Tuomas Iivanainen

ISO/IEC 27001 -TIETOTURVASERTIFIKAATIN KOKONAISKUSTANNUKSET

Liiketalouden koulutusohjelma

2019

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

ISO/IEC 27001- TIETOTURVASERTIFIKAATIN KOKONAISKUSTANNUKSET

Iivanainen, Tuomas
Satakunnan ammattikorkeakoulu
Liiketalouden koulutusohjelma
Syyskuu 2019
Sivumäärä: 41
Liitteitä: 0

Asiasanat: ISO/IEC 27001, tietoturvastandardi, tietoturvasertifikaatti, riskienhallinta, tietoturvallisuuden hallintajärjestelmä

Tässä opinnäytetyössä arvioitiin ISO/IEC 27001:2017 -tietoturvasertifikaatin hankinnasta syntyviä kokonaiskustannuksia ohjelmistoyritys Intrinsic Oy:ssä. Hankinnan kokonaiskustannuksien selvittäminen on tärkeä tieto ennen hankintaprosessiin ryhtymistä. Sertifikaattihankinnan kokonaiskustannukset muodostuvat yrityksen tietoturvallisuuden hallintajärjestelmän kehitystyöstä, ulkoisesta auditoijasta koituvista kustannuksista sekä sertifioidun tietoturvallisuuden hallintajärjestelmän ylläpidosta. Opinnäytetyön teoriaosuudessa käsiteltiin tietoturvahäiriöiden kustannuksia, riskienhallintaa sekä ISO 27001 -tietoturvastandardin vaatimuksia.

Opinnäytetyö on luonteeltaan kvalitatiivinen ja tutkimusmenetelmänä käytettiin tapaustutkimusta. Tutkimuksessa verrattiin kohdeyrityksen tietoturvallisuuden hallintajärjestelmää ISO 27001 -standardia vasten, jolloin saatiin selvitettyä tarvittavat tietoturvallisuuteen liittyvät kehitystyöt. Standardin vaatimuksien pohjalta voitiin myös arvioida sertifioidun tietoturvallisuuden hallintajärjestelmän ylläpitoon tarvittavat resurssit. Ulkoisesta auditoijasta koituvat kustannukset selvitettiin pyytämällä kustannusarvio sertifiointipalveluja tarjoavalta yritykseltä.

Sertifikaattihankinnan kokonaiskustannuksien arvioinnin avulla voidaan helpottaa yrityksen johdon päätöksentekoa varsinaiseen sertifiointiprosessiin ryhtymisestä. Tutkimuksen perusteella tietoturvasertifikaatin hankinta on raskas ja paljon resursseja vaativa prosessi, joka vaatii yritykseltä jatkuvaa sitoutumista tehokkaan tietoturvallisuuden ylläpitämiseen. Sertifioitu tietoturvallisuuden hallintajärjestelmä antaa kuitenkin organisaatiolle hyvät valmiudet tietoturvariskien torjuntaan sekä toteutuneista tietoturvahäiriöistä palautumiseen.

THE TOTAL COSTS OF ISO/IEC 27001 INFORMATION SECURITY CERTIFICATE

Iivanainen, Tuomas
Satakunnan ammattikorkeakoulu, Satakunta University of Applied Sciences
Degree Program in Business Administration
Septemper 2019
Number of pages: 41
Appendices: 0

Keywords: ISO/IEC 27001, information security standard, information security certificate, risk management, information security management system

---

This thesis evaluated the total costs of obtaining an ISO/IEC 27001:2017 information security certificate for software company Intrinsic Ltd. Estimating the total costs of acquisition is important information before proceeding to the acquisition process. The total costs of the certificate acquisition consist of development work of the company's information security management system, the cost of an external auditor and the cost of the maintenance of the certified information security management system. The theoretical part of the thesis addresses the costs of an information security incidents, risk management and the requirements of the ISO 27001 information security standard.

The character of the thesis is qualitative and a case study was used as a research method. In the research the information security management system of the target company was compared against the ISO 27001 -standard in which case the necessary actions related to the information security were clarified. On the basis of the standards requirements we were able to estimate the resources needed for maintaining a certified information security management system. The costs which incur from an external auditor were clarified by asking for the cost estimate from the company which offers certification services.

The evaluation of the total costs of the certificate acquisition can be used to ease the decision-making of the management of the company to embark on the actual certification process. On the basis of the research the acquisition process of information security certificate is difficult and requires many resources and constant commitment from the company to maintain efficient information security. However, the certified information security management system prepares organisation well for the prevention of information security risks and for the recovery from the information security incidents.

SISÄLLYS

1 JOHDANTO

Yritysten toimintaan lähes poikkeuksetta kuuluu erilaisten tietojärjestelmien sekä tiedon hyödyntäminen. Tiedon tulee olla asianmukaisesti säilytettynä ja käytettävissä. Hävitetyn tai varastetun tiedon seurauksena voi olla jopa yrityksen toiminnan päättyminen. Tietotekniikan nopea kehitys ja sen jatkuvasti laajempi hyödyntäminen on kasvattanut merkittävästi tietoturvauhkien määrää.

Tietoturvallisuus on saanut merkittävän roolin yritysten toiminnassa. Kehittyvän tekniikan, kasvaneiden tietoturvauhkien sekä myös sidosryhmien vaatimusten vuoksi, yritysten on ollut pakko kehittää omaa tietoturvallisuuttaan. ISO/IEC 27001:2017 -tietoturvasertifikaatin hankkiminen on tehokas tapa yrityksen tietoturvan varmistamiseen sekä kehittämiseen. Tietoturvastandardin vaatimukset sekä velvoittavat hallintakohteet ja niiden hallintakeinot suojaavat tehokkaasti yrityksen tietovarat ulkoisilta ja sisäisiltä uhilta sekä ohjaavat yritystä tietoturvan jatkuvaan parantamiseen. Tietoturvasertifikaatin hankinta on kuitenkin myös vaativa prosessi, joten tämän tutkimuksen tuloksena syntyvä arvio kohdeyrityksen tietoturvasertifikaattihankinnan kustannuksista osaltaan auttaa samantyyppisten yritysten päätöksentekoa sertfiointiprosessiin ryhtymisestä.

2 TYÖN TARKOITUS JA KÄYTETTÄVÄT MENETELMÄT

2.1 Tavoitteet

Opinnäytetyön tavoitteena on arvioida ISO/IEC 27001:2017 -tietoturvasertifikaatin hankinnasta kohdeyritykselle koituvat kokonaiskustannukset. Opinnäytetyössä arvioidaan kohdeyrityksen tietoturvajärjestelmään vaadittavat toimenpiteet ISO/IEC 27001:2017 -tietoturvastandardin vaatimuksiin vastaamiseksi ja näiden toimenpiteiden arvioidut kustannukset. Lisäksi arvioidaan ulkoisesta tietoturvasertifioijasta koituvat kustannukset sekä tietoturvajärjestelmän ylläpidosta koituvat kustannukset. Tietoturvasertifikaatin hankinnasta koituvien

kokonaiskustannuksien arviointi helpottaa lopullista päätöksentekoa tietoturvasertifikaatin hankintaprosessiin ryhtymisestä.

Tutkimus sisältää ISO/IEC 27001:2017 -tietoturvasertifikaatti hankinnasta koituvat arvioidut kokonaiskustannukset. Kokonaiskustannukset koostuvat yrityksen sisäisestä kehitystyöstä, sertifikaatin myöntäjästä koituvista kustannuksista sekä tietoturvallisuuden hallintajärjestelmän ylläpitokustannuksista. Lisäksi tutkimus sisältää yleisellä tasolla tietoturvajärjestelmään tehtävien tarvittavien toimenpiteiden kuvaukset.

Tutkimus ei sisällä yksityiskohtaisia tietoja tietoturvastandardin velvoittavista hallintavoitteista tai niiden hallintakeinoista eikä salassapidettäviä teknisen tietoturvallisuuden ja tarkkojen hallinnollisten tietoturvamenettelyjen toteuttamisen kuvausta.

2.2 Tutkimusmenetelmä

Laadullinen tutkimus on aina ihmisten maailman ilmiöiden tutkimusta sosiaalisessa ympäristössä, jossa tutkimus painottuu usein tulevaisuuteen. Laadullisen tutkimuksen avulla kehitetään, parannetaan tai uudistetaan tutkittavaa kohdetta. Laadullisessa tutkimuksessa aineisto analysoidaan ja analysointia tehdään tutkimusprosessin alusta saakka. (Pitkäranta 2014, 8-9.) ”Laadullisen tutkimuksen tehtävä on lisätä ymmärrystä, mahdollista erilaisia tulkintoja, antaa asioille merkityksiä ja tuottaa asioista mallinnuksia” (Pitkäranta 2014, 13).

Tapaustutkimuksessa on tavoitteena tutkitun tiedon tuottaminen kohteesta. Tapaustutkimus sopii hyvin lähestymistavaksi kehittämistyössä. Tällä lähestymistavalla halutaan ymmärtää syvällisesti jonkin organisaation tilannetta ja tarkoituksena ratkaista siellä ilmennyt ongelma tai tuottaa kehitysehdotuksia. Puhtaassa tapaustutkimuksessa ei käytännössä vielä viedä muutosta eteenpäin tai kehitetä mitään konkreettista vaan sen avulla luodaan ratkaisuehdotus tai kehitysideoita. Tapaustutkimuksessa kohdetta tutkitaan syvällisesti sen omassa ympäristössään. Tapauksen voi muodostaa koko yritys, yrityksen osasto, henkilöstö,

tuote- tai asiakasryhmä, järjestelmä tai vaikka yrityksen oma prosessi. Tapaustutkimuksessa käytetään usein monia erilaisia tiedonhankintamenetelmiä, jotta kohteesta saadaan syvällinen ja kokonaisvaltainen kuva. (Ojasalo, Moilanen & Ritalahti 2014, 37.)

Tämä opinnäytetyö on luonteeltaan kvalitatiivinen eli laadullinen ja tutkimusmenetelmänä käytettiin tapaustutkimusta. Tutkimuksen avulla on tarkoitus arvioida syntyviä kustannuksia yrityksen halutessa rakentaa kattava ISO 27001 -tietoturvastandardin mukainen tietoturvallisuuden hallintajärjestelmä. Tutkimuksen aikana ei ole tarkoituksena kehittää yrityksen tietoturvaa, vaan hankkia aiheesta oleellisia lisätietoja myöhempää käyttöä varten ja tähän tarkoitukseen tapaustutkimus on sopiva tutkimusmenetelmä. Lisäksi tutkittiin alaan liittyvää kirjallisuutta. Kirjallisuustutkimuksessa selvitettiin tietoturvahäiriöiden kustannuksia ja tietoturvastandardin vaatimuksia.

Tapaustutkimuksessa verrattiin Intrinsic Oy:n tietoturvajärjestelmää ISO/IEC 27001:2017 -tietoturvastandardia vasten ja selvitettiin tarvittavat toimenpiteet tietoturvasertifikaatin hankintaa varten. Tutkimukseen kerättiin tietoja tietoturvaan, riskienhallintaan ja investointeihin liittyvästä kirjallisuudesta. Tietoa haettiin lisäksi internetistä ja lehtijulkaisuista. Kohdeyrityksen tietoturvan arviointi oli tutkimuksen kannalta välttämätöntä. Arviointiin käytettiin aineistona yrityksen omia tietoturvaohjeistuksia ja muita dokumentteja. ISO/IEC 27001:2017 -tietoturvastandardia käytettiin laajalta osin tutkimusaineistona tietoturvavaatimusten selvittämiseksi. Kohdeyrityksellä ja sen henkilöstöllä on huomattavaa omakohtaista kokemusta sertifioinneista ja sertifiointiprosesseista. Tätä kokemusta hyödynnettiin varsinkin kohdeyrityksen tietoturvajärjestelmän kehitys- sekä ylläpitotehtävien selvittämiseen ja niistä syntyvien kustannuksien arviointiin. Lisäksi pyydettiin sertifiointeja suorittavalta yritykseltä kustannusarvio sertifikaatin hankintaan ja sen ylläpitoon liittyvistä kustannuksista.

3 TIETORISKIEN HALLINTA

3.1 Riskienhallinta

Riski merkitsee vaaratekijöitä, joille ihmiset ja yritykset ovat alttiina tietyllä hetkellä. Arkikielessä riski tarkoittaa aavistusta siitä, että jotain ikävää voi mahdollisesti sattua. Riskin luonteeseen kuuluu, että emme voi olla varmoja toivottujen ja ei-toivottujen tapahtumien sattumista. (Suominen 2003, 9-10.) Riskin toteutumisesta syntyvät menetykset voivat olla rahallisen arvon, ympäristöarvon, terveydellisen arvon tai yhteiskunnallisen arvon menetyksiä (Kuusela & Ollikainen 2009, 17).

Riskiä määriteltäessä on arvioitava riskin seuraamuksen haitallisuutta ja todennäköisyyttä. Riskit toteutuvat usein altistumisen seurauksena ja riskin hyväksyttävyys riippuu monista eri tekijöistä. (Kuusela & Ollikainen 2009, 17.)

Yritystoiminta sisältää aina riskejä toimialasta riippumatta. Tavoitteellinen sekä hyvin organisoitu riskienhallinta on tärkeä menestystekijä yritykselle. Sen tehokas toteuttaminen auttaa turvaamaan yrityksen toimintaa ja tulomuodostusta. Riskienhallinnan avulla saavutetaan myös kilpailuetuja ja imagohyötyjä. (Juvonen ym. 2014, 7.)

