sertifioitujen yritysten määrä on kasvanut tasaisesti määrän ollessa vuonna 2014 32. (International Organization of Standardization Survey.)



Kuvio 1. ISO/IEC 27001 -standardin sertifioitujen yritysten määrä ja kehitys Suomessa

Standardiperhe käsittää 40 eri vaatimusmäärittelyä eri tietoturvallisuuden tarpeisiin, läheisimpänä 27001 -standardia ovat seuraavat:

- ISO/IEC 27000:2016 (ISO 27000) Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto.
- ISO/IEC 27002:2013 (ISO 27002) Tietoturvallisuuden hallintaa koskeva menettelyohje.
- ISO/IEC 27003:2010 (ISO 27003) Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita.
- ISO/IEC 27004:2009 (ISO 27004) Tietoturvallisuuden hallinta. Mittaaminen.
- ISO/IEC 27005:2011 (ISO 27005) Tietoturvariskien hallinta.
- ISO/IEC 27006:2015 (ISO 27006) Tietoturvallisuuden hallintajärjestelmien auditointiohjeet. (IT Governance)

3.1 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä on osa yleistä hallintajärjestelmää, joka liiketoiminta-riskien arviointiin perustuen luodaan ja toteutetaan. Tietoturvallisuuden hallintajärjestelmä on dokumenttikokoelma ja moniosainen prosessi, jota tulee kehittää jatkuvasti. Tietoturvallisuuden hallintajärjestelmän osia ovat muun muassa tietoturvapolitiikka, riskianalyysi, tietoturva-, jatkuvuus- ja toipumissuunnitelmat. (SFS oppilaitosportaali.) Tietoturvallisuuden hallintajärjestelmän käyttöönotto on organisaation strateginen päätös ja ISO/IEC 27001 -tietoturvallisuuden hallintajärjestelmä tarjoaa yleiset vaatimukset sen luomiselle, käyttämiselle, valvonnalle, toteuttamiselle, katselmoinnille, ylläpidolle ja parantamiselle.

ISO/IEC 27001 on standardisarjan käytetyin standardi, jonka vaatimuksia voidaan käyttää organisaatioiden vaatimustenmukaisuuden sertifiointiin (27001 Academy). Standardia hyödynnetään organisaation tietoturvallisuuden toteutumisessa sekä varmistettaessa tietojen luottamuksellisuus, eheys, käytettävyys ja alkuperä.

- *Luotettava* tieto tarkoittaa, että tieto on käytettävissä vain siihen oikeutetuilla tahoilla.
- *Eheys* tarkoittaa, että tiedon ja tietojärjestelmien toiminnan tulee olla virheetöntä.
- *Käytettävyys* tarkoittaa, että tiedot ovat saatavilla aina tarvittaessa.
- *Alkuperä* tarkoittaa, että tiedon alkuperä ja oikeellisuus tulee aina olla todennettavissa.

ISO/IEC 27001 -dokumenttia kutsutaan standardin vaatimusmäärittelyksi ja useat yritykset ovatkin valinneet ISO/IEC 27001 -dokumentin osaksi yrityksen tietoturvaa ja ovat sitoutuneet

tietoturvallisuuden kehittämiseen standardin vaatimusten mukaan ilman, että ovat hankkineet sertifikaattia. Yritys katselmoi omatoimisesti hallintajärjestelmänsä ja ylläpitää itsenäisesti tiedon eheyttä, luotettavuutta, käytettävyyttä ja alkuperää. (ISO 27001.) ISO/IEC 27001 on standardiperheessä ainoa, johon voi sertifioitua.

3.2 Auditointi- ja riskianalyysityökaluja

ISO/IEC 27001 on yhdenmukainen perusosiltaan useiden muiden kansainvälisten standardien, kuten ISO 9001:2015 laadunhallintajärjestelmä standardin, ISO 14001:2015 ympäristöjärjestelmä standardin sekä Saksan liittovaltion tietoturvallisuuden kehittämän IT-Grundschutz -katalogin kanssa. IT-Grundschutz on järkälemäinen, yli 3000 sivun tietoturvaopas, joka kehitettiin tarjoamaan yrityksille suositukset, joilla kehitetään metodeja ja prosesseja, sekä tarjotaan käytännön keinoja parantaa yrityksen tietoturvallisuutta. IT-Grundschutz on täysin yhteensopiva ISO/IEC 27001 -standardin kanssa ja sisältää useita ISO/IEC 2700X -standardiperheen suosituksia kuten muun muassa riskienhallinnan laadintaa tai niihin varautumista. (Federal Office for Information Security.)

Katakri eli kansallinen turvallisuusauditointikriteeristö on viranomaisten laatima kriteeristö, jonka päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa kohteen turvallisuustason auditoinnin yrityksessä tai muussa yhteisössä. Turvallisuusauditointikriteeristöä voidaan käyttää myös arvioitaessa kohdeorganisaation kykyä suojata viranomaisten salassa pidettävää tietoa. Kansalliset säädökset ja kansainvälisiin velvoitteisiin perustuvat vähimmäisvaatimukset on koottu Katakriin. Katakri kriteeristö ei aseta ehdottomia vaatimuksia tietoturvallisuudelle. Katakriin on koottu vaatimuksia jotka perustuvat voimassa oleviin lainsäädäntöihin ja kansainvälisiin tietoturvallisuusvelvoitteisiin, jotka sitovat Suomea. (Puolustusministeriö Katakri 2015.)

Katakria voidaan käyttää auditointityökaluna yrityksen turvallisuusjärjestelyiden toteuttamisessa, yritysturvallisuusselvityksessä ja viranomaisten tietojärjestelmien turvallisuuden arvioinneissa. Katakria voidaan käyttää myös apuna yritysten, yhteisöjen ja viranomaisten muussa turvallisuustyössä ja kehittämisessä. (Puolustusministeriö Katakri 2015.)

4 ISO/IEC 27001 -standardin vaatimukset

ISO/IEC 27001:2013 -standardin tärkeimpänä vaatimuksena on yrityksen sitoutuminen tietoturvallisuuden hallintajärjestelmien kehittämiseen, käyttämiseen, toteuttamiseen, valvomiseen, katselmointiin, ylläpitämiseen ja parantamiseen. Tietoturvallisuuden hallintajärjestelmä on dokumentaatio, joka kattaa kaikki tietoturvan johtamisessa, hallinnoimisessa ja valvonnassa tarvittavat menettelyt ja toimenpiteet. Standardi on jaettu seuraaviin pääkohtiin (ISO/IEC 27001 -tietoturvallisuusstandardi 2013):

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
11. Liite A, (velvoittava) Hallintatavoitteiden ja -keinojen viiteluettelo

ISO/IEC 27001 -vaatimusmäärittelyssä luvut 4-10 sisältää vaatimukset kullekin osa-alueelle siitä, miten organisaation toimintaympäristössä tulee parantaa tietoturvallisuuden hallintajärjestelmän luomista, sen toteuttamista ja ylläpitoa. Vaatimukset, joita standardissa on esitelty, ovat yleisluontoisia ja tarkoitus onkin, että ne soveltuvat kaikille organisaatioille organisaation luonteesta, tyypistä tai koosta riippumatta. Jos organisaatio ilmoittaa noudattavansa ISO/IEC 27001 -standardin vaatimuksia, ei mitään kohdista 4-10 esitetyistä vaatimuksista voida rajata pois. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 8.) Seuraavissa alaluvuissa on esitelty ISO/IEC 27001 -standardin dokumentissa käsiteltävät luvut 4-10.

4.1 Organisaation toimintaympäristö

ISO/IEC 27001 -standardin vaatimusmäärittelyn luvussa neljä käydään läpi, kuinka organisaation on määritettävä ulkoiset ja sisäiset asiat, jotka ovat olennaisia organisaation tarkoituksen kannalta ja jotka vaikuttavat kykyyn saavuttaa tietoturvallisuuden hallintajärjestelmältä vaaditut tulokset. Tietoturvallisuuden hallintajärjestelmän kannalta olennaiset sidosryhmät sekä näiden sidosryhmien asettamat tietoturvallisuutta koskevat vaatimukset tulee määrittää organisaatiossa.

Vaatimukset voivat sisältää sopimusvelvoitteita sekä viranomaisten lakisääteisiä vaatimuksia. Organisaatio velvoitetaan vaatimusten mukaisesti luomaan tietoturvallisuuden hallintajärjestelmä, ylläpidettävä ja parannettava sitä edelleen. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 8.)

4.2 Johtajuus

Standardin vaatimusmäärittelyn luku 5 käsittelee useita keinoja, joilla yrityksen ylin johto osoittaa johtajuutta sekä sitoutumista tietoturvallisuuden hallintajärjestelmään. Johdon tehtävä on varmistaa, että tietoturvapolitiikka laaditaan ja tavoitteet asetetaan yhdenmukaiseksi organisaation strategian kanssa. Johdon on varmennettava, että tietoturvallisuuden hallintajärjestelmän vaatimukset voidaan yhdistää organisaation prosesseihin sekä tarvittavien resurssien saatavilla olo. Lisäksi tulee huolehtia, että halutut tulokset voidaan saavuttaa. Johdon tulee toiminnallaan viestittää hallintajärjestelmän vaatimusten noudattamisen tärkeydestä. Ihmisiä tulee ohjata hallintajärjestelmän kehittämiseen tukemalla vastuualueiden johtohenkilöstöä. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 10.)

