SAVONIA

OPINNÄYTETYÖ - **AMMATTIKORKEAKOULUTUTKINTO**
TEKNIIKAN JA LIIKENTEEN ALA

ISO/IEC 27001 -STANDARDIN MUKAINEN TIETOTURVA SERVICE DESKIIN

TEKIJÄ: Matti Mikkonen

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma Tietotekniikan koulutusohjelma	
Työn tekijä Matti Mikkonen	
Työn nimi ISO/IEC 27001 -standardin mukainen tietoturva Service Deskiin	
Päiväys 29.4.2015	Sivumäärä/Liitteet 35/1
Ohjaaja lehtori Pekka Granroth	
Toimeksiantaja/Yhteistyökumppani Enfo Oyj Service Desk	

Tiivistelmä

Tämän opinnäytetyön tavoitteena oli Service Deskin tietoturvallisuuden parantaminen ISO/IEC 27001 -standardin mukaisesti tunnistamalla suojattavat resurssit, laatimalla näille resursseille riskianalyysit ja pohtimalla tarvittavat hallintakeinot näiden riskien vähentämiseksi.

Työ aloitettiin tutkimalla ISO/IEC 27001 -standardin vaatimukset sekä rajaamalla Service Desk standardin suojauksen piiriin. Service Desk kuvattiin yleistasolla, jotta saatiin selville riippuvuussuhteet ja vastuualueet eri sidosryhmien kanssa. Service Deskin sisällä tunnistettiin suojattavat resurssit ja näihin kohdisturvat riskit. Riskit arvioitiin Enfon riskienhallintapolitiikan mukaisesti esimiesten ja johdon avulla, jotka valittiin resurssien omistajiksi. Arvioinnin perusteella riskeille pohdittiin tarvittavat hallintakeinot.

Lopputuloksena laadittiin Service Deskin yleiskuvaus, resurssiluettelo, riskianalyysit ja Statement of Applicability -dokumentti. Tehtyjen riskianalyysien perusteella tietoturvallisuuteen voidaan nyt varautua paremmin, kun tiedetään olemassa olevien riskien seuraukset. Riskien hallintakeinojen käytännön toteutus ei kuulunut tähän opinnäytetyöhön.

Avainsanat
ISO/IEC 27001, tietoturvallisuuden hallintajärjestelmä, riskianalyysi, hallintakeino

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author Matti Mikkonen			
Title of Thesis ISO/IEC 27001 Based Information Security to Service Desk			
Date	29 April 2015	Pages/Appendices	35/1
Supervisor Mr. Pekka Granroth, Lecturer			
Client Organisation/Partner Enfo Oyj Service Desk			

Abstract

The purpose of this thesis was to improve the information security of Service Desk by identifying the protectable assets of Service Desk, analyzing the risks directed to these assets and considering necessary security controls to mitigate these risks.

The thesis was started by researching the ISO/IEC 27001 standard requirements and defining Service Desk into the scope of this standard. Service Desk was described in a general way to find out Service Desk dependencies and responsibilities between many interested groups. Protectable assets and risks directed to these assets were identified. These risks were assessed according to Enfo's risk management policy with Service Desk director and supervisors who were selected to be risk owners. Necessary security controls were selected to mitigate the risks based on the assessment results.

As a result the following documents were made: General description of Service Desk, inventory of assets, risk analyses and Statement of Applicability. Service Desk can prepare to analyzed risks better when consequences of these risks are known. Implementing of necessary security controls and auditing their efficiency was beyond the scope of this thesis.

Keywords
ISO/IEC 27001, information security management system, risk analysis, security control

ESIPUHE

Haluan kiittää Enfo Oyj Service Deskin johtajaa Kyösti Vähäkainua mielenkiintoisesta opinnäytetyön aiheesta. Erityiskiitokset Enfo Oyj:n tietoturvapäällikkö Pekka Hagströmille neuvoista tietoturvallisuuden ja standardin toteutuksesta sekä Enfon tiimiesimiehille työhön tarvittujen tietojen antamisesta.

Kiitokset myös ohjaavalle opettajalle lehtori Pekka Granrothille ja toimeksiantajan ohjaajalle tiimiesimies Henna Niemiselle kannustuksesta ja ohjauksesta.

Kuopiossa 29.4.2015
Matti Mikkonen

SISÄLTÖ

LYHENTEET JA TERMIT

Active Directory (AD)	Microsoftin kehittämä hakemistopalvelu palvelimille, jossa sijaitsevat mm. käyttäjätunnukset ja toimialueen tietokonetilit.
Auditointi	Jonkin asian puolueeton tarkastelu ja arviointi. Voidaan tehdä sisäisesti tai ulkopuolisen tarkastajan avulla.
IEC	International Electrotechnical Commission. Kansainvälinen sähköalan standardisoimisjärjestö.
ISMS	Information Security Management System. Tietoturvallisuuden hallintajärjestelmä.
ISO	International Organization for Standardization. Kansainvälinen standardisoimisjärjestö.
Kattavuus (Scope)	Standardin tietoturvallisuuden hallintajärjestelmän rajaus eli mikä organisaation alue, palvelut tai resurssit halutaan järjestelmän piiriin.
Palvelutasosopimus (SLA)	Palvelun tuottajan ja asiakkaan välinen sopimus palveluille määritetyistä vaatimustasoista. Näihin kuuluu mm. palvelun nopeus, saatavuus ja työpyyntöjen ratkaisuajat.
Statement of Applicability	Dokumentti, jossa on kuvattu ISO/IEC 27002 -tietoturvakontrollit ja omat kontrollit sekä tieto niiden toteutuksesta ja perusteista.
Tiedon eheys	Luvattomat käyttäjät eivät pääse muuttamaan tietoa tiedonsiirron aikana
Tiedon luottamuksellisuus	Tietoon pääsee käsiksi vain henkilöt joilla on siihen oikeus.
Tiedon saatavuus	Tieto on saatavissa sitä tarvittaessa.

1 JOHDANTO

Tietoturvallisuus on merkittävä asia nykypäivän organisaatioissa. Tietoturvallisuus täytyy liittää jokaiseen organisaation liiketoimintaprosessiin, sillä tietoturvan heikentyessä myös liiketoiminta on vaarassa. Mahdolliset haavoittuvuudet tai tietoturvavuodot voivat heikentää yrityksen mainetta. Tämän takia organisaation on varauduttava mahdollisiin riskeihin suunnittelemalla, toteuttamalla, ylläpitämällä, valvomalla ja parantamalla tietoturva- ja riskienhallintaprosesseja sekä riskienhallintakeinoja. Näiden prosessien ja keinojen avulla organisaatiolla on toimintamalli mahdollisten uhkien vähentämiseksi.

Kaikkia riskejä on mahdoton poistaa kokonaan ja riskien poisto on taloudellisestikin erittäin kallista ja aikaa vievää, joten optimitilanteessa riskit pyritään minimoimaan alle sallitun maksimirajan, jolloin organisaation palvelut ja liiketoiminta pysyvät toimintakuntoisina. Jotkut riskit kuitenkin olla niin suuria, että organisaation täytyy pysäyttää kaikki muu toiminta näiden riskien vähentämiseksi.

Jotta organisaatio voisi valvoa ja parantaa omia järjestelmiään ja prosessejaan, on valvottava ja dokumentoitava tietoturvaan liittyviä tapahtumia, kuten tapahtuneita uhkia ja niihin kohdistettuja korjaustoimia. Näiden pohjalta voidaan katselmoida, missä organisaation osassa on parantamisen varaa ja missä riskejä tai uhkia on liian paljon, ja keskittää hallintakeinoja näihin osiin enemmän.

ISO/IEC 27001 -standardin tarkoituksena on suunnitella, toteuttaa ja ylläpitää tietoturvallisuuden hallintajärjestelmä. Lisäksi järjestelmää on parannettava säännöllisesti. Järjestelmän tavoite on suojata organisaation määrittelemät tiedot ja kohteet ja hallita niihin kohdistuvia riskejä.

Työ tehdään Enfo Oyj konsernin Service Desk -yksikölle ja tavoitteena on tutkia ISO/IEC 27001 -standardin vaatimukset ja selvittää, miten Service Desk voisi toteuttaa standardin mukaisen tietoturvallisuuden ja parantaa riskien käsittelyä sekä vähentää riskien todennäköisyyttä. Näiden tietojen perusteella tutkitaan myös, kuinka Service Deskin toimintaa täytyy parantaa tietoturvan kannalta paremmaksi ja näin saavuttaa ISO/IEC 27001 -standardin mukainen tietoturvallisuuden hallintajärjestelmä. Ulkopuolinen auditoija voi sertifioida tietoturvallisuuden toimivuuden tarvittaessa, mutta tässä työssä sertifikaatti ei ole tavoitteena.

Työssä selvitetään Service Deskin kriittiset suojattavat resurssit ja kohteet. Kohteille tunnistetaan mahdolliset riskit, jotka arvioidaan Enfo Oyj:n riskienhallintapolitiikan mukaisesti ja lopuksi riskeille valitaan tarvittavat hallintakeinot, joilla riskejä pyritään vähentämään.

2 ENFO OYJ

Opinnäytetyön toimeksiantaja on Enfo Service Desk. Enfo Oyj on pohjoismainen IT-palveluyritys, joka tuottaa yrityksille erilaisia IT- ja ulkoistuspalveluja. Yritys on perustettu vuonna 1964 Tietosavo Oy nimellä ja vuonna 2001 nimi muutettiin Enfoksi. Yritys toimii Suomessa, Ruotsissa, Norjassa ja Tanskassa. Enfo Oyj:ssä työskentelee noin 800 IT- ja talouspalvelujen ammattilaisista. Enfon liikevaihto on lähes 160 miljoonaa euroa. (Enfo Oyj 2014a.)

Yhä useammat yritykset ulkoistavat osan tai kaikki IT-palveluistaan ulkoistuspalveluja tarjoavalle yritykselle. Näin asiakasyritykset voivat keskittyä paremmin ydinliiketoimintaansa ja antaa IT-palvelujen asiantuntijoiden hoitaa tietotekniikkaa koskevat tukiprosessit. (Enfo Oyj 2014b.)

Enfon tarjoamat IT-palvelut koostuvat seuraavista palvelualueista (Enfo Oyj 2014b.):

- asiakasympäristön kehityspalvelut
- sovelluspalvelut
- integraatiopalvelut
- kommunikaatiopalvelut
- Service Desk ja käyttäjätukipalvelut
- työasemien ja laitteiden hallintapalvelut
- laitteet, lisenssit ja elinkaaripalvelut
- kapasiteetti- ja pilvipalvelut
- tietoverkko- ja tietoturvapalvelut.

3 SERVICE DESK

Service Desk on yksi Enfo Oyj:n tarjoamista ulkoistuspalveluista, johon tämä työ tehdään. Tässä luvussa kerrotaan, mikä Service Desk on, millainen Service Deskissä käytetty tikettijärjestelmä on ja miten työprosessit etenevät työpyynnön saapuessa. Koska toimeksiantajana on Service Desk ja tässä työssä tärkein suojattava kohde on sen tuottama palvelu, on tärkeää tietää millaisesta palvelusta on kyse. Kaikki opinnäytetyössä tunnistetut suojattavat resurssit liittyvät vahvasti henkilöstön tuottaman palvelun laatuun ja tietoturvallisuuteen, työpyyntöjen kirjauksiin sekä asiakaspalvelun luottamuksellisuuteen.