Riskienhallinta on organisaatioille toteutettu sisäinen prosessi, jota organisaatio hyödyntää toiminnassaan. Sen avulla tunnistetaan, hallitaan ja ennalta ehkäistään yritykseen kohdistuvia epäsuotuisia tapahtumia, jotka uhkaavat yrityksen toimintaa. Riskienhallinta on työtä, joka turvaa yrityksen toiminnan jatkuvuuden ja henkilöstön hyvinvoinnin. (Suomen riskienhallintayhdistyksen www-sivut 2019.)

Riskienhallinnan tulee kattaa koko yrityksen toiminta. Sen tehtäviin kuuluu tilanteiden arviointia, suunnittelua ja käytännön tekoja, jonka toteuttamiseen osallistuu ko. osa-alueen henkilöstön jäsen. Riskienhallinnalla pyritään, joko vaikuttamaan tapahtuman todennäköisyyteen tai seurauksien suuruuteen, sekä tunnistamaan, analysoimaan ja hyödyntämään potentiaalisia mahdollisuuksia. (Suomen riskienhallintayhdistyksen www-sivut 2019.)

Yritystoiminnan kehittäminen syntyy aina mahdollisuuksista, jotka voidaan jakaa liiketoiminnan kasvattamiseen ja kannattavuuden kehittämiseen. Liiketoiminnan kasvattaminen edellyttää liiketoimintaympäristön mahdollisuuksien ja niiden toteuttamisen esteiden tunnistamista. Kannattavuuden kehittäminen on mahdollista, kun on tunnistettu yrityksen sisäisiin prosesseihin liittyvät innovaatio-, asiakkuus- ja operatiivisen tason riskit. (Juvonen ym. 2014, 15).

3.2 Tietoturvallisuus ja tietoturva

Tietoturvallisuus koostuu tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta (Yksityisyydensuoja www-sivut 2019). Tiedon luottamuksellisuudella, eheydellä ja saatavuudella tarkoitetaan, että tieto on oikeata ja virheetöntä, tarvittaessa käytettävissä ja vain niiden saatavilla, joille se kuuluu (Korkiamäki ym. 2008, 69). Tietoturvalla tarkoitetaan tietoturvallisuuden varmistamista hallinnollisilla ja teknisillä toimilla (Traficomin www-sivut 2019). Tietoturvan hallinnollisia ja teknisiä toimia voivat olla esimerkiksi tietoturvapolitiikan luominen, varmuuskopiointimenettelyn ohjeistus ja virustorjuntaohjelmistojen hankinta.

Tiedon luottamuksellisuuden tavoitteena on pitää arkaluontoinen tieto suojassa sellaisilta tahoilta tai henkilöiltä, joilla ei ole siihen käyttöoikeutta. Esimerkiksi salasanat, tietojen salaaminen ja turvallinen tiedonhävitys ovat tärkeitä osa-alueita tiedon luottamuksellisuuden varmistamisessa. (Yksityisyydensuoja www-sivut 2019.)

Tiedon eheydellä tarkoitetaan, että tiedot eivät muutu tai tuhoudu hallitsemattomasti. Tiedon eheyden varmistamiseen liittyy myös kolme lisäominaisuutta – tiedon alkuperäisyys, koskemattomuus ja kiistämättömyys. (Rautiainen 2013.)

Tiedon saatavuuden tarkoituksena on taata, että asianmukaisilla henkilöillä on aina tarvittaessa pääsy tietoon (Yksityisyydensuoja www-sivut 2019). Saatavuudesta voidaan käyttää usein myös termiä käytettävyys (Rautiainen 2019).

Yrityksen toimintaympäristön muodostaa osaltaan yritystoimintaan liittyvä lainsäädäntö (Yritystulkki www-sivut 2019). ”Hyvä lainsäädäntö sekä kansallisella että EU-

tasolla parantaa yritysten toimintaedellytyksiä ja edistää taloudellista kasvua" (Elinkeinoelämän keskusliiton www-sivut 2019). Yritystoiminnan tietoturvaan liittyvää oleellista lainsäädäntöä ovat:

- Laki yhteistoiminnasta yrityksissä 334/2007
- Työsopimuslaki 55/2001
- Rikoslaki 39/1889
- General Data Protection Regulation (yleinen tietosuoja-asetus) 2016/679
- Tietosuojalaki 1050/2018

3.3 Tietoriskit

Yhteiskunnan, yritysten ja muiden organisaatioiden toiminnot ovat nykyisessä tietoyhteiskunnassamme voimakkaasti sidoksissa tieto- ja viestintätekniikan järjestelmien toimintaan. Tieto- ja viestintätekniikan hyödyntämisen mukana ovat tulleet tietoriskit. (Juvonen ym. 2014, 150.) Tietoriskit ovat tietoihin ja niiden käyttöön kohdistuvan tapahtuman uhka. Tilanne voidaan määritellä tietoriskiksi, kun tarvittava tieto tai tietojärjestelmä ei ole käytettävissä, tieto on valtuudettomasti muuttunut tai tieto on päässyt leviämään. (Suominen 2003, 79.) Tietoriskit johtuvat pääosin liiketoimintojen laajasta sidonnaisuudesta tietojenkäsittelyyn sekä uhista, jotka kohdistuvat tietojärjestelmiin mm. verkkohyökkäysten johdosta (Juvonen ym. 2014, 150). Tietoriskin toteutuminen aiheuttaa lähes aina menetyksiä (Suominen 2003, 79).

Viimeisten vuosikymmenien aikana teknologia on kehittynyt äärimmäisen nopeasti ja sama kehitys tulee jatkumaan. Tulevan vuosikymmenen aikana kaikki nykyisen käytössä olevat päätelaitteet ja useimmat palvelut tulevat korvautumaan uusilla tekniikoilla ja palveluilla. Toiminnan digitali- ja robotisaation myötä tarve käsitellä ja yhdistää tietoja automaattisemmin lisääntyy, mikä taas korostaa tietoturvallisuuden ja henkilötietojen käsittelyn merkitystä. (Järvinen & Rousku 2017, 43-44.)

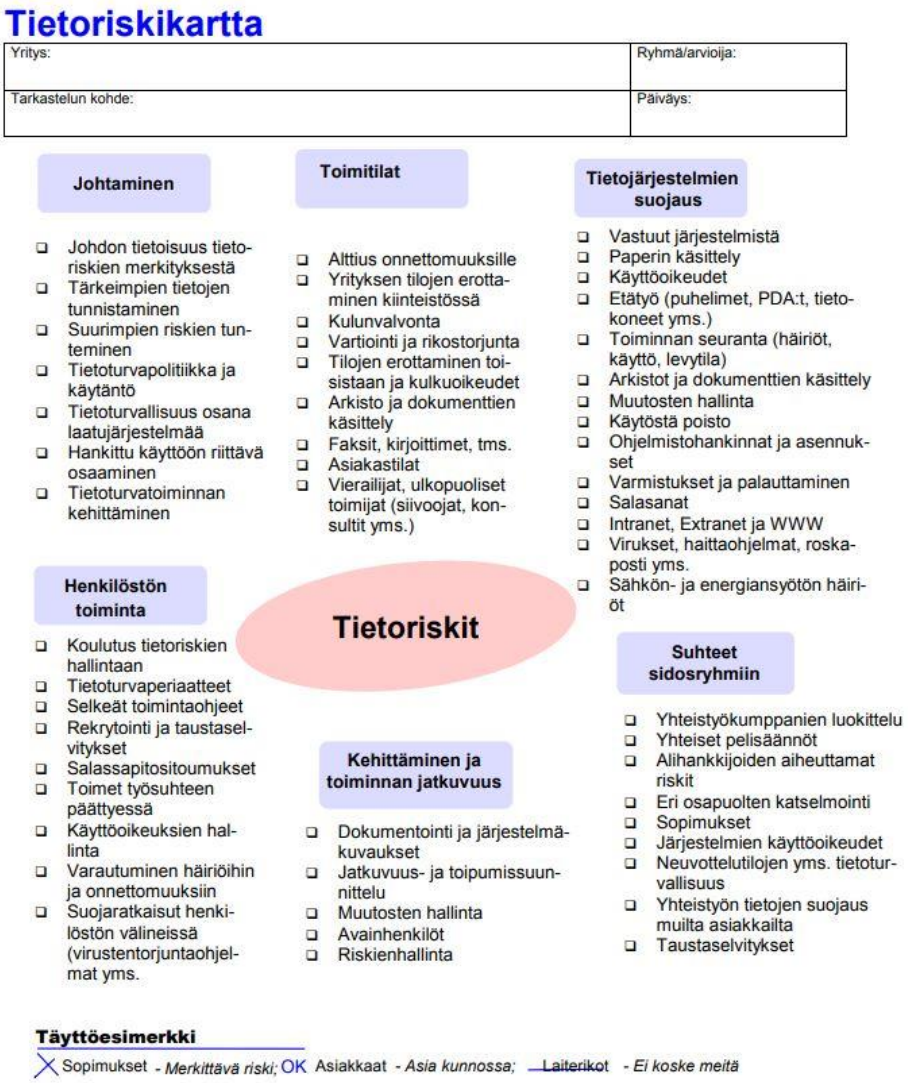
Riskin aiheuttaja voi olla ihminen, tekninen vika tai vaikka esimerkiksi vesivahinko. Vahingon aiheuttava teko voi olla tahaton tai tahallinen. Tahaton virhe on todennäköisempi uhka kuin ammattimainen hyökkäys, mutta molempiin tapahtumiin on varauduttava. Tietoriskejä voi aiheutua esimerkiksi seuraavanlaisista tapahtumista:

- Tietokone varastetaan
- Sähköposti lähetetään tai se ohjautuu väärälle vastaanottajalle
- Yrityksen asioista puhutaan kovaan ääneen julkisella paikalla
- Tietokoneen tunnistautumistiedot ovat kirjoitettuna lapulla työpisteellä
- Varmuuskopioinnin palautustoimintoja ei ole testattu
- Dokumenttien versionhallinta on puutteellinen
- Tietokoneeseen tarttuu virus
- Yrityksellä on vain yksi ihminen, joka tietää miten jokin tietty järjestelmä toimii

Tietoriskeihin tulee varautua, jotta voidaan varmistaa tietojen tietoturvallisuus, eli niiden luottamuksellisuus, eheys ja saatavuus. (Suominen 2003, 80.)

Normaalien palvelutuotannon häiriöiden lisäksi yrityksien toimintaa uhkaavat myös erilaiset henkilöt ja ryhmittymät, jotka yrittävät hyödyntää tieto- ja viestintätekniikan haavoittuvuuksia. Näiden ryhmien ja henkilöiden motivaationa on taloudellisen hyödyn saavuttaminen, salaisten tietojen hankinta tai vain halu aiheuttaa vahinkoa. (Järvinen & Rousku 2017, 44.)

Uhkien tunnistamista, riskien arviointia ja turvatoimien suunnittelua voidaan helpottaa riskien luokittelulla sekä loogisella jäsentelyllä. Tietoriskien ryhmittelyn voi tehdä monilla eri tavoilla, esimerkiksi vakuutusyhtiöissä tietoriskejä on ryhmitelty omaisuusriskeihin, keskeytysriskeihin, henkilöstöriskeihin, tietoverkkorikollisuuteen ja muihin rikosriskeihin, vastuu- ja sopimusriskeihin sekä kehittämisriskeihin, jotka koostuvat yhteensopimattomuuksista, virheistä ja laatuongelmista. (Juvonen ym. 2014, 152). Tietoriskien tunnistamisessa voidaan hyödyntää kuviossa 1 esitettyä tietoriskikarttaa.



Kuvio 1. Tietoriskikartta (Suomen riskienhallintayhdistyksen www-sivut 2019).

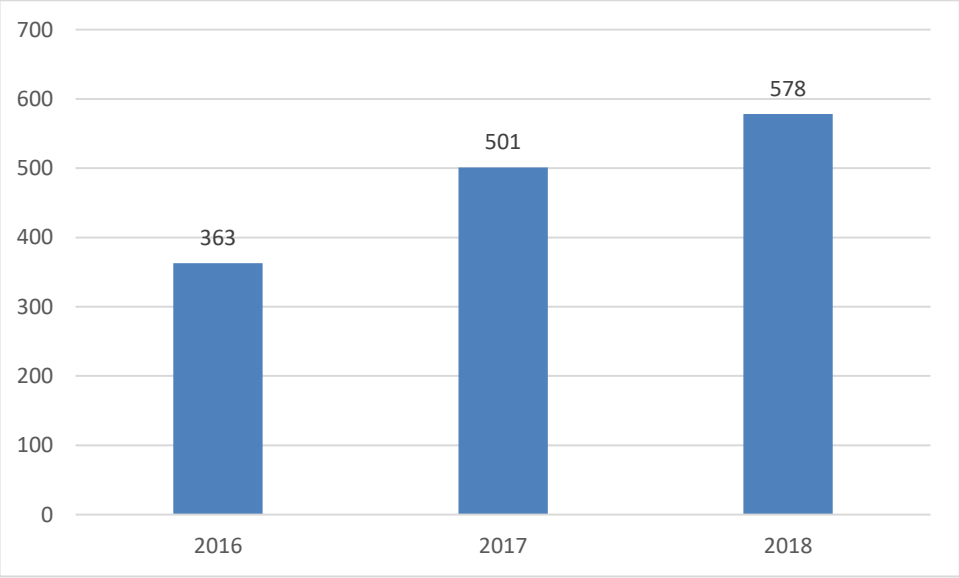
Tietoriskien hallinnan tulee kuulua yrityksen johdon normaaliin päätöksentekotoimintaan. Yrityksen johto vastaa yrityksen toiminnan sekä liiketoiminnan jatkuvuuden turvaamisesta ja valvonnan organisoinnista. Nämä edellä mainitut asiat kuuluvat omalta osaltaan tietoriskien hallintaan. Yrityksen johdon oleellinen tehtävä on määrittää yritykselle sopiva ja riittävä tietoturvataso. Sopivan tietoturvatason määrittäminen voi olla haasteellista, koska puutteellinen tietoturva voi johtaa kestämättömiin menetyksiin, ja taas toisaalta huipputasoinen tietoturva maksaa paljon eikä rahallakaan voi saada täydellistä tietoturvaa. Tietoriskejä hallitessa joudutaankin jatkuvasti tasapainoilemaan hyväksyttävän riskitason ja hyväksyttävien kustannusten välillä. (Suominen 2003, 81-82.)

