LAUREA

Yrityksen prosessien tietoturvariskien hallintamalli

Reid, Anne-Maarit

2010 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Yrityksen prosessien tietoturvariskien hallintamalli

Anne-Maarit Reid
Tietojärjestelmäosaamisen koulutusohjelma, ylempi AMK
Opinnäytetyö
Toukokuu 2010

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojärjestelmäosaamisen koulutusohjelma, ylempi AMK

Anne-Maarit Reid

Yrityksen prosessien tietoturvariskien hallintamalli

Vuosi 2010 Sivumäärä 56

Tämän suunnittelutieteellisen tutkimuksen tarkoituksena on suunnitella, rakentaa ja arvioida tietoturvariskien hallintamalli kohdeyrityksen eri prosesseille. Tutkimuksen tuloksena saadaan yritykselle tietoturvariskien hallintamalli, jossa näkökulmana on liiketoiminta ja sen luomat vaatimukset prosessin tietoturvan tasolle. Hallintamallia käyttämällä voi prosessin omistaja omatoimisesti arvioida prosessiin liittyviä uhkakuvia ja päättää käytettävistä turvamekanismeista. Viitekehyksenä hallintamallissa on käytetty soveltaen ISO 27001 ja 17799 standardeja. Kansainvälisesti hyväksyttyjä standardeja käyttämällä voidaan todistaa yrityksen eri prosessien sidosryhmille tietoturvan tason vastaavan niitä vaatimuksia, joita standardissa esitetään. Tutkimuksessa haluttiin myös testata kuinka hyvin ISO standardien käyttö soveltui pienen organisaation tietoturvariskien hallintamallin suunnitteluun ja luontiin.

Tietoturvallisuus on ennen kaikkea yrityksen johdon asia ja se tulisikin olla mukana, kun suunnitellaan liiketoimintastrategioita. Yhä enemmän tulevaisuudessa esitetään yrityksien yhteistyökumppanien, esimerkiksi viranomaisten tai vakuutusyhtiöiden tahoilta, vaatimuksia prosessien tietoturvan suhteen. Silloin hyvin hoidettu prosessien riskienhallinta korostuu kilpailtaessa markkinoilla muiden toimijoiden kanssa. Johdon sitoutuminen tietoturvallisuuteen alkaa yrityksen tietoturvapolitiikan luonnilla, jolla luodaan perusta organisaation tietoturvan hallintajärjestelmälle. Prosessikartat ja –kuvaukset, sekä vastuiden selkeä jako, antavat hyvän pohjan riskianalyysin tekemiselle ja valvontatavoitteiden määrittämiselle. Tietoturvariskien arvioinnissa tulisi arvioida erityisesti liiketoiminnan jatkuvuuden kannalta kriittisiä uhkakuvia ja niiden toteutumisen todennäköisyyttä.

Tutkimuksessa luotua tietoturvariskien hallintamallia testattiin kohdeyrityksen pää- ja tukiprosesseihin. Tutkimustuloksissa todettiin, että tietoturvariskien hallinnalle oli selkeä tilaus organisaatiossa. Jo testausvaiheessa huomattiin tietoturvan osalta useita puutteita testauksen kohteena olevissa prosesseissa. Hallintamallia tullaan käyttämään organisaatiossa jatkossa prosessikuvausten laadinnassa ja uusia hankintoja suunniteltaessa. Prosessien omistajat koulutetaan hallintamallin käyttöön ja jatkokehitysehdotuksena tullaan yrityksen eri prosesseille laatimaan sekä toipumis- että jatkuvuussuunnitelmat. Kohdeorganisaation tietoturvatyön tavoitteena on sitouttaa koko yrityksen henkilöstö tietoturvariskien hallintaan omassa työssään.

Asiasanat: ISO 27001, ISO 17799, riskikartoitus, suunnittelutieteellinen tutkimus, tietoturvapolitiikka, tietoturvallisuus, turvamekanismi

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Master Degree in Information Systems

Anne-Maarit Reid

Model for managing security risks in a company's processes

Year 2010 Pages 56

The purpose of this design science research is to plan, construct and evaluate a model of managing the security risks in a case organization's processes. As a result of this research the company obtains the management model focusing on business and the demands what it creates for the process security level. By using the created management model, the owner of the process is self-capable of evaluating the security threats and to decide which control requirements are used in the process. The management model's frame of reference uses ISO 27001 and 17799 standards. By using internationally certified standards, the case company can prove to its business partners that the level of security exceeds standards requirements. During this research, tests were performed against the ISO standards to ascertain the suitability and usability for a small organization.

Security is first and foremost the responsibility of the company's management and it must be considered when business strategies are planned. Increasingly in the future the different business partners demand a certain security level from the company's operations. For example, insurance companies and authorities have their own demands for security in different processes. Well designed and analysed security risk management is an asset when competing in the marketplace. The commitment of the company's management towards security work starts with the creation of the security policy. The security policy defines the framework and the targets for the whole information security management system of the company. Defining the process maps and charts and the clear division of responsibilities makes a solid foundation for risk analysis and determining the security control objectives. When evaluating the security risks, the emphasis should be on the critical risks from a business continuity point of view and must ascertain how plausible the risks are.

The constructed risk management model was tested for a case company's main and support processes. The test results proved that there was an urgent need for security management within the organization. Security flaws for the processes were recognised early in the test runs. As a conclusion of the research the case company decided to use a created management model in all the process descriptions to analyze and evaluate the security risks. The process owners are instructed to use the management model and as a future development proposal disaster recovery and business continuity plans will be made for all the processes. The goal of the security work in the case organization is to commit the whole personnel to manage security risks in their own work tasks.

Key words: design science, ISO 27001, ISO 17799, risk analysis, security policy, security, control requirement

Sisällys

1 Johdanto

Liiketoiminnan jatkuvuuden hallinta, riskien arviointi ja prosessien kuvaamiset ovat olleet jo pitkään yrityksissä johdon huolen aiheena ja tehtävien töiden listalla. Nykypäivänä ei enää riitä se, että yrityksen IT-organisaatio on kiinnostunut tietoturvariskien hallinnasta ja toipumissuunnitelmien kirjoittamisesta, vaan yhä enemmän on koko liiketoiminnan jatkuvuudenhallinta integroitava osaksi yrityksen päivittäistä toimintaa ja strategista suunnittelua. Suomessa yritysten toiminnan jatkuvuuden turvaamiseen on alettu kiinnittää yhä enemmän huomiota niin viranomaisten kuin vakuutusyhtiöidenkin taholta. Usein jatkuvuussuunnitteluprosessin yrityksessä käynnistääkin eri sidosryhmien asettamat vaatimukset yhteistyölle.

Tietoturvallisuus on vain pieni osa kokonaisuudesta, jota kutsutaan yritysturvallisuudeksi. Yritysturvallisuudella pyritään suojaamaan organisaation päivittäinen häiriötön toiminta, omaisuus, tieto, henkilöstö ja toimintaympäristö rikolliselta väärinkäytöltä. Yritysturvallisuuden eri osa-alueilla on monia yhtymäkohtia tietoturvallisuuteen esimerkiksi toimitilaturvallisuus ja yrityksen IT-laitetilat tai henkilöturvallisuus ja käyttöoikeuksien hallinta työsuhteen päättyessä. (Miettinen 1999, 16-17.)

Yrityksen tietoturvallisuutta voidaan tarkastella eri näkökulmista. Johdon näkökulmasta tarkasteltaessa kysytään miksi tietoturvallisuus on tärkeä asia yritykselle. Tietoturva-asioiden kehittäminen ja tietoturvapolitiikan luonti ovat yrityksen johdon tehtäviä. He näyttävät omalla sitoutumisellaan ja toiminnallaan suunnan yrityksen tietoturvatyölle. Tarkasteltaessa tietoturvallisuutta liiketoiminnan näkökulmasta on ensisijaisen tärkeää tunnistaa ne prosessit, joiden toiminta on kriittisintä yrityksen toiminnan jatkumisen kannalta. Kriittisten prosessien tietoturvan on oltava ajantasaista ja suunnitelmat ongelmatilanteisiin hyvin dokumentoitu ja testattu. (Miettinen 1999, 29-31.)

Kuka sitten on kiinnostunut tietoturvariskien hallinnoinnista ja uhkakuvien analysoinnista? Usein riskienhallinnasta kiinnostutaan vasta ensimmäisen tapahtuneen katastrofin jälkeen. Tietoturvallisuus, riskienhallinta ja eri standardit ovat usein liian vaikeaselkoisia ja ajallisesti paneutumista vaativia asioita, joihin yrityksen henkilöstöllä ei yksinkertaisesti aika riitä omien töiden ohella. Kriisin hetkellä usein kuuleekin sanottavan, ettei tiennyt tai osannut arvioida tällaista tietoturvariskiä olevan olemassakaan. (Harris 2008, 81.) Tämän tutkimuksen tarkoitus on luoda kohdeyrityksen käyttöön yksi yhtenäinen tietoturvariskien hallintamalli, josta löytyy kaikki ne työkalut mitä tietoturvariskien tunnistamiseen, arviointiin ja hallintaan yrityksen eri prosesseissa liittyy.

1.1 Opinnäytetyön aihe ja tutkimuskysymykset

Tämän opinnäytetyön aiheena on tutkia miten tietoturvariskejä hallitaan yrityksen eri prosesseissa. Tutkimuksessa keskitytään yrityksen tietoturvallisuuteen prosessitason näkökulmasta. Tutkimuksen tavoitteena on luoda yrityksen eri prosessien tietoturvariskien hallintamalli. Hallintamallin avulla prosessin omistaja voi arvioida prosessiin liittyviä tietoturvariskejä ja tunnistaa prosessin suojattavat kohteet sekä niiden merkityksen liiketoiminnan kannalta. Viitekehyksenä tutkimuksessa käytetään ISO 27001 ja 17799 standardeja. Standardissa 27001 esitetään vaatimukset ja turvamekanismit tietoturvallisuuden hallintajärjestelmän luomiseksi yrityksessä. Yrityksen tietoturvariskit kartoitetaan valittujen uhkien osalta ja niitä verrataan standardin vaatimuksiin ja turvamekanismeihin. IT-toimintojen sertifiointi ISO 27001 standardin mukaisesti vaatii kattavan riskianalyysin läpi organisaation eri IT -prosessien ja toimintatapojen. (ISO 27001 2006, 10.) Standardissa 17799 määritellään ohjeita ja yleisiä periaatteita tietoturvan hallinnan käynnistämiseen, käyttöönottoon, ylläpitoon ja parantamiseen. Ottamalla käyttöön standardin 27001 valvontatavoitteet ja turvamekanismit täytetään riskiarvioinnissa tunnistetut vaatimukset. 17799 standardia voidaan käyttää käytännön ohjeistuksena, jonka pohjalta kehitetään organisaation turvallisuusstandardeja ja käytäntöjä sekä lisätään luottamusta yritysten välisiin liiketoimiin. (ISO 17799 2006, 20.)

Opinnäytetyön avulla haetaan vastausta seuraaviin tutkimuskysymyksiin:

- Miten hyvin ISO 27001 ja 17799 standardit soveltuvat pienen organisaation tietoturvariskien hallintamallin luontiin eri prosesseille?
- Miten eri prosessien tietoturvariskit tunnistetaan hallintamallin avulla?
- Miten Hevnerin seitsemän ohjetta IT-artefaktin luontiin soveltuvat tämän tutkimuksen toteuttamiseen ja arviointiin?

1.2 Opinnäytetyön tavoite ja rajaus

Tämän opinnäytetyön tavoitteena on luoda IT-artefakti eli tietoturvariskien hallintamamalli organisaation eri prosesseille. Tutkimus on työelämälähtöinen kehittämisongelma, jolle on kohdeyrityksessä selkeä tarve. Opinnäytetyössä toteutuu Laurean Learning by Developing oppimismalli, jolla tarkoitetaan sellaista yhteistyöprosessia työelämän kanssa, jossa oppimisen kohteena ovat oikeat työelämän kehittämis- ja ongelmatilanteet. Learning by Developing –mallilla haetaan vastausta sellaiseen ongelmaan, jonka ratkaiseminen vaatii uuden tiedon luomista. Oppimisella on selvä kohde opinnäytetyössä: tietoturvariskien hallinta yrityksen prosesseissa ja oppiminen syntyy uuden osaamisen tuottamisen prosessissa. Tässä tutkimuksessa oppiminen on vaatinut perehtymistä riskienhallintaan, organisaation prosesseihin ja tiedon soveltamista hallintamallin luomiseen ja käyttöönottoon kohdeyrityksessä. (Fränti & Pirinen 2005, 55.)

Opinnäytetyö rajataan tietoturvariskien tunnistamiseen, jossa näkökulmana on yrityksen prosessit sekä ISO 27001 standardissa esitetty PDCA-mallin Plan eli suunnitteluosio. (ISO 27001 2006, 8.) Plan-osiossa määritellään tietoturvapolitiikka, -tavoitteet ja –prosessit sekä arvioidaan tietoturvariskejä ja niiden menettelytapoja. Tietoturvariskien hallinnan käytännön toteutukseen, seurantaan, katselmointiin ja ylläpitoon ei oteta kantaa tässä tutkimuksessa. ISO 17799 standardia tutkimuksessa ei ole analysoitu tarkemmin sitä on lähinnä käytetty ISO 27001 standardin tukena ja käytännön ohjeistuksena turvamekanismien valinnassa.

1.3 Opinnäytetyön aineisto ja sisältö

Teoreettisen tutkimusaineiston lähteenä on käytetty tietoturvallisuuteen ja yrityksen tietoturvariskien hallintaan liittyvää kirjallisuutta ja tieteellisiä artikkeleja. Lisäksi työn soveltavassa osassa on tietoturvan hallintamallin arvioinnissa käytetty lähteenä organisaation henkilöstön haastatteluja.

Opinnäytetyö jakaantuu yhdeksään päälukuun. Ensimmäisessä luvussa määritellään tutkimusaihe ja –kysymykset, sekä kerrotaan tutkimuskohteen rajaus ja suunnittelutieteellinen metodiikka. Luvussa 1.5. esitellään tutkimuksen keskeiset käsitteet. Toinen luku keskittyy tietoturvan hallinnointiin ja eri tietoturvastandardien esittelyyn. Kolmannessa luvussa perustellaan tutkimuksen teoreettisen viitekehyksen valinta sekä paneudutaan ISO 27001 ja 17799 standardeihin. Neljännen luvun aiheena ovat tietoturvariskit ja suojattavat kohteet sekä niiden tunnistaminen. Viidennessä luvussa esitellään eri riskien käsittelyvaihtoehtoja ja turvamekanismien valintaa. Prosessit ja niiden merkitys organisaation toiminnassa on kuudennen luvun aiheena. Lisäksi pohditaan miten tietoturvariskien tunnistaminen ja prosessit nivoutuvat yhteen. Seitsemännessä luvussa esitellään case-yritys, jolle opinnäytetyö tehdään. Kahdeksannessa luvussa on kuvattu itse tutkimusprosessi ja sen toteutus case-yrityksessä. Yhdeksännen luvun aiheena ovat tutkimustulokset. Tuloksia analysoidaan sekä suunnittelutieteellisestä näkökulmasta että kohdeyrityksen toiminnan kannalta. Johtopäätökset ja jatkotutkimusehdotukset ovat kymmenennen eli viimeisen luvun sisältönä.

1.4 Opinnäytetyön tieteellinen metodiikka

1.4.1 Suunnittelutieteellinen tutkimus

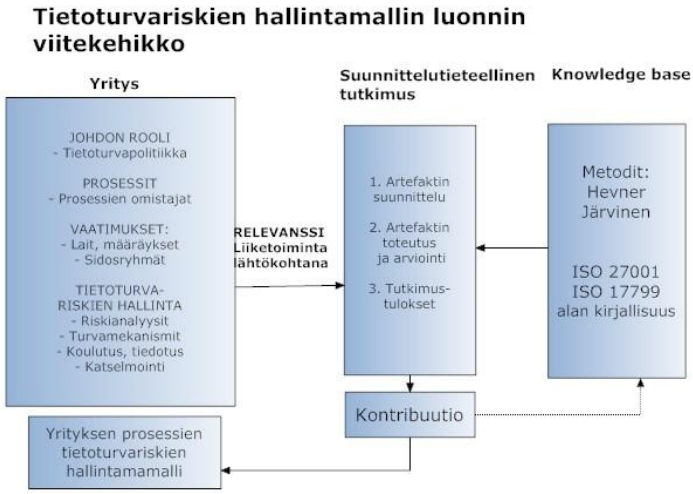
Suunnittelutiede luo ja arvioi IT -artefakteja, jotka ratkaisevat organisaatiossa olevia ongelmia. Suunnittelutieteellinen näkökulma vastaa kysymyksiin: voimmeko rakentaa innovaation ja kuinka hyödyllinen innovaatio on organisaatiolle? Voimme myös kysyä millainen innovaation tulisi olla ja miten meidän tulisi se luoda? Jos tutkimusongelma sisältää seuraavia verbejä: rakentaa, muuttaa, parantaa, luoda, korjata, jne. se mitä luultavimmin kuuluu suunnittelutieteen pariin. (Järvinen &

Järvinen 2004, 103.) Suunnittelutieteellisen tutkimuksen lopputulos on Hevnerin mielestä artefakti itsessään. Artefaktin tulee tarjota ratkaisu tutkimusongelmaan ja sen tulisi antaa uutta tutkimustietoa aihealueeseen uudella ja innovatiivisella tavalla. (Hevner, March, Park & Ram 2004, 75-105.)