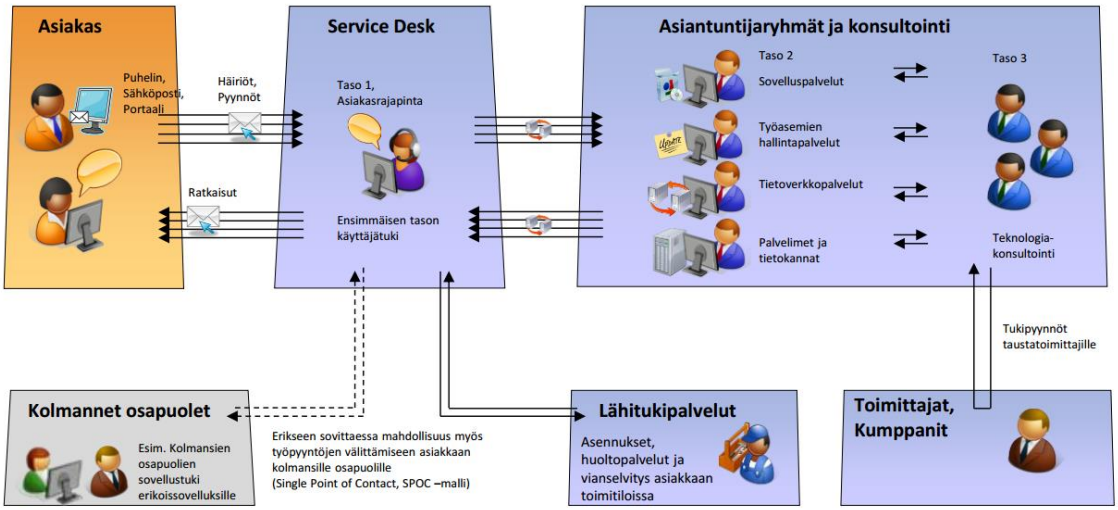
Service Desk on yhteydessä useisiin asiakasyrityksiin ja hallinnoi niiden tietojärjestelmiä järjestelmänvalvojatunnuksilla, joilla on usein hyvin paljon oikeuksia työpyyntöjen suorittamista varten. Työpyyntöjen kriittisyyden ja arkaluontoisten tietojen käsittelyn vuoksi tietoturvallinen toiminta on hyvin tärkeää Service Deskin asiakaspalvelussa. Jokaisen Service Deskin asiantuntijan olisi oltava tietoisia turvallisesta työskentelystä, jotta tietoturvallisuuden vaarantumiseen kohdistuvat riskit saataisiin minimoitua.

3.1 Toimintaperiaate

Enfon toimintaa ohjaa Enfon ja asiakkaan välinen palvelusopimus (SLA), jossa selvitetään, mitä palveluja asiakas ostaa Enfolta. Näihin voi kuulua Service Desk -palvelut, palvelinpalvelut, verkkopalvelut tai näiden yhdistelmät. Sopimuksessa on määritetty myös tarkat palveluajat ja palvelutasot sekä sanktiot, jos palveluja ei kyetä toimittamaan sovitulla tavalla. Palvelutasoissa on määritetty mm. tarkat vasteajat, jotka määrittelevät työpyyntöjen vastaanotto- ja ratkaisuajat. (Enfo Oyj 2014d.)
Service Deskin ja käyttäjätukipalveluiden avulla tarjotaan asiakasyrityksille käyttäjien toiveiden ja ongelmien mukaisia tukipalveluita (Enfo Oyj 2014c). Yleisesti tukipalvelut voivat olla seuraavanlaisia (Roos 2015-01-30):

- työpyyntöjen vastaanotto, luokittelu ja tallennus
- työpyyntöjen ratkaiseminen
- työpyyntöjen käsittelyn valvonta ja tilanteiden sekä ratkaisujen tiedottaminen asiakkaalle.

Tietyissä tapauksissa työpyynnöt voivat olla laajempia tai yksityiskohtaisempia eri tietojärjestelmiin liittyviä laajempia ongelmia. Näissä tapauksissa palvelupisteellä ei aina ole tarvittavia resursseja ratkaista asiaa. Lisäksi asiakkaiden palvelutasosopimukset voivat olla tiukkojakin, niin että palvelupisteessä ei ole aikaa ratkoa vaativampia työpyyntöjä. Tällöin työpyynnöt ohjataan kyseiseen asiaan erikoistuneelle asiantuntijalle, lähituelle tai kolmansille osapuolille ja Service Desk voi jatkaa työpyyntöjen vastaanottoa. (Kuva 1.)



KUVA 1. Service Deskin toiminta (Enfo Oyj 2014f.)

Enfon palvelupisteessä on asiakkaina useita yrityksiä. Nämä yritykset on jaettu eri asiakastiimeille, jotta työpyyntöjen hallinnointi on sujuvampaa ja palvelupisteen asiantuntijat voivat keskittyä vain tiettyihin asiakkaisiin.

3.2 Tikettijärjestelmä

Tikettijärjestelmän tarkoitus on hallinnoida asiakkaiden työpyyntöjä eli ns. tikettejä. Järjestelmässä on työkalut mm. tikettien vastaanottoon, luokitteluun sekä asiakkaan ja Service Deskin väliseen yhteydenpitoon. Tiketeillä on aina jokin yksilöivä tunnus, jolla se löytyy järjestelmästä haettaessa. Tiketeille kirjataan aina myös asiakkaan nimi ja yritys, jotta yhteydenotossa tai laskutuksessa tiedetään, kenelle työpyyntö on tehty.

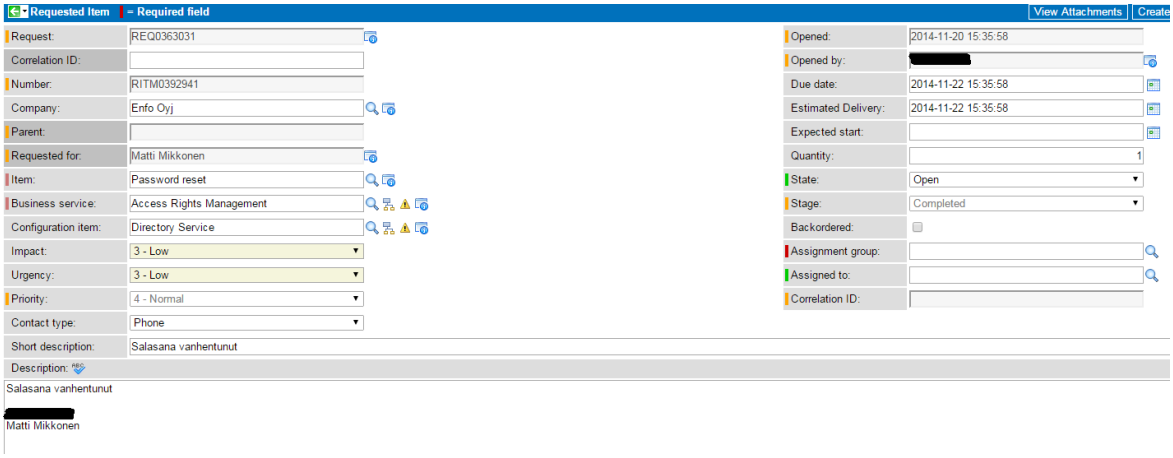
3.3 Työpyyntöjen luokittelu

Työpyynnöt voivat tulla puhelimitse, sähköpostilla tai asiakkaan oman järjestelmän kautta. Service Desk luokittelee työpyynnön itse sisällön mukaan, kerää asiakkaalta lisätietoja pyynnöstä ja tallentaa työpyynnön järjestelmään tai ratkaisee sen heti yhteydenottovaiheessa.

Työpyynnöt ovat aluksi muotoa TKTxxxxxxx, jossa x:t merkitsevät juoksevaa numerointia. Tunnuksella työpyynnöt yksilöidään, jolloin kahta samalla numerolla olevaa työpyyntöä ei voi olla olemassa. Nämä tiketit luokitellaan sisällön mukaan ja jaetaan pääasiassa kahteen eri luokkaan, pyyntöihin (Request) tai häiriöilmoituksiin (Incident).

Pyyntöjen muoto on REQxxxxxxx. Näihin liitetään pyydetty tuote (Request Item tai RITMxxxxxxx). Nämä RITM:t ovat esimerkiksi käyttöoikeuksien muutos, käyttäjätunnuksen luominen, sovelluksen asentaminen ja uuden laitteen tilaus.

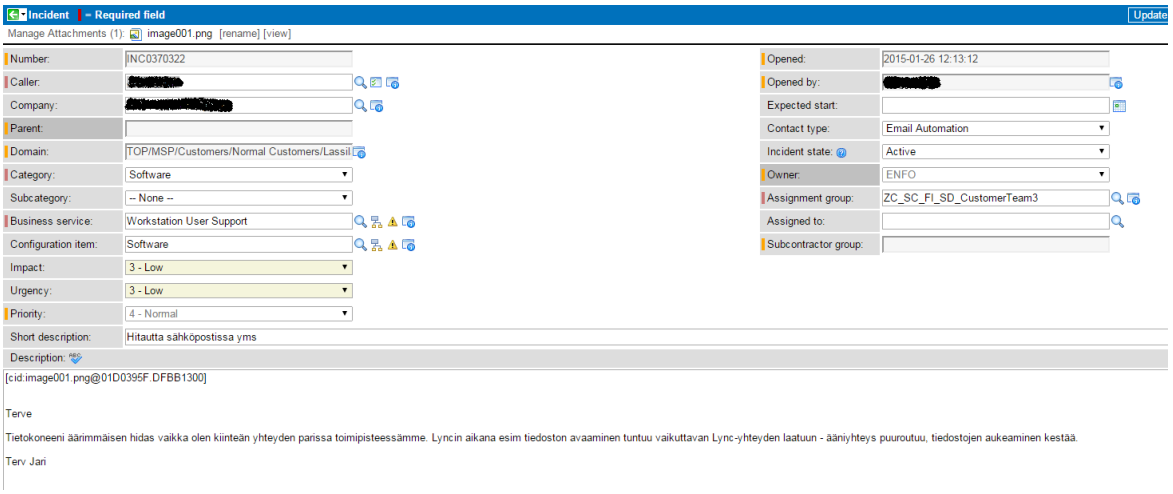
Enfon tikettijärjestelmässä pyyntöjen tiedoille on omat tekstikentät, joihin syötetään pyynnön sisällön mukaan luokitteluvaihtoehdot ja lisätiedot. (Kuva 2.)



KUVA 2. Palvelupyyntö Enfon tikettijärjestelmässä (Mikkonen 2015-01-30.)

Häiriöilmoituksien muoto on INCxxxxxxx, ja niillä kuvataan asiakkaalla tapahtuvia häiriöitä erilaisissa järjestelmissä tai ohjelmistoissa. Näihin voidaan luokitella esimerkiksi työasemien käynnistysongelmat, laitteiden rikkoutuminen ja verkkoyhteyden toimimattomuus.

Häiriöilmoitukset luokitellaan tikettijärjestelmässä samalla tavalla kuten pyynnötkin (Kuva 3).

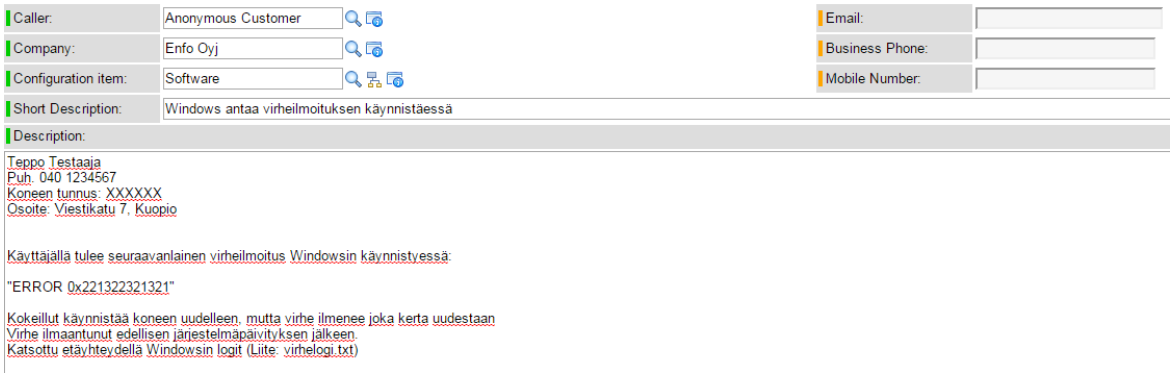


KUVA 3. Häiriöilmoitus Enfon tikettijärjestelmässä (Mikkonen 2015-01-30.)