Ylimmän johdon tehtävänä on laatia tietoturvapolitiikka, joka soveltuu organisaation toiminta-ajatukseen sisältäen tavoitteet tai muodostaen perustan tavoitteiden asettamiselle tietoturvapolitiikassa. Tietoturvapolitiikan tulee sisältää sitoutumisen tietoturvallisuutta koskevien vaatimusten täyttämiseen sekä tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen. Tietoturvapolitiikan tulee olla saatavilla dokumentoituna, koko organisaation tiedossa ja tarvittaessa sidosryhmien saatavilla. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 10.)

Ylimmän johdon tehtävä on varmistaa kenellä tai keillä on vastuut ja valtuudet tietoturvan kannalta tärkeissä rooleissa ja että niistä viestitään. Tietoturvallisuuden hallintajärjestelmä tulee olla kansainvälisessä ISO/IEC 27001 -standardissa esitettyjen vaatimusten mukainen ja ylimmälle johdolle tulee raportoida tietoturvallisuuden hallintajärjestelmän suorituskyvystä. Tarvittaessa suorituskyvyn raportoinnista organisaation sisällä voidaan määritellä vastuuhenkilö. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 10.)

4.3 Suunnittelu

Standardin vaatimusmäärittelyssä luku 6 selventää, kuinka organisaation on otettava useita eri asioita huomioon suunniteltaessa tietoturvallisuuden hallintajärjestelmää, kuten organisaation ja sen toimintaympäristön tuomat haasteet sekä sidosryhmien ja tarpeiden asettamat vaatimukset. Suunnitteluvaiheessa tulee varmistaa, että hallintajärjestelmä voi saavuttaa halutut tulokset, ei-toivotut vaikutukset estetään tai vähennetään ja saavutetaan tila, jossa saadaan aikaan jatkuvaa kehittämistä. Suunniteltaessa tulee selvittää, kuinka toimenpiteet yhdistetään tietoturvallisuuden hallintajärjestelmän prosesseihin ja kuinka niiden vaikuttavuus voidaan arvioida. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 12.)

Tietoturvariskien arvioinnissa tulee organisaation määrittää tietoturvariskien arviointiprosessi, jossa laaditaan ja ylläpidetään tietoturvariskikriteerejä. Arvioinnissa laaditaan ja ylläpidetään

riskien hyväksymiskriteerit sekä tietoturvariskien arvioinnin suorittamista koskevat kriteerit. Organisaation tulee varmistaa, että toistuvat tietoturvariskien arvioinnit tuottavat yhdenmukaisia, päteviä ja verrattavissa olevia tuloksia, joiden avulla voidaan tunnistaa tietoturvariskit. Tietoturvan arviointiprosessilla tunnistetaan tietoturvallisuuden hallintajärjestelmän kuuluvan tiedon luottamuksellisuuden, eheyden ja saatavuuden menettämiseen liittyvät riskit tunnistamalla riskien omistajat. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 12.)

Analysoimalla ja arvioimalla määritetään riskin taso tunnistamalla riskien toteutumisen seuraukset, toteutumisen realistinen todennäköisyys ja vertaamalla riskianalyysin tuloksia aiemmin laadittuun riskien hyväksymiskriteereihin. Organisaation on säilytettävä dokumentoitua tietoa tietoturvariskien arviointiprosessista. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 12.)

Tietoturvariskien käsittelyssä organisaatio määrittelee ja toteuttaa prosessia, jossa valitaan soveltuvat tietoturvariskien käsittelyvaihtoehdot. Myös riskien arvioinnin tulokset tulee määritellä sekä kaikki hallintakeinot, joita tarvitaan valittujen tietoturvariskien käsittelyvaihtoehtojen toteuttamiseen. Hallintakeinot voidaan suunnitella organisaatiossa tai niitä voidaan yksilöidä myös muista lähteistä. Hallintakeinot, jotka on määritelty tietoturvariskien käsittelyvaihtoehtojen toteuttamiseen, verrataan ISO/IEC 27001 -standardin A liitteessä oleviin hallintakeinoihin ja tarkistetaan, ettei tarvittavia keinoja ole jätetty pois. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 14.) Liite A sisältää tietoturvan hallintatavoitteet, joista tarkemmin myöhemmin.

ISO/IEC 27001 -standardin käyttäjiä kehotetaan varmistamaan liitteen A kattavasta hallintatavoite- ja keinoluettelosta, jotta tarvittavia hallintatavoitteita ei jää huomioimatta. Organisaation tulee laatia soveltuvuuslausunto, joka sisältää vaaditut hallintakeinot sekä perustelut liitteessä A esitettyjen hallintakeinojen käyttämiselle tai käyttämättä jättämiselle. Tietoturvariskien käsittelysuunnitelmaa laadittaessa tulee havaittujen riskien käsittelysuunnitelma hyväksyttää vastuu henkilöiltä. Käsittelyprosessi tulee dokumentoida ja laaditut dokumentit säilyttää. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 14.)

Tietoturvatavoitteet tulee asettaa asiaankuuluville toiminnoille ja tasoille organisaation toimesta. Tietoturvatavoitteiden tulee täyttää useita vaatimuksia. Tavoitteiden tulee olla yhdenmukaiset tietoturvapolitiikan kanssa ja olla mitattavissa, mikäli mahdollista. Tietoturva tavoitteissa tulee ottaa huomioon soveltuvat tietoturvavaatimukset sekä riskien arvioinnissa ja käsittelyssä saavutetut tulokset. Ne tulee viestittää ja päivittää tarvittaessa. Laaditut tietoturvatavoitteiden dokumentit tulee säilyttää. Suunniteltaessa tietoturvatavoitteita, tulee määritellä, miten se tehdään, mitä resursseja tarvitaan, kuka tai ketkä ovat vastuussa sekä

milloin työ saadaan valmiiksi ja kuinka tulokset arvioidaan. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 14.)

4.4 Tukitoiminnot

Standardin vaatimusmäärittelyssä luku 7 käsittelee tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitoa ja jatkuvaa parantamista, organisaation tulee määritellä ja varata tarvittavat resurssit sekä todeta henkilöiden pätevyys, joiden työ vaikuttaa sen tietoturvallisuuden tasoon. Pätevyys varmistetaan henkilöiden soveltuvan koulutuksen, harjoittelun tai kokemuksen perusteella. Tarvittaessa henkilöille hankitaan tarvittava lisäosaaminen, joka antaa valmiudet toimia tavoitellulla tietoturvallisuuden tasolla. Lisäksi tulee arvioida tehtyjen toimenpiteiden ja mahdollisten koulutusten vaikuttavuus. Tieto henkilöiden pätevyydestä tulee säilyttää asianmukaisesti dokumentoituna eli kirjallisesti todennettavissa. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 16.)

Organisaation ohjauksessa työskentelevien henkilöiden on oltava tietoisia tieturvapolitiikasta sekä siitä, miten he voivat osaltaan lisätä tietoturvallisuuden hallintajärjestelmän vaikuttavuutta. Organisaation työntekijöiden tulee tietää mitä hyötyjä tietoturvallisuuden tason parantamisesta on sekä seurauksista, joita vaatimusten noudattamatta jättämisellä voi olla. Organisaation tulee määrittää, millaista sisäistä ja ulkoista tietoturvallisuuden hallintajärjestelmän kannalta olennaista viestintää tarvitaan, esimerkiksi mistä viestitään, milloin viestitään, keiden kanssa viestitään, ketkä viestivät ja miten viestintäprosessi toteutetaan. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 16.) Viestinnällä tarkoitetaan kaikkea organisaation sisällä tapahtuvaa viestintää ja sen avulla välitetään eteenpäin yrityksen toiminnan kannalta oleellista tietoa, kuten muuttuneita tai päivitettyjä tietoturvapoliitikkoja.

Tietoturvallisuuden hallintajärjestelmän on sisällettävä ISO/IEC 27001 -standardissa edellytetty dokumentoitu tieto, jonka organisaatio on määrittänyt tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kannalta välttämättömäksi. Dokumentoidun tiedon laajuuteen vaikuttaa organisaation koko sekä toimintojen, prosessien, tuotteiden ja palveluiden tyyppi, kuten myös vuorovaikutus ja henkilöiden pätevyys. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 16.)