Marchin ja Smithin (1995) mukaan rakennamme IT-artefaktin suorittamaan jotain tiettyä tehtävää, jolloin sen rakentaminen valmiiksi osoittaa suunnitteluongelman ratkenneen. Artefaktin rakentamistoiminnon tavoite on heidän mielestään se hyöty tai arvo minkä se tuottaa käyttäjäyhteisölleen. Van Akenin (2004) mukaan suunnittelutieteen tarkoitus on luoda tietämystä konstruktio-ongelman ratkaisemista varten tai parantaa nykyisten systeemien suorituskykyä. Van Akenin mielestä innovaation hyödyllisyys tulee arvioida enemmin tai myöhemmin. (Järvinen & Järvinen 2004, 103-104.)

Hevnerin mielestä suunnittelutieteellisen tutkimuksen lopputulokset ovat neljän tyyppisiä: käsitteistöjä, malleja, metodeja ja realisointeja. Käsitteistö muodostaa tutkimusongelman sanaston, mallit ilmaisevat käsitteiden väliset suhteet, metodit ovat askeleita esim. ohjeisto, jota käytetään suorittamaan tehtävä ja realisointia on artefaktin toteutus ympäristössään. (Järvinen & Järvinen 2004, 107.)

Tässä tutkimuksessa käytetään suunnittelutieteellisenä viitekehyksenä Hevnerin luomaa seitsemää ohjetta IT-artefaktin suunnitteluun, toteuttamiseen ja arviointiin. Kuvassa 1. on kuvattu tutkimuksen tietoturvariskien hallintamallin luonnin viitekehikko, johon sulautuvat yrityksen, sidosryhmien ja lakien asettamat vaatimukset sekä suunnittelutieteellinen tutkimusmenetelmä. Tutkimuksen kontribuutiona saadaan organisaation eri prosessien tietoturvariskien hallintamalli.



Kuva 1. Tietoturvariskien hallintamallin luonnin viitekehikko (Hevner 2004)

1.4.2 Tutkimuksen IT-artefakti

Hevnerin ensimmäisen ohjeen mukaan tutkimuksen tulos on johonkin organisaation tärkeään ongelmaan rakennettu tarkoituksellinen IT-artefakti. Se voi olla toteutus, mutta myös tietojärjestelmän rakentamisessa ja käytössä sovellettu käsitteistö, malli tai metodi. IT-artefaktit ovat harvoin täysin valmiita tietojärjestelmiä, vaan innovaatioita, joilla määritellään ideat, käytännöt, tekniset kyvykkyydet ja tuotteet, joiden avulla järjestelmien analyysi, suunnittelu, toteutus ja käyttö voidaan vaikuttavasti ja tehokkaasti toteuttaa (Hevner ym. 2004, 82-83). Hevner sulkee ihmiset ja organisaation eri elementit IT-artefaktin määritelmän ulkopuolelle samoin kuin kehityksen ajan kuluessa. Artefaktin toteutus on osoitus suunnitteluprosessin ja lopputuloksen toimivuudesta. Kysymykseen voidaanko rakentaa uusi järjestelmä X? Saadaan vastaus sillä, että rakentamisen mahdollisuus osoitetaan konstruoimalla järjestelmä X tai vastaavasti osoitetaan huomattava parannus entiseen (Järvinen & Järvinen 2004, 115).

Tämän tutkimuksen IT-artefakti on tietoturvariskien hallintamalli yrityksen eri prosesseille. Artefaktin toteutus osoitetaan suunnittelemalla ja konstruoimalla tietoturvariskien hallintamalli käyttäen viitekehyksenä Hevnerin seitsemää ohjetta IT-artefaktin suunnittelulle, sekä ISO 27001 ja 17799 standardien vaatimusmäärityksiä uhkakuvien hallinnalle (ISO 27001 2006, 14).

1.4.3 Tutkimuksen relevanttius

Suunnittelutieteellisessä tutkimuksessa painotetaan tutkimusongelman tärkeyttä liiketoiminnan näkökulmasta. Tietojärjestelmätieteen tutkimuksen tarkoituksena on hankkia tietämystä ja ymmärrystä, jotka mahdollistavat teknologiaperustaisten artefaktien suunnittelun ja toteutuksen tähän asti ratkaisemattomiin tai huonosti ratkaistuihin liiketoiminnan ongelmiin. Hevner ym. (2004, 85) toteaa toisessa ohjeessaan, että tutkimus on relevanttia, jos sen avulla ratkaistaan hyödyntäjäyhteisön ongelma.

Tämän tutkimuksen relevanttius todistetaan kartoittamalla yrityksen prosessien tietoturvariskien nykytila käyttäen ISO 27001 -standardin turvamekanismeja viitekehyksenä. Liiketoiminnan näkökulmasta tutkimus on tärkeä ja merkityksellinen, koska yrityksen sidosryhmät vaativat tietoturvalta korkeaa tasoa, jotta yhteistyö voi olla saumatonta eri sidosryhmien tietojärjestelmien kanssa. Standardin käyttö viitekehyksenä antaa yritykselle etulyöntiaseman kilpailijoihin nähden tietoturvariskien kartoituksen osalta. Standardia käyttämällä voidaan osoittaa, että mitään tietoturvan osa-aluetta ei ole riskien kartoituksessa jätetty huomioimatta.

1.4.4 Artefaktin arviointi

IT-artefaktin hyödyllisyys, laatu ja vaikutus, tulee osoittaa tarkan arvioinnin ja evaluointimetodien avulla. Arvioinnin tulee perustua liiketoimintaympäristön vaatimuksiin artefaktille ja sen tulee integroitua IT-infrastruktuuriin. Arvioinnin mittaristona käytetään seuraavia ominaisuuksia: toiminnallisuus, täydellisyys, johdonmukaisuus, tarkkuus, suoritus, luotettavuus, käytettävyys, organisaatioon sopivuus ja muut tarpeelliset laatuominaisuudet. Artefaktin iteratiivinen arviointi, Hevnerin kolmas ohje, antaa palautetta rakentamiselle sekä prosessin että lopputuloksen suhteen. (Hevner ym. 2004, 85.)

Tämän tutkimuksen IT-artefaktin arvioinnissa kiinnitetään erityistä huomiota siihen, että miten hyvin valitut tutkimusmetodit soveltuvat tietoturvariskien hallintamallin suunnitteluun pienelle organisaatiolle. Liiketoiminnan näkökulmasta artefaktia arvioidaan sen soveltuvuudesta organisaation tarpeisiin. ISO 27001 ja 17799 standardien osalta arvioidaan niiden luotettavuutta tunnistaa tietoturvariskit ja kuinka hyvin standardeja voidaan soveltaa organisaation toimintaan.

1.4.5 Tutkimuksen kontribuutiot

Hevnerin neljännen ohjeen mukaan vaikuttavan suunnittelutieteellisen tutkimuksen tulee tuottaa selvää hyötyä seuraavilla osa-alueilla: suunnitellun artefaktin, konstruointitietämyksen, suunnittelua koskevan arviointitiedon ja metodologioiden alueilta. Tärkeä kysymys jokaisen suunnittelutieteellisen tutkimuksen kohdalla on se, että mitä uutta ja innovatiivista kontribuutiota se tuottaa tuloksena. Suunnittelutieteellinen tutkimus pitää sisällään kolme erilaista kontribuutioaihetta, joista ainakin yksi on löydettävä jokaisesta suunnittelututkimuksesta. Ensimmäinen kontribuution aihe on IT -artefakti itsessään. Artefaktin on annettava vastaus tutkimusongelmaan. Se voi olla ratkaisu itse tutkimusongelmaan tai se voi tuottaa huomattavaa uutta tieteellistä tietoa tutkimuskohteeseen tai soveltaa jo olemassa olevaa tietoa uudella innovatiivisella tavalla. Toinen kontribuution alue on itse artefaktin suunnittelemisen rakentamisprosessi ja mallinnus. Huomattava kontribuutio voidaan saavuttaa esimerkiksi uudenlaisen suunnitteluprosessin tai mallin kehittämisellä. Kolmas kontribuution osa-alue on metodologia. Tutkimuksessa käytetty metodi ja arviointimenetelmä itsessään tuovat tutkimusalueeseen oman kontribuutionsa. Arviointi ja mittaristo ovat suunnittelututkimuksessa tärkeitä osa-alueita itsessään. Tutkimuksen kontribuutiona saadaan tulos siitä, että miten hyvin valittu metodi soveltuu tutkimusongelman selvittämiseen. Jatkossa siitä saatu hyöty on merkittävä valittaessa tutkimusmetodia samankaltaiselle tutkimusongelmalle (Hevner ym. 2004, 87).

Tämän tutkimuksen kontribuutiona saadaan malli yrityksen tietoturvariskien hallintaan sen eri prosesseissa. Suunnittelutieteellinen kontribuutio saavutetaan tutkimalla kuinka hyvin Hevnerin seitsemän ohjetta IT-artefaktin luonnille soveltuu tietoturvariskien hallintamallin luontiin.

1.4.6 Tutkimuksen tieteellinen tarkkuus

Tutkimuksen tieteellinen tarkkuus Hevnerin viidennen ohjeen mukaan tulee todistaa käyttämällä tarkkoja tutkimusmetodeja sekä IT -artefaktin rakentamisessa että arvioinnissa (Hevner ym. 2004, 87-88). Tieteellinen tarkkuus kertoo tutkimuksen tasosta ja siitä miten se on suoritettu. Suunnittelutieteessä tutkimuksen tarkkuudella tarkoitetaan sekä olemassa olevan tutkimustiedon että teoreettisen perustan ja tutkimusmetodologian tehokasta käyttöä.

Tietoturvariskien hallintamallin luonnissa käytetään Hevnerin seitsemää ohjetta IT-artefaktin luonnille sekä ISO standardien asettamia tarkkoja määrityksiä tietoturvan tasolle ja turvamekanismeille (Hevner ym. 2004, 88). Näitä metodeja käyttämällä todistetaan tutkimuksen tieteellinen tarkkuus.

1.4.7 Ratkaisujen etsintäprosessi

Järvinen & Järvinen kertovat teoksessaan Tutkimustyön menetelmistä Hevnerin kuudennesta ohjeesta seuraavaa: hyvän suunnitteluratkaisun löytäminen on etsintäprosessi, jossa käytetään saatavilla olevia keinoja tutkimuksen tavoitteiden saavuttamiseksi noudattamalla kuitenkin ympäristössä vallitsevia lakeja. Järvisten teoksesessa todetaan, että saatavilla olevia toimenpiteitä ja ratkaisuja Hevner kutsuu keinoiksi, joilla ratkaisu konstruoidaan. (Järvinen & Järvinen 2004, 115.)

ISO 27001 ja 17799 standardit valittiin tämän tutkimuksen etsintäprosessissa parhaiksi viitekehyksiksi tietoturvariskien hallintamallin luontiin, koska ne ovat kansainvälisesti hyväksyttyjä standardeja. Hyväksyttyä standardia käyttämällä yritys todistaa käytetyn tietoturvan tason vastaavan niitä vaatimuksia, joita standardissa esitetään. ISO standardien käyttämisen merkittävin hyöty kehitettäessä yrityksen tietoturvallisuutta on se, että tietoturva saadaan integroitua osaksi päivittäistä toimintaa ja liiketoimintaprosesseja. Lisäksi kehitystyölle saadaan määrämuoto, jolloin ulkopuolisille tahoille, kuten asiakkaille, voidaan esittää toiminnan olevan standardin vaatimusten ja tason mukaista.

1.4.8 Tuloksien välittäminen tutkija- ja soveltajayhteisölle

Hevner ym. (2004, 90) viimeisen seitsemännen ohjeen mukaan tutkimuksen tulokset tulee välittää sekä johdolle että teknisesti suuntautuneille henkilöille organisaatiossa. Teknisille tahoille esitetään riittävän tarkasti kuvattu artefakti ja käytännön soveltajille kerrotaan millainen artefakti on ja kuinka se on konstruoitu.

Tietoturvariskien hallintamalli koulutetaan prosessien omistajille ennen sen käyttöönottoa kohdeyrityksessä. Lisäksi se esitellään muulle organisaatiolle ja yrityksen johdolle kuukausittaisessa henkilöstökokouksessa. Hallintamalli dokumentoidaan yrityksen laatukäsikirjaan, jota kaikki pääsevät lukemaan intranetin kautta. Prosessikohtainen tietoturvariskien hallintamalli viedään laatukäsikirjaan kyseisen prosessin yhteyteen.

1.5 Opinnäytetyön keskeiset käsitteet

Seuraavissa luvuissa on esitelty tämän opinnäytetyön keskeisimmät käsitteet.

Prosessi
Prosessi on joukko loogisesti toisiinsa liittyviä toimintoja. Prosessissa yhdistyvät eri työvaiheet eteneväksi ketjuksi, jolla on jokin alku (input esim. asiakkaan tilaus) ja lopputulos (output esim. toimitettu tuote). Prosessin toteuttamiseen tarvitaan erilaisia resursseja (resources esim. henkilöstö, tilat, laitteet jne.). Organisaation pääprosessit (esim. tilaus-toimitusprosessi) liittyvät yleensä ydinliiketoimintaan ja tukiprosessit tukevat toiminnallaan muita prosesseja (esim. taloushallinto, henkilöstöhallinto jne.).

Tietoturvapolitiikka
Tietoturvapolitiikka luo yleisen suunnan ja periaatteet yrityksessä tehtäville tietoturvatoimenpiteille sekä se sisältää tietoturvatyölle asetetut tavoitteet. Tietoturvapolitiikassa yrityksen johto kertoo näkemyksensä, siitä miten tietoturvallisuus vaikuttaa yrityksen toimintaan ja miten tietoturva-asioihin suhtaudutaan organisaatiossa. Tietoturvapolitiikalla johto osoittaa myös sitoutumisensa ja tukensa tietoturvallisuuden kehittämiselle organisaatiossa. (Laaksonen, Nevasalo & Tomula 2006, 146 - 147.)

ISO 27001–standardin mukaisesti tietoturvapolitiikassa otetaan huomioon liiketoiminnalliset ja lakisääteiset vaatimukset sekä sopimuksiin sisältyvät tietoturvavelvoitteet. Tietoturvapolitiikka tulisi standardin mukaan olla yhtenäinen yrityksen riskienhallinnan strategian kanssa ja politiikka luo kriteerit, joita vastaan uhkia ja riskejä arvioidaan. (ISO 27001 2006, 14.)

Tietoturvastandardi

Tietoturvan standardisoimisella pyritään yhteisten toimintatapojen laatimiseen ja sillä lisätään tuotteiden yhteensopivuutta ja turvallisuutta sekä helppokäyttöisyyttä. ISO 27001-standardi on kansainvälinen ohjeellinen sopimus, joka sisältää teknisiä tietoja ja muita tarkkoja kriteereitä tietoturva-asioista. Tietoturvastandardi on hyväksi havaittu käytäntö, ohjenuora, joka vastaa tietoturvaan, kuten varmistukseen, viruksilta suojautumiseen tai salasanoihin liittyviin jokapäiväisiin tarpeisiin. (Vartiainen 2008, 14 – 15.)

Tietoturvariski tai uhka

Tietoturvariski on yrityksen toimintaan kohdistuva ei-toivottu tapahtuma. Riskienhallinnan tavoitteena on havaita ja hallita näitä uhkakuvia. Tietoturvallisuuden testaamisen tavoitteena on havaita tietoturvaheikkoudet tai tehtyjen suojaustoimenpiteiden toimivuus sekä mahdolliset puutteet toiminnassa. (Laaksonen ym. 2006, 150.)

Suojattava kohde

Suojattava kohde on mikä tahansa tieto, väline tai asia, joka on arvokas organisaatiolle (ISO 27001 2006, 10).

Valvontatavoite

Valvontatavoite on se tila, johon standardissa määriteltyjä turvamekanismeja käyttäen ja soveltaen organisaatio omassa toiminnassaan pyrkii. Saavutettuaan valvontatavoitteen on organisaation turvamekanismi sen osalta kunnossa ja standardin vaatimuksen mukaista.

Turvamekanismi

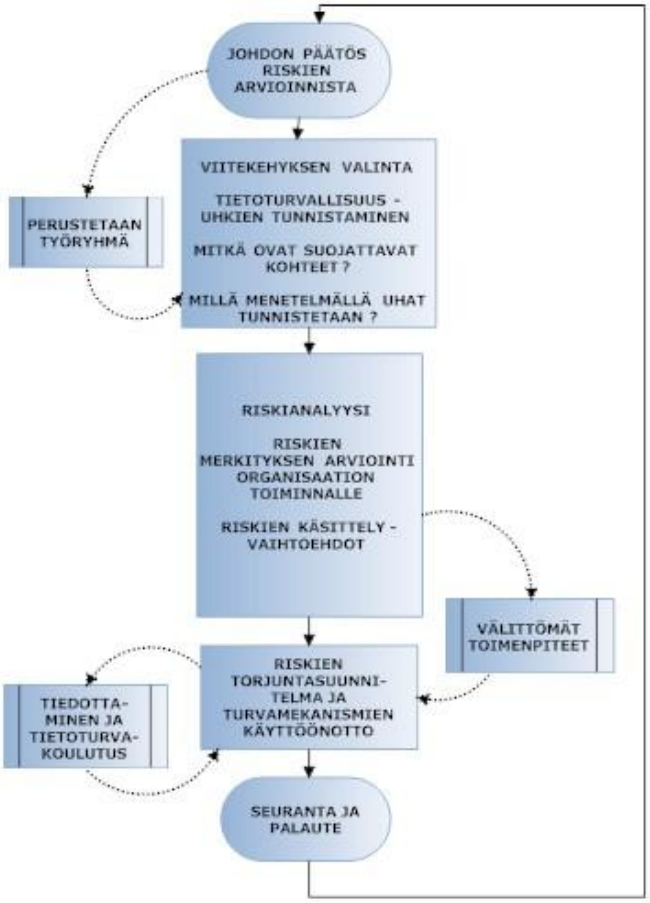
Turvamekanismi on standardissa määritelty ohje, periaate tai menettelytapa, jota käyttämällä organisaatio toimii standardin mukaisesti toteuttaessaan tietoturvallisuuden hallintajärjestelmää käytännössä.