3.4 Työpyyntöprosessin kuvaus

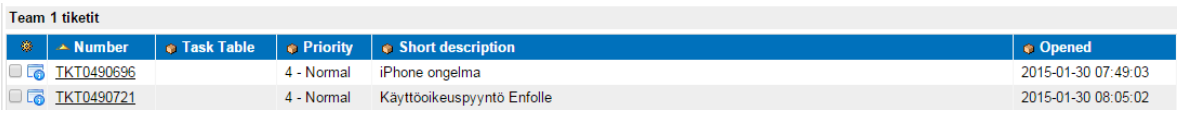
Asiakkaan ottaessa yhteyttä puhelimitse puhelu ohjautuu suoraan kyseistä asiakasta palvelevalle asiakastiimille. Tämä tiimi kirjaa mahdollisimman tarkat tiedot asiakkaalta. Näihin kuuluu mm.:

- asiakkaan nimi ja yritys
- puhelinnumero sekä mahdolliset muut osoitetiedot, jos esimerkiksi asiakas tarvitsee lähitukea
- mahdollisimman tarkka kuvaus ongelmasta tai pyynnöstä
- ongelman kohde
- kuvankaappaukset virheilmoituksista tai tilanteista
- ongelman kiireellisyys ja laajuus. (Kuva 4.)



KUVA 4. Yhteydenotto tullut puhelimitse (Mikkonen 2015-01-30.)

Asiakkaan yhteydenotto voi tapahtua myös sähköpostitse, jossa asiakas lähettää sähköpostiapalvelupisteen osoitteeseen, josta tikettijärjestelmä tekee automaattisesti TKT -tyyppisen tiketin. Palvelupiste luokittelee tämän tiketin edelleen joko pyynnöksi tai häiriöilmoitukseksi. (Kuva 5.)



KUVA 5. Tikettijärjestelmän luomat tiketit asiakkaan lähettämistä sähköposteista (Mikkonen 2015-01-30.)

4 ISO/IEC 27001 -STANDARDI

Nykypäivänä tietoturvallisuus on laajenemassa IT -organisaatiosta kaikkiin liiketoiminnallisiin osastoihin. Organisaation täytyy ottaa tietoturvallisuus huomioon kaikissa tekemissään päätöksissä. Tietoturvauhat kehittyvät jatkuvasti ja uusia hyökkäysmenetelmiä keksitään päivittäin, joten yrityksen täytyy suojata sille tärkeät kohteet ja tiedot muilta tahoilta, jotka voivat näillä tiedoilla vaarantaa yrityksen tietoturvan ja pahimmillaan koko liiketoiminnan. ISO/IEC 27001 -standardissa käsiteltävän tietoturvallisuuden hallintajärjestelmän avulla organisaatiot voivat paremmin hallita suojattavia kohteitaan.

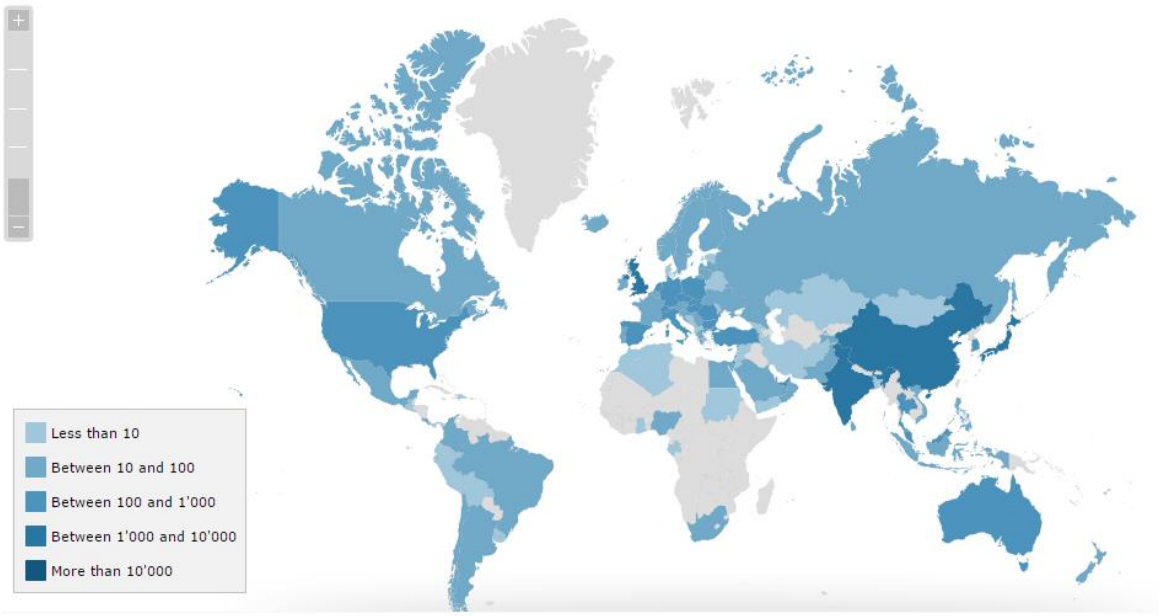
Kolme tietoturvallisuuden kannalta keskeistä asiaa, jotka täytyy olla kunnossa, ovat tiedon luottamuksellisuus, eheys ja saatavuus. Yhdenkin menettämisestä voi olla merkittäviä negatiivisia seurauksia yrityksen ja sen asiakkaiden väliselle luottamukselle sekä yhteiselle toiminnalle.

ISO/IEC 27001 -standardi on osa ISO 27000 -standardiperhettä, joka auttaa organisaatioita hallitsemaan omaisuutensa, taloustietojen, henkilötietojen ja muun informaation turvallisuutta. Tämä standardi kuvaa tietoturvan hallintajärjestelmän (ISMS) vaatimuksia. Vaatimukset on esitetty yleisellä tasolla, jotta ne soveltuvat kaikille organisaatioille riippumatta niiden koosta, tyypistä tai luonteesta. (International Organization of Standardization 2013a.)

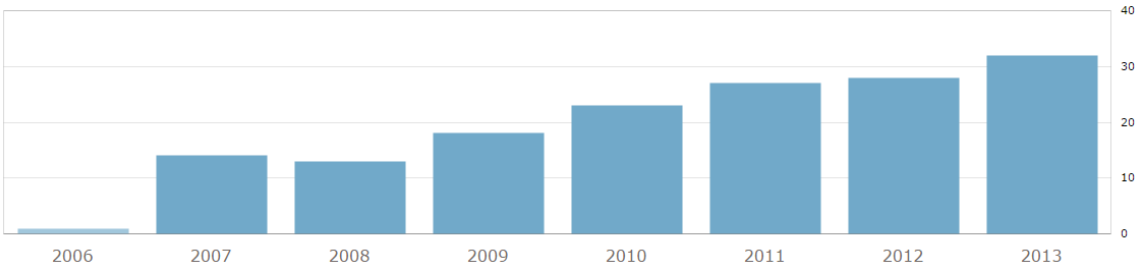
ISO/IEC 27001:2013 -standardin uudistettu versio vuoden 2005 standardista on muokattu sopimaan paremmin ISO 9000 ja ISO 20000 -standardiperheiden kanssa. Uudessa versiossa otetaan myös sovelluspohjaiset infrastruktuurit (mm. pilvipalvelut) paremmin huomioon, mitkä ovat viime vuosina yleistyneet. (Mackie 2013-04-02.)

Standardin 2013 versiossa painotetaan enemmän organisaation tietoturvan johtamisjärjetelmän suorituskyvyn mittaamiseen ja arviointiin kun 27001:2005 -version painoarvo oli prosessimaisella toimintamallilla. (The ISO 27000 Directory 2013.)

Seuraavissa kuvissa (KUVA 6 ja 7) näkyy kuinka tietoturvan ja orgaanisaatioiden sertifioinnin merkitys maailmassa kasvaa kokoajan. Vuonna 2013 maailmassa oli yhteensä 22 293 kpl ISO/IEC 27001 -sertifikaattia 105 eri valtiossa. (International Organization of Standardization 2013c.)



KUVA 6. ISO/IEC 27001 -standardin levinneisyys maailmassa vuonna 2013 (International Organization of Stand-ardization 2013b.)



KUVA 7. ISO/IEC 27001 -standardin evoluutio Suomessa (International Organization of Standardization 2013b.)

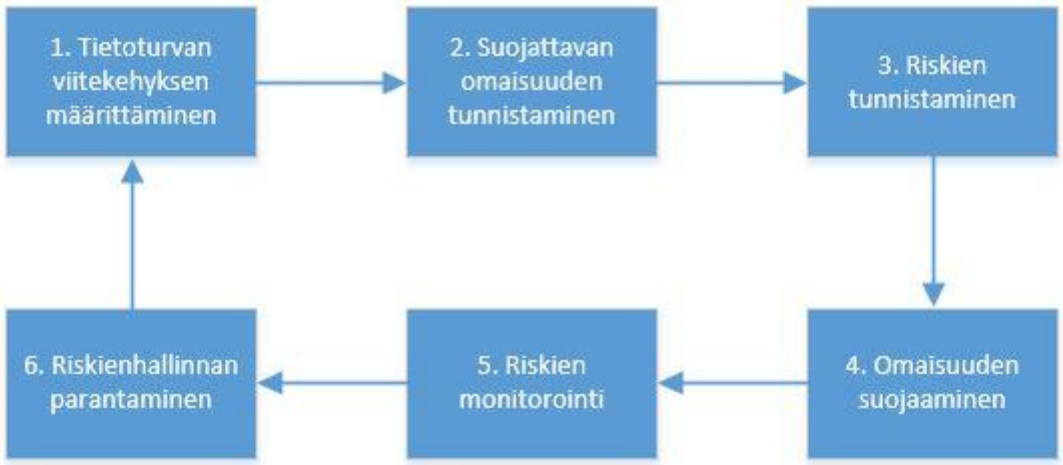
4.1 Tietoturvan hallintajärjestelmä

ISO/IEC 27001 -standardi käsittelee tietoturvallisuuden hallintajärjestelmän suunnittelua, toteutusta ja ylläpitoa. Järjestelmä on eri tietoturvaan liittyvien politiikkojen ja prosessien kokoelma, jolla parannetaan organisaation tietoturvallisuutta ja taataan sen liiketoiminnan jatkuvuus mittaamalla ja arvioimalla jatkuvasti riskejä ja suorituskykyä. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 6.)

Tietoturvallisuuden hallintajärjestelmään kuuluvan riskien hallinta- ja arviointiprosessin avulla organisaation tärkeät tietoturvaelementit luottamuksellisuus, eheys ja saatavuus saadaan suojattua ja riskeihin voidaan varautua. Tietoturvan standardisointi lisää myös eri sidosryhmien luottamusta sertifioitua organisaatiota kohtaan. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 6.)

Järjestelmää suunniteltaessa määritetään ensin viitekehys, johon järjestelmä aiotaan toteuttaa. Tämän kehyksen sisällä tunnistetaan suojattava omaisuus ja siihen kohdistuvat riskit. Riskeille toteutetaan tarvittavat hallintakeinot, että riskit saadaan vähennettyä sallittujen rajojen alle ja näiden te-

hokkuutta valvotaan säännöllisesti. Muutosten tapahtuessa ja säännöllisin väliajoin koko tietoturvallisuuden hallintajärjestelmä auditoidaan ja parannetaan sen tehokkuutta. Tällöin koko prosessi käynnistyy uudelleen. (Kuvio 1.)