Dokumentoituja tietoja luodessa ja päivittäessä organisaation tulee varmistaa niiden asianmukaisuus, merkintä ja tallennusmuoto sekä soveltuvuuden ja riittävyyden tarkistaminen ja hyväksyminen. Tietoturvallisuuden hallintajärjestelmää sekä ISO/IEC 27001 -standardissa edellytettyä dokumentoitua tietoa on hallittava, jotta se on aina saatavilla sopivassa muodossa kulloiseenkin käyttötarkoitukseen ja se on suojattu asianmukaisesti. Luottamuksellista tietoa, kuten dokumentteja tai sähköposteja ei luovuteta luvatta, eikä tietoa käytetä asiattomasti ja

tieto pysyy muuttumattomana kokonaisuutena. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 18.)

Dokumentoidun tiedon hallinta kattaa soveltuvin osin tietojen jakelun, pääsyn, esille saannin ja käytön sekä varastoinnin ja säilytyksen, johon kuuluu myös luotettavuuden säilyttäminen. Hallinta sisältää myös tiedon muutostenhallinnan sekä tiedon säilyttämisen ja hävittämisen. Organisaation tulee määritellä ja yksilöidä dokumentit, jotka ovat ulkopuolista alkuperää, mutta tarpeellisia tietoturvallisuuden hallintajärjestelmän suunnittelulle ja toiminnalle. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 18.)

4.5 Toiminta

Standardin dokumentaatiossa luku 8 pitää sisällään, kuinka organisaation tulee suunnitella ja toteuttaa prosessit, joita tarvitaan tietoturvavaatimusten täyttämiseen tietoturvariskien arviointiprosessissa sekä ohjattava niitä. Organisaation tulee toteuttaa suunnitelmat, joilla saavutetaan luvussa 6 asetetut tietoturvatavoitteet tiedon yhdenmukaisuudesta tietoturvapolitiikan kanssa. Tietoa tulee dokumentoida riittävästi ja sitä tulee säilyttää asianmukaisesti, jotta voidaan luottaa siihen, että prosessit on toteutettu suunnitelmien mukaisesti. Suunniteltuja muutoksia tulee hallita ja arvioida, jotta kyetään tahattomien muutosten seurauksien hallintaan ja pyrkiä lieventämään mahdollisia haittavaikutuksia. Ulkoiset prosessit tulee määritellä ja valvoa organisaation toimesta. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 18.)

Tietoturvariskien arviointi suoritetaan suunnitelluin aikavälein, tai kun merkittäviä muutoksia ehdotetaan tai jos tapahtuu muutoksia. Arvioinnissa tulee huomioida tietoturvariskien arvioinnissa määritellyt riskien hyväksymiskriteerit sekä arvioinnin suorittamista koskevat kriteerit. Arvioinnin tulokset tulee dokumentoida ja säilyttää asianmukaisesti. Tietoturvariskien käsittelysuunnitelma tulee organisaatiossa ottaa käyttöön ja dokumentoida käyttöönoton tulokset. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 20.)

4.6 Suorituskyvyn arviointi

Standardin vaatimusmäärittelyssä luku 9 opastaa, kuinka organisaation tulee arvioida tietoturvan tasoa. Hallintajärjestelmä dokumentaatiossa määritellään mitä täytyy seurata ja mitata, mukaan lukien tietoturvaprosessit ja hallintakeinot. Millä seuraus-, mittaus-, analysointi- tai arviointimenetelmillä varmistetaan kelvolliset tulokset. Kelvollinen tulos tulee olla vertailtavissa ja toistettavissa. Organisaation tulee määritellä, koska seuranta ja mittaus toteutetaan, ketkä toteuttavat seurannan ja mittauksen, ja koska tuloksia analysoidaan ja arvioidaan. Tä-

män lisäksi tulee määritellä ketkä analysoivat ja arvioivat saadut tulokset. Suoritetut toimenpiteet tulee kirjallisesti dokumentoida ja säilyttää todisteena tuloksista. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 20.)

Jotta voidaan arvioida, onko tietoturvallisuuden hallintajärjestelmä organisaation omien vaatimusten sekä ISO/IEC 27001 -standardin vaatimusten mukainen, tulee organisaation suorittaa sisäisiä auditointeja suunnitelluin aikavälein. Tietoturvallisuuden hallintajärjestelmän toteutusta ja ylläpitoa arvioidessa organisaation on suunniteltava, laadittava, toteutettava ja ylläpidettävä auditointiohjelmia. Auditointiohjelmissa määritellään muun muassa auditointien aikataulu, menetelmät ja vastuut, suunnitteluvaatimukset ja raportointi. Prosessien tärkeys ja edellisten auditointien tulokset tulee ottaa huomioon ja määritellä kussakin auditoinnissa käytettävä arviointikriteeri ja soveltamisala. Auditoijat tai suoritettava auditointi tulee valikoida siten, että puolueettomuus voidaan varmistaa auditointiprosessissa. Auditointien tulokset tulee raportoida johtoon kuuluville henkilöille ja auditoinnista luodut dokumentit tulee säilyttää todisteena auditointiohjelmasta sekä niiden tuloksista. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 20.)

Ylimmän johdon tehtäviin kuuluu tietoturvallisuuden hallintajärjestelmän katselmointi suunnitelluin aikavälein varmistaen, että se on edelleen soveltuva, asianmukainen ja vaikuttava. Katselmuksessa tulee ottaa huomioon aiempien katselmusten vuoksi käynnistettyjen toimenpiteiden tilanne, tietoturvallisuuden hallintajärjestelmän kannalta olennaisten ulkoisten ja sisäisten asioiden muutokset sekä tietoturvan tasoa koskeva palaute. Tietoturvan tasoa koskeva palaute sisältää poikkeamat, korjaavat toimenpiteet sekä seurannan ja mittauksen tulokset. Palautteeseen liittyy myös auditointien tulokset ja tietoturvatavoitteiden täyttyminen sekä lisäksi myös sidosryhmien antama palaute ja riskien arvioinnin tulokset. Johdon katselmuksen tuloksiin on sisällyttävä päätökset jatkuvan parantamisen mahdollisuuksista sekä hallintajärjestelmän mahdollisista muutostarpeista. Dokumentoitu tieto tulee säilyttää todisteena katselmusten tuloksista. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 22.)

4.7 Parantaminen

Standardin vaatimusmäärittelyssä luku 10 pitää sisällään, kuinka organisaation on reagoitava havaitessa poikkeama ja tilanteesta riippuen ryhdyttävä toimiin sen hallitsemiseksi ja korjaamiseksi sekä käsiteltävä sen seurauksia. Organisaation tulee arvioida mahdolliset toimenpiteet, joilla poikkeamien syitä voidaan vähentää tai poistaa. Keinoina käytetään esimerkiksi poikkeaman katselmointia, syiden selvittämistä sekä vastaavien poikkeamien tai niiden mahdollisuuksien etsimistä. Tarvittavat toimenpiteet tulee toteuttaa, niiden vaikuttavuus arvioida sekä tehdä muutoksia tietoturvallisuuden hallintajärjestelmään, jos se on tarpeellista. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 22.)

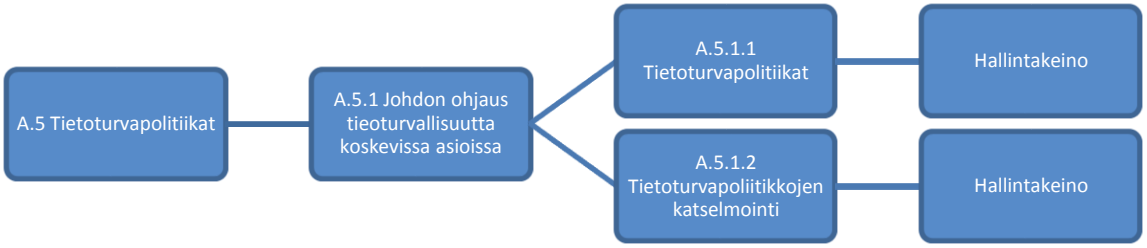
Poikkeamia korjaavien toimenpiteiden tulee olla tarkoituksenmukaisia niiden aiheuttamiin vaikutuksiin nähden ja organisaatiolla tulee olla dokumentoitua tietoa todisteena poikkeamien luonteesta sekä niiden johdosta tehdyistä toimenpiteistä sekä tehtyjen korjaavien toimenpiteiden tuloksista. Organisaation tulee parantaa jatkuvasti tietoturvallisuuden hallintajärjestelmän soveltuvuutta, riittävyyttä ja vaikuttavuutta. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 22.)

