Ehdotus ISO/IEC 27001 standardin vaatimukset täyttävästä riskienhallintamallista

Rauno Tikka

2020 Laurea

Laurea-ammattikorkeakoulu

Ehdotus ISO/IEC 27001 standardin vaatimukset täyttävästä riskienhallintamallista

Rauno Tikka
Tietojenkäsittelyn koulutus
Opinnäytetyö
4/20

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tietojenkäsittelyn koulutus
Liiketalouden ammattikorkeakoulututkinto (AMK)

Rauno Tikka
Ehdotus ISO27001 vaatimukset täyttävästä riskienhallintamallista
Vuosi 2020 Sivumäärä 24

Opinnäytetyön tavoitteena oli luoda yritykselle ISO/IEC 27001 standardin vaatimukset täyttävä riskienhallintamalli. Työn tilaajana oli kansainvälinen tietoturva-alalla toimiva IT-Asiantuntijayritys. Projektin alkaessa yritys oli jo aloittanut projektin tulla ISO/IEC 27001 sertifioiduksi ja tämä työ on osa sitä kokonaisuutta. Yritys käyttää työkalunaan Certikitin dokumenttipohjia.

Tietoperustana käytettiin ISO/IEC 27000 standardisarjaa joista oleellisimmat ovat ISO/IEC 27001:2017 sekä ISO/IEC 27005:2018. ISO/IEC 27001 standardissa kuvataan tietoturvallisuuden hallintajärjestelmän vaatimukset ja riskienhallinta on oleellisessa osassa tietoturvallisuuden hallintajärjestelmää. Ohjestandardi ISO/IEC 27005:2018 käsittelee riskienhallintaa ja on tukena ISO/IEC 27001 standardin mukaiseen riskienhallintamalliin.

Opinnäytetyössä käydään aluksi läpi lyhyesti ISO/IEC 27001 standardi ja pidemmin ISO/IEC 27005 standardin sisältö sekä vaatimuksia. Tämän jälkeen esitellään lista yritykselle tuotetuista dokumenteista ja ehdottamani määrittelyt peruskriteereille, organisaation perustamiselle sekä esitellään ehdotettu riskienhallintaprosessi. Riskienhallinnan organisaatioksi ehdotettiin seuraavia rooleja: tietoturvan ohjausryhmä, tietoturvapäällikkö ja tietoturvan ylläpitäjä. Lopuksi ehdotan kahta vuosikelloa yritykselle. Kaksi sen takia, koska ensimmäinen on ensimmäiselle vuodelle sekä toinen on toiselle vuodelle. Etenkin toisen vuoden vuosikellon sisältö täytyy analysoida, kun ensimmäinen sykli on suoritettu. Lopulliset dokumentit kirjoitettiin Certikitin dokumenttipohjiin, jotka on määritelty salassa pidettäviksi. Riskienhallintamallia on kuitenkin vielä kehiteltävä etenkin viestinnän osalta, kun tietoturvallisuuden hallintajärjestelmän viestintätavat ovat vasta vakioitumassa.

Asiasanat: ISO27005, Riskienhallinta, ISO27001, Tietoturva, ISMS

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

Rauno Tikka

A Proposal for an ISO/IEC 27001 Compliant Risk Management Model

Year 2020 Pages 24

The goal of this thesis was to create a risk management model that is compliant to ISO/IEC 27001 standard. The beneficiary of this project is an IT-company that works in the cybersecurity field. By the time this thesis project was started the company already had made efforts to start the project to become ISO/IEC 27001 compliant as a company and this thesis project was a part of that effort. The company uses document templates provided by Certikit for its certification efforts.

The knowledge base used was the ISO/IEC 27000 standard family of which the most used were ISO/IEC 27001:2017 and ISO/IEC 27005:2018. ISO/IEC 27001 standard is about information security management system (ISMS) and risk management is a key part of the overall ISMS implementation. ISO/IEC 27005 provides guides to risk management and supports ISO/IEC 27001 standard.

This thesis goes briefly through ISO/IEC 27001 standard and ISO/IEC 27005 requirements a bit more in depth. After this a list of created documents for the company is presented followed by proposed specifications for basic criteria and information security risk management roles. The following roles were suggested for the Company: Information security steering group, information security manager and information security administrator. Two annual clocks are presented, one for the first year and one for the second year. The contents of the second annual clock particularly should be reviewed after the first risk management cycle is completed. Final documents were written into Certikits document templates that are classified as internal information only. The risk management process still needs more refining particularly in the communication. This is partially because the company is still working on the communication program for the information security management system.

Keywords: ISO27005, Risk Management, ISO27001, ISMS, cybersecurity

Sisällys

Käsitteet ja lyhenteet

ISO: International Standards Organization

IEC: International Electrotechnical Commission

SFS: Suomen Standardoimisliitto

ISMS: Information Security Management System, suomeksi tietoturvan hallintajärjestelmä

Jäännösriski: Riskien hallintakeinojen valinnan jälkeen jäljelle jäävä riski

1 Johdanto

Opinnäytetyön tavoitteena oli suunnitella opinnäytetyön toimeksiantajalle ISO/IEC 27001-Standardin vaatimukset täyttävä riskienhallintamalli. Lopullinen tavoite yrityksellä on saada ISO/IEC 27001 sertifikaatti. Kun yrityksen tarve yhdistyi kiinnostukseeni tietoturvallisista käytännöistä sekä halustani opiskella ISO/IEC 27000 standardiperheestä syvemmin oli päätös lähteä toteuttamaan tätä projektia päivänselkeä.

Työ on rajattu riskienhallintaan, joka on osa ISO/IEC 27001 standardia. Riskienhallinta on kuitenkin oleellinen osa tietoturvallisuuden hallintajärjestelmää, joten yrityksellä oli kiinnostus saada riskienhallintamalli implementoitua toimintoihinsa. Vuosikellojen tekemisessä keskitytään vain riskienhallintamalliin, eikä niinkään kaikkiin tietoturvallisuuden hallintajärjestelmän toimintoihin. Nämä sisältävät pääasiassa katselmuksen, riskien arvioinnin ja hallintakeinojen implementoinnin. Käytännössä malli muistuttaa hyvin läheisesti plan, do, check, act sykliä.

Opinnäytetyössä kuvataan ensiksi lyhyesti ISO/IEC 27000 standardisarjan standardeja ja niiden suhteita toisiinsa. Yleisen kuvailun jälkeen syvennytään tarkemmin ISO/IEC 27005 vaatimuksiin, jonka jälkeen ehdotetaan riskienhallintamallia yritykselle.