2 Tietoturvan hallinnointi

2.1 Tietoturvariskien hallinnan tavoite ja prosessikuvaus

Tietoturvariskien hallinnan tavoite on tunnistaa ja arvioida organisaation toimintaan liittyvät tietoturvariskit. Organisaation toiminnan kannalta on tärkeää, että tietoa ei joudu vääriin käsiin, tietojärjestelmät ovat aina oikeiden henkilöiden saatavilla ja tieto on oikeaa sekä ajantasaista. Tietoturvallisuuden hallintajärjestelmän tavoitteena on suojata tiedon luottamuksellisuus, eheys ja käytettävyys. Tietoturvariskien hallintaprosessi voidaan kuvata kuvassa 1. esitetyllä tavalla. Prosessin ensimmäisessä vaiheessa tehdään päätös tietoturvariskien arvioinnin suorittamisesta ja

perustetaan työryhmä organisoimaan riskianalyysiä ja suojattavien kohteiden arviointia. Seuraavaksi kartoitetaan organisaation toiminnalle tärkeät tiedot ja tietojärjestelmät eli tunnistetaan suojattavat kohteet. Kolmannessa vaiheessa arvioidaan ja analysoidaan tunnistettujen riskien merkitys organisaation toiminnalle. Kolmannen vaiheen alaprosessina tehdään heti välittömät toimenpiteet niille riskeille, jotka helposti saadaan hallintaan nopeilla parannuksilla toimintatavoissa tai tekniikassa. Neljännessä vaiheessa päätetään käytettävistä turvamekanismeista, suunnitellaan miten vahingon sattuessa toimitaan sekä miten vahinkotilanteesta toivutaan normaaliin tilaan. Omana prosessina rinnalla kulkee henkilöstön tiedottaminen tietoturva-asioista ja tietojärjestelmistä vastaavien henkilöiden koulutus riskienhallintaan. Lopuksi tilannetta seurataan ja mahdollinen toteutunut riski analysoidaan ja tapahtuneesta otetaan opiksi. Riskien arviointiprosessi ei koskaan ole valmis, vaan se tulee suorittaa säännöllisin väliajoin uudestaan. (Valtiovarainministeriö 2003, 9 – 45.)



Kuva 2. Riskienhallinnan prosessikuvaus

Riskien hallintaa suunniteltaessa on otettava huomioon eri lait, määräykset ja säädökset, jotka koskevat yrityksen tietoturvallisuusvelvoitteita. Esimerkiksi Henkilötietolaki (523/1999) määrittää tarpeelliset toimenpiteet henkilötietojen suojaamiselle. (Valtiovarainministeriö 2003, 13 – 15.) Myös yrityksen eri sidosryhmiltä voi tulla vaatimuksia, jotka tulee huomioida tietoturvariskien kartoituksessa.

2.2 Johdon rooli

Tietoturvallisuus ja tietoturvariskien hallinta on osa yrityksen johtamistoimintaa. Riskien hallinnan menettelytavoissa on otettava huomioon ratkaisujen taloudellisuus ja tarkoituksenmukaisuus. Johdon tulee olla sitoutunut riskienhallinnan toimintamalleihin ja ne on huomioitava yrityksen eri prosesseissa henkilöstön tehokkaalla koulutuksella ja tiedottamisella. (Valtiovarainministeriö 2003, 10 – 11.) Ylin johto vastaa aina viime kädessä yrityksen liiketoimintariskeistä.

Tietoturvapolitiikka luo yleisen suunnan ja periaatteet yrityksessä tehtäville tietoturvatoimenpiteille sekä se sisältää tietoturvatyölle asetetut tavoitteet. Tietoturvapolitiikassa yrityksen johto kertoo näkemyksensä, siitä miten tietoturvallisuus vaikuttaa yrityksen toimintaan ja miten tietoturva-asioihin suhtaudutaan organisaatiossa. Tietoturvapolitiikalla johto osoittaa myös sitoutumisensa ja tukensa tietoturvallisuuden kehittämiselle organisaatiossa. (Laaksonen ym. 2006, 146 - 147.)

ISO 27001–standardin mukaisesti politiikassa otetaan huomioon liiketoiminnalliset ja lakisääteiset vaatimukset sekä sopimuksiin sisältyvät tietoturvavelvoitteet. Tietoturvapolitiikka tulisi standardin mukaan olla yhtenäinen yrityksen riskienhallinnan strategian kanssa ja politiikka luo kriteerit, joita vastaan uhkia ja riskejä arvioidaan. (ISO 27001 2006, 25.)

2.3 Tietoturvastandardit, viitekehykset ja toimintamallit

Tietoturvallisuuden hallinnoinnin avuksi on kehitetty joukko erilaisia standardeja, viitekehyksiä sekä toimintamalleja. Lisäksi tietoturvallisuuden eri osa-alueille on myös kehitetty omia standardeja, jotka voivat olla hyvinkin yksityiskohtaisia teknisiä ohjeita. Keskeisimmät tietoturvastandardit ovat ISO-standardeja. ISO-standardit ovat laajasti tunnustettuja ja levinneitä sekä kansainvälisesti hyväksyttyjä standardeja. (Laaksonen 83 – 85.)

Viitekehyksistä yksi tunnetuimmista on COBIT (Control Objectives for Information and related Technology), joka auttaa hahmottamaan mitä asioita ja toimintoja organisaation tietojenkäsittely pitää sisällään. COBIT antaa ohjeita yrityksen johdolle siitä, miten yhdistetään liiketoiminnan ja tietojenkäsittelyn tavoitteet sekä miten tavoitteiden saavuttamista mitataan. COBIT ei ole tekno-

logia riippuvainen viitekehys. COBIT ei myöskään anna yksityiskohtaisia ohjeita miten asiat tulisi hoitaa, vaan se toimii parhaiten yleisen tason mallina, jota seuraamalla voi varmistua siitä, että kaikki tietojenkäsittelyn eri tarpeet on otettu organisaatiossa huomioon. (Laaksonen, 92.)

ITIL (Information Technology Infrastructure Library) on kokoelma tietojenkäsittelyn liittyvistä parhaista käytännöistä palvelutuotannon näkökulmasta. Vapaan käytön ansiosta ITIL on levinnyt maailmalla laajasti ja sitä käytetään palvelujen standardoimiseen. ITIL ei ole vaatimusmäärittely, vaan kokoelma hyväksi havaittuja toimintatapoja, joita voidaan soveltaa omassa toiminnassa. Tietoturvallisuuden osalta ITIL määrittelee ne johtamisen periaatteet, joiden mukaisesti tietoturva-asiat tulee ottaa huomioon jo palvelujen suunnitteluvaiheessa. Perusajatus ei juuri poikkea ISO 27001 – standardin vaatimuksista. (Laaksonen 95 – 98.)

Suomessa valtionvarainministeriön kehittämä VAHTI-ohjeistus on kokoelma tietoturvallisuuden eri osa-alueet kattavia ohjeita, jotka on tarkoitettu pääasiassa julkishallinnon käyttöön, mutta ne soveltuvat suurelta osin myös yrityskäyttöön. VAHTI-ohjeet ovat vapaasti saatavilla valtionvarainministeriön kotisivuilta internetistä (www.vm.fi).

2.4 Standardin tai muun viitekehyksen valinta

Suomen laki ei velvoita minkään tietoturvastandardin käyttämistä tietoturvariskejä arvioitaessa, vaikka eri laeissa on kuitenkin määrityksiä tietoturvavelvoitteista ja -tavoitteista. Käyttämällä yleisesti hyväksyttyä standardia tai viitekehystä toiminnassaan yrityksen on helpompi näyttää toteen, esimerkiksi tietomurtotilanteessa, että tietoturvan taso on ollut riittävä. Standardia käyttämällä tietoturvallisuudesta vastaava henkilöstö voi myös olla suhteellisen varma siitä, että mikään tietoturvan osa-alue ei jää toiminnassa huomiotta. Jos yrityksen päämääränä ei ole IT-toimintojen sertifiointi jonkin tietyn standardin mukaisesti, voidaan erittäin hyvään lopputulokseen myös päästä valitsemalla muutama standardi tai toimintamalli ja poimimalla niistä oman yrityksen toimintaan ja tarpeisiin sopivat asiat. Yritys voi myös laatia oman sisäisen standardin tietoturvallisuudelle. Minkä tahansa toimintamallin yritys valitseekin on aina tärkeää dokumentoida valitut toimintamallit ja –tavat. Dokumentoinnilla toiminnasta tulee määrämuotoisempaa ja toistettavampaa. (Laaksonen 104 – 111.)

3 Tutkimuksen teoreettisen viitekehyksen valinta

3.1 ISO 27001 ja 17799 standardit

Tietoturvallisuuden hallintajärjestelmän käyttöönotto on johdon strateginen päätös. Tietoturvajärjestelmän suunnitteluun ja toteutukseen vaikuttavat järjestelmän tarpeet ja tavoitteet, organi-

saation turvallisuusvaatimukset, käytettävät prosessit sekä organisaation koko ja rakenne. Nämä kaikki myös muuttuvat ajan mukana, joten järjestelmän tulee olla organisaation tarpeiden mukainen. Standardin avulla voidaan arvioida tietoturvallisuuden vaatimusten-mukaisuutta.

ISO 27001 standardi on laadittu malliksi tietoturvallisuuden hallintajärjestelmän (ISMS, Information Security Management System) kehittämiselle, toteuttamiselle, käyttämiselle, valvomiselle, katselmoinnille, ylläpitämiselle ja parantamiselle (ISO 27001 2006, 6).

Standardi kattaa kaikentyyppiset organisaatiot, kuten kaupalliset yritykset, julkishallinnon virastot sekä ei-kaupalliset organisaatiot. Standardi määrittelee ne vaatimukset, jotka koskevat dokumentoidun tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, käyttämistä, valvontaa, katselmointia, ylläpitoa ja parantamista. Organisaation yleiset liiketoimintariskit on myös otettu huomioon standardissa. Organisaation toiminta, jossa käytetään resursseja ja jota johdetaan siten, että se mahdollistaa panosten muuttamisen tuotoiksi, voidaan käsittää prosessiksi. Prosessien tunnistamista, niiden johtamista ja soveltamista organisaatiossa voidaan kutsua ”prosessimaiseksi toimintamalliksi”. ISO 27001 standardissa esitelty tietoturvallisuuden hallinnan prosessimainen toimintamalli painottaa seuraavien asioiden tärkeyttä (ISO 27001 2006, 8):

- tietoturvatavoitteiden ja tietoturvapolitiikan määrittäminen
- organisaation tietoturvavaatimusten ymmärtäminen
- turvamekanismien luominen sekä käyttö tietoturvariskien hallintaan
- tietoturvallisuuden hallintajärjestelmän valvonta ja katselmointi
- objektiiviseen mittaamiseen perustuva jatkuva parantaminen

ISO 17799 standardissa esitetään toteutusohjeita eri turvamekanismien suunnitteluun ja käyttöönottoon. Kun tietoturvariskit on tunnistettu ja on tehty päätös miten ne käsitellään, on aika valita tarvittavat turvamekanismit. Mekanismien valinta riippuu organisaation päätöksistä koskien riskienhallintamenettelyä, mutta myös eri kansalliset ja kansainväliset lait ja asetukset on otettava huomioon turvamekanismeja valittaessa. 17799 standardia voidaan käyttää käytännön ohjeistuksena, jonka pohjalta kehitetään organisaation turvallisuusjohtamista ja lisätään luottamusta yritysten välisiin liiketoimiin. Standardin mukaan riskien arvioinnissa tulisi käyttää järjestelmällistä lähestymistapaa riskianalyysin teossa ja riskien vaikutusten arvioinnissa. Riskien arviointikohteena voi olla koko organisaatio, yksittäinen tietojärjestelmä, palvelu tai esimerkiksi liiketoimintaprosessi. (ISO 17799 2006, 16-20, 26.)

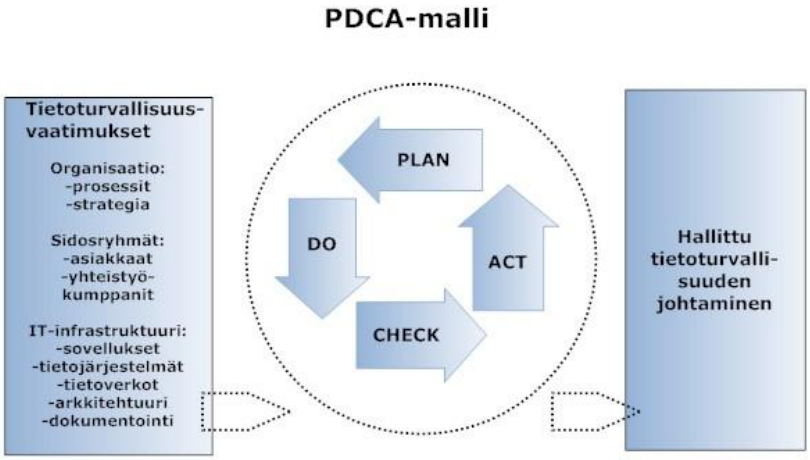
ISO 27001 ja 17799 standardit valittiin tämän tutkimuksen etsintäprosessissa parhaiksi viitekehyksiksi eri prosessien tietoturvariskien hallintamallin suunnitteluun ja riskien tunnistamiseen, koska ne ovat kansainvälisesti hyväksyttyjä standardeja. Hyväksyttyä standardia käyttämällä yritys todis-

taa käytetyn tietoturvan tason vastaavan niitä vaatimuksia, joita standardissa esitetään. Standardien käyttö viitekehyksenä antaa yritykselle etulyöntiaseman kilpailijoihin nähden tietoturvariskien kartoituksen osalta. Standardeja käyttämällä voidaan osoittaa, että tietoturvallisuuden eri osa-alueet on käyty riskien kartoituksessa kattavasti läpi. ISO 27001 standardin mukaan yrityksessä tulee olla yhteisesti päätetty ja hyväksytty tapa suorittaa riskienarviointi ja tietoturvallisuuden testausmenetelmä. Sertifiointiin tähtäävässä auditoinnissa tutkitaan kuinka hyvin organisaation käytännöt vastaavat esimerkiksi ISO 27001 standardin esittämiin vaatimuksiin.

3.2 PDCA –malli

ISO 27001 standardissa hyödynnetään ”Suunnittele-Toteuta-Arvioi-Toimi” –mallia (PDCA-malli plan-do-check-act), jota sovelletaan kaikkien tietoturvallisuuden hallintajärjestelmien prosessien rakenteessa. PDCA-malli on organisaation johtamismalli, joka kattaa toiminnan suunnittelun, ohjauksen ja kehittämisen. Mallin mukaiseen johtamiseen sisältyy neljä oleellista tehtävää (kuva 3.) (Anttila & Kajava 2006, 43-46):

1. P (plan) = Suunnittele
2. D (do) = Toteuta
3. C (check) = Arvioi
4. A (act) = Toimi



Kuva 3. Tietoturvallisuuden hallintajärjestelmä ja PDCA-malli

Seuraavassa taulukossa on kuvattu yksityiskohtaisemmin miten PDCA-mallin eri osia sovelletaan tietoturvallisuuden hallintajärjestelmän prosesseihin (ISO 27001 2006, 8).

P	Luo tietoturvallisuuden hallintajärjestelmä	Määrittele tietoturvapolitiikka, -tavoitteet, ja -prosessit sekä arvioi tietoturvariskit ja niiden menettelytavat.
D	Toteuta ja käytä tietoturvallisuuden hallintajärjestelmää	Toteuta ja käytä luotua hallintajärjestelmää, turvamekanismeja ja menettelytapoja.
C	Seuraa ja katselmoi hallintajärjestelmä	Seuraa ja mittaa prosessien suorituskykyä, vertaa tuloksia tietoturvapolitiikkaan sekä tavoitteisiin. Raportoi tulokset johdolle.
A	Ylläpidä ja paranna hallintajärjestelmää	Johdon katselmuksen tulosten perusteella tee korjaavat toimenpiteet ja keskity ehkäiseviin toimenpiteisiin, jotta tietoturvallisuuden hallintajärjestelmän jatkuva parantuminen toteutuisi.

Taulukko 1. PDCA-mallin soveltaminen prosesseihin

Liiketoiminnan johtamisen näkökulmasta tietoturvallisuusaihe sisältyy yrityksen toiminnan suunnitteluun, ohjaukseen ja kehittämiseen siten, kuin organisaation johto niitä pitää liiketoiminnan kannalta tärkeinä. Tietoturvallisuuden johtaminen PDCA-mallia hyväksi käyttäen on välttämätöntä, jotta tietoturvallisuuden hallintaa voitaisiin toteuttaa johdonmukaisesti ja määrätietoisesti sekä kokonaisvaltaisesti organisaatioiden liiketoimintaan integroituna. (Anttila & Kajava 2006, 43 - 46.)