4.8 ISO/IEC 27001 LIITE A

ISO/IEC 27001 -standardin liite A on velvoittava ja sisältää tietoturvan hallintatavoitteiden- ja keinojen viiteluettelon, jotka tulee ottaa osaksi organisaation riskien arviointi- ja käsittelyprosessia. Hallintatavoitteet on jaettu pääalueisiin:

- A.5 Tietoturvapolitiikat, johdon ohjaus tietoturvallisuutta koskevissa asioissa
- A.6 Tietoturvallisuuden organisointi, sisäinen organisaatio, mobiililaitteet ja etätyö
- A.7 Henkilöstöturvallisuus, ennen työsuhteen alkua, työsuhteen aikana ja sen jälkeen.
- A.8 Suojattavan omaisuuden hallinta, vastuu suojattavasta omaisuudesta, tietojen luokittelu ja tietovälineiden käsittely
- A.9 Pääsynhallinta, liiketoiminnalliset vaatimukset, käyttäjän vastuu ja järjestelmien ja sovellusten pääsynhallinta
- A.10 Salaus, salauksen hallinta
- A.11 Fyysinen turvallisuus ja ympäristön turvallisuus, turva-alueet, laitteet
- A.12 Käyttöturvallisuus, toimintaohjeet ja velvollisuudet, haittaohjelmilta suojautuminen, varmuuskopiointi, kirjaaminen ja seuranta, tuotantokäytössä olevien ohjelmistojen hallinta, teknisten haavoittuvuuksien hallinta, tietojärjestelmien auditointinäkökohtia
- A.13 Viestintäturvallisuus, verkon turvallisuuden hallinta, tietojen siirtäminen
- A.14 Järjestelmän hankkiminen, kehittäminen ja ylläpito, tietojärjestelmiä koskevat turvallisuusvaatimukset, kehitys- ja tukiprosessien turvallisuus, testiaineisto
- A.15 Suhteet toimittajiin, tietoturvallisuuden toimittajasuhteissa, toimittajien palveluiden hallinta
- A.16 Tietoturvallisuuden hallinta, tietoturvahäiriöiden ja tietoturvallisuuden parannusten hallinta
- A.17 Liiketoiminnan jatkuvuuden hallintaan liittyviä tietoturvanäkökohtia, tietoturvallisuuden jatkuvuus, vikasietoisuus
- A.18 Vaatimustenmukaisuus, lainsäädäntöön ja sopimuksiin sisältyvien vaatimusten noudattaminen, tietoturvallisuuden katselmoinnit
  (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 24-44)

Hallintatavoitteita on ISO/IEC 27001 -standardissa määritelty 35 kappaletta. Jokaisessa hallintatavoitteessa on yksi tai useampi hallintakeino, joilla tavoite pyritään toteuttamaan ja jota organisaation tulee arvioida riskinhallintaprosessissa. Kuviossa 2 on esimerkki hallintatavoitteen pääkohdasta A.5 Tietoturvapolitiikat, jonka alaotsikko on: ”Johdon ohjaus tietoturvallisuutta koskevissa asioissa.” Pääkohta sisältää kaksi alakohtaa, joille kullekin on standardissa määritelty hallintakeino. Hallintatavoitteeksi on asetettu johdon ohjausta ja tukea tietoturvallisuuden toteuttamiseen liiketoiminnallisten vaatimusten ja asiaankuuluvien lakien ja asetusten mukaisesti.



Kuvio 2. Esimerkki ISO/IEC 27001 -standardin Liite A viiteluettelon alarakenteesta

4.9 ISO/IEC 27002

ISO/IEC 27002 on tulkinta- ja toteutusohje, jota tulee käyttää ISO/IEC 27001 -vaatimusmäärittelyjen rinnalla. ISO/IEC 27002 -standardi on suunniteltu organisaatioille, jotka aikovat hankkia ISO/IEC 27001 -sertifikaatin tai kehittää omat tietoturvallisuuden hallintaohjeet. ISO/IEC 27002 -standardissa kuvataan kullekin hallintakeinolle sen kuvaus, toteuttamisohjeet sekä lisätiedot. Kuvio 3 havainnollistaa hallintatavoitteen A.5 tulkintaa yksityiskohtaisemmin, kuvaus on ISO/IEC 27002 -standardin vaatimusmäärittelyistä lainattu.

5.1.1 Tietoturvapolitiikat

Hallintakeino

Tietoturvallisuudelle olisi määriteltävä joukko johdon hyväksymiä politiikkoja, jotka julkaistaan ja joista tiedotetaan henkilökunnalle ja asiaankuuluville organisaation ulkopuolisille osapuolille.

Toteuttamisohjeet

Ylimmällä tasolla organisaation olisi määriteltävä "tietoturvapolitiikka", jonka johto hyväksyy ja jossa määritellään organisaation lähestymistapa tietoturvatavoitteiden hallintaan.

Tietoturvapolitiikkojen olisi katettava vaatimukset, jotka ovat peräisin

a) liiketoimintastrategiasta
b) asetuksista, laeista ja sopimuksista
c) nykyisestä ja ennustetusta tietoturvauhkaympäristöstä.

Tietoturvapolitiikan olisi sisällettävä myös lausumat, joissa

a) määritellään tietoturvallisuus, tietoturvatavoitteet ja -periaatteet, jotka ohjaavat kaikkea tietoturvallisuuteen liittyvää toimintaa
b) jaetaan määritellyille rooleille yleiset ja kohdistetut vastuut tietoturvallisuuden hallinnasta
c) määritellään prosessit, joilla käsitellään poikkeamia ja poikkeuksia.

Alemmalla tasolla tietoturvapolitiikkaa olisi tuettava asiakohtaisilla politiikoilla, jotka tukevat laajemmin tietoturvallisuuden hallintakeinojen toteuttamista ja jotka ovat yleensä rakenteeltaan sellaisia, että ne vastaavat organisaation tiettyjen kohderyhmien tarpeisiin tai kattavat tietyt aiheet.

Esimerkkejä tällaisista aiheista ovat esimerkiksi

a) pääsynhallinta (ks. kohta 9)
b) tietojen luokittelu (ja käsittely) (ks. kohta 8.2)

Kuvio 3. Esimerkki ISO/IEC 27001 -hallintakeinon tulkintaohjeesta (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2014, 14)

5 Sertifiointiprosessi

Sertifioinnin suorittaa aina jokin kolmas puolueeton osapuoli. Suomessa sertifiointeja suorittavat muun muassa Bureau Veritas Certification ja Inspecta Sertifiointi Oy. Suomen Standardoimisliitto (SFS) koordinoi suomalaisten osallistumista kansainväliseen ns. viralliseen standardisointiin. SFS:n työhön kuuluu standardien laadintaan osallistuminen, mutta ei itse sertifiointi. (Suomen Standardisoimisliitto, sähköpostihaastattelu 10.6.2016)

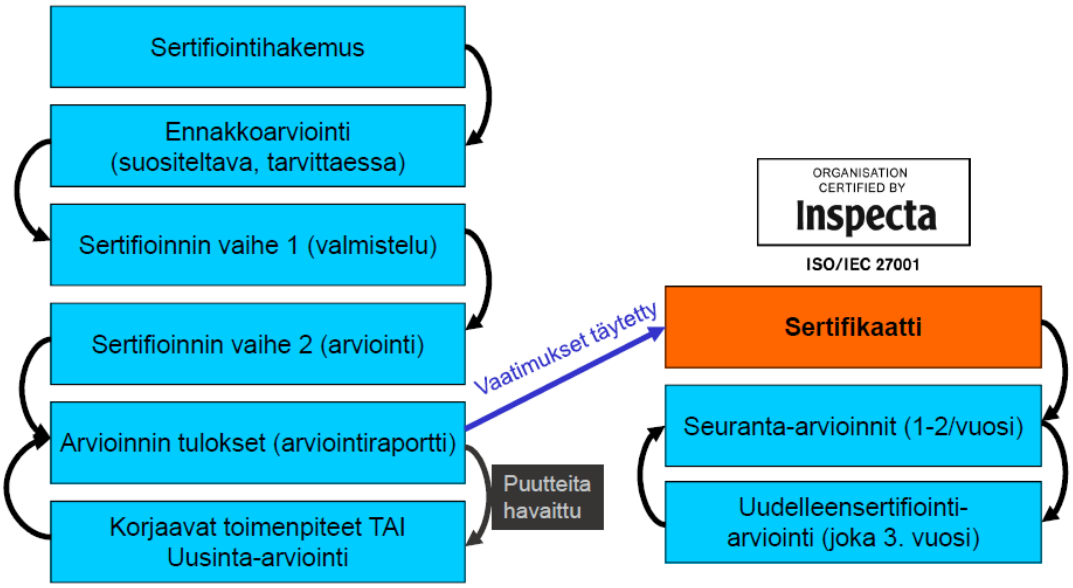
Sertifiointi on vaatimusten mukaisuuden osoittamista sertifikaatilla, todistuksella, tai merkillä. Sertifiointi voi kohdistua:

- Järjestelmiin
- Tuotteisiin
- Palveluihin
- Henkilöihin

Ennen kuin sertifikaatti myönnetään järjestelmälle, tuotteelle tai palvelulle tulee vaatimusten mukaisuus arvioida, testata tai tarkastaa (Suomen Standardisoimisliitto, usein kysyttyä.) Organisaatio voi halutessaan sertifioida ISO/IEC 27001 -sertifikaatilla vain tietyn osaston yrityksestä, organisaation toiminnon tai prosessin. Lisäksi ISO/IEC 27001 -sertifikaatilla voidaan toiseen maahan ulkoistetun prosessin laadun takeeksi kyseinen prosessi sertifioida.