Tieto on yksi yrityksen tärkeimmistä suojattavista kohteista, joten on tärkeää löytää yritykselle oikea tietoturvataso. Puutteellinen tiedon käsittely voi aiheuttaa haittaa yritykselle sekä sen asiakkaille ja yhteistyökumppaneille, mikä taas antaa etua kilpailijoille. Tietoriskien hallintaa voidaan siis pitää yrityksen kilpailutekijänä. (Suominen 2003, 82.)

3.4 Tietoturvahäiriöt

Tietoturvahäiriö tarkoittaa liiketoimintaa vaarantavaa epäsuotuista ja yllättävää tietoturvatapahtumaa, joka uhkaa yrityksen tietoturvallisuutta (ISO/IEC 27001:fi 2005, 12). Tietoturvahäiriö voi olla esimerkiksi ulkoisen tahon tietomurto tai vaikka työntekijästä johtuva luottamuksellisten tietojen päätyminen vääriin käsiin.

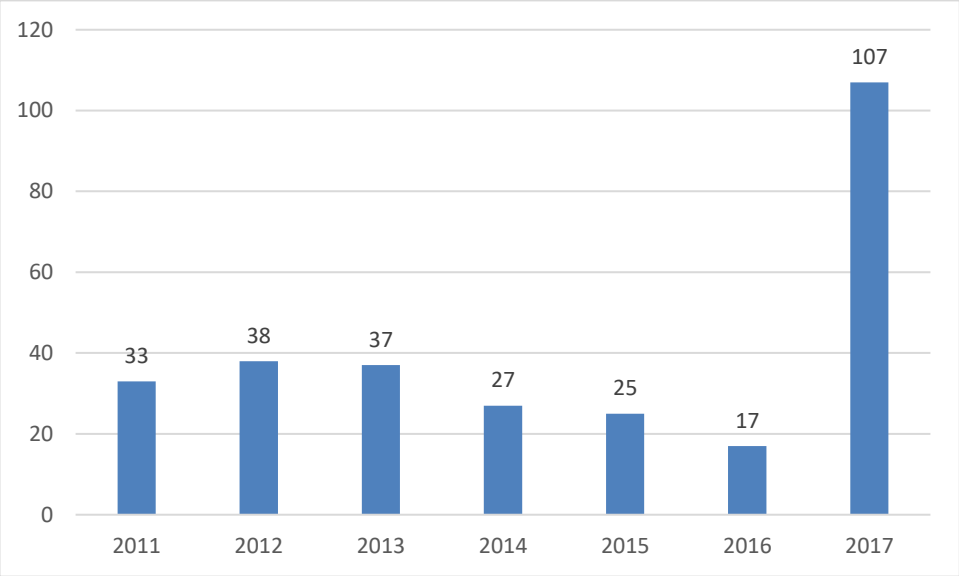
Kuviosta 2 voidaan nähdä, että tietoturvahäiriön kustannus vuonna 2018 oli keskimäärin 578 dollaria yhtä tapahtumaa kohden. Yksittäisen tietoturvahäiriön kustannukset ovat kasvaneet noin 58 % vuodesta 2016, jolloin kustannus yhtä tietoturvahäiriötä kohden oli 363 dollaria (IDG www-sivut 2019).



Kuvio 2. Yksittäisen tietoturvahäiriön keskimääräinen kustannus dollari määräisenä. (Bradgon 2017).

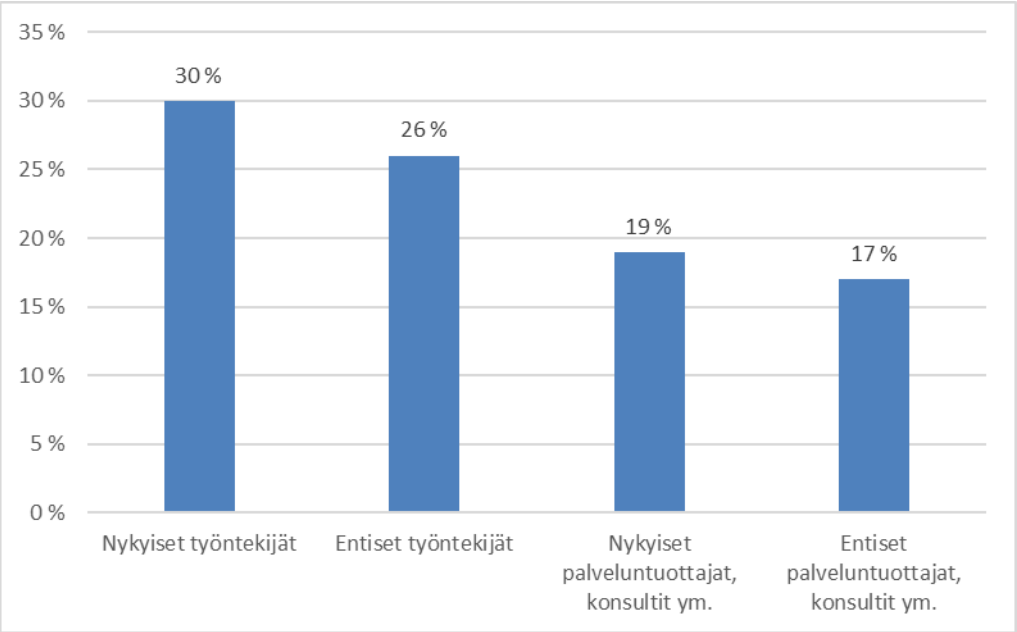
Kuviosta 3 voidaan todeta, että merkittävien tietoturvaloukkausten- ja uhkien määrä on lisääntynyt selvästi Suomessa. Vuonna 2016 vakavia tietoturvahäiriöitä ilmoitettiin 17 kappaletta, kun taas vuonna 2017 tapahtumia ilmoitettiin 107 kappaletta.

Merkittävien tietoturvahäiriöiden kasvu on johtunut pääosin asiakastietojen hallinnan virheistä, joita ilmoitettiin 79 kappaletta vuonna 2017 (Traficom www-sivut 2019).

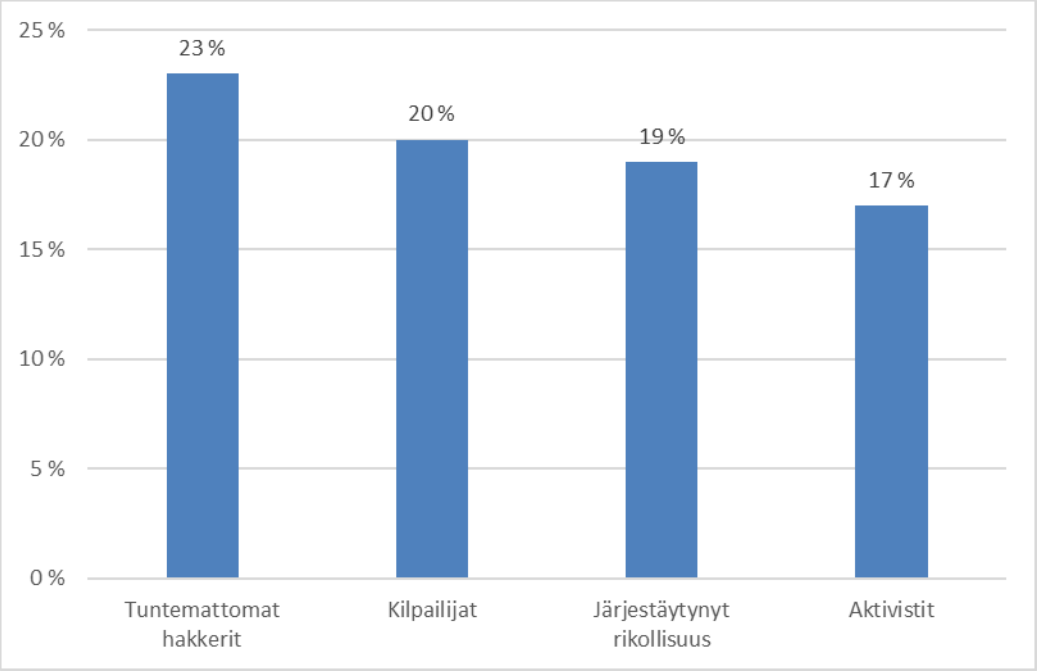


Kuvio 3. Merkittävien tietoturvaloukkausten- ja uhkien kappalemäärät Suomessa vuosittain (Traficom www-sivut 2019).

Kuvion 4 mukaan, tietoturvahäiriön todennäköisin sisäinen aiheuttaja on organisaation nykyinen työntekijä ja toiseksi suurimman uhan aiheuttaa organisaation entinen työntekijä. Yritysten nykyiset sekä entiset palveluntuottajat ja vastaavat havaittiin myös todennäköisiksi tietoturvahäiriöiden aiheuttajiksi. Kuvion 5 mukaan tietoturvahäiriön todennäköisin ulkoinen aiheuttaja on tuntematon hakkeri. Muita todennäköisimpiä tietoturvahäiriöiden ulkoisia aiheuttajia olivat yrityksen kilpailijat, järjestäytynyt rikollisuus ja aktivistit.



Kuvio 4. Oletetut tietoturvahäiriöiden sisäiset aiheuttajat (kaikki aiheuttajat eivät ole näkyvissä) (Bradgon 2017).



Kuvio 5. Oletetut tietoturvahäiriöiden ulkoiset aiheuttajat (kaikki aiheuttajat eivät ole näkyvissä) (Bradgon 2017).

Taulukoista 1 ja 2 selviää, että vuoden 2015 pienten ja keskikokoisten yritysten (alle 1500 työntekijää) suorat ja epäsuorat kustannukset tietomurto tapahtumissa olivat yhteensä keskimäärin 46 000 dollaria. Suurten yritysten (yli 1500 työntekijää) osalta

vastaavat kustannukset tietomurtotapahtumissa olivat 620 000 dollaria. Suorat kustannukset käsittävät mm. yrityksen toimintojen keskeytymisen ja ulkoisen avun tarpeet. Epäsuorat kustannukset käsittävät mm. toimenpiteet ja ohjelmistot vastaavien tietomurtojen välttämiseksi tulevaisuudessa. (Kaspersky Lab 2015.)

	SMB		Enterprise	
	Proportion of business incurring this expense	Typical losses	Proportion of business incurring this expense	Typical losses
Professional services	88%	$11K	88%	$84K
Lost business opportunities	32%	$16k	29%	$203K
Down-time	34%	$66K	30%	$1.4M
Total expected typical damage	$38K		$551K	

Taulukko 1. Suorat kustannukset tietomurtotapahtumissa. (Kaspersky Lab 2015).

	SMB		Enterprise	
	Proportion of business incurring this expense	Typical losses	Proportion of business incurring this expense	Typical losses
Staffing	41%	$5.5K	40%	$52K
Training	47%	$5k	53%	$33K
Systems	54%	$7K	54%	$75K
Total expected indirect spend	$8K		$69K	

Taulukko 2. Epäsuorat kustannukset tietoturvatapahtumissa. (Kaspersky Lab 2015).

Yritysten tietomurtojen kokonaisvaikutuksia on vaikea arvioida. Seuraukset ovat aina myös erilaisia, joillekin yrityksille tietomurto aiheuttaa vain pienen lisäyksen tietoteknisiin menoihin ja toisille merkittäviä taloudellisia- tai imagovahinkoja. Pahimmillaan tietomurto voi päättää koko yritystoiminnan. Yksi asia on kuitenkin varma, toteutuneen tietomurron kustannukset ovat aina suuremmat kuin suojautumisesta koituneet kustannukset. (Kaspersky Lab 2015.)

3.5 ISO/IEC 27001 -tietoturvasertifikaatti

Organisaatioiden tietotaitoa sisältävät tiedot sekä myös asiakkaiden tiedot tulee suojata tehokkaasti. Yrityksen tietoihin ja toimintoihin kohdistuvien uhkien torjuntaan tarvitaan usein ulkopuolista tietoturva-asiantuntemusta. Merkittävintä on saada turvattua yrityksen tietovoimavarat sekä tuotantotekijät, joihin liiketoiminta on voimakkaasti sidoksissa. Tietoturvallisuus tulee hallita kokonaisuutena. (Juvonen ym. 2014, 150).