PDCA-mallin esi-isänä pidetään amerikkalaista Walter Shewhartia, joka kehitti mallin 1930-luvulla Bell:n laboratoriossa Yhdysvalloissa. Erityisen tunnetuksi mallin teki vasta 1950-luvulla laatujohtamiseen erikoistunut W. Edwards Deming. PDCA-malli tunnetaan yleisesti myös nimellä ”the Deming Wheel” Demingin käyttämän graafisen esitysmuodon mukaisesti. (wikipedia)

Tässä opinnäytetyössä keskitytään PDCA-mallin mukaiseen tietoturvariskien hallinnan suunnitteluun (Plan) ja hallintamallin käyttöönottoon eri prosesseille (Do) kohdeyrityksessä.

4 Tietoturvariskien tunnistaminen

4.1 Riskien ja suojattavien kohteiden tunnistaminen

Riskien tunnistamisessa oleellista on tunnistaa organisaation suojattavat kohteet ja niiden omistajat. Määrittelemällä omistaja yksilöidään henkilö tai yksikkö, jolla on esimiesvastuu suojattavien kohteiden kehittämisen, tuottamisen, ylläpidon, käytön ja turvallisuuden valvonnassa. Omistajalla ei ole suojattavaan kohteeseen välttämättä minkäänlaisia omistajuusoikeuksia. Suojattaviin kohteisiin kohdistuvat uhat tulee määritellä ja arvioida systemaattisesti. Riskien analysointi auttaa yritystä priorisoimaan tietoturvariskit ja kertoo johdolle kuinka paljon on järkevää laittaa rahaa uhkien torjuntaan (Harris 2008, 83).

ISO 27001 -standardissa riskien arvioinnin ensimmäisessä vaiheessa on tunnistettava mahdolliset riskit ennen niiden aktivoitumista ja selvitettävä niiden mahdolliset aiheuttamat vahingot. Arvioinnissa otetaan kantaa siihen kuinka todennäköistä riskin toteutuminen on ja millaiset seuraukset turvallisuuden murtumisella voi liiketoiminnalle olla. (ISO 17799 2006, 16.)

Ennen uhkien tunnistamistyön aloittamista on mietittävä riskianalyysin laajuus. Riskianalyysiin ei voi eikä kannata sisällyttää kaikkia mahdollisia uhkakuvia kerralla. Uhkakuvista laaditaan lista, josta johdon on helppo poimia ne uhkakuvat, jotka riskianalyysissä käsitellään yksityiskohtaisemmin. Riskien torjunnan osalta etulyöntiasemassa ovat ne uhat, jotka kohdistuvat suoraan organisaation ydinliiketoimintaan sekä ne, joihin kohdistuu laki- tai sidosryhmävelvoitteita. (Harris 2008, 84.)

Seuraavat kysymykset helpottavat organisaation suojattavien kohteiden tunnistamista:

- Mitä voi sattua?
- Mitä siitä voi seurata?
- Kuinka usein näin voi käydä?
- Mitkä on tapahtuman taloudelliset/toiminnalliset vaikutukset? (Harris 2008, 85)

4.2 Riskianalyysityöryhmä

Tehokkain riskianalyysi saadaan aikaiseksi muodostamalla työryhmä, jossa on jäseniä jokaisesta organisaation ryhmästä, osastosta tai prosessista. Muodostamalla ryhmä eri avainhenkilöistä saadaan aikaiseksi kattava riskianalyysi, jossa otetaan huomioon eri toimintojen mahdolliset uhkakuvat. Uhkakuvat voivat vaihdella huomattavasi, jos riskiä analysoidaan IT-henkilön tai taloushallinnon henkilön näkökulmasta. Jos kaikkien henkilöiden mukaan saaminen työryhmään ei ole mahdollista, niin heitä tulisi ainakin haastatella tehtäessä uhkakuva-analyysiä. (Harris 2008, 84 - 85.)

Riskien suuruuden määrittely ja uhkakuvien tunnistaminen prosessin omistajan näkökulmasta on edellytys onnistuneelle riskianalyysille. Organisaation IT-asiantuntija ei välttämättä tiedä kaikkia prosessiin liittyviä riippuvuuksia tai prosessissa käsiteltävää tietoa, niin hyvin kuin asiaan perehtynyt prosessin omistaja. Tietoturvariskien analyysin tulisi keskittyä kaikkiin relevantteihin liiketoimintaprosesseihin eikä pelkästään esimerkiksi IT-laitetiloihin tai IT-infrastruktuuriin (Iivari 2009, 123-124.)

4.3 Kuka on riskin omistaja?

ISO 17799–standardin mukaan suojattavan kohteen omistajalla tarkoitetaan henkilö tai yksikköä, jolla on esimiesvastuu suojattavan kohteen kokonaisvalvonnasta. Omistajan vastuulla tulisi olla,

että tieto ja tiedonkäsittelypalvelut on luokiteltu asianmukaisesti. Sen lisäksi omistajan tulee määritellä ja säännöllisesti katselmoida pääsyn rajoitukset ja luokitukset ottaen huomioon pääsynvalvontaperiaatteet. Omistettava kohde voi olla esimerkiksi sovellus, liiketoimintaprosessi tai määritelty joukko tietoaineistoa. (ISO 17799 2006, 52.)

4.4 Riskien arviointi = riskianalyysi

ISO 27001 -standardin mukaan (2006, 14) riskien arviointiin tulee valita menettelytavaksi sellainen, joka soveltuu tunnistettujen liiketoimintaa koskevien lakisääteisten ja tietoturvavaatimusten toteuttamiseen. Menettelytavan tulee myös olla sopiva tietoturvallisuuden hallintajärjestelmän toteuttamisen kannalta. Valitun menettelytavan on tuotettava vertailukelpoisia ja toistettavia tuloksia. Riskianalyysissä otetaan huomioon yrityksen yleinen liiketoimintastrategia ja tavoitteet. Riskien arvioinnin tulisi yksilöidä riskit, asettaa ne tärkeysjärjestykseen ja määritellä niiden suuruus suhteessa riskien hyväksymiskriteereihin ja organisaation tavoitteisiin. Muutostilanteissa riskien arviointi tulisi suorittaa aina uudelleen. Säännöllisin väliajoin tapahtuva riskien arviointi varmistaa, että muutokset huomioidaan turvallisuusvaatimuksissa. Tehokas riskien arviointi edellyttää, että arvioinnin laajuus on selkeästi määritelty. Kohdealueena voi olla esimerkiksi koko organisaatio, organisaation osa, yksittäinen tietojärjestelmä tai palvelu. (ISO 17799 2006, 26.)

Riskianalyysi auttaa organisaatiota priorisoimaan omat riskinsä ja määrittelemään kuinka paljon rahaa kannattaa käyttää riskien ehkäisyyn. Riskianalyysi voi olla joko laadullinen (kvalitatiivinen) tai määrällinen (kvantitatiivinen). Laadullisessa eli kvalitatiivisessa riskianalyysissä otetaan huomioon henkilökunnan mielipiteet ja keskusteluissa esille tulleet asiat esitetään johdolle. Kvalitatiivinen riskianalyysi ei pyri ensisijaisesti määrittelemään riskin toteutumisen rahallisia kustannuksia, vaan se perustuu uhkaskenaarioihin ja niiden analysointiin. Skenaarioiden pohjalta luokitellaan uhkien vakavuusaste ja toteutumistodennäköisyys. Kvalitatiivinen analyysi käyttää metodeina parhaita käytäntöjä, kokemusta ja intuitiota. Laadullisia metodeja ovat mm. aivoriihet, ryhmäanalysoinnit, haastattelut, kyselyt ja tarkistuslistat. Riskianalyysityöryhmä päättää mitä menetelmää organisaatiossa käytetään. (Harris 2008, 98.) Laadullisen analyysin tulokset perustuvat joltain osin arvailuihin ja niistä on hankala saada euromääräistä vertailuinformaatiota. Määrällinen eli kvantitatiivinen riskien analysointi sisältää hinta-hyötyarvioinnin ja analyysi on helposti automatisoitavissa. Määrällinen analyysi kertoo riskin euromääräisenä, mutta analyysi vaatii monimutkaisia laskutoimituksia ja se on verraten työläs toteuttaa.

5 Riskien käsittelyn eri vaihtoehdot

Riskien käsittelylle on olemassa erilaisia toimenpiteitä ISO 27001 -standardin mukaan. Riskeiltä voidaan suojautua käyttämällä standardissa lueteltuja turvamekanismeja viitekehyksenä tai osa

riskeistä voidaan hyväksyä tietoisesti ja objektiivisesti, jos ne selkeästi toteuttavat yrityksen tietoturvapolitiikan ja siinä määritellyt riskien hyväksymiskriteerit. Riskejä voidaan myös välttää erilaisilla teknisillä toimenpiteillä kuten esimerkiksi virustorjunnalla tai palomuuritekniikalla. Osa riskeistä voidaan siirtää sidosryhmille esimerkiksi vakuutusyhtiölle tai toimittajille.

5.1 Tunnistettujen riskien käsittelymenetelmät

Niiden riskien osalta, jotka on tunnistettu arviointimenettelyssä, on tehtävä myös päätös riskien käsittelymenetelmästä. Riskien käsittelymenetelmiä ovat seuraavat vaihtoehdot:

- otetaan käyttöön turvamekanismi, jolla riskiä pienennetään
- hyväksytään riski tietoisesti edellyttäen, että hyväksyntä täyttää organisaation riskien hyväksyntäkriteerit
- vältetään tai poistetaan riski kieltämällä toiminto, joka voi aiheuttaa riskin synnyn
- siirretään riski sidosryhmälle, esimerkiksi vakuutusyhtiölle tai toimittajalle (ISO 17799 2006, 26.)

Riskin seurausvaikutusten pienentäminen on yleisin tapa hallita tietoturvallisuusuhkia. Tavallinen esimerkki riskin pienentämisestä on yrityksen lähiverkon suojaaminen palomuurilla. Palomuuriratkaisulla pyritään estämään ulkopuolisten luvaton tunkeutuminen yrityksen lähiverkkoon. Ratkaisu perustuu teknisen laitteen ja siinä olevan ohjelman kokonaisuuteen. Palomuurilaitteeseen määritellään, mikä verkkoliikenne on sallittua yrityksen lähiverkkoon päin. Luvatonta tunkeutumista ei voida kuitenkaan kokonaan estää, mutta palomuurin ohittaminen vaatii asiantuntijuutta sekä asianmukaisia käyttöoikeuksia. (Miettinen 1999, 56.)

Riskin hyväksyminen tarkoittaa sitä, että riskin hallitsemiseksi ei tehdä mitään toimenpiteitä, vaan se päätetään hyväksyä sellaisenaan. Tähän päädytään usein silloin, kun riskin vaikutus on hyvin pieni organisaation toimintaan tai sen toteutumisen todennäköisyys on olematon. (Miettinen 1999, 57.) Vähäpätöistäkin riskiä on kuitenkin syytä tarkkailla säännöllisin väliajoin, jotta se edelleen hallitaan kontrolloidusti ja että sen todennäköisyys säilyy jatkossakin vähäpätöisenä. Organisaation tulisi päättää kriteereistä, joilla määritellään voidaanko riski hyväksyä vai ei. Päätökset riskien hyväksymisestä tulee dokumentoida (ISO 17799 2006, 26). Jäännösriskeille on saatava johdon hyväksyntä, sekä johdolta on saatava valtuutus tietoturvallisuuden hallintajärjestelmän käyttöönotolle ja käytölle.

Riskin poistaminen on usein mahdotonta ja voi vaatia runsaasti ylimääräistä työtä sekä lisäkustannuksia. Mikäli riski liittyy esimerkiksi epäluotettavaan henkilöön, voidaan riski poistaa irtisanomal-

la henkilön työsopimus. Riski jää kuitenkin elämään vielä, koska henkilöllä on muistissaan tietoja yrityksen asioista. (Miettinen 1999, 56.)

Tietoturvallisuuteen liittyvän riskin voi siirtää esimerkiksi vakuutusyhtiölle. Esimerkiksi palovakuutuksen hankkiminen kiinteistölle tai muulle kiinteälle omaisuudelle on riskin siirtämistä. Palovakuutus ei kuitenkaan ota kantaa esimerkiksi tietojärjestelmien varmuuskopiointiin. Varmuuskopioiden ottaminen ja turvallinen säilyttäminen on organisaation omalla vastuullaan. (Miettinen 1999, 57.)

5.2 Valvontatavoitteiden ja turvamekanismien valinta

Valvontatavoitteet ja turvamekanismit tulee valita siten, että ne täyttävät riskien arviointi- ja käsittelyprosessissa yksilöidyt riskit. Organisaation tulee ottaa huomioon myös lakisääteiset, hallinnollisten määräysten asettamat ja sopimukselliset vaatimukset tietoturvallisuudelle. (Laaksonen, 83.) ISO 27001 -standardi sisältää kattavan luettelon valvontatavoitteista ja turvamekanismeista, joiden on huomattu olevan olennaisia organisaatioissa. Standardin turvamekanismeja käyttämällä varmistetaan se, että mitään tärkeitä valvontavaihtoehtoja ei jätetä huomiotta.

Turvamekanismit voidaan valita standardien esittämistä turvamekanismijärjestelmistä tai uusia turvamekanismeja voidaan kehittää oman organisaation erityistarpeisiin. On huomioitava, että kaikki turvamekanismit eivät sovellu sellaisenaan kaikkiin tietojärjestelmiin tai ympäristöihin. Olisikin tärkeää jo tietojärjestelmien hankinta- tai suunnitteluvaiheessa ottaa huomioon myös tietoturvavaatimukset, joita organisaatiolla on. Etukäteissuunnittelulla säästetään kustannuksia ja varmistetaan, että saavutetaan riittävä turvallisuustaso. (ISO 17799 2006, 28.)

5.3 Riskien hallinnan soveltamissuunnitelma

Riskien hallinnan soveltamissuunnitelmasta tulee käydä ilmi ISO 27001–standardin mukaan valitut valvontatavoitteet ja turvamekanismit perusteluineen. Myös soveltamissuunnitelman ulkopuolelle jätetyt valvontatavoitteet ja turvamekanismit tulee luetella ja perustella niiden poisjättö suunnitelmasta. Soveltamissuunnitelma on tiivistelmä riskien käsittelyyn liittyvistä päätöksistä. (ISO 27001 2006, 18.)

5.4 Riskien hallinnan toteuttaminen, seuranta ja koulutus

Valittujen turvamekanismien käyttöönotto on riskien hallinnan käytännön työtä. Turvamekanismien tehokkuuden mittaaminen antaa esimiehille ja henkilöstölle mahdollisuuden määrittää, miten hyvin turvamekanismi saavuttaa asetetut valvontatavoitteet (ISO 27001 2006, 18). Liitteessä 1 on

esimerkki lomakkeesta, jolla suoritetaan laitteistoturvallisuuden turvamekanismien mittausta. Mittaus suoritetaan haastattelulla ja se on rajattu sähkönsyötön ratkaisuihin. Liite 1 on osa valtiovarainministeriön VAHTI-ohjeistusta. Riskien hallinta on jatkuvaa työtä ja tehtyjä riskianalyysejä tulisi katselmoida säännöllisesti. Tehtäessä muutoksia tai hankittaessa esimerkiksi uusia tietojärjestelmiä tulee aina tehdä kattava riskianalyysi, jolla varaudutaan mahdollisiin uusiin turvamekanismeihin tai tehdään tarvittavat muutokset olemassa oleviin valvontatavoitteisiin. Riskien katselmointien tulokset dokumentoidaan ja raportoidaan johdolle. Vastuussa olevan johdon tulee viipymättä puuttua havaittuihin poikkeamiin ja käynnistää tarvittavat toimenpiteet poikkeaman korjaamiseen.

Organisaation tulee myös varmistua siitä, että henkilöstöllä, jolle on asetettu vastuita riskien omistajina, on pätevyys vaadittujen tehtävien suorittamiseen. Henkilöstölle on annettava tarpeellinen koulutus riskien arviointiin ja turvamekanismien käyttöön sekä valvontaan. Koko henkilöstölle on syytä painottaa tietoturvatehtävien merkitystä ja tärkeyttä jokapäiväisessä työssä. Selkeillä ohjeilla ja säännöillä on vain merkitystä, jos niitä noudatetaan.