ISO/IEC 27001 -sertifiointiprosessissa valtuutettu sertifioija käy läpi organisaation laatimat dokumentit standardin vaatimusmäärittelyiden mukaisesti. Sertifiointiyrityksen auditoija tarkastaa organisaation toimitilat ja tarkastaa, että vaaditut hallintakeinot ovat käytössä, kuten organisaatio ne on dokumentoinut. Sertifiointivaiheessa tärkeitä dokumentteja ovat muun muassa tietoturvallisuuden hallintajärjestelmän kattavuusdokumentti, riskianalyysit sekä Statement of Applicability, jossa luetellaan, mitkä hallintakeinot on toteutettu. (Kosutic 2016.)

Mikäli organisaatio ei täytä vaatimuksia, sertifikaattia ei myönnetä. Organisaation tulee tehdä tarvittavat korjaukset, jonka jälkeen voidaan hakea uudelleenarviointia sertifikaattiin. Sertifikaatti ISO/IEC 27001 on voimassa kolme vuotta kerrallaan. Vuosittain organisaatioon tehdään auditointitarkastuksia, joilla varmistetaan, että saavutettu vaatimusmäärittelyiden mukainen tietoturvallisuuden hallintajärjestelmän ylläpito ja parantaminen on saavutettu. (BSI Group Business Standards.) Kuvio 4 Inspecta Sertifiointi ISO/IEC 27001 -sertifikaatin eteneminen hakemuksesta sertifikaattiin.



Kuvio 4. Inspecta Sertifiointi, ISO/IEC 27001 -sertifiointiprosessi ja seuranta-arvioinnit

6 Tutkimusmenetelmä

Opinnäytetyön tavoitteena oli tuottaa kirjallinen raportti ISO/IEC 27001 -standardista ja kuvata sen asettamia odotuksia ja vaatimuksia organisaation tietoturvallisuudelle. Opinnäytetyö toteutettiin niin sanottuna toiminnallisena opinnäytetyönä. Toiminnallisen opinnäytetyön tarkoitus on muun muassa tuottaa kirjallinen raportti tietystä toimintatavasta ja näin ollen raportoinnissa painottuu käytännön osion toteuttamisen kuvaaminen ja reflektointi. Raporttiosiossa pohditaan käytännön osia peilaten niitä ammattikirjallisuuteen ja teoriataustaan.

Toiminnallisessa opinnäytetyössä tulee selvittää lähtökohdat sekä kartoittaa tilanne, tarkoitus ja tavoitteet. Opinnäytetyö rajattiin koskemaan vain yhtä standardia, johon yrityksen tietoturvallisuuden hallintajärjestelmä on mahdollista sertifioida. Edellytyksiä soveltaa raportin tuloksia yrityksen tehdessä päätöstä prosessiin lähtemisestä, haluttiin vahvistaa käyttämällä alan asiantuntijoita tutkimuksen kohteina. (Airaksinen 2009.)

Haastatteluaineistoihin perustuvissa tutkimuksissa tutkijan pyrkimyksenä on päätyä onnistuneisiin tulkintoihin, samaa haastattelutekstiä voidaan tulkita monin tavoin ja eri näkökulmista (Hirsjärvi & Hurme 2000, 151). Hirsjärvi ja Hurme toteavat (2000, 152), että haastattelututkimusta lukeva henkilö ei saa luettavakseen itse haastattelua, vaan hänen on luotettava tutkijan tulkintoihin. Tarkka selvitys johtopäätöksistä on kuitenkin yksi keinoista, joilla tulkintaa voidaan varmentaa.

6.1 Tutkimuksen validiteetti ja reliabiliteetti

Tutkimuksessa pyritään välttämään virheitä, mutta silti tulosten pätevyys ja luotettavuus vaihtelevat. Tutkimuksen reliaabeliuksella tarkoitetaan mittaustulosten toistettavuutta eli tutkimustulosten kykyä antaa ei-sattumanvaraisia tuloksia. Tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoituskin mitata, kutsutaan käsitteellä validius. Esimerkiksi kyselylomakkeella kysyttyihin kysymyksiin saatetaan vastata, mutta vastaajat ovat käsittäneet kysymykset monella eri tavalla. (Hirsjärvi, ym. 1997, 216.)

Reliaabelius voidaan todeta usealla eri tavalla, esimerkiksi jos kaksi arvioijaa päätyy samanlaiseen tulokseen, voidaan tulosta pitää reliaabelina. Laadullisen tutkimuksen luotettavuutta vahvistaa tutkijan tarkka selostus tutkimuksen toteuttamisesta, tarkkuus koskee kaikkia tutkimuksen vaiheita. Myös aineiston tuottamisen olosuhteet tulee selventää totuudenmukaisesti. Haastattelututkimuksissa kerrotaan olosuhteista ja mahdollisista häiriötekijöistä, myös haastattelijan oman näkemys ja arviointi on syytä tuoda esille. Lukijalle tulee kertoa, millä perusteella tutkija esittää tulkintoja ja mihin päätelmät perustuvat. Lukijaa auttaa, jos raportissa on käytetty suoria lainauksia haastatteluista tai kyselyistä. (Hirsjärvi, ym. 1997, 217-218.)

6.2 Raportin tulkinta

Tulkinnan ristiriidattomuus eli sisäinen validiteetti, voidaan soveltaa sellaisenaan, tutkijan pyrkiessä saamaan ilmiöstä kokonaisvaltaisen ja syvällisen kuvan. Todistelussa käytetään useita tietolähteitä uskottavuuden parantamiseksi ja tavoitteena on saada aukoton todisteluketju esitetylle ratkaisulle. Ensisijaisena tavoitteena on löytää aineiston avulla ratkaisu tutkimusongelmaan ja vastaukset ongelmasta johdettuihin tutkimuskysymyksiin. Tutkimuskysymyksiin on piilotettu se, mitä ajatellaan saatavaksi aineistosta vastaukseksi. Saatua aineistoa tutkittiin niin sanotulla induktio -mallilla, jossa lähdetään siitä, että ei ole mitään ennakko-oletuksia tai hypoteeseja, vaan katsotaan avoimin mielin, mitä aineistosta löytyy. (Kananen 2013, 107-119.)

Tarja Heikkilä (Heikkilä 2014) kuvaa luotettavaksi tutkimusraportiksi sellaista, jossa tutkija on arvioinut koko tutkimuksen luotettavuutta käytettävissä olevien tietojen perusteella. Tutkimuksen luotettavuuden kannalta on hyvin tärkeää, että otos on edustava ja kysymykset mittaavat oikeita asioita kattaen koko tutkimusongelman. Tutkimus ja sen tulokset ovat myös toistettavissa.

6.3 Tutkimuksen toteutus

Yhtenä tiedonkeruumenetelmänä käytettiin henkilöhaastattelua, jossa teemana oli ISO/IEC 27001 -tietoturvasertifikaatti ja sen myöntämisprosessi. Teemahaastattelu on sopiva metodi, kun tutkimusasetelmaa ei ole tarkoin määrätty, vaan sitä saatetaan tarkentaa hankkeen edetessä. Teemahaastattelu on keskustelua, jolle on päätetty jo etukäteen tarkoitus ja tutkija esittää pääasiassa avoimia kysymyksiä (Rautio, P 2016). Inspecta Sertifiointi Oy:n pääarvioija Jyrki Lahnalahti kertoo sertifiointiprosessista ja tuo esille niitä käytännön seikkoja, joihin auditoinneilla pyritään ja mistä sertifikaatti toimii todistuksena. Inspecta Sertifiointi suorittaa sertifiointeja muun muassa myös ISO 9000 laatujärjestelmä sekä ISO/IEC 20000-1 it-palvelunhallintajärjestelmistä, jotka monellakin tapaa tukevat ISO/IEC 270001 tietoturvasertifikaattia muodostaen moninaisen kokonaisuuden.

Jyrki Lahnalahden haastattelu toteutettiin avoimena eli niin sanottuna puolistrukturoituna, koska haastattelu oli aihepiiriltään rajattu ja toteutettiin henkilöhaastatteluna. Kuten Hirsjärvi & Hurme (2000, 48) tarkentavat, teemahaastattelusta puuttuu strukturoidulle lomakehaastattelulle luonteenomainen kysymysten tarkka muoto ja järjestys, mutta se ei ole täysin vapaa, kuten syvähaastattelu. Henkilöhaastattelun ja sähköpostikyselyn kysymykset ja teema muodostuivat tilaajayrityksen tietohallintopäällikön haastattelusta sertifikaattiin sitoutumisen haasteista sekä opinnäytetyön teorian pohjalta.

Jyrki Lahnalahden henkilöhaastattelun kysymykset poikkesivat ISO/IEC 27001 -sertifikaatilla sertifioitujen yritysten sähköpostikyselystä, vaikka teema olikin sama. Siinä missä sertifioijalta haettiin kokemuksia itse sertifiointiprosessin läpikäymiseen arvioijan näkökulmasta, pyrittiin yrityksiltä saamaan toisenlainen näkökulma. Prosessiin lähtevät yritykset joutuvat punnitsemaan resurssien sitomista pitkäjänteisiin projekteihin ja niistä saatavaa taloudellista hyötyä. Prosessiin lähteneet yritykset olivat kuitenkin vastuussa myös tavanomaisesta päivittäistoiminnastaan, eivätkä voineet kohdentaa kaikkia resursseja dokumenttien laatimiseen tai tulevaan auditointiin.