Standardit ovat kansainvälisesti tunnustettujen tahojen julkaisemia dokumentteja. Näiden dokumenttien tarkoitus on auttaa ymmärtämään yleisiä laatuvaatimuksia ja prosesseja luotettavien tuotteiden ja palveluiden toimittamiseen. Standardit sisältävät tyypillisesti protokollia ja vaatimuksia sellaisessa muodossa, että ne ovat mahdollista liittää mihin tahansa organisaatioon johdonmukaisesti. (Campbell 2016, 72-73.)

Tietyn standardin mukaan rakennetulle yrityksen osa-alueelle, toiminnolle, johtamisjärjestelmälle, henkilölle tai koko organisaatiolle voidaan hakea sertifikaattia todistukseksi standardin vaatimustenmukaisuudesta, tämä tarkoittaa siis kyseessä olevan kohteen sertifiointia. Sertifikaatin voi myöntää akkreditoitu sertifiointiorganisaatio, kun sertifioinnin kohteena oleva järjestelmä täyttää sertifiointivaatimuksissa esitetyt vaatimukset. Vaatimukset ovat esitetty useimmiten standardeissa. Akkreditoidut sertifiointiorganisaatiot ovat kolmannen osapuolen toimijoita, joilla on kansainvälisissä standardeissa määritelty pätevyys ja tarvittavat muut pätevyydet toimintaa varten. (Finas www-sivut 2019.)

Hankitut sertifikaatit ovat hyviä referenssejä asiakkaiden suuntaan ja joskus tietyillä aloilla tietoturvasertifikaattia vaaditaan esimerkiksi asiakkaan puolesta. Tietoturvasertifikaatin hankintaa tulee harkita huolellisesti, sillä hyötyjen lisäksi niistä tulee merkittäviä ja jatkuvia organisaation kannattavuuteen vaikuttavia kuluja. (Campbell 2016, 73.) Myönnetty ISO 27001 -tietoturvasertifikaatti on voimassa kolme vuotta. Sertifioidun tietoturvajärjestelmän jatkuva parantaminen varmistetaan vuosittaisten määräaikaisarviointien avulla, jotka suorittaa ulkoinen auditoija. Mikäli sertifikaatin voimassaoloa halutaan jatkaa 3 vuoden jälkeen, tulee tietoturvajärjestelmä sertifioida uudelleen ennen sertifikaatin umpeutumista. (Bureau Veritas 2019.)

Kuten muutkin liiketoimintaresurssit, tieto tuo lisäarvoa organisaatiolle ja tämän vuoksi tietoa tulee suojata asianmukaisesti. ISO 27001 -standardi määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset, mikä mahdollistaa riskien arvioinnin ja tarvittavien ehkäisevien toimenpiteiden toteuttamisen. ISO 27001 mukaisen tietoturvan hallintajärjestelmän tavoitteena on pitää organisaation tietovarat luottamuksellisina, ehyinä ja saatavilla asianmukaisille henkilöille. (Bureau Veritas 2019.)

ISO 27001 -standardi auttaa organisaatiota säilyttämään kilpailukykynsä, kannattavuutensa ja maineensa varmistamalla tiedon, tietojärjestelmät, tiedon luotettavuuden, eheyden ja saatavuuden luotettavuuden sekä käyttövarmuuden. Standardi tukee myös yrityksen lakisääteisten ja sopimusluonteisten vaatimusten noudattamista. ISO 27001 -standardista saa johdolle hyvän työkalun toiminnan ohjaukselle ja myönnetty standardi on osoitus sidosryhmille tietoturvallisuuden hallinnasta. Lisäksi vaatimustenmukaisella riskienhallinnalla tunnistetaan organisaatioon kohdistuvat uhat, jolloin investoinnit pystytään kohdistamaan tarkasti oikeisiin asioihin. (Bureau Veritas 2019.)

ISO 27001 -standardi kattaa kaikentyyppiset organisaatiot ja sopii kaikille toimialoille. Standardi ei koske pelkästään tietotekniikkaa vaan kattaa kaikki näkökulmat tiedon siirrosta julkisiin keskusteluihin ja tietojen jakamiseen. (Bureau Veritas 2019.) Standardista sovelletaan uusinta ISO/IEC 27001:2017 versiota, joka korvaa vanhan ISO/IEC 27001:2013 version. ISO/IEC 27002:2017 standardi sisältää ohjeita ISO 27001 -standardin vaatimusten mukaisen tietoturvallisuuden hallintajärjestelmän luomiseen, joten sitä on järkevää hyödyntää valmistautuessa ISO 27001 sertifiointiin.

3.6 Tietoturvasertifikaatti-investointi tietoriskien hallintakeinona

Yrityksen pitkän aikavälin toimintaedellytysten ylläpitäminen ja toiminnankehittäminen vaatii yritykseltä erilaisia investointeja. Investoinnit voivat liittyä aineellisiin tai aineettomiin hyödykkeisiin. Aineelliset hyödykkeet voivat olla esimerkiksi rakennuksia, tuotantovälineitä tai laitteita. Aineettomia hyödykkeitä voivat esimerkiksi olla

henkilöstön pitkäaikainen koulutus, tutkimus tai tuotekehitys. Informaatioteknologiaan sekä johtamisjärjestelmiin toteutetut investoinnit voivat sisältää aineettomia ja aineellisia investointeja. (Järvenpää, Länsiluoto, Partanen & Pellinen 2013, 373.) Investoinnit muuttavat usein yrityksen toimintaa peruuttamattomasti. Pitkä ajallinen kesto, laajat vaikutukset, suuri sitoutunut pääoma sekä epävarmuus ovat tyypillisiä piirteitä investoinneille. (Ikäheimo, Malmi & Walden 2016, 165.)

Investoinnit voidaan luokitella finanssi- ja reaali-investointeihin. Raha- tai osakemarkkinoilla tehdyt investoinnit luokitellaan finanssi-investointeihin. Reaali-investoinneilla tarkoitetaan pitkäaikaisiin tuotannontekijöihin tehtyjä investointeja. Reaali-investoinnit voidaan ryhmitellä hyödyn mukaisesti laajennusinvestointeihin, korvausinvestointeihin, pakollisiin investointeihin ja muihin tuottamattomiin investointeihin sekä tutkimukseen ja tuotekehitykseen tehtäviin investointeihin. Investointien hyödyn mukainen ryhmittely on tärkeää, koska sillä on merkittävää vaikutusta investointipäätöksiin ja niiden toteutustapaan. Investoinneilta odotetaan erilaisia tuottovaatimuksia riippuen investoinnin luokittelusta. (Järvenpää ym. 2013, 373-374.)

Laajennusinvestoinnit voivat kohdistua esimerkiksi nykyisen tuotantokapasiteetin lisäämiseen tai laajentumiseen uusille tuotesegmenteille ja markkina-alueille. Laajennusinvestoinneilta voidaan niiden suurempien riskien vuoksi edellyttää korkeampaa tuottovaatimusta verrattuna muihin investointiryhmiin. (Järvenpää ym. 2013, 374.)

Korvausinvestoinneilla tarkoitetaan jo aiemmin tehtyjen investointien laitteiston tai kaluston korvaamista uudella, jotta tuotantoa pystytään jatkamaan. Korvausinvestointeja voivat olla myös investoinnit, joissa toimintaa kyetään tehostamaan korvaamalla vanha teknologia uudella. (Ikäheimo ym. 2016, 165.) Korvausinvestointeja voidaan tehdä ilman erityistä investointisuunnittelua tai tuottovaatimusta, koska laitteiston uusiminen on välttämätöntä toiminnan jatkamiseksi (Järvenpää ym. 2013, 374).

Pakollisilla investoinneilla ja muilla tuottamattomilla investoinneilla on usein eri tavoin yhteys yrityksen yhteiskuntavastuun toteuttamiseen. Yrityksen vastuullinen toiminta edellyttää taloudellisia, sosiaalisia ja ympäristövastuullisia investointeja. Taloudellisen vastuun investointeja voivat olla esimerkiksi investoinnit tehtaiden lähialueiden infrastruktuuriin ja yleishyödyllisten palveluiden tason nostamiseen. Sosiaalisen

vastuun investointeja ovat esimerkiksi yrityksen henkilöstön työturvallisuuden parantamiseen tehtävät investoinnit. Ympäristövastuun investoinnit tarkoittavat esimerkiksi investointeja tehtaan päästöjen vähentämiseen. Pakollisille ja muille tuottamattomille investoinneille ei aseteta erikseen tuottovaatimuksia, vaikka näillä investoinneilla voi olla vaikutusta yrityksen taloudelliseen menestymiseen. (Järvenpää ym. 2013, 375.)

Tutkimus- ja tuotekehitysinvestoinneilla on merkittävä vaikutus yrityksen tulevaisuuteen (Järvenpää ym. 2013, 375). Uusien tuotteiden kehittäminen vaatii merkittävää tutkimus- ja kehitystyötä sekä myöhemmin investointeja tuotantokapasiteettiin ja tuotteen menekin edistämiseen (Ikäheimo ym. 2016, 165).

ISO 27001 -tietoturvastandardin mukaisen sertifikaattihankinnan voidaan ajatella kuuluvan pakollisiin ja muihin tuottamattomiin investointeihin. Investoinnilla ei ole tuottovaatimusta, mutta sillä voi olla ratkaiseva merkitys yrityksen kannattavuuteen ja toimintaedellytyksiin.

Riskienhallinta on yrityksen yksi tärkeimmistä tehtävistä ja saatavilla on erilaisia työkaluja yritysten riskienhallinnan tueksi. ISO 27001 -tietoturvastandardi on tehokas työkalu tietoturvariskien hallintaan. ISO 27001 -tietoturvastandardin vaatimusten mukaiseksi rakennetulle yrityksen tietoturvajärjestelmälle voidaan akkreditoidun sertifiointiorganisaation toimesta myöntää tietoturvasertifikaatti. Voimassa oleva ISO 27001 -tietoturvasertifikaatti viestii asiakkaille ja muille sidosryhmille ko. yrityksen hyvästä tietoturvatasosta.

4 ISO/IEC 27001 -STANDARDI JA SEN VAATIMUKSET

Seuraavissa kohdissa käydään läpi ISO/IEC 27001:2017 -standardin vaatimuksia. Vaatimukset ovat laadittu niin, että ne soveltuvat kaikenlaisille organisaatioille. Mitään seuraavista vaatimuksista ei voi jättää käsittelemättä, mikäli organisaatio ilmoittaa noudattavansa ISO/IEC 27001:2017 -standardin vaatimuksia. (ISO/IEC 27001:fi 2017, 5.)

4.1 Toimintaympäristön määrittely

Organisaation tulee määrittää sisäiset ja ulkoiset asiat, jotka ovat organisaation kannalta olennaisia. Tämä tarkoittaa organisaation sisäisen ja ulkoisen toimintaympäristön määrittämistä. (ISO/IEC 27001:fi 2017, 6.) Sisäisen toimintaympäristön muodostavat organisaation sisäiset tekijät, jotka vaikuttavat tai voivat vaikuttaa yrityksen toimintaan ja tulostavoitteiden saavuttamiseen. Näitä tekijöitä voivat olla esimerkiksi organisaation kulttuuri, tietojärjestelmät ja organisaation hallintotapa. Ulkoinen toimintaympäristö käsittää yrityksen ulkoisia tekijöitä, joita voivat esimerkiksi olla suhteet kansalaisiin tai asiakkaisiin, keskeiset kehityssuunnat yhteiskunnassa ja lainsäädäntö. (VAHTI 2 2016.) Organisaation tulee lisäksi määrittää tietoturvallisuuden hallintajärjestelmän kannalta olennaiset sidosryhmät ja näiden sidosryhmien asettamat tietoturvallisuuteen vaikuttavat vaatimukset. Sidosryhmien vaatimukset voivat sisältää sopimusvelvoitteita, lakisääteisiä vaatimuksia ja viranomaisten vaatimuksia. (ISO/IEC 27001:fi 2017, 6.)

Organisaatiolle on luotava tietoturvallisuuden hallintajärjestelmä. Hallintajärjestelmää on ylläpidettävä ja parannettava jatkuvasti ISO 27001 -standardin vaatimusten mukaisesti. (ISO/IEC 27001:fi 2017, 6). Tietoturvallisuuden hallintajärjestelmä toimii yrityksen työvälineenä tietoturvan hallinnassa, johtamisessa ja kehittämisessä.

Tietoturvallisuuden hallintajärjestelmän soveltamisala tulee päättää organisaation toimesta. Soveltamisalaa päätettäessä tulee huomioida ylempänä mainitut ulkoiset ja sisäiset asiat, sidosryhmät ja niiden vaatimukset sekä organisaation ja muiden organisaatioiden toimintojen rajapinnat ja riippuvuudet. (ISO/IEC 27001:fi 2017, 6.)