KUVIO 1. Tietoturvallisuuden hallintajärjestelmä (Mikkonen 2015-03-08.)

4.2 Standardin vaatimukset

Seuraavissa luvuissa on kuvattu ISO/IEC 27001 -standardin vaatimukset.

4.2.1 Organisaation toimintaympäristö

Organisaation ydintoiminnan tarkoituksen ja tietoturvallisuuden hallintajärjestelmän vaikutuksien kannalta on määritettävä olennaisimmat ulkoiset ja sisäiset asiat. Näihin kuuluu mm. tietoturvan kannalta olennaisimmat sidosryhmät sekä näiden vaatimat tietoturvavaatimukset. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 8.)

Organisaation on suunniteltava ja luotava tietoturvallisuuden hallintajärjestelmä ja ylläpidettävä ja aina kehitettävä sitä ISO/IEC 27001 -standardin vaatimusten mukaisesti. Tälle järjestelmälle on määriteltävä kattavuus, joka on dokumentoitava. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 10.)

Kattavuudella tarkoitetaan sitä, mitä kaikkea organisaatiossa täytyy suojata. Nämä kohteet täytyy suojata riippumatta siitä, miten tietoja käsitellään tai kuka niitä käsittelee. Erityisen tärkeää on kohteiden ja tietojen tarkka määrittely, sillä pois jätettäviä kohteita täytyy käsitellä kuten ulkomaailmaa. Kohteita voi jättää pois vain, jos niille ei ole riskejä tai vaatimuksia. (Kosutic 2014-10-13.)

Kattavuuden on oltava dokumentoituna tietona ja se voidaan tarvittaessa yhdistää esimerkiksi organisaation tietoturvapolitiikkaan. Tähän dokumenttiin kannattaa sisällyttää myös lyhyt kuvaus organisaation toimitiloista ja organisaatioyksiköistä. Kuvaus ei ole pakollinen, mutta sertifioijat haluavat usein nähdä sen. (Kosutic 2014-10-13.)

4.2.2 Johto ja tuki

Organisaation ylimmän johdon täytyy osoittaa johtajuutta ja sitoutumista tietoturvallisuuden hallintajärjestelmään. Johdon täytyy varmistaa (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 10)

- tietoturvapolitiikan ja tietoturvatavoitteiden dokumentointi ja yhdenmukaistaminen organisaation muiden strategioiden ja prosessien kanssa
- hallintajärjestelmän vaatimuksien yhdistäminen muihin prosesseihin
- hallintajärjestelmän vaatimien resurssien saatavuus
- kommunikointi sidosryhmille järjestelmän toimivuudesta ja vaatimusten noudattaminen
- hallintajärjestelmän tulosten saavutus
- hallintajärjestelmän kehityksestä vastaavan henkilöstön ohjaus
- hallintajärjestelmän jatkuva kehitys
- tuki muulle johdolle
- tietoturvallisuuden roolien ja niiden vastuiden määrittely
- hallintajärjestelmän suorituskyvyn raportoinnin vastuuhenkilöiden määrittäminen.

Johdon on laadittava tietoturvapolitiikka ja määritettävä se organisaation toimintaan sopivaksi. Politiikan tulisi sisältää tietoturvatavoitteet, sitoutumisen tietoturvallisuuden hallintajärjestelmän vaatimusten täyttöön sekä kehitykseen. Tämän tietoturvapolitiikan on oltava dokumentoituna koko organisaation ja tarvittaessa myös muiden sidosryhmien saatavilla. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 10.)

4.2.3 Riskien arviointi ja käsittely

Tietoturvallisuuden hallintajärjestelmän suunnittelussa on huomioitava sidosryhmät ja niiden tietoturvavaatimukset, suojattaviin kohteisiin kohdistuvat riskit sekä mahdolliset poikkeamat. Näin voidaan varmistaa haluttujen tulosten saaminen, kehittää järjestelmää jatkuvasti sekä vähentää ja mahdollisuuksien mukaan kokonaan estää negatiivisia vaikutuksia. Riskeille ja mahdollisille muille tapahtumille on suunniteltava toimenpiteet ja mietittävä, miten toimenpiteet arvioidaan, yhdistetään ja toteutetaan tietoturvallisuuden hallintajärjestelmässä. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 12.)

Organisaation määrittelemät tietoturvariskit täytyy arvioida ja laatia näille riskeille hyväksymiskriteerit ja arvioinnin suorituskriteerit. Riskien arvioinnissa on varmistettava yhdenmukaiset ja pätevät tulokset, joita voidaan tarvittaessa myöhemmin verrata. Arviointeja on suoritettava ja dokumentoitava säännöllisin väliajoin ja muutoksia ehdotettaessa tai muutosten tapahtuessa. Riskeille on määriteltävä (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 12.)

- riskin kohdistuminen (eheys, luottamuksellisuus, saatavuus)
- omistaja
- seuraukset
- todennäköisyys

- riskin taso
- riskianalyysin vertaaminen riskikriteereihin
- riskien käsittelyn priorisointi
- riskien käsittelyn suunnittelu ja toteutus riskien arviointia apuna käyttäen.

Organisaation on luotava ns. Statement of Applicability -dokumentti, joka toimii linkkinä riskien arvioinnin ja käsittelyn sekä tietoturvallisuuden toteutuksen välillä. Dokumentissa määritellään, mitä omia tai ISO 27002 -hallintakeinoja käytetään tietoturvallisuustoteutuksissa. Kontrollien käyttö tai käyttämättä jättäminen täytyy perustella. Hyvä tapa on myös kuvata, miten keinot on toteutettu. (Kosutic 2011-04-18.)

Organisaation on määritettävä tietoturvatavoitteet, jotka ovat yhdenmukaisia tietoturvapolitiikan kanssa, ja otettava tavoitteissa huomioon riskianalyysin tulokset sekä tietoturvavaatimukset. Tavoitteiden suunnittelussa täytyy määrittää toimet tavoitteiden saavuttamiseksi, tarvittavat resurssit, vastuuhenkilöt, valmistumisaika ja tulosten arviointi. Tavoitteet on saatava dokumentoituna tietona, päivitettävä ja niistä on viestittävä. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 12.)

4.2.4 Toiminta

Organisaatiossa on oltava prosessit ja suunnitelmat, joilla täytetään tietoturvavaatimukset, riskienhallinta- ja tietoturvatavoitteiden saavutus ja toteutus. Näistä prosesseista ja suunnitelmista on säilytettävä dokumentteja. Ulkoistetut prosessit on eriteltävä ja valvottava. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 18.)

Suunniteltujen tai suunnittelemattomien muutosten tapahtuessa on arvioitava niiden vaikutuksia ja pyrittävä vähentämään haittavaikutuksia. Tähän kuuluu myös riskien säännöllinen arviointi, vaikka muutoksia ei tapahtuisikaan. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 18.)

4.2.5 Suorituskyvyn arviointi

Organisaation on seurattava ja mitattava tietoturvallisuuden tehokkuutta ja tietoturvallisuuden hallintajärjestelmän vaikuttavuutta. Mittauksissa ja seuraamisessa on määritettävä, mitä, millä ja milloin mitataan. Näiden lisäksi on määriteltävä myös henkilöstöroolit, kuten mittauksien toteuttaja ja analysointituloksien katselmoija. Analysoinnille on määritettävä suoritusväli. Seuraamisen ja mittaamisen tuloksista on säilytettävä dokumentointi. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 20.)

Tietoturvallisuuden hallintajärjestelmä on auditoitava suunnitelluin aikavälein. Auditoinnissa tarkistetaan järjestelmän vaatimusten mukaisuus ja sen vaikuttavuus. Auditointisuunnitelmat on oltava tarkoin määritelty ja dokumentoitu. Auditoinnin on oltava puolueetonta ja tuloksista on raportoitava johdolle sekä säilytettävä dokumentointia todisteena sekä auttamaan tulevaisuuden auditointeja. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 20.)

Organisaation ylimmän johdon on osallistuttava tietoturvallisuuden hallintajärjestelmän katselmointiin. Katselmoinnissa varmistetaan hallintajärjestelmän nykytilan soveltuvuus, asianmukaisuus ja tehokkuus. Katselmoinneissa on otettava huomioon tietoturvan hallintajärjestelmän kannalta tapahtuneet olennaiset muutokset, auditointien tulokset, tietoturvaan liittyvä palaute, aiempien katselmusten takia käynnistetyt toimenpiteet, riskien nykyinen arviointi ja hallintapolitiikka ja hallintajärjestelmän parantaminen. Tulokset on dokumentoitava ja niissä on oltava esillä mahdolliset parannus- tai muutosmahdollisuudet. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 22.)

4.2.6 Tietoturvallisuuden hallintajärjestelmän jatkuva parantaminen

Tietoturvallisuuden hallintajärjestelmää on parannettava jatkuvasti. Poikkeamien tapahtuessa niihin on reagoitava ja käsiteltävä niistä aiheutuneet haitat ja seuraukset. Poikkeamien syyt on selvitettävä ja toteutettava toimenpiteet niiden ennaltaehkäisemiseksi tulevaisuudessa. Näiden toimenpiteiden tehokkuus on arvioitava. Poikkeamista, niiden syistä ja niihin suunnatuista korjaustoimenpiteistä ja toimenpiteiden tuloksista on säilytettävä dokumentoitu tieto. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 22.)

4.3 Standardin vaatima dokumentointi

Tässä luvussa on luetteloitu ISO/IEC 27001 -standardin vaatimat dokumentit. Dokumenttien sisällöstä ja vaatimuksista on kerrottu tarkemmin luvussa 4.2. Osa dokumenteista voi olla yhdistettyjä samaan dokumenttiin, jolloin dokumenttien ei välttämättä tarvitse olla erillisiä.

Dokumentointia laadittaessa täytyy ottaa huomioon sen asianmukaisuus. Dokumenttiin täytyy olla merkittynä otsikko, päiväys, laatija, viitenumero, muokkaaja ja muokkauspäiväys. Dokumenttien soveltuvuus ja riittävyys on tarkistettava ja hyväksyttävä. Dokumentointi on myös oltava saatavilla sopivassa muodossa ja ne on asianmukaisesti suojattu, säilytetty sekä luokiteltu dokumentin luottamuksellisuuden mukaan. (Tietoturvallisuuden hallintajärjestelmän vaatimukset 2013, 18.)

Kaikki seuraavat dokumentit ovat pakollisia jos organisaatio tähtää sertifiointiin: (Kosutic 2013-09-30.)

- tietoturvallisuuden hallintajärjestelmän kattavuusdokumentti
- tietoturvapolitiikka
- Statement of Applicability
- tietoturvariskien arviointiprosessi ja arvioinnin tulokset
- tietoturvariskien käsittelysuunnitelma
- tietoturvatavoitteet
- tietoturvallisuuteen liittyvän henkilöstön roolit ja vastuut
- tarvittavat salassapito- ja vaitiolosopimukset
- luettelo suojattavista kohteista ja niiden hyväksyttävästä käytöstä
- pääsynhallintapolitiikka
- tietojenkäsittelyn toimintaohjeet

- turvallisen järjestelmän suunnittelun periaatteet
- tietoturvavaatimukset ulkopuolisista toimittajista johtuvista riskeistä
- häiriönhallintaprosessit
- tietoturvallisuuden hallinnan jatkuvuusprosessi
- lakien, viranomaisten ja sopimusten asettamat vaatimukset sekä toimintamalli vaatimusten täyttämiseen.