ISO/IEC 27001 -sertifikaatin saaneiden kyselytutkimus päätettiin suorittaa sähköpostitse, sillä kohderyhmä oli etukäteen määritelty ja rajallinen. Kuten Pertti Suhonen (2006, 30) kertoo mielipidetutkimuksista, ”otoksen suuruudella ja edustavuudella tavoitellaan tulosten tilastollista yleistävyyttä kohteena olevaan perusjoukkoon”. Kysymysten tehtävä on antaa tietohallinnosta vastaavien henkilöiden henkilökohtainen mielipide ISO/IEC 27001 -sertifikaatin prosessista, siihen sitoutumisesta, ajan ja resurssien vaatimuksista sekä hyödyistä yrityksen imagolle ja asiakashankinnoille.

Sampsa Hyysalo kirjassaan Käyttäjätieto (2006, 121) käy läpi haastatteluissa käytettäviä rakenteita, jotka otettiin huomioon kysymyksiä laadittaessa. Kysymykset eivät olleet johdattelevia ja kysymykset kohdistettiin henkilön kokemuksiin, ei päättelyihin tai oletuksiin. Kysymykset laadittiin koskemaan vain tietoturvallisuuden kehittämiseen liittyviä sertifikaatteja eikä aiheesta poikettu.

Erityisesti kyllä-ei tai joko-tai muotoiset kysymykset ovat petollisia, koska vastaaja on pakotettu mustavalkoistamaan kantaansa, joka voisi olla monivivahteisempi tai sijaita paljon ääripäitä keskemmällä (Hyysalo, 122). Vastausohjeiden mukaisesti vastaukset olivat ytimekkäitä ja henkilökohtaisia, eikä vastaajista kukaan ryhtynyt pohtimaan asiaa kysymyksen ulkopuolelta. Sähköpostikyselyssä ja henkilöhaastattelussa käytetty teema sekä kysymykset noudattivat samaa aihetta, vaikkakin kysymysten asettelu oli vastakkain, jotta tulokset olisivat vertailukelpoisia ja vastaukset olisivat keskenään verrattavia antaen näkemyksiä molemmin puolin prosessia.

Kohderyhmänä sähköpostikyselyssä oli yritysten tietohallinnosta vastaavat henkilöt, joiden vastuualueella on ISO/IEC 27001 -sertifikaatti ja sen auditoinnit. Kysely lähetettiin viidelletoista yritykselle, joista kahdeksan vastasi siihen. Osa ISO/IEC 27001 -sertifikaatin saaneista yrityksistä jätettiin haastattelun ulkopuolelle toimialan takia, kuten esimerkiksi datakeskukset. Sähköpostihaastatteluun vastanneista yrityksistä yhdellä oli ISO/IEC 27001 -tietoturvasertifikaatin lisäksi myös ISO 9000 laatujärjestelmän sertifikaatti sekä ISO/IEC 20000-1 it-palvelunhallintajärjestelmä -sertifikaatti.

Sähköpostikyselyssä kysymykset olivat yksiselitteisiä, eivätkä johdatelleet. Kysymykset muodostuivat väittämistä ISO/IEC 27001 -sertifikaattiin liittyen, sen hankinnasta, aikataulutuksesta ja hyödyistä. Vastaaja saattoi lisätä omia mielipiteitään tai näkemyksiä tilanteesta halutessaan. Kaikki kyselyyn vastanneet täydensivät vastauksiaan tarkentavilla käytännön esimerkeillä tai henkilökohtaisilla näkemyksillä. Näin voitiin varmistaa tulosten vertailukelpoisuus toisiinsa, ja kuten Hirsjärvi ja Hurme (2000, 169) kirjoittavat, analysoida tuloksia sanallisessa muodossa, jolloin teksti voi olla tutkijan kuvausta tutkittavasta aiheesta.

6.4 ISO/IEC 27001 -sertifioitujen yritysten sähköpostikysely

Sähköpostikysely suoritettiin valikoidusti sähköpostitse Suomessa toimiville yrityksille, joilla on ISO/IEC 27001 -sertifikaatti ollut jo useamman vuoden. Yritykset valikoituivat Inspecta Sertifiointi Oy:n sertifioitujen yritysten tietokannasta. Yritykset toimivat eri aloilla, kuten it-palveluiden myynnissä tai joiden liiketoimet nojaavat vahvasti tietotekniikkaan.

It-yritysten sähköpostikyselyssä käytettiin kaikille samoja vapaamuotoisia kysymyksiä, noudattaen puolistrukturoitua teemakyselyä. Teemakyselyssä pyrittiin mahdollisimman luonnollisiin mielipiteisiin ISO/IEC 27001 -sertifioinnin prosessista sekä sertifikaatin hyödyistä. Kysymykset rakennettiin siten, että niillä rajattiin aihealue. Yritysten nimet ja niiden edustajien tiedot jätettiin sähköpostihaastatteluiden tulosten käsittelyssä pois, jotta myös ongelmat ja ristiriidat voitaisiin tuoda rohkeammin esille.

Yrityksille esitetyt kysymykset:

- Edistikö ISO/IEC 27001 -sertifikaatti yrityksenne tietoturvan jatkuvaan kehittämiseen sitoutumista siinä mittakaavassa kuin olitte suunnitelleet?
- Mainostatteko ISO/IEC 27001 -sertifikaattia asiakkaillenne kilpailutusten yhteydessä?
- Opinnäytetyöni tilaaja ei toimi It-palveluiden myyjänä, vaan käyttää niitä osana palveluitaan. Koetteko, että sertifikaatista olisi etua asiakaskilpailutuksissa?
- Koetteko ISO/IEC 27001 -sertifikaatin kohottavan yrityksen imagoa?
- Koetteko ISO/IEC 27001 -sertifikaatin antavan kuvan tietoturvan kehittämiseen sitoutuneesta yrityksestä?
- Hakiessanne ISO/IEC 27001 -sertifikaattia, koitteko sertifiointiin suunnitellun ajan ja resurssit riittäviksi?
- Onko sertifikaatin uusiminen vuosittain koettu mielekkääksi tavoitteeksi tietoturvallisuuden laadun pitämiseksi korkealla?
- Vastasiko ISO/IEC 20000-1 it-palvelunhallintajärjestelmän standardi odotuksia? (kysymys esitettiin vain yritykselle, jolle oli myönnetty ISO/IEC 20000-1 -sertifikaatti)

Kyselyyn vastanneet yritykset yleisesti ottaen kokivat, että ISO/IEC 27001 -tietoturvastandardi edisti tietoturvan jatkuvaa kehittämistä, jopa ehkä enemmän kuin mitä oltiin kuviteltu. Standardin suureksi eduksi koettiin, että standardi asettaa yhteiset linjaukset ja tavoitteet tuottamaan laadukasta ja turvallista palvelua asiakkaille. Useassa vastauksessa oltiin tyytyväisiä toiminnan tehostumiseen, sillä toimintoja ohjattiin yhden standardin vaatimuksilla. Kerran luodut ohjeet ja dokumentaatiot olivat helppo pitää ajan tasalla, eikä hyväksi havaittuja toimintatapoja tarvinnut muuttaa.

Yritykset kokivat, että hyöty yrityksen imagolle jo yksinään riitti perusteluksi sertifikaatin hankkimisille ja sen tietoturvan jatkuvan kehittämiseen sitoutumiselle. Kaikissa haastatelluissa yrityksissä yksimielisesti todettiin, että sertifikaatista oli korvaamatonta etua kilpailutuksissa ja se toimi luontevana osana palveluntarjontaa ja se nostettiin aina esille, kun mahdollista, tai se oli luontevaa. Useampikin kyselyyn vastannut yritys kertoi, että tarjouskilpailuissa tuovat ISO/IEC 27001 -tietoturvasertifikaatin esille todisteena asiakkaille, että yritys turvaa heidän tietotekniset ratkaisunsa ja tukee keskeytyksetöntä liiketoimintaa. ISO/IEC 27001 tietoturvallisuuden hallinnan sertifikaattia ei mielletty vain puhtaasti it-yrityksille, vaan sen hyöty nähtiin kaikissa organisaatioissa koosta tai alasta riippumatta. Sertifikaatti antaa sidosryhmille vahvan signaalin siitä, että yrityksen johto on päämäärätietoista ja sitoutunutta.