2 Opinnäytetyön toimeksiantajasta

Opinnäytetyön toimeksiantaja on kansainvälinen tietoturva-alalla toimiva yritys. Toimialansa arkaluonteisuuden perusteella yritys ei halunnut nimeään näkyville opinnäytetyöhön.

Yrityksellä on Suomen ulkopuolella sijaitsevia toimipisteitä, jotka on jo ISO/IEC 27001 sertifioitu ja yrityksen tavoitteena on saada kaikki muutkin toimipisteet ISO/IEC 27001 sertifioitua. Opinnäytetyötä aloittaessani oli jo sertifiointiprosessi käynnissä. Huomioon otettavaa on, että yrityksellä on jo useita riskien hallintakeinoja käytössään sekä joitain tietoturvalinjauksia jo tehtynä.

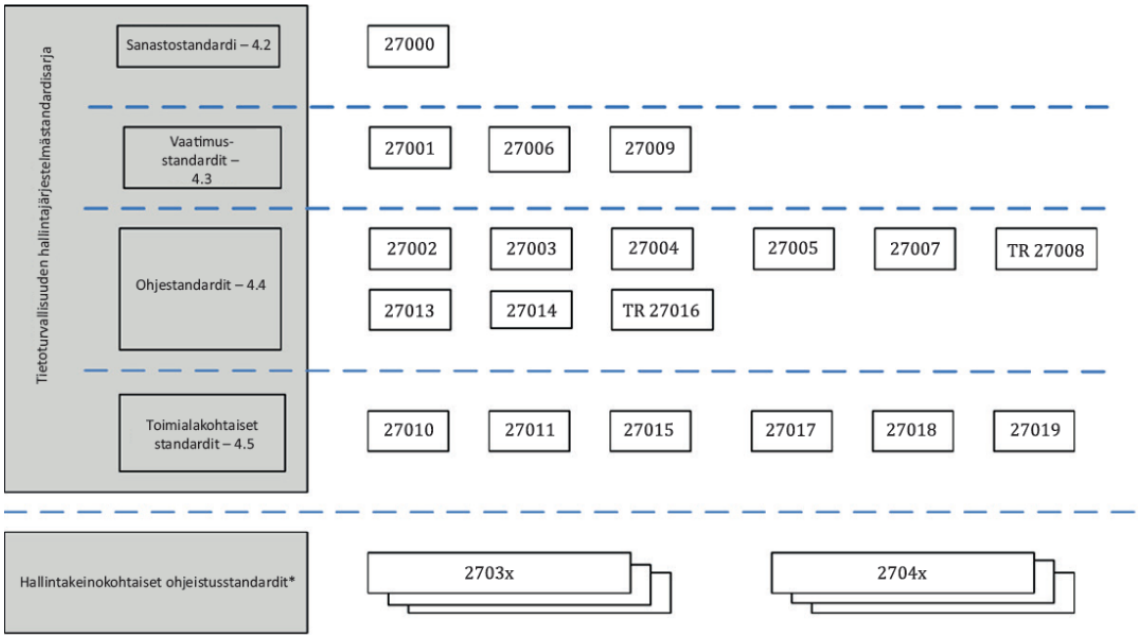
3 Tietoperusta

Kohdeyrityksen ISO/IEC 27001 sertifiointiprosessiin otettiin pääasialliseksi työkaluksi Certikitin tarjoama ”ISO 27001 toolkit” joka tarjoaa dokumenttipohjat ISO/IEC 27001 standardille sekä ohjeistukset dokumenttien käyttämiselle. Nämä dokumentit on kuitenkin muokattava kullekin yritykselle sopivaksi sisällöltään. Certikitin dokumenttipohjien ohjeiden lisäksi myös SFS-EN ISO/IEC 27001 ja SFS-EN ISO/IEC 27005 standardeja käytettiin lähteinä. SFS-EN ISO/IEC versiot

standardista ovat Suomen standardisoimisliiton julkaisemia ja suomentamia. Kirjaa ”Implementing the ISO/IEC 27001:2013 ISMS Standard” käytettiin ohjeistuksena implementoinnille. ISO/IEC 27001:2013 standardiin perustuva ohjekirja käy sisällöltään hyvin tähän työhön, vaikka uusin sertifikaatti onkin ISO/IEC 27001:2017. Tämä perusteltiin sillä, että vuoden 2017 päivitys ei tuonut mitään uusia vaatimuksia sertifikaatille. (Is partners 2019.)

4 ISO/IEC 27000 Standardisarjasta yleisesti

ISO/IEC 27000 standardisarja koostuu useasta eri standardista, jotka on esitetty kuviossa 1.



Kuvio 1: ISO/IEC 27000 standardiperhe. (SFS-EN ISO/IEC 27000, 26.)

Tämän opinnäytetyön kannalta relevantit standardit ovat ”ISO/IEC 27001 informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset.” ja ”ISO/IEC 27005 Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta”. ISO/IEC 27001 standardissa määritellään vaatimukset koskien tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitoa ja jatkuvaa parantamista organisaation toimintaympäristössä. (SFS-EN ISO/IEC 27000, 27). ISO/IEC 27005 standardi sisältää ohjeistuksen tietoturvariskien hallintaan, kuitenkaan vaatimatta mitään tiettyä riskienhallintamenetelmää vaan menetelmä jätetään yrityksen valittavaksi.

Muut keskeisimmät standardit mitkä kuuluvat ISO/IEC 27000 Standardisarjaan ovat:

- ISO/IEC 27000 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto.

- ISO/IEC 27002 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintakeinojen menettelyohjeet. Tässä standardissa selvitetään ohjeet ISO/IEC 27001 standardin liite A:n hallintakäytännöille.
- ISO/IEC 27003 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Ohjeistusta. Tässä standardissa annetaan ISO/IEC 27001 standardiin ohjeistusta.
- ISO/IEC 27004 Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. Tämä standardi avustaa tietoturvallisuuden hallintajärjestelmän vaikuttavuuden analysoimista.
- ISO/IEC 27007 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmien auditointiohjeet. Tämä standardi sisältää kokonaisvaltaiset ohjeet tietoturvallisuuden hallintajärjestelmän auditoinnille sekä auditointiohjelmien hallinnalle.