4.2 Tietoturvapolitiikka ja johtajuus

Ylin johto vastaa yrityksen tietoturvallisuuden hallintajärjestelmästä. Johto laatii yrityksen toimintastrategiaan nivelletyn tietoturvapolitiikan. (ISO/IEC 27001:fi 2017, 7.) Yrityksen tietoturvapolitiikka on lyhyehkö yleinen dokumentti, joka on johdon hyväksymä ja osoittaa johdon sitoutumisen tietoturvallisuuteen. Politiikan tarkoituksena on antaa perusteet, ohjata ja velvoittaa tietojenkäsittelyn sekä

tietoturvallisuuden kehittämistyötä. Tietoturvapolitiikassa kuvataan tietoturvallisuuden merkitys liiketoiminnalle, johdon asettamat tavoitteet sekä vaatimukset. Tietoturvapolitiikassa kuvataan myös tietoturvallisuuden johtamisen malli, organisointi ja vastuut. Tietoturvapolitiikan toteutuminen ja ylläpito varmistetaan ohjeilla, menettelytavoilla, teknisillä apuvälineillä sekä seurannalla ja valvonnalla. (Juvonen ym. 2014, 162-163.) Johdon on varmistettava, että tietoturvallisuuden hallintajärjestelmän vaatimukset yhdistetään organisaation prosesseihin ja että hallintajärjestelmän vaatimat resurssit ovat saatavilla. Johdon tulee myös viestiä tietoturvallisuuden hallintajärjestelmän vaatimusten noudattamisen tärkeydestä ja varmistaa, että hallintajärjestelmä saavuttaa halutut tulokset. Lisäksi ylimmän johdon tehtäviin kuuluu ohjata ihmisiä tietoturvallisuuden hallintajärjestelmän vaikuttavuuden kehittämiseen, edistää hallintajärjestelmän jatkuvaa parantamista, sekä tukea muiden johtoon kuuluvien johtajuutta omilla vastuualueillaan. (ISO/IEC 27001:fi 2017, 7.)

Ylimmän johdon luoman tietoturvapolitiikan tulee soveltua organisaation toiminta-ajatukseen, sisältää tietoturvatavoitteet ja sitoutumisen tietoturvallisuutta koskevien vaatimusten täyttämisen sekä sitoutumisen tietoturvallisuuden hallintajärjestelmän jatkuvaan parantamiseen (ISO/IEC 27001:fi 2017, 7). Tietoturvatavoitteet voivat olla tietoturvatoimintoihin liittyviä tavoitteita tai ne voivat olla myös johdettuja muista organisaation tavoitteista, joissa tietoturvallisuus on tärkeässä asemassa. Tietoturvatavoitteita voivat olla esimerkiksi tietoturvahäiriöiden vähentyminen, koulutuksen toteutuminen tai tietoturvatoiminnan kustannuksiin liittyvät tavoitteet. (Valtiovarainministeriö 2006, 24-25.) Tietoturvapolitiikan on oltava dokumentoituna koko organisaation tiedossa ja tarvittaessa organisaation sidosryhmien saatavilla. (ISO/IEC 27001:fi 2017, 7).

Ylimmän johdon tehtävänä on varmistaa, että tietoturvaan liittyvät roolit ja vastuut on määritelty ja koko organisaation tiedossa. Johdon tulee myös määritellä henkilö tai henkilöt, joiden vastuulla on varmistaa yrityksen tietoturvallisuuden hallintajärjestelmän vaatimustenmukaisuus sekä valtuudet raportoida johdolle hallintajärjestelmän suorituskyvystä. (ISO/IEC 27001:fi 2017, 7.)

4.3 Tietoturvallisuuden hallintajärjestelmän suunnittelu

Suunniteltaessa tietoturvallisuuden hallintajärjestelmää, organisaation on otettava huomioon organisaation toimintaympäristö ja sidosryhmien asettamat tietoturvallisuutta koskevat vaatimukset sekä määritettävä ne riskit ja mahdollisuudet, joita on käsiteltävä. Määriteltyihin riskeihin ja mahdollisuuksiin on suunniteltava toimenpiteitä sekä miten nämä toimenpiteet yhdistetään tietoturvallisuuden hallintajärjestelmän prosesseihin ja miten ne toteutetaan. Lisäksi on suunniteltava, kuinka näiden toimenpiteiden vaikuttavuutta arvioidaan. (ISO/IEC 27001:fi 2017, 8.)

Organisaation pitää toteuttaa tietoturvariskien arviointiprosessi. Arviointiprosessiin laaditaan riskien hyväksymiskriteerit sekä tietoturvariskien arvioinnin suorittamista koskevat kriteerit. Prosessissa tunnistetaan yrityksen tietoturvajärjestelmän soveltamisalaan kuuluvan tiedon tietoturvallisuuteen liittyvät riskit ja näiden riskien omistajat. (ISO/IEC 27001:fi 2017, 8.) Riskin omistaja tarkoittaa henkilöä tai tahoa, kenellä on valtuudet ja vastuu hallita riskiä (VAHTI 2017). Arviointiprosessissa havaitut tietoturvariskit analysoidaan arvioimalla riskin seuraukset ja riskin toteutumisen realistinen todennäköisyys. Riskin analysoinnin jälkeen voidaan määrittää riskitaso kyseiselle riskille. Lopuksi tietoturvariskejä verrataan riskikriteereihin ja riskit priorisoidaan riskien käsittelyyn. Tietoturvariskien arviointiprosessista on säilytettävä dokumentoitua tietoa. (ISO/IEC 27001:fi 2017, 8.)

Tietoturvariskien käsittelyyn on määriteltävä ja toteutettava tietoturvariskien käsittelyprosessi, jossa valitaan soveltuvat tietoturvariskien käsittelyvaihtoehdot ja näille käsittelyvaihtoehdoille määritetään hallintakeinot (ISO/IEC 27001:fi 2017, 9). Hallintakeinot ovat toimenpiteitä, joiden tavoitteena on ensisijaisesti estää vahinkojen syntyminen tai vähentämään niiden seurauksia. Tarvittavien toimenpiteiden laajuus riippuu riskin suuruudesta. (PK-RH 2019.) Hallintakeinoja sovelletaan ISO 27001 -standardin liitteessä A oleviin velvoittaviin hallintatavoitteisiin ja varmistetaan ettei mitään hallintakeinoja ole jätetty huomioimatta. Tämän riskienhallinnan käsittelyprosessin avulla luodaan soveltuvuuslausunto. Soveltuvuuslausunnossa esitetään tarvittavat ja perustellut hallintakeinot sekä perustelut mikäli jotain hallintakeinoja jätetään käyttämättä. Havaituille tietoturvariskeille laaditaan käsittelysuunnitelma, jolle lopuksi hankitaan riskien omistajilta hyväksyntä.

Tietoturvariskien käsittelyprosessista tulee säilyttää dokumentoitua tietoa (ISO/IEC 27001:fi 2017, 9.) ISO 27001 -standardin Liite A sisältää yhteensä 125 eri hallintatavoitetta.

Organisaation on asetettava omat tietoturvatavoitteet ja suunniteltava niiden saavuttamiseen tarvittavat toimet. Tietoturvatavoitteiden on oltava yhdenmukaisia tietoturvapolitiikan kanssa ja mahdollisuuksien mukaan mitattavissa. Tietoturvatavoitteissa on otettava huomioon soveltuvat tietoturvavaatimukset sekä riskien arvioinnin ja käsittelyn tulokset. Tietoturvatavoitteista on viestittävä ja niitä on päivitettävä tarvittaessa. Tietoturvatavoitteidensa saavuttamiseen organisaation on suunniteltava toimenpiteet ja aikataulu, varattava resurssit, määritettävä vastuut sekä arvioida saatuja tuloksia. (ISO/IEC 27001:fi 2017, 9-10.)

4.4 Tietoturvallisuuden hallintajärjestelmän tukitoiminnot

Tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja sen jatkuvaan parantamiseen on määritettävä ja varattava tarvittavat resurssit. Organisaation on määritettävä yrityksen tietoturvatasoon vaikuttavien henkilöiden pätevyysvaatimukset. Näiden tietoturvaan vaikuttavien henkilöiden pätevyys on varmistettava koulutuksen, harjoittelun tai kokemuksen perusteella. Henkilöiden pätevyystiedot tulee säilyttää asianmukaisesti dokumentoituna. (ISO/IEC 27001:fi 2017, 10.)

Henkilöstön pitää olla tietoisia organisaation tietoturvapolitiikasta ja siitä, miten he voivat omalta osaltaan lisätä tietoturvallisuuden hallintajärjestelmän vaikuttavuutta. Henkilöstön pitää myös olla tietoisia tietoturvallisuuden parantamisen hyödyistä sekä myös tietoturvallisuuden hallintajärjestelmän vaatimusten laiminlyönneistä koituvista seurauksista. (ISO/IEC 27001:fi 2017, 10.)

Organisaatiolle on määritettävä tietoturvallisuuden hallintajärjestelmän kannalta olennaiset ohjeet sisäiselle ja ulkoiselle viestinnälle. On määritettävä esimerkiksi mistä ja milloin viestitään, keiden kanssa viestitään, ketkä viestivät ja minkälaiset viestintäprosessit on toteutettava. (ISO/IEC 27001:fi 2017, 10.)

Organisaation tietoturvallisuuden hallintajärjestelmän on sisällettävä ISO 27001 -standardin edellyttämän tiedon lisäksi tieto, jonka se on itse määrittänyt tietoturvan kannalta välttämättömäksi. Organisaation on dokumentaatiossaan varmistettava asianmukainen dokumenttien merkintä ja kuvaus, tallennusmuoto ja tallennusväline, soveltuvuuden ja riittävyyden tarkistaminen sekä hyväksyminen. (ISO/IEC 27001:fi 2017, 11.)

Dokumentoitua tietoa on hallittava siten, että pystytään varmistamaan sen saatavuus sopivassa muodossa ja että tieto on suojattuna asianmukaisesti. Organisaation dokumentoidun tiedon hallinnan on katettava soveltuvin osin tiedon jakelu, pääsy tietoihin, esillesaanti ja tiedon käyttö. Lisäksi tiedon varastointi, säilytys, muutostenhallinta, säilyttäminen ja hävittäminen tulee hallita asianmukaisesti. Ulkopuolista alkuperää olevan tiedon, jonka organisaatio on määritellyt tarpeelliseksi, tulee yksilöidä tarvittavalla tavalla ja sitä on hallittava. (ISO/IEC 27001:fi 2017, 11.)

4.5 Organisaation toiminta

Yrityksen tulee luoda tietoturvallisuuden hallintaprosessi, jolla varmistetaan tietoturvallisuuden kannalta välttämättömien toimenpiteiden suorittaminen ja tietoturvavaatimusten täyttyminen. Organisaation on myös tehtävä suunnitelmat, joiden avulla saavutetaan määritetyt tietoturvatavoitteet. (ISO/IEC 27001:fi 2017, 12.)

Organisaation suunniteltuja muutoksia tulee hallita ja tahattomien muutosten seurauksia täytyy arvioida ja tarpeen mukaan pyrittävä lieventämään mahdollisia haittavaikutuksia. Ulkoistetut prosessit on määritettävä ja niitä on valvottava. (ISO/IEC 27001:fi 2017, 12.)

Tietoturvariskien arviointi on suoritettava suunniteltuin aikavälein. Tietoturvariskit pitää myös arvioida, kun merkittäviä muutoksia tapahtuu sekä myös silloin, kun muutoksia ehdotetaan. Riskien arvioinnissa on noudatettava organisaatiolle luotuja tietoturvariskikriteerejä. Lisäksi organisaation on otettava käyttöön tietoturvariskien

käsittelysuunnitelma. Tietoturvariskien arviointien ja käsittelyjen tuloksista on säilytettävä dokumentoitua tietoa. (ISO/IEC 27001:fi 2017, 12.)

4.6 Tietoturvallisuuden hallintajärjestelmän suorituskyvyn arviointi

Organisaation tietoturvallisuuden hallintajärjestelmän vaikuttavuutta sekä tietoturvan tasoa tulee arvioida. Arviointia varten organisaation on määritettävä seurattavat ja mitattavat kohteet sekä sopivat seuranta-, mittaus-, analysointi-, ja arviointimenetelmät. Organisaation tulee määrittää seurannan ja mittauksen toteuttajat ja ajankohdat. Lisäksi on määritettävä tuloksien analysoinnin ja arvioinnin ajankohdat sekä niiden suorittajat. (ISO/IEC 27001:fi 2017, 12.)

Sisäiset auditoinnit on suoritettava suunnitelluin aikavälein (ISO/IEC 27001 2017). Sisäinen auditointi on organisaation kehittämistyökalu. Sen avulla voidaan selvittää, miten organisaation sovitut toimintatavat, sidosryhmien odotukset ja viranomaisvelvoitteet toteutuvat käytännössä. (Itä-Suomen yliopiston www-sivut 2019.) Auditoinneista saatujen tietojen perusteella voidaan määrittää, onko organisaation tietoturvallisuuden hallintajärjestelmä organisaation omien vaatimusten sekä ISO 27001 -standardin vaatimusten mukainen ja onko hallintajärjestelmä toteutettu ja ylläpidetty vaikuttavasti. (ISO/IEC 27001:fi 2017, 13.)

Organisaation on luotava ja ylläpidettävä auditointiohjelmia. Auditointiohjelmissa määritellään auditointien ajankohdat, vastuut, menetelmät, suunnitteluvaatimukset ja raportointi. Auditointiohjelmissa otetaan huomioon edellisten auditointien tulokset. Organisaation on määriteltävä kunkin auditoinnin auditointikriteerit ja soveltamisala sekä valittava auditoijat. Sisäisen auditoinnin objektiivisuus sekä puolueettomuus on varmistettava. Auditointien tuloksista pitää raportoida asiaankuuluville henkilöille ja auditoinneista on säilytettävä dokumentoitua tietoa. (ISO/IEC 27001:fi 2017, 13.)