Eräs kyselyyn vastannut edustaja totesi, että prosessi vaati panostusta, mutta valtaosa vaadituista toiminnoista oli syytä tehdä joka tapauksessa. Myös työkuorma koettiin taakkana, joka kuitenkin kontrollien pikkuhiljaa mukautuessa osaksi perusprosesseja helpottui. Eräs ISO/IEC 27001 -sertifioitu yritys koki, että mitään ei ansaita ilmaiseksi, vaan standardin ylläpito vaatii jatkuvaa kehitystä ja sitoutumista koko organisaatiolta. Kyselyyn vastanneet yritykset eivät kokeneet rahallista kustannusta kovinkaan suureksi saatuun hyötyyn nähden. Täsmällisisiä kustannuksia oli kyselyyn vastanneen yrityksen mielestä vaikea laskea, sillä työntekijät dokumentoivat toimintojaan ja suorittivat riskikartoitusta päivittäisen työnsä ohella. Sertifiointiprosessin hyötyinä koettiin, että yrityksen tietoturvallisuus kartoitettiin perusteellisesti ja riskeille alttiit toiminnot saatiin joko poistettua kokonaan tai niiden vaikuttavuutta vähennettyä merkittävästi.

Kyselyyn vastanneet yritykset kokivat osanneensa mitoittaa prosessiin sidottavat resurssit. Sertifiointiprosessin alussa suoritettu esiarviointi auttoi suunnittelussa sekä vaadittavien työntekijöiden resursoinnissa. Auditoinneista todettiin, että ne tuovat hyvin esille ulkopuolisen silmin asioita, joita ei välttämättä muuten olisi osattu huomioida ja mitkä edistivät toimintaa sekä lyhyellä, että pitkällä aikavälillä. Vuosittaiset tarkastukset koettiin pitävän tietoturvallisuuden ja riskienhallinnan tason korkealla. Eräs kyselyyn vastannut yrityksen edustaja totesi-

kin, että sertifikaatin vaatimukset voi toteuttaa vain auditointeja varten, tai toteuttaa ne yritystä ja sen asiakkaita varten, tehokkaasti, joustavasti ja järkevästi, jälkimmäisestä on yritykselle suurempi hyöty. Kyselyyn vastannut yritys koki, että auditoinnit ovat ennen kaikkea yrityksen ja organisaation johdon työkalu. Auditoinnissa selviää tietoturvallisuuden hallintajärjestelmän tila ulkopuolisen ammattilaisen toimesta. Auditoijat tuovat oman kokemuksensa ja tukensa johdon käyttöön korjaavien toimenpiteiden ja kehitysehdotusten muodossa.

Eräs tietohallinnosta vastaava työntekijä koki, että ISO/IEC 27001 -tietoturvastandardi turvallisuuden hallintajärjestelmänä ja ISO/IEC 20000-1 it-palvelunhallintajärjestelmä täydensivät kokonaisvaltaisemmin turvallisuuden kontrollien toteuttamisessa ja ohjenuorana kuin se olisi yksinään kyennyt toteuttamaan. Sama henkilö jatkoi, että ISO/IEC 27001 -standardi on sitouttanut, etenkin uusimman version myötä, myös ylimmän johdon edustajat turvallisuussuunnitteluun ja tavoitteellisuuteen, joka näkyy laajasti eri toiminnan osa-alueilla. Sähköpostikyselyissä ei tullut esille negatiivisia asioita sertifikaatista, vaikka itse prosessi alkuun saattoikin olla työläs. Kaikissa yrityksissä oltiin tyytyväisiä päätöksestä sitoutua sertifikaattiin ja tietoturvan jatkuvaan kehittämiseen.

6.5 Henkilöhaastattelu Inspecta Sertifiointi Oy:n pääarvioija Jyrki Lahnalahti

Inspecta Sertifiointi Oy:n pääarvioija Jyrki Lahnalahti kertoo, että yhteydenottoja yrityksiltä ISO/IEC 27001 -sertifikaattiin tulee viikoittain, yhteydenotoista noin 90% sitoutuu sertifikaatin hankintaan. Vain muutama yritys vuosittain jättää prosessin kesken, eivätkä saa sertifikaattia. Syitä keskeyttämiseen on monia, esimerkiksi yritysjärjestelyt tai toiminnan lopettaminen.

Lahnalahti kertoi, että sertifikaattiin johtava prosessi vie aikaa ja vaatii sitoutumista yrityksen johdolta. Ajallista kestoa on mahdoton sanoa, sillä se riippuu yrityksen koosta, kuin myös organisaation sen hetkisestä tietoturvan tasosta sekä ISO/IEC 27001 -vaatimuskokoelman kokonaisvaltaisesta ymmärtämisestä. Sertifiointiprosessin kesto on lyhyimmillään kolme kuukautta ja pisimmillään yhdeksän kuukautta. Sertifiointiprosessiin kuuluu esiarviointi, jossa sertifiointeja myöntävä yritys, kuten esimerkiksi Inspecta Oy, käy asiakkaan kanssa läpi vaatimuskokoelman sisältöä. Esiarvioinnin ansiosta yrityksissä on varsinaisten auditointien alkaessa kyetty vastata vaatimuksiin erittäin kattavasti, eikä korjattavaa välttämättä ole ollut lainkaan. Jyrki Lahnalahti kertoi, että suurimmat yllätykset yrityksille prosessin aikana on ollut riskien- ja kokonaisuuden hallinta, koska sertifikaatissa ei ole kyse vain tietohallinnosta tai tietotekniikasta vaan yhdenmukaisesta kokonaisuudesta. Lahnalahti kertoi, että ajoittain myös puutteiden korjaamisessa tuli yllätyksiä.

Yleisesti ottaen, pahoja puutteita ei ole juuri koskaan havaittu sertifioitavissa yrityksissä auditointien aikana ja useampikin yritys oli saanut sertifikaatin ilman huomautettavaa. Sertifi-

ointiprosessi käytännössä tarkoittaa, että sertifioijat käyvät asiakasyrityksen tiloissa tarkastamassa laaditut dokumentit ja haastattelevat valikoituja työntekijöitä varmistaen, että laaditut politiikat on myös onnistuneesti jalkautettu yrityksessä. Sertifikaatissa ja sen myöntämisessä kyse on pääasiassa siitä, että yritysten johdon pitää tietää riskimaailmasta ja puuttua niihin sekä kyetä jatkuvuuden hallintaan, jatkuvaa testausta unohtamatta. Vaatimuskokoelma auttaa yrityksiä tunnistamaan riskit ja miten niihin tulee puuttua. Siksi on tärkeää, että yritykset luovat jatkuvuus suunnitelman.

Lahnalahti kertoo, että kokemuksensa mukaan varsinainen rahallinen säästö tulee, kun prosessi on mietitty loppuun. Hankalinta on, jos koskaan ei ole tapahtunut mitään poikkeavaa, joka vaikuttaisi liiketoimintaan tai jatkuvuuteen. Joka vuosi suoritetaan suppeampi auditointitarkastus, joka ajallisesti vie noin kolmasosan alkuperäisestä sertifikaatin hankkimiseen menneestä ajasta, itse sertifikaatti uusitaan kolmen vuoden välein, joka ajallisesti vie noin kaksi kolmasosaa alkuperäisestä myöntämiseen menneestä ajasta. Aikaa on todellisesti vaikea arvioida, mikäli organisaation koko tai yrityksen tietoturvapolitiikkaa ajava johto on muuttunut.

Jyrki Lahnalahti kuvailee tietoturvanhallintajärjestelmän johtavan yrityksen tietoturvaa, mutta työntekijöiden tulee tietää käytännöt, jotka heidän tulee osata. Auditoinneissa haastatellaan työntekijöitä ja pyritään selvittämään yrityksen sisäisen viestittämisen onnistumista, käytäntöjen onnistunutta jalkauttamista. Suurimpia hyötyjä sertifikaatista on saavutettu sillä, että se vähentää, tai jopa poistaa kokonaan, asiakkaiden tarpeen yritysten auditoinneille. Sertifikaatti toimii todisteena hyvästä työstä, eikä yritysten tarvitse näin ollen tarvitse todistella omien menetelmien luotettavuutta tai järjestää omien tilojen, tai toimintatapojen auditointitilaisuuksia asiakkailleen tai yhteistyökumppaneille.

Lahnalahti toteaa, että sertifikaatti maksaa yritykselle sen, mitä yrityksessä joudutaan sisäisesti korjaamaan toimintaa. Jyrki Lahnalahti kertoo, että ISO/IEC 27001 -tietoturvastandardi on yksi standardi muiden joukossa, jonka voi hyvin yhdistää muihin standardeihin. ISO/IEC 27001 on hieman raskaampi, kuin esimerkiksi ISO 90001 laadunhallintastandardi, joten on suositeltavaa siirtyä tietoturvastandardista laadunhallintastandardiin, jolloin prosessi ja vaatimuskokoelmien tavoitteet ovat yrityksille tuttuja.

Jyrki Lahnalahti tähdentää, että julkisen hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaava johtoryhmä VAHTI, pyrkii tieto- ja kyberturvallisuuden kehittämiseen parantamalla valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. VAHTIn toiminnalla parannetaan valtion tietoturvallisuutta ja työn vaikuttavuus on nähtävissä hallinnon ohella myös yrityksissä ja kansainvälisesti. Jyrki Lahnalahti tähdentää, että yritysten tietoturva ja sen kehittäminen ovat tehokkaampaa, kun

tietohallinnosta vastaavat henkilöt verkostoituvat ja pysyvät ajan hermoilla jakaen tietoa uusista uhista ja selviytymisen mekanismeista.