4.1 ISO/IEC 27001 Standardista

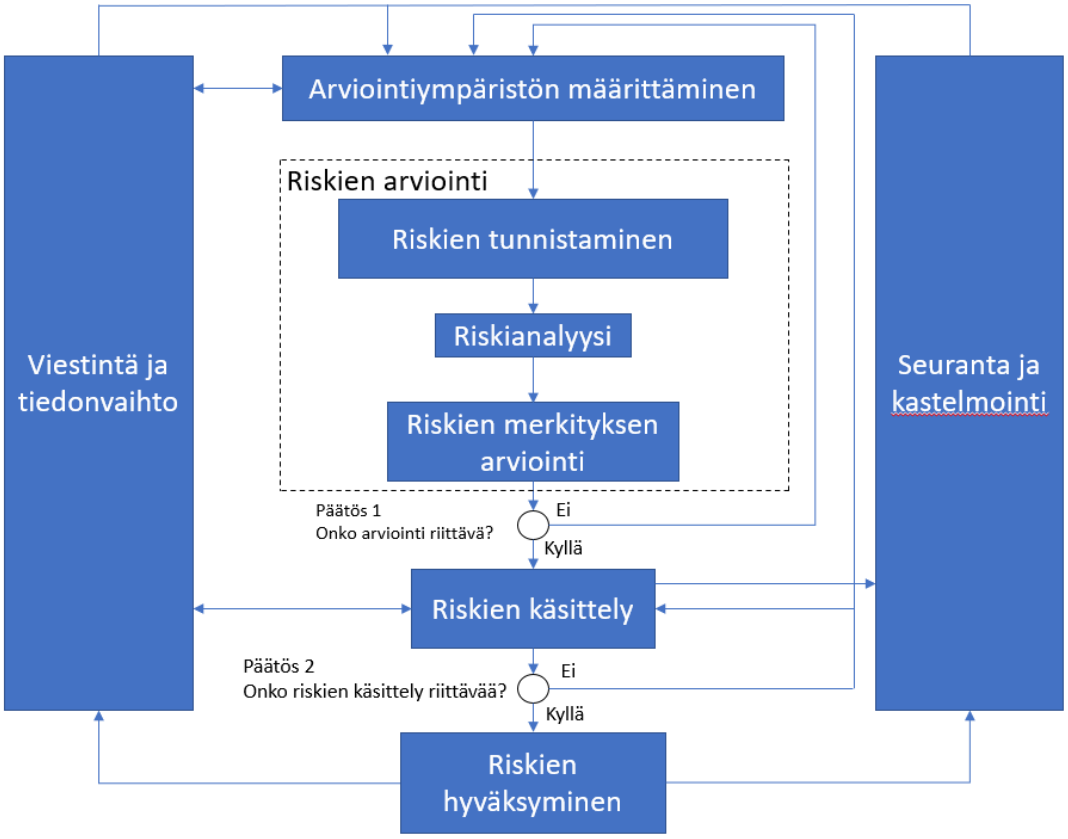
ISO/IEC 27001 on kansainvälinen tietoturvallisuuden hallintajärjestelmän standardi. Se perustuu riskien arviointiin ja organisaation riskien hyväksyntätasoihin, jotka on suunniteltu riskien tehokasta käsittelyä ja hallintaa varten. (SFS-EN ISO/IEC 27000:2017, 19). ISO/IEC 27001 asettaa kriteerit tietoturvariskien tunnistamiselle, arvioinnille sekä käsittelyprosessille. Lisäksi yrityksen on laadittava soveltuvuuslausunto, joka sisältää perustelut liitteen A hallintakeinojen käyttämiselle tai käyttämättä jättämiselle. (SFS-EN ISO/IEC 27001:2017, 9). ISO/IEC 27005 ei tarjoa suoraa ohjeistusta riskienhallintamallille joka täyttää ISO/IEC 27001 standardin vaatimukset. ISO/IEC 27001 standardiin sisältyy myös liite A, jossa listataan yleisesti parhaaksi hyväksyttyjä uhkien hallintakeinoja. Liite A:ssa listattuja hallintakeinoja ei ole pakko käyttää, mutta on pakollista koostaa soveltuvuuslausunto.

4.2 ISO/IEC 27005 Standardista

ISO/IEC 27005 on ohjestandardi, joka tukee ISO/IEC 27001 tietoturvallisuuden hallintajärjestelmän standardin implementointia. ISO/IEC 27005 perustuu tietoturvallisuuden riskienhallintaan, toisin kuin ISO/IEC 31000 joka käsittelee riskienhallintaa yleisesti. (The risk academy 2018.)

4.3 Hallintaprosessi yleisesti

Tietoturvan hallintaprosessi koostuu kuudesta kohdasta. Nämä ovat: Toimintaympäristön määrittäminen, riskien arviointi, riskien käsittely, riskien hyväksyntä, riskejä koskeva viestintä ja tiedonvaihto sekä riskien seurannasta ja katselmoinnista. (SFS-ISO/IEC 27005 2018, 9). Kuviossa 2 on kuvattuna prosessin eteneminen ja suhteita toisiinsa.



Kuvio 2: ISO/IEC 27005 Riskienhallintaprosessi (SFS-EN ISO/IEC 27005:2018, 8.)

4.4 Toimintaympäristön määrittäminen

ISO/IEC 27005 standardin mukaisessa riskienhallinnassa on määriteltävä sekä ulkoinen ja sisäinen toimintaympäristön hallinta. Määritelmään liittyy peruskriteerien asettaminen, laajuuden ja rajojen määrittäminen sekä tietoturvariskien hallintaan liittyvän organisaation perustaminen. Peruskriteerit ISO/IEC 27005 sertifikaatin mukaisessa riskienhallinnassa ovat: Riskienhallintaan perustuva toimintamalli, riskien merkityksen arviointikriteerit, vaikutuskriteerit, riskien hyväksymiskriteerit. (SFS-EN ISO/IEC 27005:2018, 10.)

Riskienhallintaan perustuva toimintamallin peruskriteeri pitää sisällään vaatimuksen valita tai kehittää soveltuva toimintamalli, jossa tarkastellaan kolmea peruskriteeriä: riskien merkityksen arviointikriteerejä, vaikutuskriteerit ja riskien hyväksymiseen liittyvät kriteerit. (SFS-EN ISO/IEC 27005:2018, 11.)

Riskien merkityksen arviointikriteereissä on otettava huomioon eri liiketoiminnan osa-alueita ja riskin realisoitumisen haitalliset arvot maineelle ja liikearvolle. Näitä arviointikriteerit on käytettävissä myös riskien käsittelyn tärkeysjärjestyksen määrittelyssä. (SFS-EN ISO/IEC 27005:2018, 11.)

Vaikutuskriteereissä organisaation on arvioitava tietoturvatapahtuman aiheuttaman vahingon tai kustannuksen taso huomioiden suojattavan tiedon luokitustaso, vaikutus organisaation toimintoihin ja liiketoimintatappiot sekä rahallinen arvo. (SFS-EN ISO/IEC 27005:2018, 11-12.)