6 Organisaation prosessien merkitys

Yrityksen prosessien kuvaamiselle perustan luo organisaation visio, strategia, toimintaperiaatteet ja operatiivinen toiminta. Prosessien kuvaaminen liittyy kiinteänä osana yrityksen toiminnan suunnittelua ja kehittämistä. Prosessikuvaukset ovat johtamisen ja toiminnan hallinnan työvälineitä, mutta niitä voidaan myös hyödyntää perehdyttämisessä, koulutuksessa ja tietojärjestelmien kehittämisessä. Prosessien kuvaaminen on myös edellytys onnistuneelle liiketoiminnan jatkuvuussuunnittelulle. Ilman kokonaiskuvaa organisaation ydin- ja tukiprosesseista ei voida tietää, mihin kaikkeen prosessissa tapahtuva häiriö tai poikkeama voi vaikuttaa. Hyvin dokumentoidut prosessit ja ohjeet auttavat yritystä selviytymään häiriötilanteesta hallitusti takaisin normaalitoimintaan. (Iivari & Laaksonen 2009, 104-107.) Strategisella tasolla on tärkeää selvittää ja huomioida mitkä ovat ne yrityksen kriittiset prosessit, jotka vaikuttavat eniten sen ydinliiketoimintaan. Nykyään kriittisiin prosesseihin liittyy lähes aina myös tietojärjestelmiä, joita voidaan myös kutsua kriittisiksi järjestelmiksi. Jatkuvuussuunnittelun pääperiaatteena on kriittisten prosessien toiminnan turvaaminen erilaisissa häiriötilanteissa. (ENISA 2006, 7.) Tietoturvariskien osalta kriittiset tietojärjestelmät on analysoitava tarkasti ja uhkakuvat tunnistettava sekä luokiteltava. Kriittisen prosessin omistajan on kyettävä määrittämään ne vasteajat, joita häiriötilanteesta toipumiseen menee ja kuinka liiketoiminta sen kestää ilman huomattavia taloudellisia tappioita. (Iivari & Laaksonen 2009, 104-107.)

Liiketoiminnan kannalta kriittisten prosessien ja niihin liittyvien tietoturvariskien analysoinnissa ja luokittelussa voidaan käyttää erilaisia taulukoita apuna. ENISA European Network and Information

Security Agencyn kotisivuilta (www.enisa.europa.eu) löytyy alla olevan taulukon 3. kaltaisia valmiita materiaaleja riskien hallintaan ja arviointiin. (ENISA 2006, 16.)

LIIKETOIMINTAPROSESSI	PROSESSIN KRIITTISYYS LIIKETOIMINNAN KANNALTA
Tuotanto	Korkea
Taloushallinto	Keskitaso
Henkilöstöhallinto	Korkea
Markkinointi	Matala

Taulukko 2. Liiketoimintaprosessien kriittisyys organisaation ydintoiminnan kannalta

Jotta taulukossa olevat liiketoimintaprosessit saadaan suoritetuksi, tarvitaan yrityksessä X tietojärjestelmiä. Tietojärjestelmien kriittisyyden arviointiin liiketoiminnan näkökulmasta pk-yrityksissä ENISA ehdottaa seuraavaa alla olevaa taulukkoa numero 3.

	Liiketoimintaprosessit					
Tietojärjestelmät liiketoiminta-kriittisyys	**Tuotanto korkea**	**Taloushallinto keskitaso**	**Henkilöstö-hallinto korkea**	**Markkinointi matala**	**Huom!**	Kokonais-kriittisyys
Nettisivupalvelin ja sovellus	erittäin kriittinen	erittäin kriittinen	ei merkitystä	vähäinen kriittisyys	yritys myy pääasiassa tuotteita nettikaupan kautta	Korkea
Asiakkuuden-hallintaohjelma	erittäin kriittinen	melko kriittinen	ei merkitystä	vähäinen kriittisyys	asiakastiedot tallennetaan tietokantaan	Korkea
Tulostuspalvelin	melko kriittinen	vähäinen kriittisyys	ei merkitystä	ei merkitystä	asiakkaille tulostetaan tilauksen mukaan lähetysluettelo	Vähäinen
Sähköposti-järjestelmä	erittäin kriittinen	melko kriittinen	erittäin kriittinen	melko kriittinen	sähköpostia käytetään sisäiseen kommunikointiin sekä yhteydenpitoon asiakkaisiin	Korkea
IT-infrastruktuuri	erittäin kriittinen	melko kriittinen	vähäinen kriittisyys	melko kriittinen	laitteistot, verkko, sovellukset	Korkea

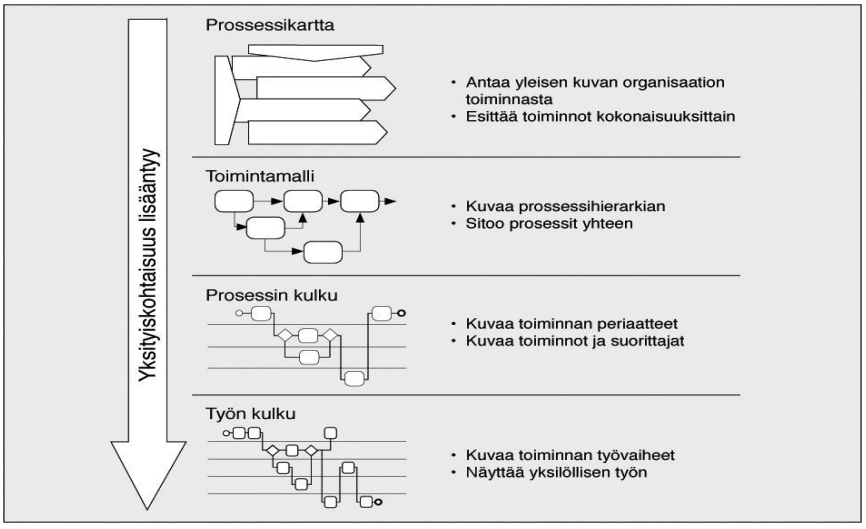
Taulukko 3. Tietojärjestelmien ja liiketoiminnan kriittisyys

Viimeinen sarake kertoo liiketoimintaprosessin kokonaiskriittisyyden suhteessa tietojärjestelmien kriittisyyteen, jos tietojärjestelmä on erittäin kriittinen liiketoiminnan näkökulmasta yhdessäkin prosessissa, on sen kokonaiskriittisyys korkea. (ENISA 2006, 16.)

6.1 Prosessien kuvaaminen

Prosessit tulisi kuvata tarpeeksi yksityiskohtaisesti, jotta muut henkilöt voivat ne toistaa prosessikuvasten perusteella. Prosessin dokumentoinnista tulisi käydä ilmi ainakin prosessin nimi ja omistaja, yksittäisten toimintojen kuvaus, resurssit ja riippuvuudet, prosessin suorittajat sekä kriittisyys toiminnan kannalta. Usein prosessit kuvataan vuokaavioksi, joka on yksinkertaistettu kuvaus prosessin eri vaiheista ja tehtävistä. (Iivari 2009, 107.)
Prosessien kuvaamiseen löytyy apuvälineitä esimerkiksi JSH-suosituksesta (Julkisen hallinnon tietohallinnon neuvottelukunnan suositukset http://www.jhs-suositukset.fi), joka on julkishallinnon käyttöön tarkoitettuja menettelytapoja, määrittelyjä ja ohjeita, joiden tavoitteena on parantaa tietojärjestelmien yhteensopivuutta ja kehitystyötä. JHS-suosituksessa 152 annetaan ohjeita prosessien kuvaamiselle. Ohjeessa prosessit on jaettu neljään kuvaustasoon: prosessikartta, toimintamalli, prosessin kulku ja työnkulku. Ohjeita voidaan soveltaa myös yritysmaailman prosessien kuvaukseen. (Iivari 2009, 108.)

Kuvassa 4. on kuvattu prosessien eri kuvaustasot (http://docs.jhs-suositukset.fi/jhs-suositukset/JHS152/JHS152.pdf 2008, 7). Prosessikuvausten yksityiskohtaisuus lisääntyy mitä tarkemmin prosessia kuvataan. Yleistason prosessikartasta, jota käytetään usein organisaation toimintojen kokonaiskuvaan, voidaan työnkulun tasolla kuvata yksityiskohtaisesti jonkin yksittäisen prosessin työvaiheet.



Kuva 4. Prosessien kuvaustasot

6.2 Prosessit ja tietoturvariskien tunnistaminen

Itse prosessien kuvaaminen ennen tietoturvariskien analysointia helpottaa huomattavasti mahdollisten riskien tunnistamistyötä. Hyvä prosessin tuntemus ja dokumentaatio on suureksi avuksi riskityöryhmän työlle ja uhkakuvien analysoinnille. (Iivari 2009, 118.) Prosessin tietoturvariskianalyysiä

tehtäessä tulisi erityisesti kiinnittää huomiota sellaisten uhkakuvien tunnistamiseen, jotka voivat toteutuessaan aiheuttaa organisaation ydinprosessien keskeytymisen. Riskianalyysissä tulisi ottaa huomioon eri prosessien väliset riippuvuudet, sillä jonkin prosessin ongelmat voivat joko välittömästi tai viiveellä heijastua myös analyysin kohteena olevaan prosessiin. Erilaisia tapahtumaketjuja aiheuttavia tilanteita voivat olla mm. laiteviat, ihmisten tekemät virheet tai voimakkaat sääilmiöt. Uhkakuvat kannattaa käydä perusteellisesti läpi prosessin tietoturvariskejä arvioitaessa ja niiden mahdolliset vaikutukset liiketoimintaan. Tyypillisiä IT-prosesseja haittaavia tilanteita ovat esimerkiksi seuraavien palvelujen saatavuusongelmat: sähkö, tele- ja tietoliikenneverkko, varahenkilön tai varalaitteen puuttuminen. Esimerkiksi sähkökatkoihin voidaan varautua hankkimalla varavoimajärjestelmä tai tietojärjestelmän avainhenkilön ollessa lomalla on koulutettu varahenkilö vastuussa järjestelmän toiminnasta. (Iivari 2009, 109-110.)

Tutkija Richard J. Kepenach on määritellyt julkaisussaan ”Business Continuity Plan Design 8 Steps for Getting Started Designing a Plan” kahdeksan askelta jatkuvuussuunnittelun aloittamiselle kriisin sattuessa. Neljännessä askeleessa hän tähdentää organisaation kriittisten prosessien tunnistamista, jotka täytyy toimia vaikka organisaation muu toiminta pysähtyisi. Prosessit tulisi dokumentoida ja niiden toipumisaika, avainhenkilöt sekä sijaiset määritellä. Hän esittää mm. seuraavia kysymyksiä: kuinka nopeasti saadaan hankittua varalaitteisto? voidaanko prosessi hoitaa etätyönä esim. kotoa käsin? mitä teknologiaa tarvitaan etätyötä varten? jne. Myös sellaiset prosessit on Kepenachin mukaan tunnistettava, joilla voidaan vähentää riskejä jo etukäteen. (Kepenach 2007, IEEE Second International Conference on Internet Monitoring and Protection.)

7 Tutkimuksen kohdeyritys

Rosk’n Roll Oy Ab on Länsi-Uudellamaalla toimiva 12 kunnan (Hanko, Inkoo, Karjaa, Karjalohja, Karkkila, Lohja, Nummi-Pusula, Pohja, Sammatti, Siuntio, Tammisaari ja Vihti) omistama jätehuoltoyhtiö. Yrityksessä työskentelee 25 vakituista ja 3 määräaikaista työntekijää. Yhtiö on saanut tehtäväkseen hoitaa mm. pääosan kuntien jätehuoltoon liittyvistä velvoitteista säännösten ja määräysten mukaisesti. Tehtävät pyritään hoitamaan tehokkaasti ja ympäristöä säästäen kuntarajoista riippumatta (Rosk’n Roll Oy kotisivut). Rosk’n Roll Oy:n tehtävät voidaan tiivistää seuraavasti:

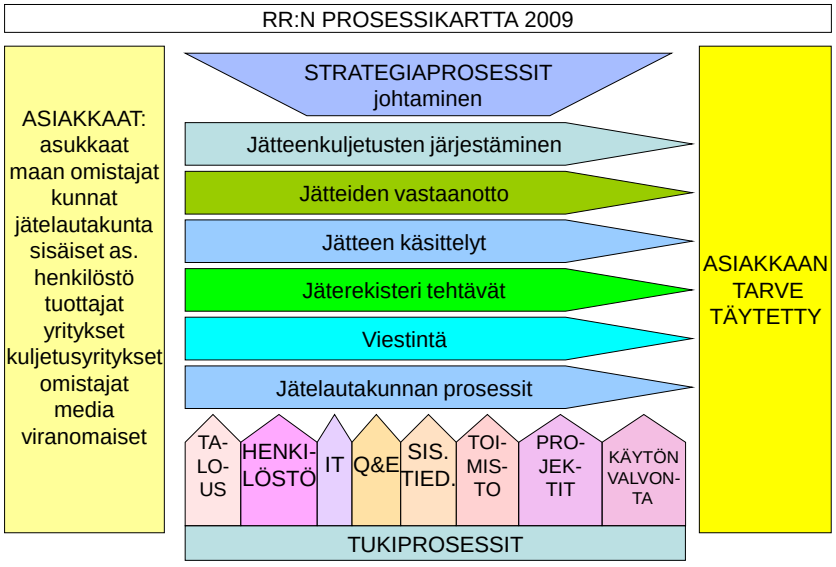
- jätehuollon suunnittelu, kehitys ja koordinointi
- kierrätyksen järjestäminen
- ongelmajätehuollon hoitaminen
- yhteisen alueellisen kaatopaikan ja jätteenkäsittelylaitosten ylläpito
- biojätteiden erilliskeräys
- jätepisteverkoston rakentaminen ja ylläpito
- sekajätekuljetusten kilpailutus

- neuvonta ja tiedotus
- toimintaa ohjaavat lainsäädäntö ja kunnalliset

Yrityksen vuoden 2008 vuosikertomuksessa mainitaan, että tulevaisuuden kehityshankkeena organisaatiolle luodaan tietoturvallisuuden hallintajärjestelmä, jonka viitekehyksenä käytetään ISO 27001–standardia (Rosk'n Roll Oy Vuosikertomus 2008, 6). Opinnäytetyön tekijä toimii yrityksessä IT-asiantuntijana.

7.1 Tutkimuksen lähtötilanne kohdeyrityksessä

Rosk'n Roll Oy:ssä on vuosien 2008 - 2009 aikana kuvattu yrityksen prosessikartta kuvan 4. osoittamalla tavalla. Kuvan keskiosassa on yrityksen ydintoimintaan eli jätehuoltoon liittyvät pääprosessit ja alareunassa on kuvattu toiminnan tukiprosessit. Prosessien määrittelytyö tehtiin ryhmätyönä, jossa oli edustajia eri organisaatioryhmistä. Ryhmätyön tuloksena tunnistettiin eri prosessit ja niiden omistajat. Omistajien vastuulla on tehdä omista prosesseistaan tarkemmat kuvaukset, joissa nähdään tarkasti eri työvaiheet ja resurssit mitä prosessiin liittyy.



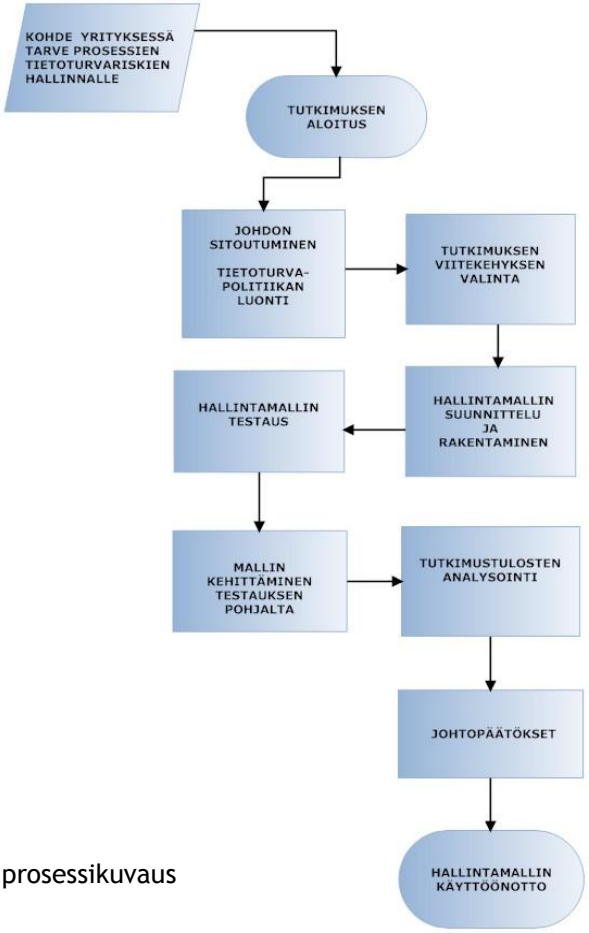
Kuva 5. Rosk'n Roll Oy:n prosessikarttakuvaus

Lähes kaikkiin yrityksen prosessikuvauksessa oleviin prosesseihin kohdistuu erilaisia tietoturvariskejä. Perinteisesti organisaatiossa ovat kaikki tietoturvaan liittyvät asiat olleet IT-asiantuntijan vastuulla. Ongelmana toiminnassa on ollut se, että IT-asiantuntijan on vaikea, ellei mahdoton, havaita yksin kaikkea prosessissa liikkuvaa tietoa ja sen eri riippuvuuksia muihin prosesseihin. Tämän opinnäytetyön tarkoituksena on tehdä prosessikohtainen tietoturvariskien hallintamalli, jota käyttämällä prosessin omistaja voi arvioida ja tunnistaa prosessiin liittyviä uhkakuvia omatoimises-

ti. Turvamekanismien valinta ja tekninen käyttöönotto toteutetaan yhdessä IT-asiantuntijan kanssa.

8 Tutkimusprosessin kulku

Seuraavissa luvuissa kerrotaan miten tutkimus ja tietoturvariskien hallintamallin rakentaminen eteni kohdeyrityksessä. Tutkimuksen prosessikuvaus on kuvattu kuvassa numero 6.