Seuraavassa luettelossa on sertifioinnin vaatimat mittaukset ja tulokset: (Kosutic 2013-09-30.)

- sisäinen auditointiohjelma ja sen tulokset
- tietoturvan tason ja tietoturvallisuuden hallintajärjestelmän mittaus- ja seurantatulokset
- näyttö henkilöstön pätevyydestä, jotka vaikuttavat tietoturvan tasoon ja sen ohjaukseen
- johdon katselmuksen tulokset
- havaitut poikkeamat, virheet, tietoturvatapahtumat ja niihin tehdyt korjaustoimenpiteet
- lokitiedot käyttäjien suorittamista toiminnoista
- lokitiedot pääkäyttäjien ja operaattoreiden suorittamista toiminnoista.

4.4 Sertifiointiprosessi

Yleisesti sertifoinnilla tarkoitetaan, että organisaation palvelussa, tuotteessa, henkilöstön osaamisessa tai johdossa täytetään kansainväliset, kansalliset tai paikalliset vaatimukset. Sertifioinnin suorittaa yleensä jokin kolmas puolueeton osapuoli.

Sertifioimalla organisaatiolle ISO/IEC 27001 -tietoturvallisuusstandardi, osoitetaan organisaation henkilöstölle sekä muille sidosryhmille, kuten asiakkaille, yrityksen panostuksesta tietoturvallisuuteen ja luotettavuudesta. Sertifioinnilla on myös suuri merkitys markkinoiden kilpailutuksissa. (Inspecta 2013.)

Ensimmäiseksi organisaatio tekee päätöksen ISO/IEC 27001 -tietoturvallisuusstandardin toteutuksesta. Johto sitoutuu koko projektiin ja jakaa standardisointiprojektin tehtävät vastuussa olevalle henkilöstölle. (Kuvio 2.)

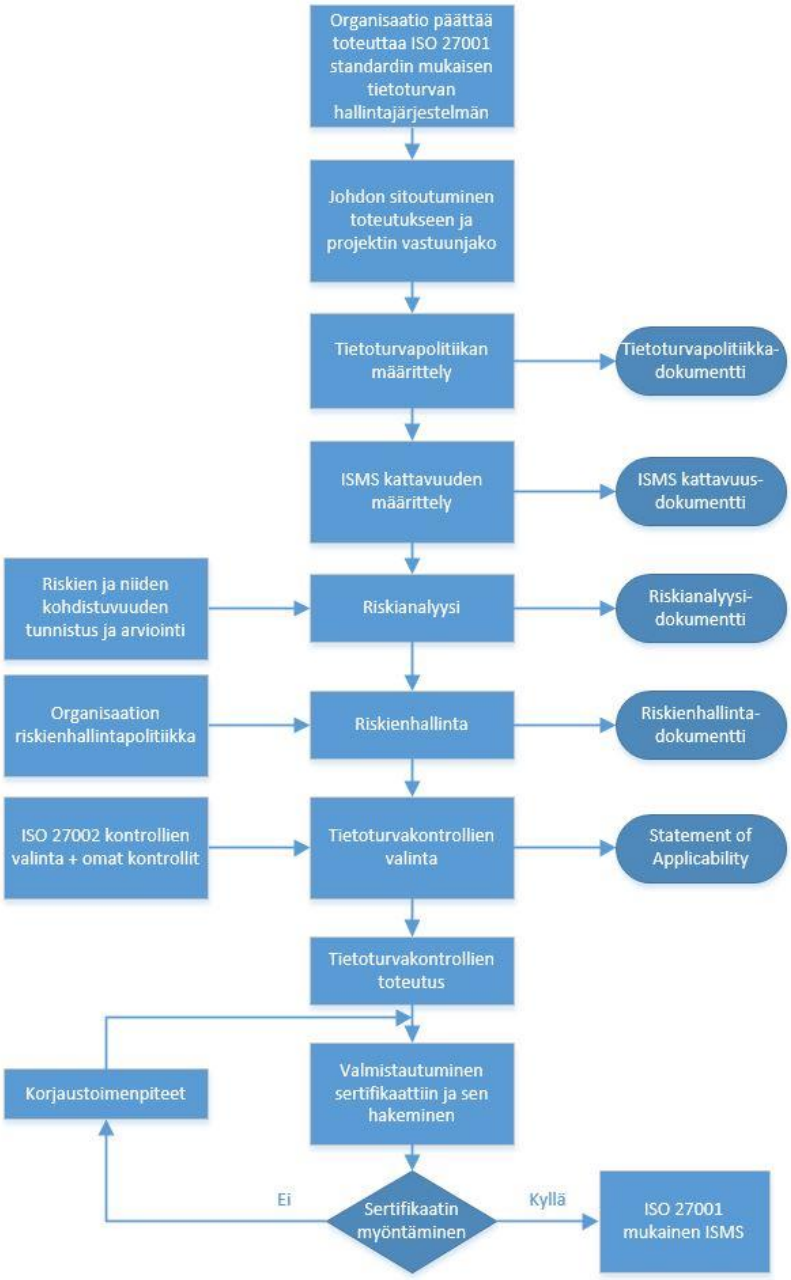
Toteutus alkaa määrittämällä tietoturvallisuuden hallintajärjestelmän kattavuus ja suojattavat resurssit. Kattavuuden ympärille luodaan standardin vaatimusten mukainen dokumentointi ja tietoturvallisuusprosessit. Organisaation täytettyä kaikki standardin vaatimukset se voi hakea sertifiointia valtuutetulta sertifiointikumppanilta. (Kuvio 2.)

Valtuutettu sertifiointikumppani tarkastaa organisaation vaatimustenmukaisuuden luotujen dokumenttien avulla. Tärkeitä dokumentteja sertifiointivaiheessa ovat tietoturvallisuuden hallintajärjestelmän kattavuusdokumentti, riskianalyysit ja Statement of Applicability, jossa on lueteltu, mitkä hallintakeinot on toteutettu. (BSI Group 2015.) Sertifiointiyrityksen auditoija tarkastaa kaikki vaaditut hallintakeinot sertifikaattia hakevan organisaation toimitiloissa (Kosutic 2011-04-18).

Jos organisaatio ei täytä kaikkia vaatimuksia, sertifikaattia ei saada ja organisaatio tekee tarvittavat toimenpiteet havaittujen puutteiden osalta. Tämän jälkeen organisaatio voi hakea uudelleenarviointia. (Kuvio 2.)

Organisaation täyttäessä vaatimukset se saa ISO/IEC 27001 -sertifikaatin, joka on voimassa kolme vuotta. Tämän voimassaoloajan aikana organisaatioon tehdään säännöllisiä tarkastuksia, joilla varmistetaan vaatimuksien mukainen tietoturvallisuuden hallintajärjestelmän jatkuva ylläpito ja parantaminen. (BSI Group 2015.)

Seuraavassa kuviossa on kuvattu standardin sertifiointiprosessi. (Kuvio 2.)



KUVIO 2. ISO/IEC 27001 sertifiointiprosessi (The ISO 27000 Directory 2013.)

4.5 ISO/IEC 27002 -standardin hallintakeinot

ISO/IEC 27001 -standardiin sisältyy velvoittava liite, jossa on lueteltu erilaisia hallintakeinoja. Keinot on lueteltu tarkemmin ISO/IEC 27002 -standardissa, jossa on myös yksityiskohtaisemmat toteuttamisohjeet näiden keinojen käyttöönottamiseksi.

Hallintakeinot on jaettu 14 pääkohtaan ja pääkohdat edelleen pienempiin osa-alueisiin. Yhteensä standardin uudessa vuoden 2013 versiossa on 114 hallintakeinoa. Pääkohtia ovat mm. tietoturvapolitiikat, henkilöstöturvallisuus, pääsynhallinta, salaus ja fyysinen turvallisuus. (Kosutic 2011-04-18.)

Hallintakeinot ovat käytännön toteutuksia, joita käytetään tietoturvallisuuden hallintajärjestelmän suunnitelmassa ja toteutuksessa. Keinot ovat yleisesti hyväksyttyjä, joilla organisaatiot voivat parantaa tietoturvallisuutta. Hallintakeinot ovat velvoittavia, jotka täytyy ottaa käyttöön jos liitteessä olevat keinot liittyvät organisaatioon kohdistuviin riskeihin. (Raggad 2010, 492.)

Yksi standardin ISO/IEC 27001 -standardin vaatimuksista on laatia dokumentti toteutetuista hallintakeinoista, eli Statement of Applicability. Toteuttamattomat keinot luetellaan myös tähän dokumenttiin. Dokumenttissa kerrotaan myös perustelut toteutuksen syistä. Hallintakeinoja voi luoda omiakin, joilla tietoturvallisuutta ylläpidetään ja parannetaan. (Kosutic 2011-04-18.)

5 SERVICE DESKIN TIETOTURVAN STANDARDISOINTI

Enfolla on tällä hetkellä ISO/IEC 27001 -standardin mukaisesti sertifioitu tietoturvallisuuden hallintajärjestelmä konesalipalveluissa Kuopiossa ja Karlskronassa Ruotsissa. Seuraava vaihe oli Suomen Service Deskin liittäminen tähän hallintajärjestelmään. Standardisointiprosessia ei tarvinnut aloittaa aivan alusta, koska tietoturvallisuuden hallintajärjestelmä oli jo toiminnassa ja standardin vaatimat dokumentit laadittu aiemmassa sertifiointiprojektissa. Esimerkiksi Enfolla on dokumentoitu tietoturvapolitiikka, joka myös on standardin vaatimus. Ainoastaan Service Deskin osalta täytyi tehdä tarvittavat muutokset dokumentointiin, tunnistaa suojattavat resurssit, laatia riskianalyysit ja riskienhallintatoimenpiteet.

Työ aloitettiin tutkimalla standardin vaatimukset sekä näiden vaatimat dokumentit. Vaatimuksien pohjalta hallintajärjestelmän rajaukseksi valittiin Service Desk. Rajauksen sisällä tunnistettiin suojattavat resurssit, valittiin näille omistajat, sekä analysoitiin näihin kohdistuvat riskit. Lopuksi riskeille valittiin hallintakeinot, että riskit saatiin vähennettyä sallittujen rajojen alle. Keinojen valvonta jäi Service Deskin vastuulle eikä kuulunut enää tähän opinnäytetyöhön valvonnan vaatiman ajan takia.

5.1 Service Deskin yleiskuvaus

Sertifioinnin toteutus alkoi määrittelemällä Service Desk yleisellä tasolla. Kuvauksessa käsiteltiin Service Deskin yleisiä asioita, kuten sijainti, vastuuhenkilöt, yhteyshenkilöt, palvelukuvaukset, riippuvuussuhteet eri sidosryhmien kanssa. Asiat käsiteltiin hyvin käytännöllisellä tasolla, joten liian tarkkoja yksityiskohtia kuvauksessa ei käsitelty. Tarkoitus oli hahmottaa rajat tietoturvallisuuden hallintajärjestelmälle, eli kattavuudelle.

Riippuvuussuhteiden määrittelyn avulla hahmotettiin paremmin Service Deskin rajat ja ne asiat, joista Service Desk on itse vastuussa. Tähän kuuluivat mm. mistä Service Desk on riippuvainen ja mitkä tahot ovat riippuvaisia Service Deskistä. Esimerkiksi Service Deskin verkkoyhteyksistä vastaa Enfon verkkoasiantuntijat, joten verkkoihin kohdistuvat riskit ulkoistetaan tälle ryhmälle. Kuitenkin Service Deskin käyttäjillä on vastuu työasemien ja verkkoyhteyden hyväksyttävästä käytöstä ja tämä otettiin huomioon riskianalyyseissä.