7 Yhteenveto ja johtopäätökset

Tietoturvallisuuden hallintajärjestelmät ovat organisaation laatu- ja prosessiviitekehyksiä, jotka kattavat muun muassa tietoturvallisuuden organisoinnin, suunnittelun, tietoturvapolitiikat, vastuut, menettelytavat sekä resursoinnin. Tämän opinnäytetyön tarkoituksena oli selvittää ISO/IEC 27001 -tietoturvallisuusstandardin hankintaa, etuja yrityksen tietoturvallisuuden kehittämiselle sekä siihen sidottavien resurssien määrää. Yritysten tietoturvallisuutta voi kehittää ja ohjata useiden eri tietoturvaoppaiden ja standardien avulla. ISO/IEC 27001 -tietoturvallisuusstandardi valikoitui opinnäytetyön aiheeksi sen ollessa ainoa, jolle on saatavissa sertifikaatti osoituksena vaatimukset täyttämästä tietoturvan hallintajärjestelmästä. Yleisesti voidaan todeta, että ISO/IEC 27001 -standardin avulla kaiken kokoiset ja tyyppiset organisaatiot voivat varmistaa tietoturvallisuuden hallittavuuden sekä turvallisen tiedon vaihdon kaikkien sidosryhmien välillä. Standardi takaa, että yritys on sitoutunut jatkuvaan tietoturvallisuuden korkeiden vaatimusten ylläpitoon ja kehittämiseen.

Teoreettisen viitekehyksen tueksi opinnäytetyötä varten suoritettiin henkilöhaastattelu Inspecta Sertifiointi Oy:n pääarvioija Jyrki Lahnalahdelle sekä sähköpostikysely yrityksille, joilla on jo ISO/IEC 27001 -tietoturvallisuusstandardi myönnetty. Vastausten tulkintaa helpottaakseni, on haastatteluiden tulkinnassa käytetty suoria lainauksia ISO/IEC 27001 -sertifioitujen yritysten vastuuhenkilöiltä. Kyselyissä ja vastauksissa ei havaittu ristiriitaisuuksia.

Tutkimustulosten luotettavuutta arvioidessa tulee arvioida mitä tutkimuksella mitattiin ja tehtiinkö se tarpeeksi kattavasti ja tehokkaasti. Kuten Hirsjärvi ja ym. (1997, 209) toteavat, kerätyn aineiston tulkinta, analyysi ja johtopäätösten teko ovat tutkimuksen ydinasia. Tutkimus katsotaan olevan validi, koska tutkimusta tarkastellaan kokonaisuudessaan kriittisesti ja tutkimusstrategia valittiin tutkittavan kohteen mukaisesti. Valitut kohteet edustivat alan ammattilaisia, joiden kanssa verkostoituminen tietoturvallisuuden eri hallintamenetelmiä kehittäessä oli luonnollista.

Haastattelututkimuksen katsotaan olevan luotettava, sillä haastattelutilanteessa ei ollut häiriöitä ja kysymykset esitettiin siten, että kysymys ei ole tulkinnanvarainen. Haastattelutilanne on tarvittaessa toistettavissa samoissa olosuhteissa Inspecta Sertifiointi Oy:n toimitiloissa. Vastaukset noudattivat tiettyä kaavaa ja haastateltavalla oli vastaustensa perusteena luotettavaa virallista dokumentaatiota sertifikaatin vaatimuksista sekä tilastoja suoritetuista sertifioinneista. Sähköpostikyselyn katsotaan olevan luotettava, sillä sähköpostikyselyn vastauksissa ei ollut epätarkkoja viittauksia, eivätkä vastaukset olleet epätarkkoja tai pohjautuneet arveluihin. Kysymykset laadittiin valitun teeman mukaisiksi ja vastausohjeet olivat selkeät.

Saadut tulokset eivät johtuneet sattumasta ja mikäli kyselytutkimus toteutettaisiin uudestaan olisi saadut vastaukset yhtenevät. Sähköpostikysely voidaan tarvittaessa toistaa samoilla kysymyksillä ja voidaan olettaa, että vastaukset noudattaisivat samaa linjaa.

Opinnäytetyön tulokset vahvasti puoltavat prosessiin lähtemistä ja tietoturvallisuuden kehittämiseen sitoutumista ISO/IEC 27001 -tietoturvastandardin avulla. ISO/IEC 27001 -standardi on maailmanlaajuisesti tunnettu sertifikaatti todisteena yrityksen tietoturvan korkeasta tasosta sekä luotettavasta sitoutumisesta sen kehittämiseen. Siitäkin huolimatta, että sertifikaattia ei Suomessa vielä asiakkaat tuntisi tai osaisi vaatia, pidetään sitä muualla maailmassa erittäin luotettavana todisteena tietoturvan tasosta, ja se onkin usein vaatimuksena. Esimerkiksi vuonna 2014 Englannissa ISO/IEC 27001 -sertifioituja yrityksiä oli yli 2000 ja Saksassakin 640 yritystä oli sertifioitu. Kansainvälisissä suhteissa ISO/IEC 27001 -tietoturvasertifikaatilla on suuri painoarvo, joka saattaakin olla juuri se mikä ratkaisee, kenen palveluihin luotetaan ja sitoudutaan.

Lähteet

Kirjallisuus

Hirsjärvi, S. & Hurme, H. 2000. Tutkimushaastattelu. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 1997. Tutki ja kirjoita. Jyväskylä. Gummerus kirjapaino Oy.

Hyysalo, S. 2006. Käyttäjätieto ja käyttäjätutkimuksen menetelmät. Helsinki. Edita Prima Oy.

Kananen, J. 2013. Case-tutkimus opinnäytetyönä. Jyväskylä: Suomen Yliopistopaino Oy.

Suhonen, P. 2006. Mielipidetutkimukset ja yhteiskunta. Tampere. Tampereen Yliopistopaino.

Sähköiset lähteet

Airaksinen, T. 2009. Toiminnallisen opinnäytetyön kirjoittaminen verkkomateriaali. Viitattu 9.8.2016
http://www.slideshare.net/TiinaMarjatta/toiminnallinen-opinnytety-tekstin

BSI Group Business Standards. 2016. Certification to ISO/IEC 27001 Information Security Management, viitattu 3.8.2016.
http://www.bsigroup.com/en-GB/iso-27001-information-security/Certification-for-ISO-27001/

BSI Standards. 2016. Federal Office for Information Security. Viitattu 6.6.2016
https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Heikkilä, T. 2014. Tilastollinen tutkimus verkkomateriaali. Tutkimuksen luotettavuus. Viitattu 8.8.2016
http://www.tilastollinentutkimus.fi/7.RAPORTOINTI/TutkimuksenLuotettavuus.pdf

ISO. 2016. The ISO survey. Viitattu 29.7.2016
http://www.iso.org/iso/home/standards/certification/iso-survey.htm

IT Governance. 2016. The ISO/IEC 27000 family of information security standards.
http://www.itgovernance.co.uk/iso27000-family.aspx. Viitattu 5.5.2016

Kosutic, D. 2016. The importance of Statement of Applicability for ISO 27001. Viitattu 1.8.2016 http://www.advisera.com/27001academy/knowledgebase/the-importance-of-statement-of-applicability-for-iso-27001/

Puolustusministeriö. Katakri 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Viitattu 1.8.2016
http://www.defmin.fi/puolustushallinto/puolustushallinnon_turvallisuustoiminta/katakri_2015_-_tietoturvallisuuden_auditointityokalu_viranomaisille

Rautio, P. 2016. Taideteollinen korkeakoulu. Virtuaaliyliopisto. Teemahaastattelu. Viitattu 10.9.2016
http://www2.uiah.fi/virtu/materiaalit/tuotetiede/html_files/1364_empiir.html#teemahaas

SFS ISO/IEC 27002:2014. 2014. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Viitattu 10.7.2016

SFS ISO/IEC 27001:2013. 2013. Tietoturvallisuuden hallintajärjestelmän vaatimukset. Viitattu 10.7.2016

SFS Oppilaitosportaali. 5.10.2015. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät kalvosarja. Viitattu 14.8.2016
www.SFSedu.fi

Suomen Standardisoimisliitto SFS ry. Usein kysyttyä. 2016. Viitattu 1.8.2016
http://www.sfs.fi/usein_kysyttya

27001 Academy. 2016. What is ISO 27001? Viitattu 5.6.2016
http://advisera.com/27001academy/what-is-iso-27001/

Haastattelut

Lahnalahti, J. 5.8.2016. Pääarvioijan haastattelu. Inspecta Sertifiointi Oy. Helsinki.

Lamminaho, S. 10.6.2016. Viestintäassistentti. Suomen Standardisoimisliitto SFS. Opinnäytetyönä ISO/IEC 27001 tietoturvastandardi. Sähköposti Arto Saloselle.