Tietoturvallisuuden hallintajärjestelmä on katselmoitava johdon toimesta tietyin aikavälein, jotta voidaan varmistaa sen soveltuvuus, asianmukaisuus ja vaikuttavuus. Johdon katselmuksessa on otettava huomioon aiempien johdon katselmusten vuoksi käynnistettyjen toimenpiteiden tilanne ja tietoturvan kannalta olennaisten asioiden

muutokset. Katselmuksessa tulee ottaa huomioon tietoturvan tasoa koskeva palaute, joka sisältää tietoturvapoikkeamat ja niiden korjaavat toimenpiteet, tietoturvallisuuteen liittyvät seurannan ja mittauksen tulokset, ulkoisten ja sisäisten auditointien tulokset sekä asetettujen tietoturvatavoitteiden täyttyminen. Lisäksi tulee huomioida sidosryhmien palaute, jatkuvan parantamisen mahdollisuudet, riskien arvioinnin tulokset sekä riskinkäsittelysuunnitelman tilanne. (ISO/IEC 27001:fi 2017, 13.)

Johdon katselmuksen tuloksiin on kirjattava päätökset tietoturvallisuuden hallintajärjestelmän mahdollisista muutostarpeista ja jatkuvan parantamisen mahdollisuuksista. Johdon katselmukset säilytetään dokumentoituna tietona (ISO/IEC 27001:fi 2017, 13.)

4.7 Jatkuva parantaminen

Organisaatiossa havaittuihin poikkeamiin on reagoitava ja tilanteesta riippuen ryhdyttämä toimiin poikkeaman hallitsemiseksi ja korjaamiseksi tai käsiteltävä sen seurauksia. (ISO/IEC 27001:fi 2017, 14.) Tietoturvapoikkeama tarkoittaa tahallista tai tahatonta tapahtumaa, jonka seurauksena organisaation vastuulla olevien tietovarojen tai palveluiden tietoturvallisuus on tai saattaa olla vaarantunut (VAHTI 2016). Yritykseltä vaaditaan toimenpiteitä tietoturvapoikkeaman korjaamiseksi ja juurisyyn selvittämiseksi. Toimenpiteillä varmistetaan, että poikkeama ei toistu uudelleen tai esiinny muualla organisaatiossa. Tällaisia toimenpiteitä ovat mm. poikkeaman katselmointi, syiden selvittäminen, vastaavien poikkeamien tai niiden mahdollisuuksien etsiminen. Mikäli korjaavia toimenpiteitä tarvitaan, ne on toteutettava ja niiden vaikuttavuutta on arvioitava. Tarpeen mukaan organisaatio voi tehdä muutoksia tietoturvallisuuden hallintajärjestelmään havaitun poikkeaman johdosta. Korjaavien toimenpiteiden tulee olla tarkoituksenmukaisia poikkeaman aiheuttamiin vaikutuksiin nähden. (ISO/IEC 27001:fi 2017, 14.)

Organisaation on säilytettävä dokumentoitua tietoa poikkeaman luonteesta ja tehdyistä toimenpiteistä sekä korjaavien toimenpiteiden tuloksista. Organisaation

tietoturvallisuuden hallintajärjestelmää on parannettava jatkuvasti sen soveltuvuuden, riittävyyden ja vaikuttavuuden kannalta. (ISO/IEC 27001 2017.)

5 ISO/IEC 27001 -SERTIFIKAATIN KOKONAISKUSTANNUKSET

5.1 Kohdeyrityksen esittely

Tutkimuksen kohdeyrityksenä toimii Intrinsic Oy. Intrinsic Oy on tamperelainen vuonna 1984 perustettu ohjelmistoyritys. Yrityksellä on yksi toimipiste, jossa työskentelee 5 työntekijää toimitusjohtajan lisäksi. Intrinsic Oy toimittaa korkean vaativuustason tiedonkeruu- ja hallintajärjestelmiä tiesäätietoon ja liikenteenhallintaan liittyviin järjestelmiin sekä teollisuuden laadunohjausjärjestelmiin. Yrityksellä on kokemusta esimerkiksi ISO 9001 -laatusertifikaatin hankinnasta, mikä helpottaa ISO 27001 -tietoturvasertifikaatin kokonaiskustannuksien arvioimista.

ISO 27001 -tietoturvasertifikaatin hankinnan voidaan ajatella kuuluvan pakollisiin ja muihin tuottamattomiin investointeihin. Sertifikaattihankinnan ei oleteta lisäävän yrityksen tuottoja. Kuitenkin hankinnalla voi olla ratkaiseva merkitys yrityksen kannattavuuteen ja yritystoiminnan jatkumiseen tulevaisuudessa. ISO 27001 -tietoturvasertifikaattihankinnan kokonaiskustannuksien arvioiminen antaa yritykselle oleelliset tiedot hankinnan vaatimista resursseista ja euromääräisistä kustannuksista, kun arvioidaan lopullisen investointipäätöksen tekemistä.

5.2 Tietoturvallisuuden hallintajärjestelmän kehitystyön kustannukset

Seuraavaksi arvioidaan yleisellä tasolla toimenpiteitä, työmäärää ja euromääräisiä kustannuksia, joita koituu kohdeyrityksen tietoturvallisuuden hallintajärjestelmän saattamisesta ISO 27001 -standardin vaatimusten mukaiseksi. Työmääräarviot sisältävät vaadittavien toimenpiteiden lisäksi kaikkien luotujen tai muokattujen dokumenttien ja ohjeistuksien sisäiset katselmoinnit, todennukset ja hyväksynnät. Yhden työtunnin

kustannukseksi on arvioitu 60 euroa. Työtuntikustannus sisältää sosiaalikulut, loma-ajan palkan ja lomakorvaukset jaettuna työntekijän normaaleilla läsnäolotunneilla.

Ennen tietoturvallisuuden hallintajärjestelmän kehitystyön aloittamista, arvioitiin Intrinsic Oy:n tietoturvatasoa. Yritykselle oli hankittu aikaisemmin ISO 9001- laatusertifikaatti. ISO 9001- laatustandardin vaatimuksissa on paljon vastaavuuksia ISO 27001- tietoturvastandardiin, joten tietoturvallisuuden hallintajärjestelmän kehitystyötä ei tarvinnut aloittaa aivan tyhjästä. ISO 27001- standardin vaatimuksia verrattiin nykyiseen Intrinsic Oy:n tietoturvallisuuden hallintajärjestelmään. Lisäksi asiakkaiden kanssa tehdyt tietoturvasopimukset olivat velvoittaneet Intrinsic Oy:n kehittämään tietoturvallisuuttaan. Näin ollen kohdeyrityksen tietoturvatason arvioidaan olevan hyvällä tasolla ennen tietoturvallisuuden hallintajärjestelmän kehitystyön aloittamista.

5.2.1 Toimintaympäristön määrittely

Kohdeyrityksen toimintaympäristö on pääosin määritelty yrityksen tietoturvaohjeistuksissa. Toimintaympäristön määrittelyyn täytyy tehdä muutamia pieniä lisäyksiä ja tarkennuksia koskien sidosryhmiä ja tietoturvallisuuden hallintajärjestelmän soveltamisalaa.

Työmääräarvio: 15 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 900 euroa

5.2.2 Tietoturvapolitiikka ja johtajuus

Johtajuus ja sitoutuminen osa-alueesta tulee luoda ohjeistus. Organisaatiolle on luotu tietoturvapolitiikka, joka vastaa standardin vaatimuksia. Organisaatiolle on myös määritelty tietoturvan kannalta tärkeiden roolien vastuut ja valtuudet. Dokumentaatiota tulee muokata.

Työmääräarvio: 20 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 1200 euroa

5.2.3 Tietoturvallisuuden hallintajärjestelmän suunnittelu

Kohdeyrityksellä on luotuna riskinarviointi dokumentti riskien käsittelyyn. Riskien arviointiin on olemassa käytäntö, mutta dokumentoitua riskien arviointi- ja käsittelyprosessia ei ole luotuna. Nämä prosessit on määriteltävä ja toteutettava. Tietoturvastandardin vaatimukset tulee yhdistää yrityksen omiin prosesseihin. Lisäksi organisaatiolle tulee luoda tietoturvatavoitteet asiaankuuluville toiminnoille ja tasoille.

Työmääräarvio: 300 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 18 000 euroa

5.2.4 Tietoturvallisuuden hallintajärjestelmän tukitoiminnot

Organisaation tietoturvallisuuden hallintajärjestelmän luomiseen, toteuttamiseen, ylläpitoon ja jatkuvaan parantamiseen on luotava resurssisuunnitelma. Tietoturvan tasoon vaikuttavien henkilöiden pätevyysvaatimukset tulee luoda. Viestinnän ohjeistusta tulee päivittää.

Työmääräarvio: 50 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 3000 e

5.2.5 Organisaation toiminta

Organisaatiolle on luotava tietoturvariskien arviointisuunnitelma. Lisäksi tulee luoda vuosittainen tietoturvan arviointiohjelma yrityksen tietoturvallisuuden hallintajärjestelmän vaikuttavuuden ja jatkuvan parantamisen mahdollistamiseen.

Työmääräarvio: 20 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 1200 euroa

5.2.6 Tietoturvallisuuden hallintajärjestelmän suorituskyvyn arviointi

Organisaation on luotava arviointimenetelmät tietoturvatason ja tietoturvallisuuden hallintajärjestelmän vaikuttavuuden mittaamiseen. Lisäksi organisaation tulee luoda suunnitelma sisäisten auditointien sekä johdon katselmuksien suorittamiseen.

Työmääräarvio: 30 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 1800 euroa

5.2.7 Jatkuva parantaminen

Organisaatiolla on tietoturvapoikkeamien käsittelyyn kattavat ohjeistukset, mutta poikkeamien käsittelydokumentti on luotava.

Työmääräarvio: 15 h
Laitteisto ja muut kustannukset: 0 euroa
Kustannukset yhteensä: 900 euroa

5.2.8 Tietoturvallisuuden hallintajärjestelmän kehitystyö yhteensä

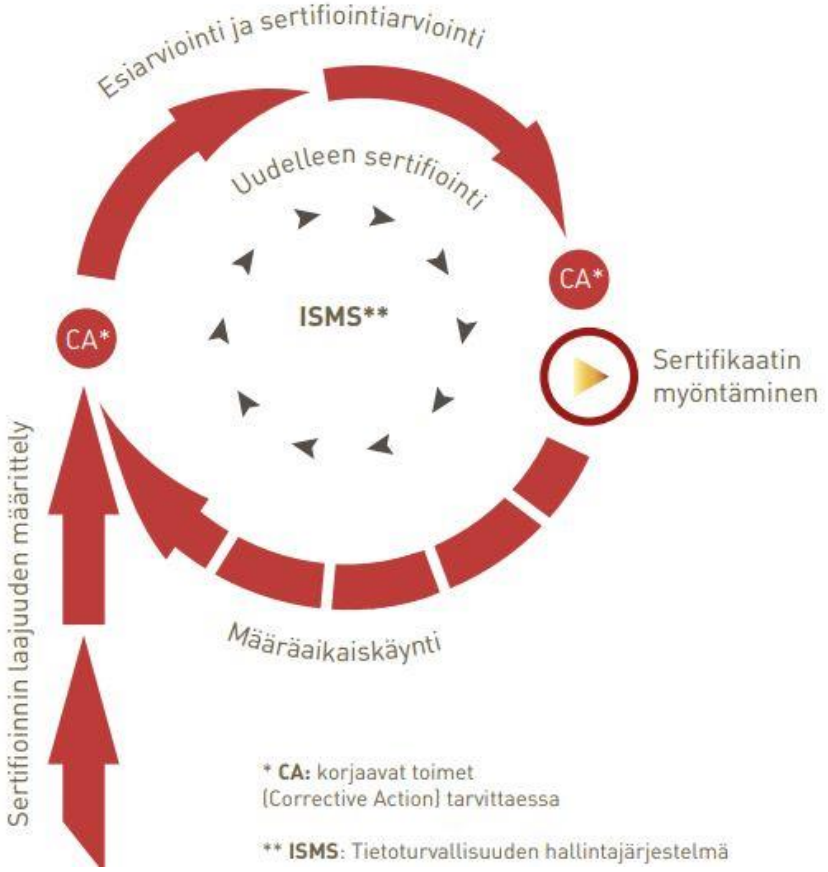
Kehitystyötä arvioitiin kertyvän yhteensä 450 tuntia. Uusia ohjelmisto- tai laitehankintoja ei tarvita. Kehitystyönkustannuksiksi arvioitiin yhteensä 27 000 euroa.

5.3 Sertifikaatin myöntäjästä koituvat kustannukset

Sertifikaatin myöntäjästä koituvat kustannukset syntyvät auditoinneista sekä vuosittaisesta akkreditointimaksusta. Laskelmissa arvioidut kustannukset ovat arvonlisäverottomia.

Yrityksen on mahdollista tehdä auditoijan tuella GAP analyysi ennen varsinaisen sertifioinnin aloittamista. GAP analyysissä auditoija vertaa yrityksen nykytilaa standardin vaatimuksiin. Vertailun tuloksena saadun raportin avulla yritys voi kehittää toimintojaan standardin vaatimusten mukaisiksi. GAP analyysin kustannus on 1245,00 euroa/päivä sekä auditoijan matka-, majoitus- ja päivärahakulut 400,00 euroa, jolloin kustannukset ovat yhteensä 1645,00 euroa.