Riskien hyväksymiskriteereissä asetetaan vaatimus, että organisaatio määrittelee kriteerit riskien hyväksymiselle. Kukin organisaatio määrittelee itse omat riskien hyväksymistasonsa. (SFS-EN ISO/IEC 27005:2018, 12.)

Jotta varmistuisi, että kaikki oleellinen on riskienhallinnan piirissä, täytyy määritellä riskienhallintaprosessin laajuus ja rajat. Mikäli organisaatio haluaa jättää osa-alueita pois laajuudesta täytyy perustella syyt miksi jokin on jätetty pois. (SFS-EN ISO/IEC 27005:2018, 12-13.)

Viimeisenä on vaatimus perustaa organisaatio ja jakaa vastuut sekä oikeudet organisaation kaikille jäsenille. Tämä organisaatio on oltava ylimmän johdon hyväksymä. (SFS-EN ISO/IEC 27005:2018, 13.)

4.5 Tietoturvariskien arviointi

Tietoturvariskien arviointi koostuu kolmesta osasta: Riskien tunnistaminen, riskien analyysi ja riskien merkityksen analysointi. Riskien tunnistamisessa ohjeistetaan perusteelliseen analyysiin ja riskien tunnistusprosessin täytyy kattaa kaikki riskit. Huomioon on otettava esimerkiksi haavoittuvuudet, mahdolliset yritykseen kohdistuvat uhat ja yrityksellä jo käytössä olevat riskienhallintakeinot. (SFS-EN ISO/IEC 27005:2018, 13-21.)

4.6 Tietoturvariskien käsittely

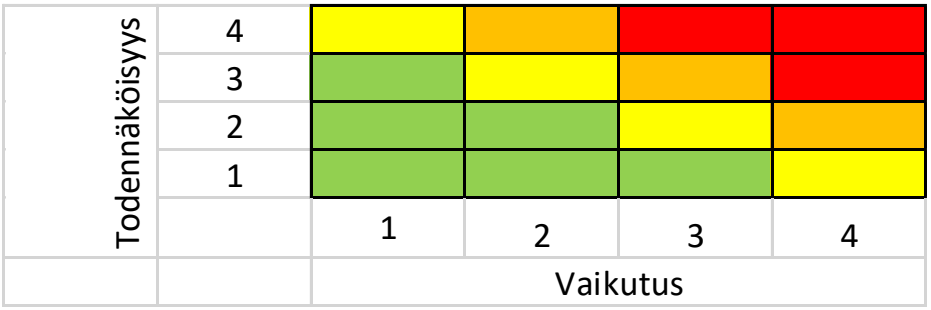
Tietoturvariskien käsittelyn lähtökohtana on se, että riskien tunnistaminen on tehty ja riskit on asetettu tärkeysjärjestykseen. Kun riskien listaus on tehty, täytyy valita riskienkäsittelytapa seuraavista vaihtoehdoista: Riskin muokkaaminen, riskin säilyttäminen, riskin välttäminen ja riskin jakaminen.

- Riskin muokkaamisella tarkoitetaan sitä, että valitaan hallintakeinot riskille, jolloin jäännösriski on hyväksyttävällä tasolla yrityksen linjaukseen nähden.
- Riski voidaan myös halutessaan perustellusti hyväksyä ja säilyttää sellaisenaan.
- Riskin välttämisellä tarkoitetaan sellaisten toimintojen lopettaminen kokonaan, jotka aiheuttaa riskiarvoiltaan liian ison riskin tietoturvariskien hyväksymisarvoon nähden.

Riskin jakaminen on toiminto jossa riski jaetaan tai siirretään jollekin muulle toimijalle. Esimerkiksi yksi yleinen tapa on vakuuttaminen jolloin osa riskistä siirtyy vakuutusyhtiölle. (Kyberturvallisuuskeskus 2019.)

4.7 Riskikertoimien arviointi

Yrityksen on määritettävä hyväksyttävät riskiarvot, joilla riski voidaan hyväksyä eikä toimenpiteitä tarvitse tehdä. Tässä voi käyttää apuna kuvion 3 mukaista riskimatriisia.



Kuvio 1: Esimerkki riskimatriisista

Riskienhallinnassa on asetettava kullekin riskille arvot todennäköisyydelle sekä vaikutukselle ja verrattava lopullista arvoa riskimatriisiin. Kuviossa vihreällä olevat arvot ovat hyväksyttävissä olevia riskejä, kun taas keltaiset, oranssit ja punaiset kriittisempiä. Riskimatriisin hyväksyttävät arvot vaihtelevat tapauskohtaisesti ja jokaisen yrityksen tulisi määritellä omat arvot sille mikä on hyväksyttävä riskiarvo. (Humphreys 2016, 50.)

4.8 Tietoturvariskejä koskeva viestintä ja tiedonvaihto

Riskienhallinnassa toimivalla viestinnällä on kriittinen rooli, sillä ilman toimivaa tiedonvaihtoa ei pystytä takaamaan, että jokaisella on riittävä tietopohja päätöksille. Yleinen tietoturvallisuuden tietoisuus myös kärsii, mikäli viestintä tietoturvauhista ja hallintakeinoista yrityksen jokaiselle työntekijälle on puutteellinen.

4.9 Tietoturvariskienhallinnan seuranta, katselmointi ja parantaminen

ISO/IEC 27001:2005 standardissa oli vaatimus plan-do-check-act prosessista, mutta tämä vaatimus on poistettu myöhemmistä ISO/IEC 27001 standardeista. ISO/IEC 27001 standardissa määritellään kuitenkin vaatimus jatkuvasta parannuksesta koko tietoturvallisuuden hallintajärjestelmälle ja riskienhallinta on osa sitä. Täten riskienhallinnan seurannan, katselmoinnin ja parantamisen on oltava järjestelmällistä ja jatkuvaa toimintaa.

5 Riskienhallintamalli yritykselle

5.1 Yritykselle luodut dokumentit

Projektin aikana tuotettiin dokumentteja, joissa määritellään riskienhallinnan vaiheet sekä alustava vuosikello. Kuvaukset riskienhallintaprosessin rooleista ja vastuista lisättiin jo olemassa olevaan ISMS dokumenttiin, jossa määriteltiin tietoturvallisuuden hallintajärjestelmän ylläpitoon vaaditut roolit. Riskienhallintaa varten tuotettiin seuraavat dokumentit:

- Riskien arviointi ja riskien käsittelyprosessi
- Ensimmäisen riskien arviointikokouksen agenda
- Johdon katselmuskokouksen alustava agenda
- Alustava resurssiluettelo

Seuraavat dokumentit on valmisteltu valmiiksi käytettäväksi:

- Resurssipohjainen riskien tunnistamistyökalu
- Riskien käsittelyprosessin raportti
- Suunnitelma riskien käsittelylle

Yritykselle luodut dokumentit yhdessä muokattujen ISMS dokumenttien kanssa täyttävät ISO/IEC 27001 standardissa määritellyt kriteerit. Näiden dokumenttien sisältöä kuvaillaan seuraavissa kappaleissa.