Service Desk tarjoaa tukipalveluja asiakkaille, joten Service Desk on vastuussa tästä tarjotusta palvelusta ja turvallisesta palvelun toteutuksesta. Tässä tapauksessa riskit kohdistuvat suurimmaksi osaksi Service Deskin henkilöstön tekemiin toimenpiteisiin, joten henkilöstöllä täytyy olla ohjeistukset ja palveluihin liittyvät käytännöt ja toimintaprosessit hyvin tiedossa.

Yleisesti Service Deskin tarjoamat palvelut sidosryhmille sekä sidosryhmien palvelut Service Deskille on määritelty palvelutasosopimuksissa. Näissä sopimuksissa kerrotaan, mitkä palvelut sopimukseen kuuluvat ja kenelle esimerkiksi sopimusrikkomuksien tapahtuessa aiheutuvat sanktiot kuuluvat.

Yleiskuvauksen määrittely tapahtui useiden vastuuhenkilöiden ja henkilöstön haastatteluilla sekä Enfon oman valmiin dokumentoinnin avulla. Yleiskuvaukseen sisältyi myös Service Deskin tuottamien palveluiden ja niiden omistajien määrittäminen. Service Deskin palvelut jaetaan kuuteen eri luokkaan, jotka on lueteltu taulukossa 1. Näitä palveluja käytetään työpyyntöjen luokittelussa ja ne valitaan asiakkaan haluaman palvelun mukaan. Esimerkiksi Active Directory -käyttäjätunnusten oikeusmuutokset kuuluvat pääsääntöisesti Access Rights Management -palveluun.

TAULUKKO 1. Service Deskin palvelukuvaukset

Palvelu	Kuvaus
Access Rights Management	Käyttöoikeuksien tukipalvelut
Workstation User Support	Työasemien tukipalvelu
Work Order Management	Työpyyntöjen hallinta
Mobile Device User Support	Mobiililaitteiden tukipalvelu
On-Site User Support & Incident Management	Tuki ja vianselvitys asiakkaan toimitiloissa
On-Site Service	Lähitukipalvelut

Tuloksena Service Deskin yleiskuvauksesta syntyi yleiskuvausdokumentti, johon on kuvattu Service Deskin vastuualueet, liiketoiminta-arvo, toimintaperiaate, palvelukuvaukset, vastuuhenkilöt ja laadunhallinta.

5.2 Suojattavien resurssien tunnistaminen

Suojattavilla resursseilla tarkoitetaan kaikkea sitä, mikä on organisaatiolle tärkeää ja minkä eheys, luottamuksellisuus ja saatavuus täytyy suojata. Resursseihin voi kuulua laitteet, ohjelmistot, informaatio, fyysiset tilat, henkilöstö, palvelut ja prosessit. (Kosutic 2014-05-27.) ISO/IEC 27001 -standardin mukaan suojattavista resursseista on laadittava luettelo, joka on pidettävä ajan tasalla. Jokaiselle resurssille on määriteltävä omistaja ja resurssit on luokiteltava. (Tietoturvallisuuden hallintajärjestelmien vaatimukset 2013, 26.)

Resurssien luetteloiminen on tärkeää varsinkin, jos riskien arviointi tehdään näiden resurssien perusteella, sillä kunkin rersurssin riskit arvioidaan erikseen (Kosutic 2014-05-27). Dokumentoituja resursseja ja niiden omistajuutta voidaan tarvita muuallakin kuin tietoturvallisuuden hallintajärjestelmän yhteydessä. Syitä voivat olla mm. työturvallisuus, vakuutukset tai talous. (Tietoturvallisuuden hallintakeinojen menettelyohjeet 2013, 40.)

Resursseille nimetyt omistajat ovat vastuussa siitä, että resursseihin liittyvä tieto on asianmukaisesti suojattu. Omistajaksi nimetään yleensä resurssia käyttävä henkilö tai henkilö, jolla on laajempi hallintavastuu kyseiseen resurssiin. Nimetyllä omistajalla ei välttämättä ole resurssiin omistajuusoikeuksia. (Kosutic 2014-05-27; Tietoturvallisuuden hallintakeinojen menettelyohjeet 2013, 40.) Organisaation hallussa oleva tieto on myös resurssi, ja se täytyy luokitella ja suojata organisaation luokittelukäytäntöjen mukaisesti (Tietoturvallisuuden hallintakeinojen menettelyohjeet 2013, 42).

Service Deskissä tarkoitus oli suojata sen tuottama palvelu. Palvelut on luokiteltu taulukossa 1. Palvelu tuotetaan Service Deskin toimistossa ja siellä olevilla työasemilla ja verkkolaitteilla, joten nämäkin ovat resursseja, joille täytyy tehdä riskianalyysi. Työntekijät ovat vastuussa työasemien, matkapuhelimien ja verkkolaitteiden hyväksyttävästä käytöstä, vaikka näiden tekninen ylläpito ja saatavuus ovat Enfon muiden sisäisten sidosryhmien vastuulla. Vastuiden erittely otettiin huomioon tietoturvallisuuden hallintajärjestelmän kattavuudessa, jonka sisällä suojattavat resurssit tunnistettiin.

Resurssien määrittelyssä pohdittiin Service Deskille mietityn kattavuuden perusteella, mitkä palvelut ja niiden tuottamiseen tarvittavat asiat ovat tärkeitä ja kriittisiä Service Deskin liiketoiminnan kannalta. Tunnistaminen tehtiin Service Deskin johtajan kanssa. Resursseiksi tunnistettiin palvelut, työasemat, matkapuhelimet, toimistotilat, henkilöstö ja monet prosessit, kuten etätyö-, perehdytys-, rekrytointi- ja liiketoimintaprosessit.

Standardin vaatimusten mukaisesti resursseista laadittiin Service Deskin johdon avulla luettelo. Luetteloon merkittiin resursseittain omistajat, tunnistamispäivämäärät ja kuvaukset. Resurssien merkitys luokiteltiin riskianalyysivaiheessa, josta Enfolla on omat luokittelu- ja riskienhallintapolitiikat.

Resurssien omistajaksi valittiin yksi tai useampi Service Deskin esimies. Valintakriteereinä olivat esimiesten vastuualueet ja resurssien laajuus eli se, käyttääkö sitä yksi vai useampi henkilö. Esimerkiksi jokaiselle taulukon 1 palveluille on määritetty oma palveluvastaavansa, mutta etätyöprosessi kuuluu jokaiselle Service Deskin asiakastiimille, joten etätyöprosessin omistajiksi valittiin kaikki tiimiesimiehet.

5.3 Riskianalyysi

Riskianalyysi on monivaiheinen prosessi. Se alkaa riskienhallintapolitiikan luomisella, joka tässä opinnäytetyössä oli luotu jo aiemmassa konesalipalveluiden sertifiointiprosessissa. Riskit tunnistetaan resursseittain ja arvioidaan tämän politiikan mukaisesti. Lopuksi riskeille valitaan hallintakeinot ja riskit uudelleenarvioidaan hallintakeinojen tehokkuuden varmistamiseksi.

5.3.1 Riskienhallintapolitiikka

Riskienhallintapolitiikan tarkoituksena on muodostaa yhdenmukainen riskien arviointi- ja hallintasuunnitelma. Politiikassa kerrotaan riskienhallinnan tavoitteet, merkitys liiketoiminnalle, lakien noudattamisen edellytys, riskien arviointikriteerit, organisaation riskienhallintaroolit ja riskien audiointiprosessit. (Enfo Oyj 2014e.) Enfon riskienhallintapolitiikka toimi tässä opinnäytetyössä käytetyn riskianalyysin perustana ja riskit arvioitiin tämän politiikan mukaisesti.

5.3.2 Riskien tunnistaminen

Seuraava vaihe oli riskien tunnistaminen resurssi- ja palvelukohtaisesti. Riskit tunnistettiin erikseen jokaisen resurssin omistajan ja Service Deskin johdon kanssa.

Tunnistamisessa pyrittiin saamaan mahdollisimman täydellinen luettelo mahdollisista uhkista ja haavoittuvuuksista. Haavoittuvuudella tarkoitetaan asiaa, jota uhkat voivat käyttää vahingontekoon (Tietoturvariskien hallinta 2013, 38). Riskejä havaittiin organisaation sisällä ja ulkopuolella. Merkittävä osa riskeistä johtui henkilöstön tekemistä inhimillisistä virheistä. Service Desk –palvelu on asiakaspalvelutyötä ja henkilöstön tiedot ja taidot vaikuttavat suuresti työn laatuun ja suoritukseen.

Toinen merkittävä riskiryhmä oli etätyö, jossa Service Deskin työasemia viedään toimiston ulkopuolelle. Etätyöntekijän omassa kotiverkossa työasemat ja sen sisältämät arkaluontoiset tiedot voivat joutua helpommin väärien henkilöiden käsiin kuin Service Deskin valvotussa ympäristössä. Etätyöstä ei ollut mitään henkilöstön tiedossa olevaa virallista dokumentointia ja siitä ohjeistettiin käyttäjiä vain suullisesti.

Ulkoistettavat riskit olivat kolmas merkittävä ryhmä. Service Desk on hyvin riippuvainen muiden sidosryhmien toimittamista palveluista, jotka selvitettiin alustavassa yleiskuvausdokumentissa. Esimerkiksi verkko- ja palvelinlaitteiden saatavuus ei ole Service Deskin ylläpidossa, eikä tämä voi vaikuttaa niiden saatavuuteen.

5.3.3 Riskien arviointi

Riskien arvioinnissa painoarvona oli liiketoiminnallinen kriittisyys, seurauksien laajuus (Impact) ja todennäköisyys (Probability). Liiketoiminnallisesti kriittisimmät resurssit ovat tärkeimpiä ja niiden prioriteetti on korkea.

Riskien arvioinnissa mitattiin todennäköisyyttä ja seurauksien laajuutta. Seurauksien laajuudella tarkoitettiin sitä, kuinka suureen osaan organisaatiota, liiketoimintaa, palveluita tai henkilöstöä riskit voivat kohdistua. Todennäköisyydella mitattiin, kuinka suurella todennäköisyydellä riski toteutuu. Molemmissa käytettiin viisiportaista asteikkoa ja kaikilla sanallisilla arvoilla oli myös numeerinen arvo. Numeerisella arvolla laskettiin riskin seurauksien ja todennäköisyyden perusteella riskin todellinen prioriteetti. Laskemiseen käytettiin kaavaa 1.

$$\text{Prioriteetti} = \text{Todennäköisyys} * \text{Seuraus} \quad (1)$$

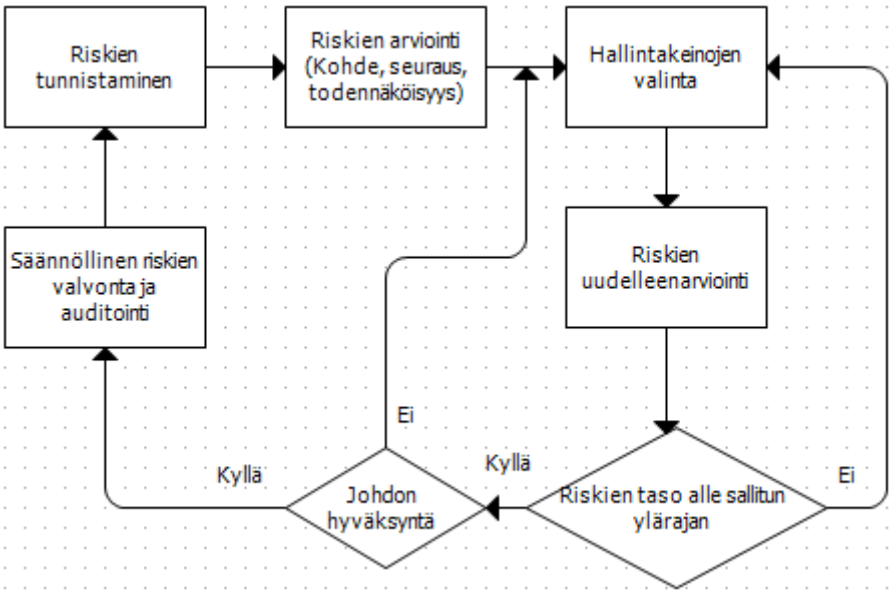
Kuvassa 8 on kuvattu todennäköisyyden ja seurauksien perusteella lasketut prioriteetit ja niiden hyväksymisrajat. Vihreät Accepted-prioriteetin riskit ovat hyväksyttäviä ja sallittujen rajojen alapuolella. Extreme-prioriteetin riskit ovat sellaisia, joihin täytyy reagoida välittömästi riskien vähentämiseksi. Medium- ja Major-prioriteetin riskeillä on omat valvontavaatimukset ja vähentämistä koskevat reagointiajat, jotka oli määritetty Enfon riskienhallintapolitiikkaan.