Kuviossa 6 kuvataan ISO 27001 -sertifioinnin päävaiheita. Ennen sertifioinnin aloittamista tulee sertifioinnin laajuus määritellä, jonka jälkeen sertifiointi alkaa esiarvioinnilla. Esiarvioinnissa selvitetään onko kaikki ISO 27001-standardin vaatimukset huomioitu. Esiarvioinnin jälkeen yritys voi korjata mahdolliset puutteet, jotka sertifioija on havainnut esiarvioinnissa. Kun yritys katsoo olevansa valmis, voidaan siirtyä varsinaiseen sertifiointiarviointiin. Sertifikaatti voidaan myöntää ja julkaista, kun kaikki arvioinnin aikana havaitut poikkeamat on korjattu hyväksytysti. Mikäli yrityksen tietoturvajärjestelmässä havaitaan vakava poikkeama, voidaan tarvita seuranta-arviointi.



Kuvio 6. Sertifioinnin päävaiheet (Bureau Veritas 2019).

Esiarviointi, 1 päivän kustannus: 1245,00 euroa sekä auditoijan matka-, majoitus- ja päivärahakulut 400,00 euroa eli yhteensä 1645,00 euroa.

Varsinainen sertifiointiarviointi, 1 päivän kustannus: 1245,00 euroa sekä auditoijan matka-, majoitus- ja päivärahakulut 400,00 euroa eli yhteensä 1645,00 euroa.

Mahdollinen uusinta arviointi, 1 päivän kustannus: 1245,00 euroa sekä auditoijan matka-, majoitus- ja päivärahakulut 400,00 euroa eli yhteensä 1645,00 euroa.

Myönnetty sertifikaatti kuuluu palvelun hintaan. Vuosittaiset kiinteät kulut koostuvat akkreditointimaksusta, joka on 300,00 euroa kun yrityksessä työskentelee alle 50 henkilöä. Vuosittain ulkoinen sertifioija tekee määräaikaisarvioinnin, jossa varmistetaan yrityksen tietoturvallisuuden hallintajärjestelmän standardin vaatimustenmukaisuus. Määräaikaisauditoinnin kustannukset päivältä ovat 1245,00 euroa sekä auditoijan matka-, majoitus- ja päivärahakulut 400,00 euroa eli yhteensä 1645,00 euroa.

5.4 Sertifioidun tietoturvallisuuden hallintajärjestelmän ylläpitokustannukset

Tietoturvallisuuden hallintajärjestelmän ylläpitokustannukset koostuvat pääosin ylläpitotehtävistä sekä mahdollisista laite- ja ohjelmistohankinnoista. Ylläpitotehtäviä ovat mm. tietoturvallisuuden hallintajärjestelmään liittyvät päivitykset, katselmoinnit, vuosittaisen tietoturvaohjelman tehtävien suorittaminen, tietoturvatapahtumien kirjaus, tietoturvatavoitteiden seuranta sekä tietoturvallisuuden hallintajärjestelmään tehtävät pienet kehitystyöt.

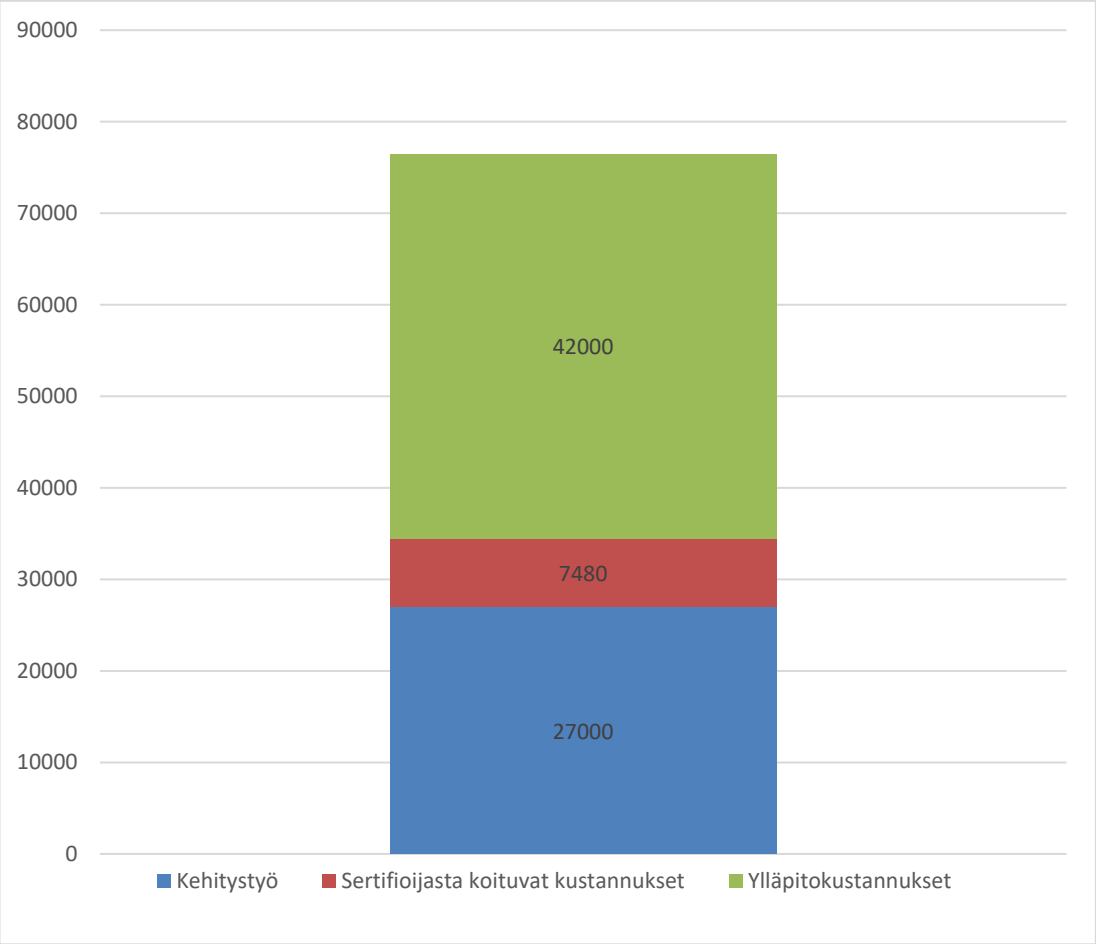
ISO 27001- sertifioidun tietoturvallisuuden hallintajärjestelmän ylläpitotehtäviin arvioidaan käytettävän vuosittain 200 työtuntia. Laite- ja ohjelmistohankintoihin arvioidaan käytettävän vuosittain 2000 euroa. Vuosittaisten ylläpitokustannuksien arvioidaan olevan yhteensä 14 000 euroa. Sertifikaatin 3 vuoden voimassaoloajan ylläpitokustannukset ovat yhteensä 42 000 euroa.

5.5 ISO/IEC 27001 -tietoturvasertifikaattihankinnan kokonaiskustannukset

Sertifikaattihankinnan kokonaiskustannuksia arvioitiin sertifikaatin voimassaoloajalta, joka on 3 vuotta. Laskelmissa oletetaan, että kohdeyritys ei tilaa auditoijalta vapaaehtoista GAP analyysiä. Lisäksi oletetaan aikaisempiin Intrinsicille tehtyihin laatujärjestelmän sertifiointiarvioinneista saatuihin kokemuksiin perustuen, että varsinaista sertifiointiarvioinnin jälkeistä laaja-alaista uusinta-arviointia ei tarvitse tehdä.
Taulukosta 3 sekä kuviosta 7 selviää, että ISO 27001- tietoturvasertifikaattihankinnan arvioidut kustannukset 3 vuoden ajalta ovat yhteensä 76 480 euroa. Ylläpitokustannukset arvioitiin suurimmaksi kulueräksi ollen 3 vuoden ajalta yhteensä 42 000 euroa. Tietoturvallisuuden hallintajärjestelmän kehitystyöstä arvioitiin syntyvän kustannuksia 27 000 euroa. Sertifioinnin myöntäjästä koituvia kustannuksia arvioitiin syntyvän 7 480 euroa.

	Kustannukset (€):
Kehitystyö	27000
Sertifioijasta koituvat kustannukset	7480
Ylläpitokustannukset	42000
Yhteensä	**76480**

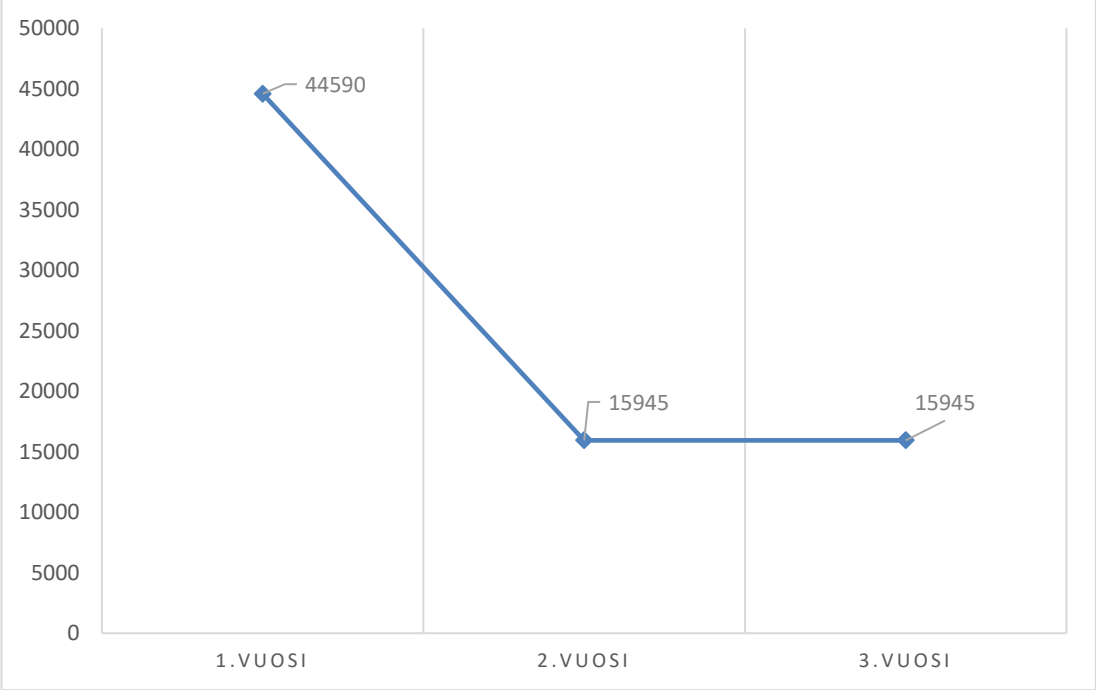
Taulukko 3. Tietoturvasertifikaattihankinnan arvioidut kokonaiskustannukset 3 vuoden ajalta.



Kuvio 7. Tietoturvasertifikaattihankinnan arvioidut kokonaiskustannukset 3 vuoden aikajaksolta.

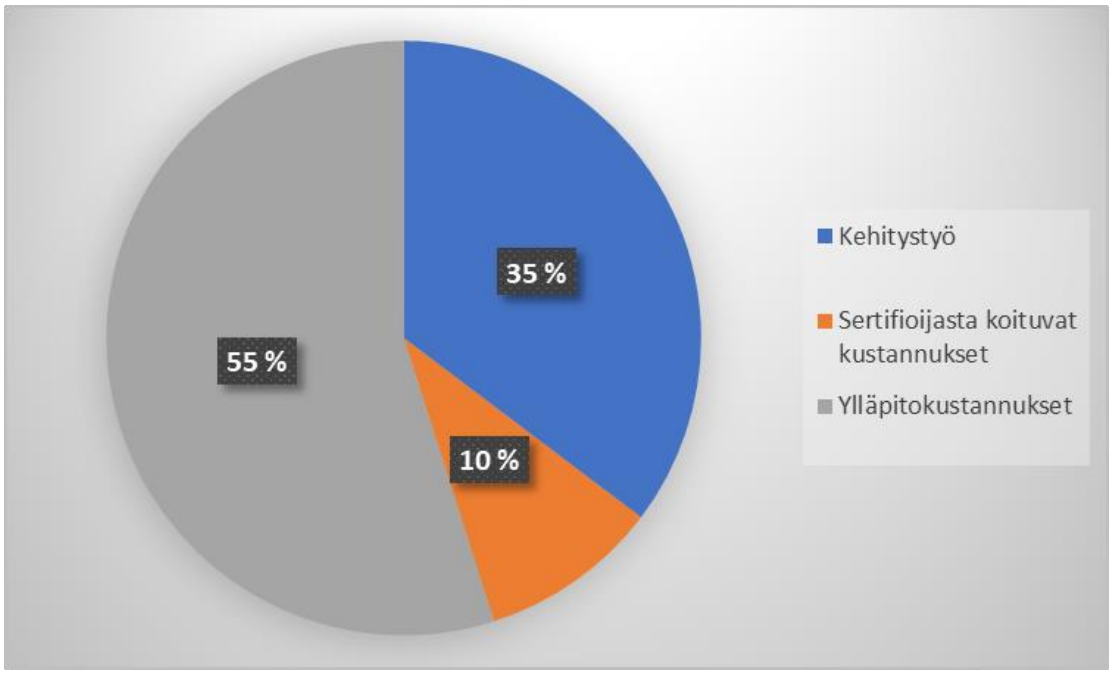
Kuviossa 8 kuvataan ISO 27001- tietoturvasertifikaattihankinnan arvioituja kustannuksia vuosittain eriteltynä 3 vuoden ajalta. Kuviosta nähdään, että ensimmäisen vuoden kustannuksien arvioidaan olevan yhteensä 44 590 euroa. Ensimmäisen vuoden kustannukset sisältävät tietoturvallisuuden hallintajärjestelmän kehitystyön, esiarvioinnin, varsinaisen sertifioinnin, ylläpitokustannukset sekä vuosittaisen akkreditointi-

maksun. Toisen ja kolmannen vuoden kustannuksien arvioidaan olevan selvästi pienemmät kuin ensimmäisen vuoden kustannukset. Toisen ja kolmannen vuoden arvioidut kustannukset ovat vuosittain yhteensä 15 945 euroa sisältäen ylläpitokustannukset, auditoijan määräaikaisarvioinnit sekä akkreditointimaksut.