5.2 Toimintaympäristön määrittäminen

Riskienhallintamallia aloittaessani yrityksellä oli toimintaympäristön määrittäminen jo kuvailtuna ja ISMS laajuus päätettynä. Toimintaympäristön määrittämisessä kirjataan yrityksen tiedot, yrityksen tarjoamat palvelut, myytävät tuotteet ja yhteistyökumppanit. Käytännössä tavoitteena on määritellä konteksti, jossa ISMS ja siten myös riskienhallintamalli toimii. Tässä opinnäytetyössä ei kuvata yrityksen sisäistä tai ulkoista toimintaympäristöä tietoturvasyihin vedoten. Mikäli nämä kuvattaisiin tähän työhön, saattaisi opinnäytetyön toimeksiantaja olla pääteltävissä.

Yksittäisten riskienhallintatyöpajan toimintaympäristö, laajuus ja rajat kirjataan ”riskien käsittelyprosessin raportti” dokumenttiin. Nämä voivat olla eri kuin ISMS:ssä määritetyt laajuus ja rajat, sillä esimerkiksi tarve ylimääräiselle riskienhallintatyöpajalle voi olla äkisti muuttuneet olosuhteet, jolloin saatetaan tarkastella hyvinkin rajattua ilmiötä. Ensimmäisten riskienhallintatyöpajojen kuuluisi kattaa koko ISMS laajuus, jotta koko ISMS laajuus saadaan suojattua asianmukaisesti.

6 Peruskriteerien täyttäminen

6.1 Riskien merkityksen arviointikriteerit

Ehdotukseni yritykselle on käyttää Certikitin suosittelemaa resurssipohjaista (eng. Asset based) riskienhallintamallia. Ehdottomassani mallissa riskien tunnistaminen koostuu resurssiluettelon kokoamisesta ja jo olemassa olevien hallintakeinojen arvioinnista. Resurssiluettelossa arvioidaan riskien merkityksen arviointikriteereitä.

6.2 Resurssiluettelon kokoaminen

Resurssipohjaisessa riskienhallinnassa aluksi kootaan kaikki resurssit tärkeysjärjestyksessä ja kategorisoidaan seuraavin ehdoin: Lakisääteinen vaatimus, taloudellinen arvo, liiketoiminnan kriittisyys, herkkyys luvattomalle näkyvyydelle tai muokkaamiselle, sisältääkö resurssi henkilötietoja, resurssin tietoturvaluokitus ja resurssin sijainti. Kuviossa 4 esitellään esimerkki resurssiluettelosta.

Resurssin nimi	Resurssin tyyppi	Onko lakisääteisiä vaatimuksia?	Taloudellinen arvo	Kriittisyys liiketoiminnalle	Herkkyys luvattomalle muokkaamiselle tai näkyvyydelle	Sisältääkö henkilötietoja?	Tietoturvaluokitus	Sijainti
Resurssin nimi	Esimerkiksi: software, hardware, työvoima	Kyllä/ei	Pieni/keskikokoinen/iso	Pieni/keskikoinen/iso	pieni/keskikokoinen/iso	Kyllä/Ei	Yrityksen sisäisen politiikan mukaan	Resurssin sijainti

Kuvio 3: Esimerkki resurssiluettelosta

6.3 Vaikutuskriteerit

Jotta riskienhallintatyöpajoilla saadaan tuotettua arviointeja, jotka ovat toistettavissa täytyy määritellä kriteerit eri arvoille. Riskien realisoitumisen vaikutus arvostellaan taulukon 1 ja 2 mukaisesti asteikolla 1-5 seuraavissa kategorioissa: Asiakasvaikutukset, taloudelliset vaikutukset, uhka terveydelle ja turvallisuudelle, vaikutus maineelle, oikeudellinen vaikutus. Taulukot sisältävät myös kuvaukset riskien realisoitumisen vaikutuksista kullakin arvolla.

Pis-tey-tys	Sanallinen Kuvaus	Asiakasvaikutukset	Taloudelliset vaikutukset
1	Merkityksetön	Ei vaikutusta	Vähäinen tai ei ollenkaan
2	Vähäinen	Joitain häiriöitä normaa-leille liiketoiminnoille	Joitain
3	Keskisuuri	Kykenee silti liiketoimintaan joillakin vaikeuksilla	Ei toivottavaa, mutta kuitenkin siedettävissä
4	Suuri	Kriittiset toiminnot ovat lamaantuneet	Vakava vaikutus tuloille ja liikevoitolle
5	Erittäin suuri	Liiketoiminta on lakannut kokonaan	Lamauttava: Yrityksen on hakeuduttava konkurssiin

Taulukko 1: Certikitin ohjeistuksen mukainen vaikutusten arviointi

Pis-tey-tys	Uhka terveydelle ja turvalli-suudelle	Vaikutus maineelle	Oikeudellinen vaikutus
1	Hyvin pieni riski	Vähäinen vaiku-tus	Ei vaikutusta
2	Hyväksyttävien rajojen puitteissa	Vähäinen	Pieni riski, ettei toiminta ole ohjeistuksen mukaista (eng. Non compliant)
3	Kohonnut riski, joka vaatii välittömiä toimenpiteitä	Keskisuuri	On vaara, että jotkin toiminnot ovat laittomia
4	Merkittävä uhka hengelle	Suuri	Jotkin toiminnot ovat laittomia
5	Todellinen tai suuri riski kuolemalle	Erittäin suuri	Mittavat sakot ja mahdolliset oikeudelliset toimenpiteet

Taulukko 2: Taulukko 1 jatkettuna

Riskien vaikutusten arvioinnin lisäksi on määriteltävä riskien realisoitumisen todennäköisyydet. Taulukossa 3 kerrotaan sekä kuvataan määritelmät pisteytyksille.