Kuva 6. Tutkimuksen prosessikuvaus

Prosessikuvauksen ensimmäisessä vaiheessa haettiin tehtävälle tietoturvatyölle yrityksen johdon sitoutuminen. Johto sitoutui tietoturvan hallintaan luomalla yrityksen tietoturvapolitiikan, jossa määritellään tietoturvallisuuden merkitys ja tavoitteet yrityksen toiminnassa. Prosessin toisessa vaiheessa etsittiin yrityksen toimintaan soveltuva viitekehys, jolla saatiin selkeät raamit toteutettavalle tietoturvatyölle ja riskienhallinnalle. Valitun viitekehyksen pohjalta aloitettiin itse hallintamallin luonti ja määrittely. Hallintamalli luotiin excel-taulukkolaskentaohjelmalla. Prosessin viimeisessä vaiheessa valmis malli testattiin käytännössä valitsemalla yksi yrityksen pääprosesseista ja yksi tukiprosesseista testikohteiksi. Testauksen tulokset raportoitiin ja analysoitiin. Lopuksi

hallintamallin käyttö koulutetaan prosessin omistajille ja otetaan käyttöön tehtäessä ja määriteltäessä prosessikuvauksia.

8.1 Tietoturvapolitiikka ja johdon rooli

Tutkimuksen lähtökohtana kohdeyrityksessä oli johdon sitoutuminen tietoturvatyöhön. Tietoturvapolitiikan luomisella yrityksen johto osoittaa perustan ja näkemyksen yrityksen tietoturvallisuuden hallintajärjestelmälle, johon sisältyy myös tietoturvariskien johdonmukainen hallinta.

Rosk'n Roll Oy:n tietoturvapolitiikka on organisaation johdon hyväksymä näkemys yhtiön tietoturvan päämääristä, periaatteista, vastuista ja toteutuksesta. Päämäärät on johdettu liiketoiminnan sanelemista tietojen turvaamistarpeista. Tietoturvapolitiikka ohjaa henkilöstön käyttäytymistä sekä suoraan että tarkempien tietoturvaohjeistusten kautta.

Tietoturvapolitiikassa todetaan, että organisaation tietoturvatyön päämääränä on turvata yrityksen toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien joutuminen ulkopuolisille, sekä estää niiden valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen tai vääristyminen, sekä minimoida aiheutuvat vahingot. Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen. Tietoturvapolitiikan tavoitteena on, että yrityksen tietoturvajärjestelyt ovat kansallisen lainsäädännön ja asetuksien mukaisia ja että ne vastaavat laadultaan sidosryhmien asettamia vaatimuksia. Viitekehyksenä yrityksen tietoturvallisuuden hallintajärjestelmän luonnille käytetään ISO 27001 ja 17799 standardeja.

Jokainen yrityksen tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on viime kädessä vastuussa tietoturvan toteutumisesta omalta osaltaan. Kukin yrityksen tietojärjestelmien ja niiden sisältämien tietojen omistaja vastaa tietojensa ja tietojärjestelmiensä suojaamisesta. Ylin vastuu tietoturvan toteutumisesta on yrityksen toimitusjohtajalla. Hän yhdessä johtoryhmän kanssa vastaa kokonaisturvallisuuden kehittämisestä yrityksessä.
Tietoturvallisuuden kehittämisestä, toteutuksen valvonnasta ja tietoturvatietouden edistämisestä yrityksessä vastaa yrityksen johdolta saamien resurssien ja toimintavaltuuksien puitteissa yrityksen tietoturvavastaava (IT-asiantuntija) apunaan IT-ryhmä, jossa on edustajia eri organisaatioryhmistä.

Organisaation prosessien omistajat vastaavat, että tietoturva-asiat huomioidaan prosessin eri vaiheissa. Prosessin omistajan tehtäviä tietoturvan näkökulmasta ovat:

- riskikartoituksen tekeminen tai teettäminen

- prosessin asianmukaisesta suojauksesta päättäminen
- suojaustason varmistaminen
- suojattavien kohteiden luokittelu
- jatkuvuussuunnitelman laatiminen ja testaus yhdessä IT-asiantuntijan kanssa
- tiedonkäsittelytapojen tunteminen
- henkilöstön koulutus
- poikkeamien määrittely, seuranta ja raportointi

Erityisen tärkeää on prosessin ja sen toimintatapojen dokumentointi, jotta varmistetaan tietoturvan jatkuvuus kaikissa tilanteissa.

8.2 Teoreettisen viitekehyksen valinta tutkimukselle

Riskienhallintamallin viitekehyksen valinnasta kohdeyrityksessä vastasi IT-asiantuntija yhdessä palvelu- ja kehityspäällikön kanssa. Viitekehyksen valinnassa perusteluina käytettiin seuraavia argumentteja:

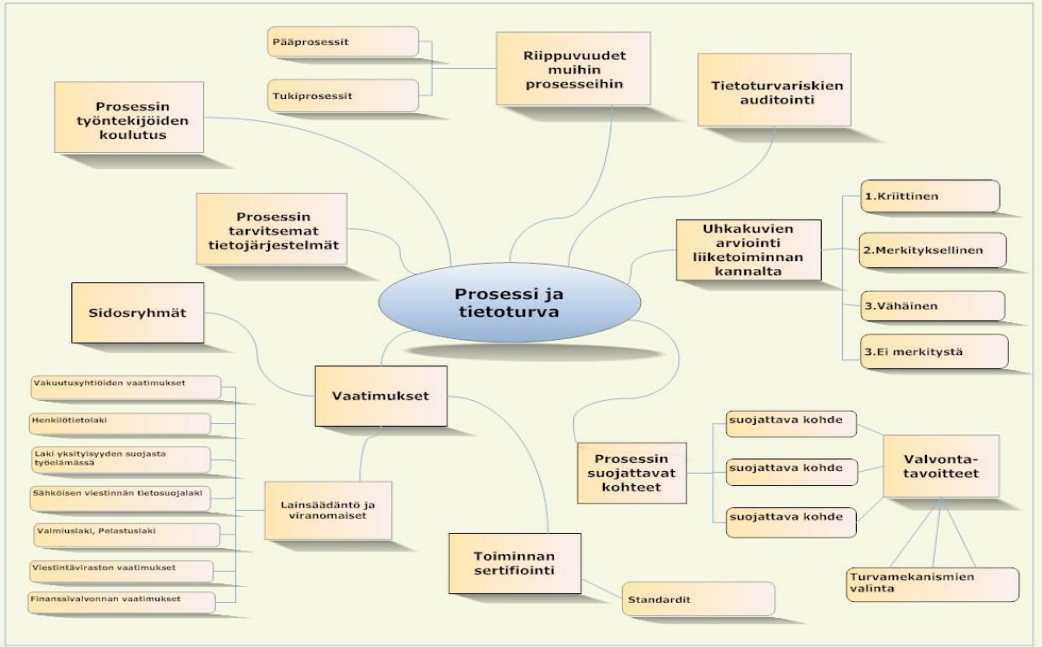
- soveltuvuus pk-yrityksen käyttöön
- helppokäyttöisyys
- soveltuvuus kohdeyrityksen toimintaan
- yleisesti hyväksytty toimintamalli

Useimmat tietoturvallisuuteen liittyvät toimintamallit ja standardit on luotu suuren organisaation tarpeisiin ja niiden noudattaminen pienessä organisaatiossa voi luoda turhaa byrokratiaa ja hallinnollisia menettelytapoja. Viitekehyksen valinnan tärkein kriteeri oli sen käyttäjäystävällisyys ja sovellettavuus organisaation prosesseihin.

Rosk'n Roll Oy:ssä on laatu- ja ympäristöjärjestelmän rakentamisessa käytetty ISO 14001 standardia viitekehyksenä. Tietoturvallisuuden hallintajärjestelmän viitekehyksenä oli luontevaa käyttää samaan standardiperheeseen kuuluvaa ISO 27001 ja 17799 standardeja. Kansainvälisesti hyväksyttyjä standardeja käyttämällä voidaan yrityksen sidosryhmille todentaa tietoturvatyön laatu ja tunnistettujen turvamekanismien käyttö.

8.3 Tietoturvariskien hallintamallin luonti

Hallintamallin rakentaminen aloitettiin kartoittamalla Mindmap-tekniikalla ensin tietoturvaan ja prosesseihin liityviä asioita kohdeyrityksessä. Mindmap-kartan avulla saatiin kokonaiskuva niistä tekijöistä, joita täytyy ottaa huomioon hallintamallin suunnittelussa.

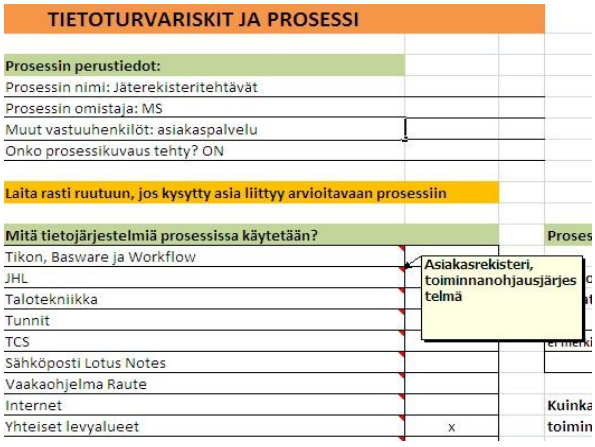


Kuva 7. Mindmap- kartta prosessiin liittyvistä tietoturva-asioista

Hallintamalli tehtiin Microsoft Excel 2007 -taulukkolaskentaohjelmalla. Hallintamallin pohjaksi valittiin sellainen tuote, joka on jokaisen prosessin omistajan käytettävissä. Hallintamalli jaettiin neljään eri välilehteen: perustiedot, riskianalyysi, ISO 27001 turvamekanismit ja riskien arviointi-taulukko. ISO 17799 standardia ei sovelluttu suoraan hallintamallin taulukoihin, koska standardi sisältää pääasiassa tarkempia yksityiskohtaisia ohjeita eri turvamekanismien soveltamiseen.

8.4 Tietoturvariskien hallintamallin esittely ja testaus

Hallintamallin ensimmäisellä sivulla täytetään prosessin perustiedot (Liite 3). Perustiedoissa kysytään prosessin omistajan ja muiden vastuuhenkilöiden tietoja sekä mitä tietojärjestelmiä prosessissa käytetään. Taulukko täytetään laittamalla rasti ruutuun niiden tietojen osalta, joita prosessissa käsitellään. Tietojärjestelmistä saa lyhyen selostuksen viemällä hiiren punaisen kolmion päälle (Kuva 8.).

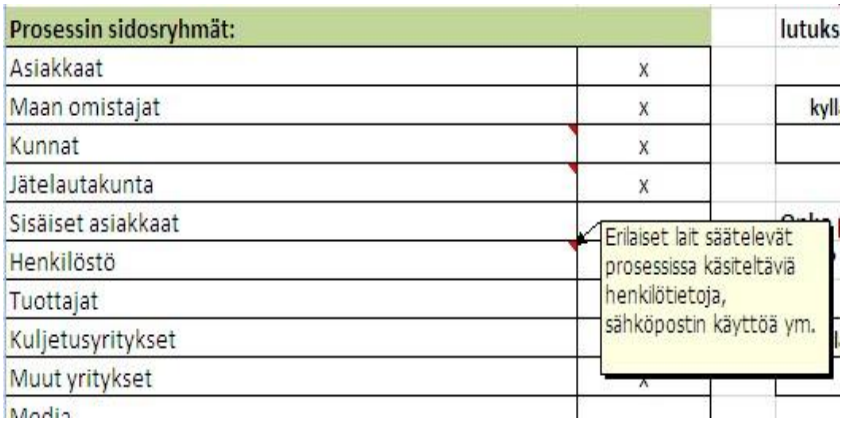


Kuva 8. Prosessin perustiedot

Perustiedot välilehdellä määritellään myös prosessin merkitys yrityksen liiketoimintaan.
Jälleen viemällä hiiren punaisen kolmion päälle saadaan lisätietoa termien määrittelystä. Jos prosessin merkitys on kriittinen liiketoiminnalle on yrityksen toiminnan jatkuminen mahdotonta ilman prosessia ja prosessin puuttuminen aiheuttaa mittavat taloudelliset tappiot (Kuva 9.).

Kuva 9. Prosessi ja liiketoiminta

Prosessin omistajan on myös hyvä miettiä mitä sidosryhmiä (Kuva 10.) prosessiin kuuluu. Yhä useammin eri sidosryhmät asettavat omia vaatimuksiaan prosessin tietoturvan tasolle. Esimerkiksi valtionhallinnossa on alettu vaatia, että järjestelmien ja palveluiden toimittajat sitoutuvat valtionhallinnon tietoturvatasojen mukaisiin vaatimuksiin. Tietoturvasta on myös yhä useammin tulossa osa sopimusehtoja. Tällöin on helpointa viitata johonkin olemassa olevaan normistoon esimerkiksi ISO standardeihin kuin kirjata oma vaatimuslista itse sopimukseen. (Kaila 2010, 40-41.)



Kuva 10. Prosessin sidosryhmät

Perustietojen täytön jälkeen siirrytään riskianalyysi välilehdelle (Liite 4), johon on laadittu ISO 27001 standardin valvontatavoitteiden pohjalta kysymyspatteristo, jolla pyritään mahdollisimman kattavasti arvioimaan prosessin tietoturvariskejä ja niiden nykytilaa. Kysymyksiin vastataan Kyllä, jos uhkatekijä on otettu huomioon prosessissa ja Ei, jos riskiä ei ole huomioitu tai sen nykytilasta ei ole tietoa. Vastaus vaihtoehto Ei kuulu prosessiin valitaan silloin, jos käsiteltävä kysymys ei sisälly prosessin kulkuun tai siinä käsiteltäviin tietoihin (Kuva 11.).

TÄYTTÖOHJE
Arvioi prosessin tietoturvariskejä vastaamalla esitettyyn kysymykseen KYLLÄ, jos uhkatekijä on otettu huomioon prosessissa tai vastaamalla EI, jos riskiä ei ole huomioitu prosessissa. Valitse vastaus: Ei kuulu prosessiin siinä tapauksessa, jos prosessissa ei käsitellä kysyttyä asiaa lainkaan.

PROSESSIN TIETOTURVARISKIEN ARVIOINTI			
PROSESSI JA HENKILÖSTÖTURVALLISUUS (turvamekanismi A8)	KYLLÄ	EI	Ei kuulu prosessiin
Oma työntekijä tai ulkopuolinen urakoitsija/konsultti			
Uusi työntekijä			
Onko prosessiin kuuluvan uuden työntekijän tausta tarkistettu asianmukaisesti?	x		
Onko prosessin tietojärjestelmiin tarvittavat käyttöoikeudet annettu asianmukaisesti?	x		
Onko prosessiin liittyvän tietojärjestelmän käyttöoikeudet dokumentoitu?	x		
Onko työntekijä tietoinen siitä, että allekirjoittamalla työsopimuksen hän sitoutuu noudattamaan yrityksen ja prosessin tietoturvaohjeita?	x		
Onko työntekijälle perehdytetty prosessiin liittyvät tietoturva-asiat?	x		
Onko prosessin työntekijä osallistunut yleisiin tietoturvakoulutustilaisuuksiin?	x		
Tietääkö työntekijä mistä löytyy prosessin tietoturvaohjeistus?	x		
Onko prosessin tietojärjestelmien käyttöoikeudet poistettu työsuhteen päättyessä/muuttuessa?			x
Tunteeko työntekijä prosessin tietojen luokittelun (luotamuksellinen, salainen jne.)?		x	

Kuva 11. Riskianalyysin kysymyksiä

Riskianalyysin kysymysten otsikkotietoihin on luotu suora hyperlinkki kyseiseen aihealueeseen ISO 27001 standardiin. Linkki näkyy sinisenä tekstinä otsikossa.

Hallintamalliin on tuotu ISO 27001 valvontatavoitteet ja turvamekanismit (Liite 5). Ne ovat hallintamallin kolmannella välilehdellä omana taulukkonaan (Kuva 12.).

A.11 Pääsyoikeuksien valvonta	Turvamekanismi
A.11.1 Liiketoiminnan asettamat vaatimukset pääsynvalvonnalle *Tavoite: Tietoihin käsiksi pääsyn valvonta.*	
A.11.1.1 Pääsynvalvonnan toimintaperiaatteet	Pääsyoikeuksia koskevien liiketoiminta- ja turvallisuusvaatimusten perusteella tulee laatia, dokumentoida ja katselmoida pääsynvalvontaperiaatteet.
A.11.2 Käyttöoikeuksien hallinta *Tavoite: Varmistaa valtuutettu käyttäjien pääsy ja estää luvaton pääsy tietojärjestelmiin.*	
A.11.2.1 Käyttäjien rekisteröinti	Käyttöoikeuksien rekisteröintiin ja rekisteröinnin poistoon tulee kaikissa usean käyttäjän tietojärjestelmissä ja palveluissa olla menettelyohjeet.
A.11.2.2 Pääkäyttäjän oikeuksien hallinta	Etuoikeuksien jakamista ja käyttöä tulee rajoittaa ja valvoa.
A.11.2.3 Käyttäjän salasanojen hallinta	Salasanan myöntämistä tulee valvoa määritellyllä hallintaprosessilla.
A.11.2.4 Käyttöoikeuksien uudelleenarviointi	Johdon tulee sovitun menettelyn mukaisesti säännöllisin välein tarkistaa uudelleen käyttäjien käyttöoikeudet.