Kuvio 8. Tietoturvasertifikaattihankinnan arvioidut euromääräiset kustannukset vuosittain.

Kuviossa 9 kuvataan tietoturvasertifikaattihankinnan arvioitujen kokonaiskustannuksien jakautumista prosenttiosuuksin eri osa-alueittain. Kokonaiskustannuksista 55 prosenttia arvioitiin syntyvän ylläpitokustannuksista. Tietoturvallisuuden hallintajärjestelmän kehitystyön arvioitiin olevan 35 prosenttia ja sertifioijasta koituvien kustannuksien 10 prosenttia hankinnan kokonaiskustannuksista.



Kuvio 9. Tietoturvasertifikaattihankinnan kokonaiskustannuksien jakautuminen prosenttiosuuksin kokonaiskustannuksista.

6 YHTEENVETO SEKÄ JOHTOPÄÄTÖKSET

Riskienhallinta on yritystoiminnan yksi tärkeimpiä tehtäviä. Riskien tehokkaalla ja toimivalla hallinnalla pystytään varmistamaan yrityksen toimintaedellytykset yllättävissäkin tilanteissa. Riskin toteutuminen aiheuttaa lähes aina jonkin arvon menetyksiä, toisaalta riskienhallinta voi olla yritykselle myös kilpailutekijä.

Tietotekniikan kehitys on pakottanut yrityksien panostamaan tietoriskien hallintaan. Tietoriskien hallintaa vaikeuttaa se, että riskin aiheuttajaksi on monia eri vaihtoehtoja. Tietoriskin aiheuttaja voi olla vaikka nykyinen tai entinen työntekijä, rikollinen, tekninen vika tai vaikkapa vesivahinko. Tietoriskeille ominaista on myös se, että riskin toteutuessa menetykset voivat olla suuria, pahimmillaan koko yritystoiminnan jatkuminen voi olla uhattuna. ISO 27001- tietoturvastandardi on nimenomaan tietoriskien hallintaan tarkoitettu työkalu yrityksille.

ISO 27001- tietoturvasertifikaattihankinnan voidaan ajatella kuuluvan pakollisiin ja muihin tuottamattomiin investointeihin, joten sillä ei ole tuottovaatimusta. Vaikka ISO 27001- sertifikaattihankinnan ei oleteta tuovan yritykselle tuottoa, hankinnan merkitys saattaa olla yritykselle todella suuri. Vakavan tietoriskin toteutuminen voi mahdollisesti lopettaa koko yritystoiminnan. Yhdenkin tämänlaisen tilanteen välttäminen sertifioidun tietoturvallisuuden hallintajärjestelmän avulla tekee hankinnasta yritykselle kannattavan.

ISO 27001- tietoturvastandardin vaatimusten mukaisesti rakennettu tietoturvallisuuden hallintajärjestelmä vahvistaa yrityksen toimintaedellytyksiä ja antaa hyvät työkalut yrityksen tietoturvan jatkuvaan parantamiseen. Yritykselle myönnetty tietoturvasertifikaatti viestii sidosryhmille yrityksen luotettavasta sekä vaikuttavasta tietoturvan hallinnasta. ISO 27001- tietoturvasertifikaatin hankinta vaatii yritykseltä isoja panostuksia sekä koko henkilöstön sitoutumista tietototurvallisuuden kehittämiseen ja ylläpitämiseen.

Yrityksen tietoturvallisuuden lähtötaso vaikuttaa tietoturvallisuuden hallintajärjestelmään tarvittavan kehitystyön määrään. ISO 27001- standardin vaatimuksiin vastaaminen vaatii todennäköisesti monessa organisaatiossa paljon sisäistä kehitystyötä, mikäli kyseessä olevan yrityksen tietoturvallisuuden hallintajärjestelmää ei ole aikaisemmin laajasti ja suunnitelmallisesti kehitetty. Sertifioidun tietoturvallisuuden hallintajärjestelmän ylläpito vaatii paljon työpanosta koko organisaatiolta ja ylläpitokustannukset ovat suurin osa sertifikaattihankinnan kokonaiskustannuksista. Ulkoisesta auditoijasta koituvien kustannuksien arvioitiin olevan vain pieni osa tietoturvasertifikaattihankinnan kokonaiskustannuksiin verraten.

Kohdeyrityksessä tietoturvallisuuden lähtötaso koettiin hyväksi, mutta standardin laajuuden vuoksi tietoturvaan liittyvään sisäiseen kehitystyöhön arvioitiin kuluvan yhteensä 450 tuntia, jolloin tietoturvallisuuden hallintajärjestelmän kehitystyön arvioiduksi euromääräiseksi kustannukseksi muodostui 27 000 euroa. Yrityksellä nähtiin olevan tarvittavat laitteet ja ohjelmistot, joten kehitystyöhön ei arvioitu tarvittavan muita laite- tai ohjelmistohankintoja. Sertifioidun tietoturvallisuuden hallintajärjestelmän ylläpitoon arvioitiin tarvittavan vuosittain 200 työtuntia, jolloin euromääräisiksi kustannuksiksi muodostui 12 000 euroa. Lisäksi arvioitiin tarvittavan

2 000 euroa esimerkiksi tietoturvaohjelmistoihin ja palvelimiin. Tällöin vuosittaisiksi ylläpitokustannuksiksi muodostui 14 000 euroa, eli sertifikaatin 3 vuoden voimassaoloajalta ylläpitokustannukset olisivat yhteensä 42 000 euroa. Kohdeyritykselle auditoijasta koituviksi kustannuksiksi arvioitiin 3 vuoden ajalta yhteensä 7 480 euroa, olettaen ettei ylimääräisiä auditointikäyntejä tarvita.

ISO 27001 -tietoturvasertifikaatin hankinta on raskas sekä aikaa vievä prosessi. Prosessista aiheutuu yritykselle toimialasta ja yrityksen koosta riippumatta merkittäviä lisäkustannuksia. Lisäksi hankinta vaatii organisaatiolta jatkuvaa sitoutumista tietoturvallisuuden ylläpitämiseen, kehittämiseen ja jatkuvaan parantamiseen. Vastineeksi tästä panostuksesta organisaatio saavuttaa erinomaisen tietoturvan tason ja valmiuidet vastata nykypäivän sekä tulevaisuuden tietoturvallisuuden jatkuvasti muuttuviin haasteisiin.

Tutkimuksen tuloksena syntyneiden kustannus- ja työmääräarvioiden perusteella yrityksen johto voi arvioida tietoturvasertifikaattihankinnan kannattavuutta kohdeyritykselle. Saatujen tuloksien avulla voidaan myös välittömästi aloittaa tietoturvan kohdennetut kehittämistoimenpiteet yrityksen toiminnan tietyillä osa-alueilla.

LÄHTEET

Bradgon, B. 2017. 2018 Global State of Information Security Survey. Viitattu 22.2.2019. https://www.idg.com/tools-for-marketers/2018-global-state-information-security-survey/

Bureau Veritas. 2019. ISO 27001 sertifiointi. Viitattu 5.2.2019. https://www.bureauveritas.fi/e3af93004db0c46a9b5fdf10c0640809/BureService_ISO27001_FI_web.pdf?MOD=AJPERES&CACHEID=e3af93004db0c46a9b5fdf10c0640809

Campbell, T. 2016. Practical Information Security Management: A Complete Guide to Planning and Implementation. New York: Apress. Viitattu 26.2.2019. https://www.apress.com/us/book/9781484216842

Elinkeinoelämän keskusliiton www-sivut. 2019. Yrityslainsäädäntö. Viitattu 3.9.2019. https://ek.fi/mita-teemme/yrityslainsaadanto/

Finas www-sivut. 2019. Sertifiointiorganisaatiot. Viitattu 21.8.2019. https://www.finas.fi/akkreditointi/Akkreditointialueet/Sivut/Sertifiointiorganisaatiot.aspx

Ikäheimo, S., Malmi, T. & Walden, R. 2016. Yrityksen laskentatoimi. 6. uud. p. Helsinki: Talentum Pro.

ISO/IEC 27001:fi. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. 2017. Suomen Standardisoimisliitto SFS. Helsinki: SFS.

Itä-Suomen yliopiston www-sivut. 2019. Auditointi. Viitattu 17.7.2019. http://www.uef.fi/auditointi

Juvonen, M., Koskensyrjä, M., Kuhanen, L., Ojala, V., Pentti, A., Porvari, P. & Talala, T. 2014. Yrityksen riskienhallinta. Helsinki: Finva. Viitattu: 4.7.2019

Järvenpää, M., Länsiluoto, A., Partanen, V. & Pellinen, J. 2013. Talousohjaus ja tuloslaskenta. 2. uud. p. Helsinki: Sanoma Pro Oy

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Helsinki: Alma Talent

Kaspersky Lab. 2015. Damage Control: The Cost Of Security Breaches. Viitattu 22.2.2019. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf

Korkiamäki, J., Laukkala, H., Mustonen, J., Peltonen, J., Vesterinen, P. & Heljaste, J. 2008. Yrityksen turvallisuusopas. Helsinki: Helsingin kauppakamari. Viitattu 27.3.2019. https://www.ellibslibrary.com/book/9789529982363

Kuusela, H. & Ollikainen, R. 2009. Riskit ja riskienhallinta. 2. uud. p. Tampere: Tampereen Yliopistopaino Oy

Ojasalo, K. Moilanen, T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro. Viitattu 4.3.2019. https://samk.finna.fi/Record/tyrni.120570

Pitkäranta, A. 2014. Laadullinen tutkimus opinnäytetyönä – Työkirja ammattikorkeakouluun. Jokioinen: e-Oppi Oy. Viitattu 3.4.2019. https://www.elibslibrary.com/book/9789522828019

PK-RH. 2019. Pk-yrityksen riskienhallinta. Viitattu 17.7.2019. http://virtual.vtt.fi/virtual/pkrh/startti-riskienhallintaan/mita-riskienhallinta-on/riskien-hallintakeinoja/tunnistettujen-riskien-hallintakeinoja/index.html

Rautiainen. ´Tietoturvan kolme kovaa: Luottamuksellisuus, eheys ja saatavuus´. Juhan IT-blogi. 25.8.2013. Viitattu 28.3.2019. https://juhanit.wordpress.com/2013/08/25/tietoturvallisuuden-kolme-kovaa-luottamuksellisuus-eheys-ja-saatavuus/

Suomen riskienhallintayhdistyksen www-sivut. 2019. PK-RH-riskienhallinta. Viitattu 29.3.2019. https://www.pk-rh.fi/riskienhallinta.html

Suomen riskienhallintayhdistyksen www-sivut. 2019. Tietoriskien hallinta. Tietoriskit. Viitattu 12.8.2019. https://www.pk-rh.fi/uploads/riskikartat/tietoriskikartta.pdf

Suominen, A. 2003. Riskienhallinta. 3. uud. p. Vantaa: Dark Oy.

Traficom www-sivut. 2019. Teleyritysten tietoturvahavainnot. Viitattu 21.2.2019. https://www.traficom.fi/fi/teleyritysten-tietoturvahavainnot

Yksityisyydensuoja www-sivut. 2019. Tietoturva. Viitattu 28.3.2019. https://www.yksityisyydensuoja.fi/tietoturva

Yritystulkki www-sivut. 2019. Liiketoimintasuunnitelmat. Viitattu 3.9.2019. https://www.yritystulkki.fi/fi/alue/oulu/aloittava-yrittaja/suunnittelu/liiketoimintasuunnitelmat/

VAHTI. 2016. Tietoturvapoikkeamatilanteiden hallinta. Viitattu 17.7.2019. https://vm.fi/documents/10623/3176167/VAHTI+3-2016+Tietoturvapoikkeamien+hallinta-ohjeen+lausuntoversio/7c691366-ff70-45e1-b650-a3abfce6c325/VAHTI+3-2016+Tietoturvapoikkeamien+hallinta-ohjeen+lausuntoversio.pdf

VAHTI. 2017. Ohje riskienhallintaan – LIITTEET 1-6. Viitattu 17.7.2019. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/Liitteet_VM22_2017.pdf

Valtiovarainministeriö. 2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. Viitattu 16.7.2019. https://www.vahtiohje.fi/c/document_library/get_file?uuid=b3a59fa6-570f-4cd6-9a67-79e34f3c4b38&groupId=10229

VAHTI 2. 2016. Toiminnan jatkuvuuden hallinta. Viitattu 29.8.2019. https://www.vahtiohje.fi/web/guest/vahti-2/2016