Pisteytys	Sanallinen kuvaus	Yhteenveto
1	Erittäin epätodennäköistä	Riski ei ole koskaan realisoitunut eikä ole syytä olettaa, että realisoitumisen todennäköisyys olisi kasvanut
2	Epätodennäköistä	Riskin realisoituminen on mahdollinen, mutta varsin epätodennäköinen
3	Todennäköistä	Riskin mahdollisuus realisoitua on isompi kuin olla realisoitumatta
4	Hyvin todennäköistä	Olisi yllättävää, mikäli riski ei realisoituisi perustuen vallitseviin olosuhteisiin tai menneeseen realisoitumistiheyteen
5	Melkein varmaa	Riski joko realisoituu säännöllisesti tai on perustelu syy olettaa, että riskin realisoituminen on välitöntä

Taulukko 3: Todennäköisyyksien määritelmät

6.4 Riskien hyväksymiskriteerit

Yrityksellä oli jo valmiiksi määritettynä riskien hyväksymiskriteerit ja näitä samoja kriteereitä käytetään myös tässä projektissa. Nämä kriteerit pätevät myös ulkomaan toimipisteillä, jotta saavutetaan mahdollisimman läheinen yhdenmukaisuus. Yrityksellä on käytössään myös kuviossa 3 kuvattu riskimatriisi. Tietoturvasyistä tarkkoja hyväksymiskriteereitä ei julkaista tässä opinnäytetyössä.

7 Riskianalyysi

Riskianalyysissä määritellään arvot riskien realisoitumisen todennäköisyyksille ja vaikutuskriteerit. Vaikutuskriteerit ovat kuvattuna projektissa tuotetussa dokumentissa ”Riskien arviointi ja riskien käsittelyprosessi”.

Kun yrityksen resurssit ovat koottu niin suoritetaan riskianalyysi käyttämällä Certikitin tarjoamaa resurssipohjaista riskienarviointityökalua, jossa määritellään riskien realisoitumisen vai-

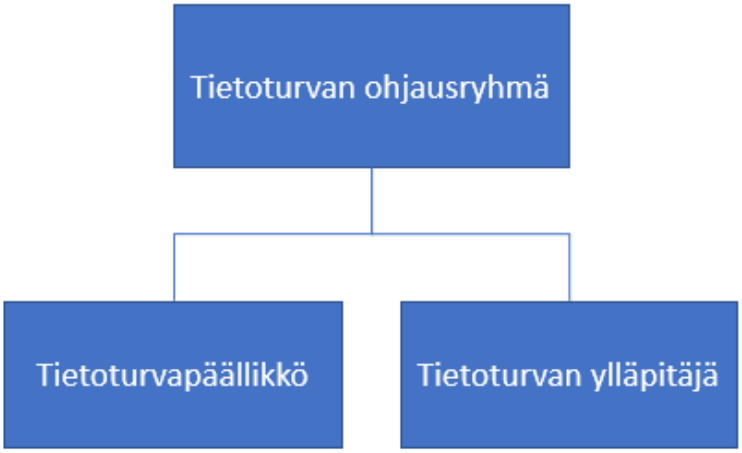
kutukset sekä todennäköisyys riskien realisoitumiselle. Lopullinen pisteytys verrataan riskimatriisiin ja selvitetään, että onko riski hyväksyttävä vai ei. Mikäli riskiarvo ei ole hyväksyttävissä rajoissa, valitaan sopiva hallintakeino riskin pienentämiseksi. Kuviossa 5 riskianalyysin työkalua on havainnollistettu.

Resurssi	Uhka	Haavoittuvuus	Käytössä olevat hallintakeinot	Todennäköisyys	Vaikutus	Riskiarvo	Valittu käsittelytapa	Valittu hallintakeino
Resurssin nimi	Kuvaus uhasta	Kuvaus haavoittuvuudesta	Mahdollinen jo käytössä oleva hallintakeino uhalle	Riskin realisoitumisen todennäköisyys asteikolla 1-5	Riskin realisoitumisen vaikutuksen arvo skaalalla 1-5	Lopullinen riskiarvo	Käsittelytapa: Riskin hyväksyminen, riskin jakaminen, riskin muokkaaminen, riskin välttäminen	Kuvaus valitusta hallintakeinosta

Kuvio 4: Havainnekuva riskianalyysin työkalusta

8 Organisaation perustaminen

Koska yrityksen tavoitteena on perustaa tietoturvallisuuden hallintajärjestelmä, niin rooleja jo määritelty ISMS:n osalta. Nämä jo määritellyt roolit on otettu huomioon ja riskienhallinnan tehtäviä on jaettu ennalta määritetyille tietoturvarooleille.



Kuvio 5: ISMS Riskienhallinnan roolit

Kuviossa 6 on kuvattuna riskienhallintaorganisaatio ja niiden suhde toisiinsa. Riskientunnistamisen työpajaan voi osallistua tarpeen mukaan kuka vain, eikä heidän tarvitse olla riskienhallinnan organisaatiossa erikseen määriteltyjä. Huomionarvoista on, että tietoturvasyistä kuvioon 3 ei ole kuvattuna kaikkia yrityksen tietoturvarooleja ja sen toimintoja.

Riskienhallinnan organisaation osalta roolien vastuut sekä oikeudet ovat jaettuna seuraavalla lailla:

- Tietoturvan ohjausryhmä

  Ohjausryhmän vastuita ovat: Valvoa organisaation riskienhallintaa, vastata kommunikoinnista, tarjota resursseja tietoturvallisuuden parantamiseen, järjestää johtoryhmän tietoturvallisuuden katsauksia, asettaa jatkuvan parantamisen politiikan yritykseen, käydä läpi tietoturvan loukkaustapaukset.

  Ohjausryhmän oikeuksia ovat: Hyväksyä riskienhallinnan työpajassa ehdotettuja riskien hallintakeinoja, käynnistää tietoturvan loukkausten hallintatoimia.

- Tietoturvapäällikkö

  Tietoturvajohtaja vastaa tietoturvallisuuden hallintajärjestelmästä ja raportoi tieturvan ohjausryhmälle kaikista tietoturvallisuuteen liittyvistä asioista. Tietoturvapäällikkö vastaa siitä, että hallintakeinot ovat käytössä ja dokumentoitu sekä määrittelee parannus suunnitelmat ja raportoi niiden etenemisestä.

  Tietoturvapäällikön oikeuksia on julistaa tietoturvahäiriö tapahtuneeksi ja tehdä katsaus kaikista organisaation hallintakeinoista.