		Probability				
		RARE	UNLIKELY	POSSIBLE	LIKELY	ALMOST CERTAIN
Impact	NEGLIGIBLE	Accepted	Accepted	Accepted	Accepted	Medium
	MINOR	Accepted	Accepted	Medium	Medium	Major
	MODERATE	Accepted	Medium	Major	Major	Major
	MAJOR	Medium	Major	Major	Extreme	Extreme
	CATASTROPHIC	Medium	Major	Extreme	Extreme	Extreme

KUVA 8. Riskien prioriteettiasteikko (Enfo Oyj 2014e.)

Riskeille arvioitiin seurauksien ja todennäköisyyksien lisäksi pääkohde ja aiheuttaja. Riskien tapahtuessa se voi kohdistua kolmeen eri asiaan: tiedon eheyteen, luottamuksellisuuteen tai saatavuuteen. Jokaiselle riskille tunnistettiin, mihin kolmesta kohteesta se vaikuttaa merkittävimmin. Aiheuttaja voi olla jokin ulkoinen tekijä, tuntematon, käyttäjä, ylläpitäjä tai palvelu.

Kokonaisarviointi tehtiin analyysivaiheessa kaksi kertaa, ennen ja jälkeen vähennystoimia. Aluksi riskeille arvioitiin prioriteetti, kun riskeille ei tehty vielä mitään. Riskien käsittelyn, eli hallintakeinojen valinnan jälkeen riskit arvioitiin uudelleen. Jos riskien prioriteetti oli alle sallitun ylärajan, riskeille ei valittu enää lisää hallintakeinoja. Riskien ollessa liian suuria, muutettiin hallintakeinot sopivammiksi tai lisättiin uusia, että prioriteetti saatiin alle sallitun ylärajan. Arviointivaiheessa oli tärkeää varmistaa, että Service Deskin johto hyväksyi jäännösriskit. (Kuvio 3.)



KUVIO 3. Riskien arviointiprosessi (Mikkonen 2015-03-23.)

5.3.4 Riskien käsittely

Käsittelyvaiheessa hallintakeinojen valinnassa täytyy huomioida keinojen toteutuksen kustannus, tehokkuus, organisaation tietoturvapolitiikan noudattaminen, lait ja säännökset, tekniset vaatimukset ja luotettavuusvaatimukset (Raggad 2010, 95). Kaikkia riskejä on mahdotonta poistaa kokonaan

ja se on taloudellisesti kannattamatonta. (Tietoturvariskien hallinta 2013, 48). Service Deskissä hallintakeinot valittiin näiden kriteerien perusteella. Vähäisiin riskeihin ei kannattanut panostaa rahallisesti tai organisaatiomuutoksilla.

Service Deskin nykyinen tietoturva oli jo hyvällä tasolla ja havaittujen riskien prioriteetti oli jo alkuvaiheessa pieni, joten kovin paljon uusia hallintakeinoja ei tarvinnut pohtia. Puutteita löytyi olemassa olevien keinojen toteutuksista ja dokumentoinnista. Jotkin keinot oli suunniteltu, mutta näitä ei ollut toteutettu tai toteutus oli vasta alkuvaiheessa.

Riskien prioriteettien vähentäminen aloitettiin kriittisyysjärjestyksessä. Työvaihe helpottui joidenkin palveluiden osalta, koska alustavia hallintakeinoja oli toteutettuna aiemmista riskianalyyseistä. Palveluiden, joiden alustava riskianalyysi oli tehty, nykyiset hallintakeinot tarkastettiin sekä arvioitiin prioriteetit tarvittaessa uudelleen. Osaan resursseista ja palveluista hallintakeinot täytyi valita ensimmäistä kertaa.

TAULUKKO 2. Riskien käsittelytoimet (Enfo Oyj 2014e).

Toiminta	Kuvaus
Hyväksyminen	Riskin prioriteetti on sallittujen rajojen sisällä ja riskejä vain valvotaan.
Välttäminen	Riskiä tapahtumista vähennetään välttämällä sitä vaihtoehtoisilla toimilla.
Vähentäminen	Riskin todennäköisyyttä ja seurauksia vähennetään tarvittavilla hallintakeinoilla.
Siirtäminen	Vastuu riskistä siirretään toisille sidosryhmille.
Säilyttäminen	Riskiä ei vähennetä, mutta se tiedostetaan ja tiedotetaan riskin vaikuspiiriin kuuluville, jotta siihen voidaan varautua.

Riskien käsittelyssä riskeille voidaan tehdä taulukon 2 mukaiset toimet, jotka riippuvat riskien tyypistä. Esimerkiksi Service Deskissä olevat palvelimien tai verkkoyhteyksien saatavuuteen liittyvät riskit siirrettiin Service Deskiltä kyseisistä asioista vastaaville asiantuntijoille.

Toisena esimerkkinä on Service Deskin sähkönsyöttö, joka kuuluu kiinteistön omistajan vastuulle. Sähkökatkokset ovat mahdollisia ja niitä on hankala hallita kustannustehokkaasti, koska se vaatisi paljon investointeja varasähkönsiirtoon. Sähkökatkosten takia kaikki verkkoyhteydet katkeavat toimistosta ja kannettavat tietokoneet jäävät akun varaan. Kustannussyistä riski säilytettiin ja siihen valittiin hallintakeinoiksi toisen Puolassa sijaitsevan Service Desk -toimiston ja etätyön hyödyntäminen sekä mahdollisesti 3G- tai 4G-tukiasemien käyttö väliaikaisena varayhteytenä.

Henkilöstöriskit osoittautuivat suurimmaksi ryhmäksi Service Deskissä. Työntekijöiden toimiin, kuten tietoturvarikkomuksiin tai oikeusjakoihin liittyvät riskit vähennettiin rekrytointiprosessien, koulutuk-

sien ja ohjeistuksien avulla. Aikaisemmin perehdytysprosesseissa ei käsitelty tietoturvallista toimintaa mitenkään, mutta tässä opinnäytetyössä perehdytyksestä vastaaville esimiehille ehdotettiin tietoturvapolitiikan lisäämistä uusien työntekijöiden perehdytysprosessiin ja lisäämään mahdollisia lisäkoulutuksia tietoturvallisuuteen liittyen.

Yhtenä henkilöstöön liittyvänä riskinä on informaation siirtäminen uudelle työntekijälle työsuhteen äkillisessä päätöksessä. Työntekijät voivat lopettaa yhtäkkiä työsuhteensa ja viedä tärkeää tietotaitoa mukanaan, jos työsuhteessa ei ole irtisanomisaikaa, jonka aikana uuden työntekijän ehtisi perehdyttää. Vastaavasti myös eräässä työtehtävässä on tällä hetkellä liian vähän työntekijöitä, jolloin kaikki työtehtävät pysähtyvät kokonaan, jos kaikki työntekijät ovat poissa. Näissä päätettiin hajottaa palvelua suuremmalle alalle, jolloin vastuuta saadaan siirrettyä useammalle henkilölle ja palvelun saatavuus saadaan säilytettyä.

Käsittelyprosessin tuloksena laadittiin Statement of Applicability -dokumentti, johon lueteltiin kaikki ISO/IEC 27001 -standardin liitteessä olevat riskienhallintakeinot. Liitteessä 1 on malli dokumentista. Mallissa on vain yksi sivu todellisesta dokumentista, jossa on kaikki standardin liitteen hallintakeinot lueteltuna.

Ensimmäisessä ja toisessa sarakkeessa on lueteltu hallintakeinot ja niiden tunnukset standardissa. Kolmas sarake kertoo keinon käyttökelpoisuuden. Neljännessä sarakkeessa on kerrottu perustelut keinon käyttöönotolle tai käyttämättä jättämiselle. Perusteluina voi olla esimerkiksi laki- tai sopimusvaatimukset, riskianalyysi ja parhaat käytännöt. Viides ja kuudes sarake kertoo hallintakeinojen toteutustavan ja sen, missä vaiheessa toteutus on. Tässä työssä keinot oli joko täysin toteutettu, osittain toteutettu tai suunnitteluvaiheessa. (Liite 1).

Suunnitteluvaiheessa olevia hallintakeinoja ei tässä opinnäytetyössä toteutettu käytännössä resurssien puutteen takia. Nämä vaativat enemmän suunnittelua, investointeja, aikaa ja kommunikointia muiden sidosryhmien kanssa. Havaituista tietoturvapuutteista ja parannusehdotuksista tiedotettiin kuitenkin Service Deskin johdolle, jolloin ylin johto tekee päätöksen riskeihin varautumisesta.

5.4 Valvonta ja auditointi

Yhtenä standardin vaatimuksesta on hallintajärjestelmän jatkuva valvonta ja parantaminen. Valvontaa suoritetaan säännöllisin väliajoin sekä muutosten tapahtuessa organisaation sisällä. Uhkia ja haavoittuvuuksia ilmenee jatkuvasti lisää ja myös riskit lisääntyvät. (Kuvio 1 ja 2.) Riskejä täytyy auditoida säännöllisesti ja tarvittaessa vähentää tehokkaammilla hallintakeinoilla jos riskien havaitaan nousevan. (Raggad 2010, 54).

Resurssien ja riskien omistajien tulee valvoa ja arvioida Service Deskille laadittua riskianalyysiä alustavan analyysin jälkeen. Resurssien omistajia ohjeistettiin keräämään standardin vaatimuksien mukaisia tuloksia kontrollien toiminnasta, jotta niitä voidaan käyttää hyväksi säännöllisissä auditoinneissa. Tuloksia ovat mm. tietoturvatapahtumien määrä ja laatu sekä niiden korjaustoimenpiteet,

käyttöoikeuksien auditointitulokset, säännöllisten auditointien tulokset ja uusien palveluiden riskianalyysit. Kaikkia edellä mainittuja tapoja hyödynnetään tietoturvallisuuden hallintajärjestelmän ja riskien auditoinneissa. Tuloksien avulla kerrotaan toimiiko nykyiset kontrollit tehokkaasti ja tarvitseeko niitä muuttaa tai lisätä.

Enfon Riskienhallinta- ja tietoturvapolitiikan mukaan omistajien lisäksi myös muilla resurssien käyttäjillä on vastuu ilmoittaa havaitsemistaan riskeistä tai tietojärjestelmien väärinkäytöksistä esimiehille. (Enfo Oyj 2014e.)

Hallintajärjestelmän ja riskien valvonnan ja auditoinnin toteutus ei kuulunut tähän opinnäytetyöhön.

6 TULOKSET

Opinnäytetyön tuloksena Service Deskille syntyivät tämän raportin lisäksi seuraavat dokumentit:

- yleiskuvaus Service Deskistä
- resurssiluettelo
- riskianalyysidokumentti jokaiselle resurssille ja palvelulle
- dokumentti valituista riskien hallintakeinoista (Statement of Applicability).