Kuva 12. ISO 27001 standardin tavoitteet ja turvamekanismit

Hallintamallin neljännellä välilehdellä (Kuva 13.) annetaan vielä työkalu yksittäisen riskin vakavuuden ja todennäköisyyden arviointiin (Liite 6). Mitä todennäköisempi ja vakavampi riski on, sitä huolellisemmin ja tarkemmin on riskin osalta tehtävä tarvittavat suojaukset tietoturvan osalta kuntoon. Riskit on taulukossa luokiteltu sen mukaisesti kuinka merkityksellinen riski on liiketoiminnan kannalta. Suurin riskiluokka on V sietämätön riski, silloin riski on todennäköinen ja erittäin haitallinen yrityksen toiminnan kannalta. Hyvin epätodennäköisen ja merkitykseltään riskiluokka I merkityksetön riski voi olla esimerkiksi sellainen riski, jonka olemassaolo hyväksytään ilman mitään turvamekanismien käyttöä. Liiketoiminnan kannalta merkityksettömään riskiin on turha investoida mittavia turvatoimenpiteitä.

RISKIEN ARVIOINTITAULUKKO

OHJE: Voit arvioida allaolevan taulukon mukaan eri tietoturvariskien todennäköisyyden ja vakavuuden.
Mitä todennäköisempi ja vakavampi riski on sitä nopeammin tulisi turvamekanismit riskin osalta saattaa kuntoon.

Vakavuus → / Todennäköisyys ↓	1. lievästi haitallinen	2. haitallinen	3.erittäin haitallinen
1.hyvin epätodennäköinen	I merkityksetön riski	II siedettävä riski	III kohtalainen riski
2. epätodennäköinen	II siedettävä riski	III kohtalainen riski	IV merkittävä riski
3. todennäköinen	III kohtalainen riski	IV merkittävä riski	V sietämätön riski

Kuva 13. Riskien arviointitaulukko

Kaikkien niiden kysymysten osalta, joihin vastattiin riskianalyysi osassa EI on syytä tehdä kuvan 13 mukainen tarkempi riskienarviointi ja päätös käytettävästä turvamekanismista.

Luotua hallintamallia testattiin sekä pää- ja tukiprosessien osalta. Kummastakin ryhmästä valitiin yksi testattava prosessi. Prosessien omistajat tekivät hallintamallin testit omatoimisesti. Tutkimuksen tekijä haastatteli kumpaakin prosessin omistajaa hallintamallin käytöstä ja taulukoiden täytöstä (Liite 2). Testin tarkoituksena oli ensisijaisesti testata taulukoiden toimivuutta ja kysymysten loogisuutta sekä sitä kuinka hyvin sillä löydetään prosessiin liittyviä uhkakuvia.

8.4.1 Pääprosessin testaus ja tulokset

Pääprosessiksi valittiin jäterekisteritehtävät -prosessi, koska se on yrityksen toiminnassa avainasemassa. Jäterekisterissä ylläpidetään asiakkaiden kiinteistöjen tietoja, laskutusta, palautteita sekä jäteastioiden tyhjennysvälejä. Jäterekisteri sijaitsee toiminnanohjausjärjestelmässä (JHL), jonka keskeytymätön ja häiriötön toiminta on oleellinen osa kohdeyrityksen liiketoimintaa. Asia-

kaspalvelun työn kannalta jäterekisterin ylläpito, hallinta ja tietojen oikeellisuus on välttämätöntä. Jäterekisterin pääkäyttäjä on myös kyseisen prosessin omistaja.

Ennen testausta prosessin omistajalle annettiin lyhyt kirjallinen ohjeistus (Liite 1) tietoturvariskien hallintamallin käyttöön ja taulukoiden täyttämiseen. Hallintamallia ei koulutettu tarkemmin prosessin omistajalle ennen testausta. Testauksella pyrittiin selvittämään onko laajemmalle koulutukselle tarvetta ennen hallintamallin käyttöönottoa. Prosessin omistaja ohjeistettiin täyttämään Perustiedot -taulukko ja sen jälkeen siirtymään Riskianalyysi -taulukkoon. Perustiedot taulukon täytöstä testaaja totesi, että taulukko oli selkeä ja helppo täyttää. Oman prosessin merkitys yrityksen liiketoimintaan oli testattavalle selkeä. Riskianalyysitaulukko oli myös helppotajuinen ja otsikoissa sijaitsevat linkit ISO 27001 standardiin helpottivat huomattavasti lisätiedon etsimisessä. ISO standardin käyttämä terminologia olisi vaatinut ennen taulukon käyttöä avaamista. Testauksen tuloksena saatiin seuraava vastausjakauma:

Kyllä –vastauksia (uhkatekijä on kunnossa prosessin osalta)	28 kpl
Ei –vastauksia (uhkatekijä ei ole ajan tasalla)	6 kpl
En tiedä –vastauksia (uhkatekijän nykytilaa ei tiedetä)	35 kpl
Ei kuulu prosessiin –vastauksia (asia ei kuulu prosessiin)	1 kpl

Riskianalyysissä löytyi paljon sellaisia kysymyksiä, joihin oli käytettävä En tiedä -vaihtoehtoa. Osa En tiedä – vastauksista johtui siitä, ettei testin tekijä ymmärtänyt tarkasti kysymystä ja osa siitä ettei prosessin omistaja tiedä mikä on riskitekijän nykytila prosessissa. Prosessin omistaja oli sitä mieltä, että ennen hallintamallin käyttöä olisi ollut hyvä olla yhteinen koulutustilaisuus, jossa mallin käyttö olisi demonstroitu lyhyesti ja kerrottu käytetyistä termeistä enemmän sekä ISO standardin sisällöstä pääpiirteittäin. Testattavan mielestä hallintamalli oli kokonaisuudessaan onnistunut ja herätti jo nyt paljon kysymyksiä prosessin tietoturvan tilasta.

8.4.2 Tukiprosessin testaus ja tulokset

Tukiprosessiksi valittiin taloushallinnon kirjanpito –prosessi. Taloushallinto käyttää päivittäisessä työssään erilaisia tietoteknisiä sovelluksia, jotka sisältävät arkaluonteisia ja luottamuksellisia asioita. Kirjanpito pitää sisällään niin henkilötietoja kuin yrityksen liiketoiminnan tunnuslukuja. Lisäksi kirjanpidon sovelluksesta on mm. yhteydet maksuliikenteeseen sekä toiminnanohjausjärjestelmään.

Ennen testausta tukiprosessin omistajalle annettiin lyhyt kirjallinen ohjeistus (Liite 1) tietoturvariskien hallintamallin käyttöön ja taulukoiden täyttämiseen. Hallintamallia ei koulutettu tarkemmin prosessin omistajalle ennen testausta. Testauksella pyrittiin selvittämään onko laajemmalle

koulutukselle tarvetta ennen hallintamallin käyttöönottoa. Prosessin omistaja ohjeistettiin täyttämään Perustiedot -taulukko ja sen jälkeen siirtymään Riskianalyysi -taulukkoon.

Perustietojen osalta hallintamallin täyttö sujui hyvin. Eniten päänvaivaa aiheutti ensimmäisessä vaiheessa tunnistaa prosessiin liittyvät sidosryhmät. Lähes kaikki yrityksen sidosryhmät liittyvät jollain tavalla myös kirjanpitoon. Tukiprosessit ovat usein sellaisia, joiden merkittävyys liiketoiminnan jatkuvuuden kannalta ei ole huomattava, mutta ne voivat silti sisältää sellaisia tietoturvariskejä, jotka toteutuessaan aiheuttavat huomattavaa haittaa yrityksen toiminnalle tai ainakin imagolle.

Prosessin omistaja vastasi riskianalyysitaulukon kysymyksiin omatoimisesti. Hallintamallin taulukoiden osalta testin tekijä totesi, että ne olivat selkeitä ja helppokäyttöisiä. Hän ei kaivannut kysyttyihin tietoihin lisäselvennystä. Tukiprosessin vastuuhenkilö oli sitä mieltä, että hallintamalli tulisi ehdottomasti täyttää omatoimisesti. Kirjanpidon osalta on prosessin omistaja kohdeyrityksen talouspäällikkö. Testin tekijä on prosessin toinen vastuuhenkilö. Hallintamallin suurin hyöty testattavan mielestä saavutetaan sillä, että testin tekevät kaikki prosessin vastuuhenkilöt erikseen. Tällä tavoin saadaan arvokasta tietoa siitä, että miten asiat nähdään eri tavoin ja miten asiat ovat prosessin eri vastuuhenkilöiden kesken tiedossa. Tulee varmasti paljon ilmi sellaisia asioita, joista vain toiselle on tieto, vaikka asia pitäisi olla koko prosessin tiedossa. Hallintamallin tulosten analysoinnin osalta testattava oli sitä mieltä, että se olisi antoisinta suorittaa ryhmässä, jossa olisi mukana IT-henkilö ja muita prosessien omistajia. Testattavan mielestä hallintamallin käyttö ei vaadi erillistä koulutusta. Hallintamallin terminologia oli hänelle tuttua jo aikaisemmasta työelämästä. Tietoturvariskien hallintamalli oli myös tukiprosessin vastuuhenkilön mielestä onnistunut ja herätti jo nyt ajatuksia tietoturvan nykytilasta sekä mm. eri sidosryhmien vaatimuksista tietoturvan suhteen. Tukiprosessin riskianalyysin vastaukset jakautuivat seuraavasti:

Kyllä –vastauksia (uhkatekijä on kunnossa prosessin osalta)	35 kpl
Ei –vastauksia (uhkatekijä ei ole ajan tasalla)	1 kpl
En tiedä –vastauksia (uhkatekijän nykytilaa ei tiedetä)	33 kpl
Ei kuulu prosessiin –vastauksia (asia ei kuulu prosessiin)	0 kpl

8.4.3 Testauksen yhteenveto

Molempien pää- ja tukiprosessin testauksien tuloksena voidaan todeta, että hallintamallin taulukoiden ulkonäkö, ohjeistus, helppotajuisuus ja käyttäjäystävällisyys todettiin hyväksi. Riskianalyysin kysymykset olivat kattavia ja ne soveltuivat hyvin testattavien prosessien tietoturvariskien tunnistamiseen. Lukuisista En tiedä –vastauksista voidaan päätellä, että perinteisesti kohdeyrityksen tietoturva-asiat ovat olleet IT-henkilön vastuulla ja monista uhkatekijöiden nykytilasta vain

hänellä on tarkka tieto. Hallintamallin käyttöönoton yksi tavoitteista onkin saattaa tietoturvariskien arviointi ja turvamekanismien hallinta jatkossa prosessin omistajan vastuulle. Vaikka hallintamalli oli helppokäyttöinen, vaatii sen laajempi käyttöönotto organisaatiossa koulutuksen, jossa mallin käyttö demonstroidaan ja kerrotaan ISO standardin merkityksestä sekä avataan terminologiaa. Molempien testattavien mielestä olisi hyvä riskianalyysin tulokset käydä läpi yhdessä ryhmätyönä, jossa mukana IT-asiantuntija sekä muita prosessin omistajia. Hallintamallin käyttö nähtiin kaiken kaikkiaan positiivisena asiana, joka herättää huomaamaan monia sellaisia riskitekijöitä, joita ei tule ajatelleeksi normaalissa päivittäisessä työssään.

8.5 Hallintamallin käyttöönotto, koulutus ja seuranta

Tietoturvariskien hallintamalli tullaan ottamaan kohdeyrityksessä käyttöön vaiheittain. Prosessikuvaukset ovat vielä työn alla ja niiden valmistuttua on myös luontevaa arvioida prosessiin kohdistuvia tietoturvariskejä. Ennen riskianalyysien tekoa hallintamalli koulutetaan prosessin omistajille sisäisenä koulutuksena. Lisäksi hallintamalli ohjeineen viedään sähköiseen dokumenttien hallintajärjestelmään, josta ne ovat kaikkien helposti löydettävissä. Haastavinta hallintamallin käyttöönotossa on herättää ihmisten mielenkiinto turvallisuusasioihin ja saada heidät aktiivisesti huomioimaan tietoturvariskejä omassa työssään. Prosessin omistajien oman tietoturva-ajattelun motivointi ja heillä olevan hiljaisen tiedon saattaminen koko prosessin käyttöön on hallintamallin avaintavoite. (Puhakainen 2010, 22-23.)

IT-toimintoja ja riskien hallintaa katselmoidaan Rosk'n Roll Oy:ssä sisäisellä auditoinnilla vuosittain. Auditoinnin kohteet ja näkökulma vaihtelevat säännöllisesti. Vuonna 2009 sisäinen auditointi kohdistui internet- ja sähköpostiliikenteeseen liittyvään tietoturvaan ja tieto- ja turvallisuusjärjestelmien dokumentointiin sekä työsuojelunäkökohtiin.

9 Tutkimuksen tulokset

9.1 Tutkimuskysymysten analysointi

Opinnäytetyön avulla haettiin vastausta seuraaviin tutkimuskysymyksiin:

- Miten hyvin ISO 27001 ja 17799 standardit soveltuvat pienen organisaation tietoturvariskien hallintamallin luontiin eri prosesseille?
- Miten eri prosessien tietoturvariskit tunnistetaan hallintamallin avulla?
- Miten Hevnerin seitsemän ohjetta IT-artefaktin luontiin soveltuvat tämän tutkimuksen toteuttamiseen ja arviointiin?

Opinnäytetyön tuloksena saatiin tietoturvariskien hallintamalli organisaation eri prosesseille. Hallintamalli toteutettiin excel-taulukon muodossa, jonka avulla prosessin omistaja voi arvioida prosessin tietoturvauhkia ja niiden vaikuttavuutta yrityksen ydinliiketoimintaan. Hallintamalli perustuu kysymyspatteristoon, jossa kartoitetaan eri tietoturvan osa-alueiden riskejä prosessissa. Vastaamalla kysymyksiin saa prosessin omistaja kattavan kuvan eri tietoturvan osa-alueista, niihin liittyvistä uhkatekijöistä sekä tietoturvan nykytilasta prosessissa. Uhkatekijöitä voidaan arvioida vielä yksitellen peilaamalla niiden merkitystä yrityksen liiketoiminnan jatkuvuuteen käyttäen hallintamallin mukana olevaa riskien arviointitaulukkoa.

Ensimmäinen tutkimuskysymys: Miten hyvin ISO standardit 27001 ja 17799 soveltuivat pienen organisaation tietoturvariskien hallintamallin luontiin? Standardit antoivat selkeät raamit työlle ja niiden ohjeita sekä määritelmiä pystyi hyvin soveltamaan käytännön suunnittelutyössä laadittaessa hallintamallin kysymyspatteristoa prosessien omistajille. Standardien antamat määritelmät ja käytetty kieli sekä termistö oli helppotajuista ja niiden antamien ohjeiden perusteella voidaan pk-yrityksenkin tietoturva saattaa valvontatavoitteiden tasalle. Pienessä yrityksessä suurimmaksi ongelmaksi muodostuukin henkilöstön määrä, joka on käytettävissä standardeissa kuvatun toiminnan kehittämiseksi ja toteuttamiseksi. Tietoturvan saattaminen sellaiselle tasolla, jotta toiminta olisi sertifiointiin valmis vaatii paljon työtä ja paneutumista asiaan. Monessa pienessä organisaatiossa ei ole työhön vaadittavaa ammattitaitoista henkilöstöä eikä aikaa sitoutua pitkäkestoiseen projektiin oman työn ohella. Paras hyöty standardeista kohdeyrityksessä saadaan soveltamalla niiden tavoitteita, turvamekanismeja ja ohjeita omaan toimintaan. Standardit kaiken kaikkiaan ovat hyviä ja käyttökelpoisia, mutta työläitä viitekehyksiä tietoturvanhallintamallin luonnille.

Toinen tutkimuskysymys: Miten eri prosessien tietoturvariskit tunnistetaan hallintamallin avulla? Tutkimuksen tavoitteena oli, että prosessin omistaja pystyisi hallintamallia käyttämällä itse tunnistamaan prosessiin liittyvät tietoturvariskit. Hallintamallin kysymyspatteriston avulla prosessin omistaja saa selkeän kuvan prosessin tietoturvariskien nykytilasta ja tietoturva-aukoista. Kysymykset on laadittu ISO 27001 standardin pohjalta ja ne kattavat standardissa esitetyt eri valvontatavoitteet. Riskien tunnistaminen vaatii perehtymistä standardiin ja siihen on varattava aikaa, jotta kaikki tietoturvan eri osa-alueet käydään kattavasti ja aukottomasti läpi. Tunnistettujen uhkakuvien turvamekanismien valinta vaatii yhteistyötä prosessin omistajan ja IT-asiantuntijan kesken. ISO 17799 standardi antaa selkeitä käytännön ohjeita turvamekanismien valintaan ja käyttöön.