- Tietoturvan ylläpitäjä

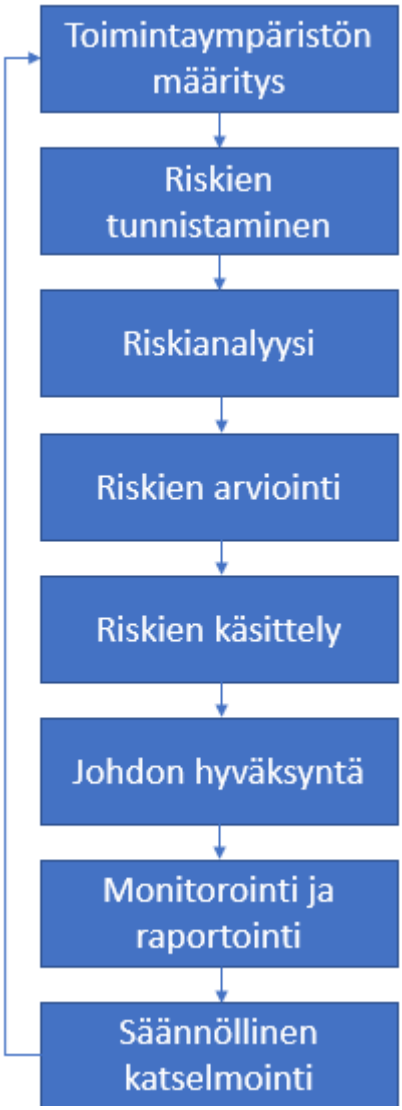
  Tietoturvan ylläpitäjä on tietoteknisempi rooli, joka vastaa tietoteknisten hallintakeinojen implementoinnista ja dokumentoinnista.

  Tietoturvan ylläpitäjillä on oikeus estää tietoturvan häiriö tai eskaloituminen ja ylläpitää tieturvarekisteriä ohjeistusten mukaisesti.

9 Riskienhallinnan prosessi

Kun riskienhallintaprosessin osalta on määritelty peruskriteerit, riskienhallintaorganisaatio ja riskienhallintametodi on mahdollista käynnistää itse riskienhallintaprosessi. Riskienhallinta-

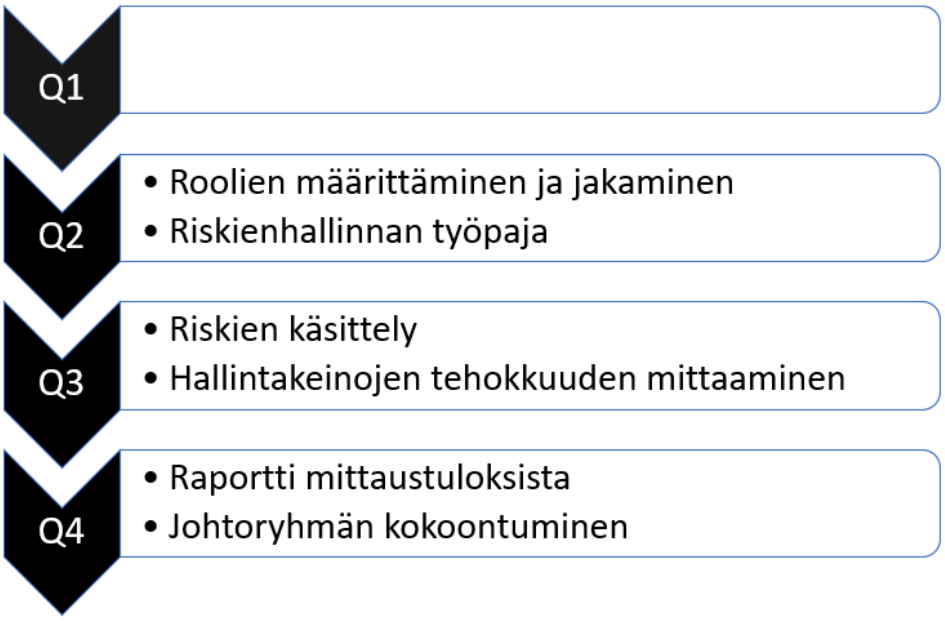
työpaja alkaa aina toimintaympäristön määrityksellä, jossa määritellään aina kussakin riskienhallintatyöpajassa käsiteltävä laajuus ja rajat sekä kuvataan mahdolliset muuttuneet sisäiset ja ulkoiset toimintaympäristöt. Riskien tunnistamisvaiheessa päivitetään resurssiluettelo tai kootaan resurssiluettelo, mikäli kyseessä on ensimmäinen riskienhallintatyöpaja. Resurssiluettelon koostamisen jälkeen listataan perustellut uhat kullekin resurssille. Näiden uhkien realisoitumismahdollisuuksia arvioidaan vaikutuskriteerien mukaisesti ja valitaan riskien käsittelytapa. Ennen hallintakeinojen implementointia tai riskien hyväksyntää on tietoturvan ohjausryhmän hyväksyttävä valitut riskien käsittelytavat. Hallintakeinojen tehokkuutta mitataan ja raportoidaan tietoturvan ohjausryhmälle, joka pitää yrityksen johtoryhmän kokoontumisen, jossa käsitellään riskienhallinnan tuloksia. Tämän jälkeen prosessi alkaa alusta. Riskienhallinnan työpaja voidaan järjestää myös tarpeen vaatiessa kesken syklin, mikäli äkisti muuttunen tilanteen takia on tarvetta sille. Kuviossa 7 esitellään prosessi kuvana.



Kuvio 6: Riskienhallinnan prosessikaava

10 Ensimmäinen vuosikello

Yritykselle tuotettiin kuvion 8 mukainen vuosikello, jonka mukaan voitaisiin edetä riskienhallintamallin implementoinnissa. Ensimmäinen riskienhallinnan vuosikello alkaa vasta toisella vuosineljänneksellä, joka johtuu siitä, että tämä työ palautetaan toisella vuosineljänneksellä yritykselle.



Kuvio 7: Ensimmäinen vuosikello

10.1 Vuosineljännesten tapahtumat

Toisella vuosineljänneksellä tulisi yrityksen johtoryhmän hyväksyä ehdottamat roolit, tai tarpeen vaatiessa muokata niitä. Tämän jälkeen täytyisi jakaa roolit henkilöstölle. Tässä kannattaa käyttää apuna pätevyyskyselyä, jotta samalla selviää osaamisen osa-alueet, jotka mahdollisesti vaativat lisäkoulutusta. Kyselyn teettäminen on pakollinen osa ISMS perustamiselle, joten en näe syytä miksi jättää riskienhallinta pois kyselystä.