Yleiskuvausdokumentissa kuvattiin Service Deskin yleiset asiat käytännöllisellä tasolla. Dokumenttiin sisällytettiin mm. sijainti, henkilöstö, organisaatiokaaviot, palvelukuvaukset ja riippuvuussuhteet. Tietojen avulla saatiin selville, mitkä vastuualueet kuuluvat Service Deskille ja mitkä palvelut ulkoistetaan muille sidosryhmille. Dokumenttia voi käyttää myös tulevien työntekijöiden perehdytystarkoituksessa, jolloin he saavat Service Deskistä yhden dokumentin avulla paremman käsityksen.

Resurssiluettelossa tunnistettiin Service Deskin omaisuus, palvelut, työasemat, matkapuhelimet ja aineettomat asiat kuten liiketoiminta-, rekrytointi- ja etätyöprosessit. Luetteloon merkittiin omistajat ja resurssien kuvaus sekä tunnistamispäivämäärä. Luetteloa päivitetään uusia resursseja tunnistettaessa tai muokattaessa nykyisiä.

Riskianalyysidokumentissa resursseille tunnistettiin mahdolliset uhat ja haavoittuvuudet. Riskien prioriteetti arvioitiin todennäköisyyden ja seurauksien laajuuden perusteella. Hallintakeinojen valinnalla riskejä pyrittiin vähentämään sallitulle tasolle ja riskit arvioitiin vielä uudelleen riskien prioriteetin laskun varmistamiseksi.

Statement of Applicability -dokumentissa on kaikki ISO/IEC 27001 -standardin A-liitteen hallintakeinot sekä riskienkäsittelyvaiheessa valitut omat hallintakeinot. Keinoihin dokumentoitiin tieto soveltuvuudesta, nykytilasta ja pieni selitys toteuttamistavasta sekä toteuttamisen syistä.

Dokumenttien salaisuuden, tietoturvallisuuden ja arkaluontoisen materiaalin vuoksi ne eivät ole tässä raportissa esillä ja ne julkaistaan vain Enfon sisäiseen käyttöön.

Puutteita standardiin liittyvässä yleisessä tietoturvallisuudessa löytyi resurssien ja palveluiden omistajuuksista ja tietoturvan säännöllisessä valvonnasta. Omistajuudet oli määritetty pintapuolisesti, mutta monet omistajiksi nimetyt eivät olleet tietoisia omistajuuden merkityksestä ja vastuista tai koko omistajuudestaan.

Standardin mukaisesti mahdollisia riskejä ja riskienhallinnan tehokkuutta täytyy valvoa säännöllisesti, mutta tätä ei ollut toteutettu täysin. Riskianalyysejä oli tehty alustavasti, mutta sen enempää niihin ei ollut perehdytty. Jos Service Desk haluaisi joskus sertifioida palvelunsa, on sen kerättävä mittaustuloksia hallintakeinojen tehokkuudesta ja todisteita jatkuvasta valvonnasta ja tietoturvan parantamisesta.

7 YHTEENVETO

Työn tavoitteena oli tunnistaa ISO/IEC 27001 -standardin vaatimusten mukaisesti Service Deskin suojattavat resurssit ja palvelut ja tehdä näille riskianalyysi. Riskianalyysin perusteella resursseille ja palveluille pohdittiin tarvittavat hallintakeinot, joilla riskit saadaan vähennettyä. Kunkin resurssin riskit arvioitiin erikseen ja hallintakeinot valittiin kriittisyysjärjestyksessä.

Opinnäytetyön tavoitteeseen päästiin osittain. Riskianalyysit saatiin tehtyä useimmille palveluille ja resursseille. Esimiesten saatavuuden takia osa analyyseistä jäi tämän opinnäytetyön ulkopuolelle. Palveluista löytyi useita riskejä, joihin ei ollut varauduttu ennen tätä opinnäytetyötä. Tämän työn seurauksena nämä riskit tiedostetaan ja näihin voidaan nyt varautua paremmin.

Työ oli hyvin mielenkiintoinen ja työssä pääsi tutustumaan syvemmin Service Deskin toimintaan ja muihin Enfon sidosryhmiin. Työssä sai myös paremman käsityksen ISO/IEC 27001 -standardista ja tietoturvallisuuden laajuudesta organisaatioissa.

Ongelmia aiheutti kokemattomuus uudesta ISO/IEC 27001 -standardista ja liiketoimintalähtöisestä ajattelusta. Standardi oli itselle aivan uusi käsite, jonka käytännön toteutuksesta ei löytynyt paljoa kirjallisuutta lukuun ottamatta Standardisoimisliiton dokumentoituja standardeja ja asiantuntijoiden blogikirjoituksia. Standardissa käsitellään paljon organisaation liiketoimintaan kohdistuvia riskejä, joten liiketoiminnan huomioon ottaminen tuotti haasteita työn toteutukseen. Resurssien tunnistamiset ja riskianalyysit tehtiin Service Deskin johdon, tiimiesimiesten ja muiden sisäisten sidosryhmien avulla. Heidän työkiireidensä ja lomiensa takia työssä täytyi noudattaa heidän aikataulujaan.

Service Desk ei aio tällä hetkellä hakea sertifikaattia tietoturvallisuuden hallintajärjestelmälleen, mutta työn tuloksena saadut Service Deskin yleiskuvaukset, resurssiluettelot ja riskianalyysit parantavat tietoturvaa entisestään. Tulokset toimivat hyvänä pohjana, jos Service Desk aikoo myöhemmin hakea sertifikaattia. Ruotsissa toimiva Service Desk voi myös hyödyntää työn tuloksia omassa tietoturvallisuuden hallinnassaan.

LÄHTEET JA TUOTETUT AINEISTOT

BSI GROUP. Certification to ISO/IEC 27001 Information Security Management. [Viitattu 2015-02-08.] Saatavissa: http://www.bsigroup.com/en-GB/iso-27001-information-security/Certification-for-ISO-27001/

ENFO OYJ 2014a. Enfo lyhyesti. [Viitattu: 2015-01-29.] Saatavissa: http://www.enfo.fi/enfo-group/enfo-lyhyesti/

ENFO OYJ 2014b. Johdanto IT-palveluihin ja ulkoistuksiin. [Viitattu: 2015-01-29.] Saatavissa: http://www.enfo.fi/it-palvelut-ja-ulkoistukset/johdanto-it-palveluihin-ja-ulkoistuksiin/

ENFO OYJ 2014c. Service Desk ja käyttäjätukipalvelut. [Viitattu: 2015-01-29.] Saatavissa: http://www.enfo.fi/it-palvelut-ja-ulkoistukset/service-desk-ja-kayttajatukipalvelut/

ENFO OYJ 2014d. Service Deskin laatukäsikirja [sisäinen dokumentti]. [Viitattu: 2015-03-23.]

ENFO OYJ 2014e. Risk Management Policy [sisäinen dokumentti]. [Viitattu: 2015-03-23.]

ENFO OYJ 2014f. Intranet [sisäinen järjestelmä]. [Viitattu: 2015-03-20.]

INSPECTA 2013. Tietoturvajärjestelmän sertifiointi (ISO/IEC 27001). [Viitattu: 2015-02-07.] Saatavissa: http://www.inspecta.com/fi/Palvelut/Sertifiointi/Jarjestelmasertifiointi/Tietoturvajarjestelman-sertifiointi-ISO-IEC-27001/

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 2013a. ISO/IEC 27001. [Viitattu: 2015-02-20.] Saatavissa: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 2013b. ISO Survey. [Viitattu: 2015-01-30.] Saatavissa: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certificate=ISO%209001&countrycode=AF

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 2013c. ISO Survey Executive summary. [Viitattu: 2015-01-30.] Saatavissa: http://www.iso.org/iso/iso_survey_executive-summary.pdf?v2013

KOSUTIC, Dejan 2014-10-13. How to define ISMS Scope [verkkoaineisto]. 27001 Academy. [Viitattu: 2015-02-02.] Saatavissa: http://www.iso27001standard.com/blog/2014/10/13/how-to-define-the-isms-scope/

KOSUTIC, Dejan 2014-05-27. How to handle Asset register according to ISO 27001 [verkkoaineisto]. 27001 Academy. [Viitattu 2015-03-12.] Saatavissa: http://www.iso27001standard.com/blog/2014/05/27/how-to-handle-asset-register-asset-inventory-according-to-iso-27001/

KOSUTIC, Dejan 2013-09-30. List of mandatory documents required by ISO 27001 (2013 revision) [verkkoaineisto]. 27001 Academy. [Viitattu: 2015-02-04.] Saatavissa: http://www.iso27001standard.com/blog/2013/09/30/list-of-mandatory-documents-required-by-iso-27001-2013-revision/

KOSUTIC, Dejan 2011-04-18. The Importance of Statement of Applicability [verkkoaineisto]. 27001 Academy. [Viitattu: 2015-02-02.] Saatavissa: http://www.iso27001standard.com/blog/2011/04/18/the-importance-of-statement-of-applicability-for-iso-27001/

MACKIE, Ryan 2013-04-03. ISO 27001:2013 – Understanding the new standard. Brightline [verkkoartikkeli]. [Viitattu: 2015-01-30.] Saatavissa: https://www.brightline.com/2013/04/iso-270012013-understanding-the-new-standard-2/

RAGGAD, Belgacem 2010. Information Security Management. Boca Raton, Florida: Taylor & Francis Group.

ROOS, A. Tietohallinnon johtaminen. Organisaatio ja johtaminen. IT-palvelunhallinta ja ITIL. Kauppalehti [verkkojulkaisu]. [Viitattu 2015-01-30.] Saatavissa: http://johtaminen.kauppalehti.fi.ezproxy.savonia-amk.fi/book/tietohallinnon-johtaminen/organisaatio-ja-johtaminen/it-palvelunhallinta-ja-itil

THE ISO 27000 DIRECTORY 2013. An Introduction to ISO 27001. [Viitattu: 2015-01-30.] Saatavissa: http://www.27000.org/iso-27001.htm

TIETOTURVALLISUUDEN HALLINTAKEINOJEN MENETTELYOHJEET 2013. SFS-ISO/IEC 27002. Vahvistettu 2014. International Organization for Standardization ja International Electrotechnical Commission. 1. painos. Helsinki: Suomen Standardisoimisliitto.

TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMIEN VAATIMUKSET 2013. SFS-ISO/IEC 27001. Vahvistettu 2013. International Organization for Standardization ja International Electrotechnical Commission. 2. painos. Helsinki: Suomen Standardisoimisliitto.

TIETOTURVARISKIEN HALLINTA. SFS-ISO/IEC 27005. Vahvistettu 2013. International Organization for Standardization ja International Electrotechnical Commission. 2. painos. Helsinki: Suomen Standardisoimisliitto.

LIITE 1: STATEMENT OF APPLICABILITY -DOKUMENTIN MALLI

TAULUKKO 3. Statement of Applicability (Kosutic 2011-04-08).

ID	Controls according to ISO/IEC 27001	Appli-cability (YES/ NO)	Justification for selection/ non-selection	Implementation method	Status
A.5	Information security policies				
A.5.1	Management direction for information security				
A.5.1.1	Policies for information security				
A.5.1.2	Review of the policies for information security				
A.6	Organization of information security				
A.6.1	Internal organization				
A.6.1.1	Information security roles and responsibilities				
A.6.1.2	Segregation of duties				
A.6.1.3	Contact with authorities				
A.6.1.4	Contact with special interest groups				
A.6.1.5	Information security in project management				
A.6.2	Mobile devices and teleworking				
A.6.2.1	Mobile device policy				
A.6.2.2	Teleworking				
A.7	Human resource security				
A.7.1	Prior to employment				
A.7.1.1	Screening				
A.7.1.2	Terms and conditions of employment				
A.7.2	During employment				
A.7.2.1	Management responsibilities				