Kun ISMS roolit on jaettu, tulisi järjestää ensimmäinen riskienhallinnan työpaja. Ehdotukseni ensimmäisen työpajan alustavasta agendasta on seuraavanlainen:

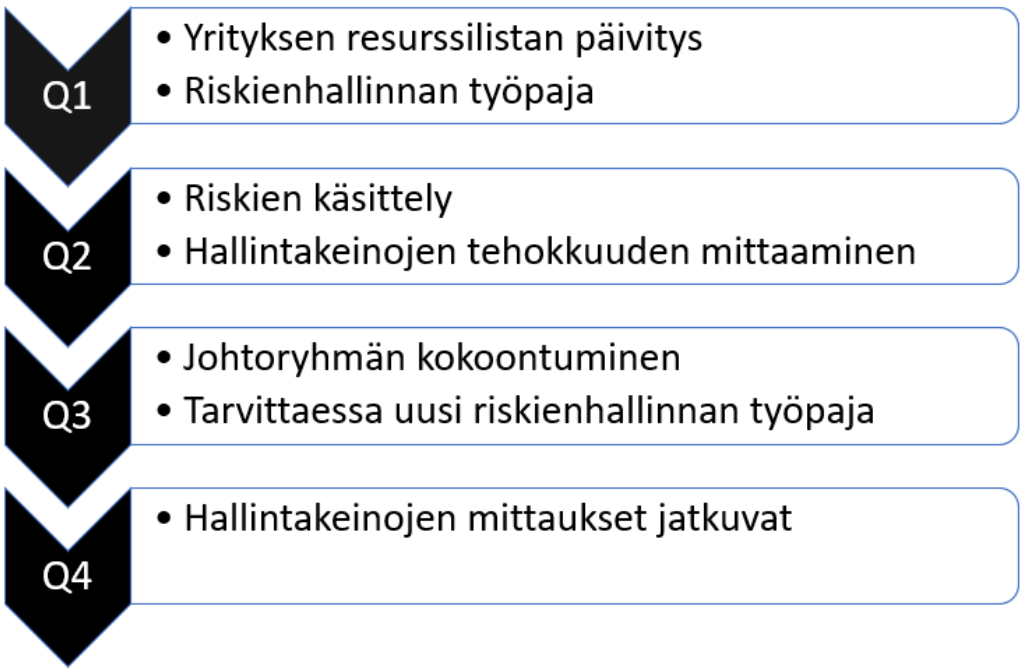
- Koosta lista yrityksen resursseista
- Käydään läpi jo olemassa olevat hallintakeinot

- Resurssipohjaisen riskienhallinnan suorittaminen resurssipohjaisen riskienarvioinnin työkalua käyttäen
- Valitse hallintakeinot ISO/IEC 27001 liite A:n listasta ja täytä soveltuvuuslausuntoon valitut hallintakeinot
- Riskien käsittelyn suunnitelman koostaminen, mikäli riskit eivät ole hyväksyttävissä rajoissa

Kolmannen vuosineljänneksen aikana toteutetaan riskien käsittelyä suunnitelmien mukaisesti ja aloitetaan hallintakeinojen tehokkuuden mittaaminen. Tietoturvapäällikkö seuraa suunnitelman etenemistä ja riskien käsittelyn toteutumista. Näitä toimintoja voi aloittaa aikaisemminkin kuin kolmannella vuosineljänneksellä, mutta viimeistään sen aikana hallintakeinojen tulisi olla implementoituna. Mikäli hallintakeinojen implementointiin liittyy henkilökunnan koulutusta, tulee nekin järjestää tämän vuosineljänneksen aikana.

Neljännellä vuosineljänneksellä raportoidaan mittaustulokset johtoryhmälle, joka arvioi perusteellisesti ISMS toimivuuden ja tehokkuuden. Myös keskeneräiset hallintakeinojen implementoinnit käydään läpi johtoryhmän kokouksessa.

11 Toinen vuosikello



Kuvio 8: Toinen vuosikello

Kuvion 9 mukaisella vuosikellolla ei ole tarvetta kaikille ensimmäisen vuosikellon mukaisille toiminnoille, sillä esimerkiksi roolit on jo jaettu. Huomionarvoista on, että myös riskienhallintamenetelmää tulisi tarkastella johtoryhmän kokoontumisissa ja riskienhallintaprosessin toimivuutta tarkastelun tulosten mukaan tarpeen mukaan parannella, joten tämä vuosikello voi muuttua hyvinkin radikaalisti.

12 Pohdinta

Työn tavoitteena oli esittää opinnäytetyön toimeksiantajalle ISO/IEC 27001 standardit täyttävä riskienhallintamalli. Työssä tuotettiin dokumentteja riskienhallintamallia varten ja vuosikellot yritykselle. Tuloksena on riskienhallintamalli, jonka jalkauttamisen mahdollisuus pitäisi arvioida ja toki tarpeen vaatiessa riskienhallintamallia tulisi muokata sopivammaksi yritykselle. Osittain riskienhallintamalli on vähän puutteellinen viestinnän suhteen. Tämä johtuu jossain määrin myös siitä, että ISMS viestintäprosessi yrityksessä on yleisestikin ottaen työn alla. Ohjeistukset eri raporttien luontiin ja niiden lähettämiselle on kuitenkin olemassa. Viestintäkäytännöt varmasti vakioituvat ja kehittyvät kunkin iteraation aikana, eikä ISMS ole koskaan niin sanotusti valmis.

Työssä haasteina oli sovittaa ISO/IEC 27001 standardin vaatimuksia yrityksen toiveisiin. Koin että pääsimme kuitenkin yhteisymmärrykseen lukuisien kokouksien myötä, kun ymmärsin mitä tavoitteita yrityksellä oli koskien tietoturvallisuuden hallintajärjestelmää. Työn aikana tutustuin lukuisiin ISO/IEC 27000 standardiperheen standardeihin ja opin etenkin ISO/IEC 27005 standardista paljon, joka oli minulle paljon vähemmän tutumpi kuin ISO/IEC 27001 standardi. Riskienhallintamallia olisi voinut jalostaa vielä enemmän käyttämällä myös ISO/IEC 31000 standardia apuna. Jatkoa ajatellen suosittelen syventymään myös ISO/IEC 31000 ja kehittämään riskienhallintamallia eteenpäin sitä standardia käyttäen.

Lähteet

Painetut

SFS-EN ISO/IEC 27000:2017. 2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Yleiskuvaus ja sanasto. Helsinki: Suomen Standardoimisliitto.

SFS-EN ISO/IEC 27001:2017. 2017. Tietoturvallisuuden hallintajärjestelmän vaatimukset. Helsinki: Suomen Standardoimisliitto.

SFS-ISO/IEC 27005:2018 Informaatioteknologia. Turvallisuustekniikat. Tietoturvariskien hallinta Helsinki: Suomen Standardoimisliitto.

Humphreys, E. 2016. Implementing the ISO/IEC 27001 ISMS Standard. Lontoo: Artech House.

Sähköiset

IS Partners. 2019. Viitattu 29.3.2020. What You Need to Know about ISO 27001 Changes Between 2013 and 2017. https://www.ispartnersllc.com/blog/iso-27001-2013-2017/

The Risk Academy. 2018. Viitattu 3.4.2020. Comparing ISO 31000 and ISO 27005. https://theriskacademy.org/is0-31000-iso-27005/

Kuviot

Taulukot