9.2 Suunnittelutieteelliset tutkimustulokset

Opinnäytetyön suunnittelutieteellisenä metodologiana käytettiin Hevnerin seitsemää ohjetta IT-artefaktin luontiin. Suunnittelutieteellinen tutkimus tulisi Hevnerin mielestä tuottaa kontribuutiota ainakin kolmella eri osa-alueella: IT-artefaktina itsessään sekä artefaktin konstruointi ja evalu-

ointiprosessina. IT-artefakti tässä tutkimuksessa on itse hallintamalli, jolla prosessin omistaja voi arvioida ja tunnistaa prosessiin liittyviä tietoturvariskejä. Hallintamallia käyttämällä prosessin omistaja saa kattavan kuvan tietoturvan eri osa-alueista ja osaa soveltaa niihin liittyviä turvamekanismeja prosessin toiminnassa. Hallintamallin peruslähtökohta oli, että tietoturva-asioista tietämätön henkilö saa mallin avulla selkeän kuvan prosessin eri uhkakuvista ja turvamekanismeista. Hevner sulkee ihmiset ja organisaation elementit IT-artefaktin määritelmän ulkopuolelle, mutta Järvinen tulkitsee tutkimuksessaan ”On reviewing results of design research” IT-artefaktin määritelmää siten, että siihen oleelliseti liittyy myös käyttäjänäkökulma. Järvisen mukaan Hevnerin ohjeeseen IT-artefaktin määritelmästä tulisikin lisätä käyttäjän osuus siitä syystä, että hyväkään innovaatio ei ole toimiva, jos se ei ole käytännössä sitä mitä artefaktin käyttäjät tarvitsevat tai sen toiminta on epäkäytännöllistä ”goodness of the IT artefact depends on its users”. (Järvinen 2007, 1395.) Tutkimuksen IT-artefakti on case-yrityksen testikäytössä osoittautunut yksinkertaiseksi ja selkeäksi käyttää, joten voidaan todeta sen olevan käyttäjän näkökulmasta varsin toimiva innovaatio.

Hevnerin seitsemän ohjetta antaa tutkimuksen suorittamiselle loogisen ja selkeän raamin, jonka avulla oli helppo toteuttaa käytännön tutkimustyö. Itse kehittämiskohteen rakentamiseen Hevner ei anna käytännön työvälineitä, joten perusteellisen ja riittävän yksityiskohtaisen teorian ja viitekehyksen löytäminen on oleellista. Tässä tutkimuksessa kehittämiskohteen eli tietoturvariskien hallintamallin teoreettisena viitekehyksenä käytettiin alan kirjallisuutta, artikkeleita ja ISO standardeja.

10 Johtopäätökset ja jatkoehdotukset

Käyttämällä viitekehyksenä Hevnerin seitsemää ohjetta tutkimusprosessi eteni johdonmukaisesti vaiheesta toiseen. Vaikein osio tutkmuksessa oli itse hallintamallin luonti. Haastavinta oli pohtia mallin luontia prosessin omistajan näkökulmasta, jolla ei mahdollisesti ole mitään IT-pohjaista taustatietoa tietoturva-asioihin. Kysymyspatteriston laatimiseen ISO 27001 standardi antoi selkeät raamit ja ohjeistuksen. Tutkimus onnistui hyvin vastaamaan kohdeyrityksen tarpeisiin ja sen avulla on mahdollista kartoittaa organisaation prosessien tietoturvan nykytila. Tehdyt testaukset pää- ja tukiprosesseihin osoittivat, että hallintamallin avulla löydetään ne riskitekijät prosesseista, joihin ei ole mietitty turvamekanismeja ollenkaan tai ei olla edes tietoisia uhkakuvien olemassaolosta. Tietoturvariskien hallintamalli tullaan kouluttamaan kohdeyrityksen prosessien omistajille ja sitä käytetään jatkossa prsessikuvauksia tehtäessa tai esimerkiksi uusia hankintoja tai projekteja suunniteltaessa.

Yrityksen johdon merkitys tietoturvariskien hallinnassa on merkittävä. Johdon tulee olla sitoutunut tietoturvan hallintaan ja ymmärrettävä tietoturvauhkien merkitys yrityksen toiminnan jatkuvuuden

suunnittelussa. Jo yrityksen strategioita suunniteltaessa tulisi miettiä keinoja, joilla varmistutaan strategian toteuttamisesta myös kriisitilanteessa. Strategioiden toteuttamista voidaan edistää neljällä asialla: kattavalla riskianalyysillä ja varasuunnitelmalla, strategisella valvontajärjestelmällä, strategisella tiedottamisella ja koulutuksella sekä operatiivisella johtamisella. Erityisesti olisi pyrittävä löytämään ne riskitekijät, joilla on yhtymäkohtia strategiseen suunnitelmaan yrityksen toiminnasta. Varasuunnitelma eli toipumissuunnitelma tulisi olla kaksijakoinen sisältäen toimenpideohjelman, jolla riskin toteutuminen pyritään estämään sekä ohjelma, jolla varaudutaan siihen vaihtoehtoon, että riski toteutuu. (Kamensky 2006, 297-299.)

Jatkoehdotuksena tutkimuksen pohjalta tulisi seuraavaksi yrityksessä keskittyä liiketoiminnan ja eri prosessien jatkuvuussuunnitteluun. Jatkuvuussuunnittelun tarkoitus on turvata yrityksen toiminnan jatkuminen häiriötilanteissa tai poikkeusolojoen aikana. Jatkuvuussuunnittelu ei ole projekti, vaan jatkuva prosessi, jonka tavoitteena on ennalta varautuminen ongelmatilanteisiin. Toipumissuunnitelma on osa jatkuvuussuunnitelmaa, joka sisältää toimenpideohjeet katastrofista toipumiseen. Case –yrityksessä tulisi laatia eri prosessien tietojärjestelmien toipumissuunnitelmat, jossa määritellään varajärjestelmävaatimukset, vastuuhenkilöt ja toimet sekä yksityiskohtaiset ohjeet miten toimitaan häiriötilanteessa. Jatkuvuussuunnittelu tulisi olla osa yrityksen jokapäiväistä toimintaa. Uusia sopimuksia laadittaessa tai esimerkiksi IT-laitteita huollettaessa tulisi aina pitää mielessä prosessien jatkuvuusvaatimukset. (Iivari 2009, 18-23.)

Lähteet

Anttila, J. & Kajava, J. 2006. PDCA-malli tietoturvallisuuden integroinnissa organisaation liiketoiminnan johtamiseen. SFS-Tiedotus 38 VSK 2/2006, 43 - 46.

ENISA European Network and Information Security Agency. 2006. http://www.enisa.europa.eu/act/rm/files/deliverables/information-packages-for-small-and-medium-sized-enterprises-smes. Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)

Fränti, M. & Pirinen, R. 2005. Tutkiva oppiminen integratiivisissa oppimisympäristöissä BarLaurea ja REDLabs. Espoo: Laurea.

Harris, S. 2008. All-in-one CISSP Exam Guide 4th edition. USA: The McGraw-Hill Companies.

Hevner, A.R., March, S. T., Park, J. & Ram, S. 2004. Design science in information systems research. MIS Quarterly Vol. 28 No. 1, 75 - 105.

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tallinna: Tietosanoma Oy.

JHS-suositukset. 2008. http://docs.jhs-suositukset.fi/jhs-suositukset/JHS152/JHS152.pdf 2008. JHS 152 Prosessien kuvaaminen. JUHTA: Julkisen hallinnon tietohallinnon neuvottelukunta.

Järvinen, P. & Järvinen, A. 2004. Tutkimustyön menetelmistä. Tampere: Opinpajan kirja.

Järvinen, P. 2006. Onko innovaatioiden suunnittelu tiedettä? Systeemityö 2/2006, 25 - 27.

Järvinen, P. 2007. On reviewing results of design research. Tampere: Department of computer sciences. University of Tampere.

Kaila, U. 2010. Tietoturvasta tuli sopimusehto. Turvallisuus 2/2010, 40-41.

Kamensky, M. 2006. Strateginen johtaminen. Helsinki: Talentum Media Oy.

Kepenach, R.J. 2007. Business Continuity Plan Design 8 Steps for Getting Started Designing a Plan. IEEE Second International Conference on Internet Monitoring and Protection.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita. 146-147.

Miettinen, J. E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Puhakainen, P. 2010. Suomen turvallisuusalan vuosikirja 2009-2010. Forssa: Forssan kirjapaino Oy. 22-23.

Rosk'n Roll Oy Vuosikertomus 2008. 2009. Lohja: Star-Offset Oy.

Rosk'n Roll Oy. 2009. Viitattu 27.7.2009. http://www.rosknroll.fi

SFS ISO/IEC 27001. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS.

SFS ISO/IEC 17799. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardisoimisliitto SFS.

Tietoturvan ja Tietosuojan erikoislehti. Tietosuoja 2/2007. Forssa: Kirjapaino Oy. 22.

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003. Helsinki: Edita Prima Oy.

Valtiovarainministeriö. 2006. Tietoturvallisuuden arviointi valtionhallinnossa Liite 6 Laitteistoturvallisuus. VAHTI 8/2006. Helsinki: Edita Prima Oy.

Vartiainen, J. 2008. Tietoturvatekniikoita standardisoimassa. Hetky ry:n jäsenlehti 2/2008. Helsinki: MCI Press Oy. 14 - 15.

Kuvat

Taulukot

Liite 1

Hyvä prosessin omistaja

Olen tekemässä opinnäytetyönä tietoturvariskien hallintamallia yrityksen prosesseille. Työ on rakennettu ISO 27001 standardin ympärille. ISO standardissa määritellään vaatimukset yrityksen tietoturvallisuuden hallintajärjestelmän rakentamiselle. Tehty hallintamalli on nyt käytännön testausta vaille. Valitsin testiin kaksi prosessia pääprosessin: Jäterekisteritehtävät ja tukiprosessin: Taloushallinto kirjanpito.

Kansiossa U:\Tietotekniikka AR\Ohjeet kaikille\ONT löytyy excel-taulukko (tietoturvariskien arviointi.xlsx), jonka pyytäisin teitä täyttämään oman prosessinne osalta.

Taulukossa on neljä eri välilehteä. Ensimmäisellä Perustiedot välilehdellä kysytään yleisiä asioita prosessin omistajuudesta ja merkittävyydestä liiketoiminnan kannalta. Punaisista kolmioista saa aina lisäopastusta kyseiseen kohtaan. Toisella välilehdellä Riskianalyysi on koottu ISO 27001 standardin vaatimuksista kysymyksiä, joilla pyritään selvittämään prosessin tietoturvan nykytilaa. Jos asia on otettu huomioon prosessissa, vastataan **Kyllä**, jos asia on hoitamatta, vastataan **Ei** ja jos ei ole tietoa asian nykytilasta, vastataan **En tiedä.** Vastausvaihtoehto **Ei kuulu prosessiin** valitaan, jos asiaa ei käsitellä prosessissa lainkaan.

Riskianalyysin kysymyksistä päästään otsikkolinkkien avulla suoraan ISO standardin vastaavaan kohtaan (kolmas välilehti). Standardissa on lyhyesti kerrottu miten asia tulisi tietoturvan osalta hoitaa kuntoon. Turvamekanismilla tarkoitetaan välinettä tai toimintatapaa, jolla kohde suojataan riskeiltä. Neljännellä välilehdellä on työkalu Riskien arviointitaulukko tarkempaan riskin merkittävyyden arviointiin. Sitä teidän ei tarvitse tässä vaiheessa tehdä. Niiden kohtien osalta joihin mahdollisesti vastasitte Ei, on syytä yhdessä miettiä tarvittavia suojaustoimenpiteitä, joissa voidaan apuna käyttää riskien arviointitaulukkoa.

Kiitos
Anne Reid

Liite 2

HAASTATTELU TIETOTURVARISKIEN HALLINTAMALLIN ARVIOINTI

1. Oliko lomake helppotajuinen? ymmärsitkö ohjeet, löysitkö punaisista kolmioista lisätietoa?
2. Miten helppo/vaikea oli arvioida prosessin merkitystä liiketoimintaan?
3. Olisiko sitä pitänyt miettiä ryhmässä?
4. Prosessin tietoturvariskien arviointi onko parempi tehdä yksin/ryhmässä?
5. Olisitko tarvinnut koulutusta mallin käyttöön?
6. Oliko ISO-standardi tuttu ennestään?
7. En tiedä vastausten runsas määrä viittaa mielestäsi mihin?
8. Muita kommentteja?

Pääprosessi Jäterekisteritehtävät MS

1. Lomake oli helppotajuinen ja ohjeet riittävät. Punaiset kolmiot löytyivät hyvin.
2. Prosessin arviointi liiketoiminnan kannalta ok. Ehkä korkeintaan asiasta olisi voinut keskustella esimiehen kanssa.
3. Ei välttämättä, ehkä esimiehen kanssa.
4. Riskianalyysin monet En tiedä vaihtoehdot johtuivat siitä, että ei tiedä onko asiaa hoidettu IT:n toimesta tai toimittajan toimesta. Analyysin olisi voinut tehdä yhdessä yrityksen IT-henkilön kanssa tai esimiehen kanssa.
5. Hallintamallin käyttö olisi MS:n mielestä vaatinut pohjustuksen, jossa käyty mallin käyttö läpi ja selvennetty termejä sekä kerrottu lyhyesti ISO standardin sisällöstä.
6. Ei ollut tuttu ennestään.
7. Ei tiedetä riskitekijän nykytilaa.
8. Testaus oli hyvä. Herätti jo nyt keskustelua mm. kulunvalvonnan tilasta ja muista uhkatekijöistä.

Tukiprosessi Taloushallinto kirjanpito SNY

1. Lomake oli helppotajuinen ja ohjeet hyvät. Punaiset kolmiot löytyivät. Tosin testin tekijä ei kokenut niitä edes hirveästi tarvitsevansa.
2. Oli hyvä arvioida prosessin merkitystä liiketoimintaan omatoimisesti, koska asiat tulevat silloin esille eri näkökulmasta. Testattavan mielestä onkin mielenkiintoista nähdä miten asiaa arvioisi toinen taloushallinnon vastuuhenkilö.
3. Ei tarvitse.
4. Riskianalyysi testattavan mielestä ehdottomasti tehtävä itsenäisesti. Tällä tavoin saadaan arvokasta tietoa siitä, että miten asiat nähdään eri tavoin ja miten asiat ovat prosessin eri vastuuhenkilöiden kesken tiedossa. Tulee varmasti paljon ilmi sellaisia asioita, joista vain toiselle on tieto, vaikka pitäisi olla koko prosessin tiedossa.
5. En koe tarvitsevani koulutusta. Ohjeet olivat riittävät.
6. Ei ollut tuttu ennestään.
7. Ei tiedetä riskitekijän nykytilaa. Tieto ehkä jollain muulla.
8. Tulosten analysointi olisi antoisinta suorittaa ryhmässä, jossa mukana IT-henkilö ja muita prosessien omistajia.

TIETOTURVARISKIEN HALLINTAMALLI

LIITE 3

Prosessin perustiedot:

Prosessin nimi:
Prosessin omistaja:
Muut vastuuhenkilöt:
Onko prosessikuvaus tehty?

Laita rasti Kyllä-ruutuun, jos kysytty asia liittyy arvioitavaan prosessiin. Viemällä hiiren punaisen kolmion päälle saa lisätietoa aiheesta.

Mitä tietojärjestelmiä prosessissa käytetään?	Kyllä
Tikon, Basware ja Workflow	
JHL	
Talotekniikka	
Tunnit	
TCS	
Sähköposti Lotus Notes	
Vaakaohjelma Raute	
Internet	
Yhteiset levyalueet	
Valvontakamerat	

Prosessin sidosryhmät:	Kyllä
Ulkoiset asiakkaat	
Sisäiset asiakkaat	
Maan omistajat	
Kunnat	
Jätelautakunta	
Henkilöstö	
Tuottajat	
Kuljetusyritykset	
Muut yritykset	
Media	
Viranomaiset	
Tavaroiden toimittajat	
Vakuutusyhtiöt	

Laita rasti siihen ruutuun, joka kuvaa prosessia parhaiten

Prosessin vaikutus organisaation toimintaan:

Mikä on prosessin merkitys yrityksen liiketoiminnan jatkuvuuden kannalta?

ei merkitystä	vähäinen käyttökatkos max 1vko	melko kriittinen käyttökatkos max 1vrk	kriittinen käyttökatkos max 1-2h

Onko prosessin avainhenkilöt olleet tietoturvakoulutuksessa?

kyllä	ei	en osaa sanoa

Onko prosessin tietoturva-asioita auditoitu säännöllisesti?

kyllä	ei	en osaa sanoa

RISKIANALYYSI

LIITE 4

TÄYTTÖOHJE

Arvioi prosessin tietoturvariskejä vastaamalla esitettyyn kysymykseen KYLLÄ, jos riski on otettu huomioon prosessissa tai vastaamalla EI, jos riskiä ei ole huomioitu prosessissa tai En tiedä, jos et tiedä riskin nykytilaa. Valitse vastaus: Ei kuulu prosessiin siinä tapauksessa, jos prosessissa ei käsitellä kysyttyä asiaa lainkaan.

PROSESSIN TIETOTURVARISKIEN ARVIOINTI

PROSESSI JA HENKILÖSTÖTURVALLISUUS (turvamekanismi A8)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Oma työntekijä tai ulkopuolinen urakoitsija/konsultti				
Uusi työntekijä				
Onko prosessiin kuuluvan uuden työntekijän tausta tarkistettu asianmukaisesti?				
Onko prosessin tietojärjestelmiin tarvittavat käyttöoikeudet annettu asianmukaisesti?				
Onko työntekijä tietoinen siitä, että allekirjoittamalla työsopimuksen hän sitoutuu noudattamaan yrityksen ja prosessin tietoturvaohjeita?				
Onko työntekijälle perehdytetty prosessiin liittyvät tietoturva-asiat?				
Vanha työntekijä				
Onko prosessin työntekijä osallistunut yleisiin tietoturvakoulutustilaisuuksiin?				
Tunteeko työntekijä prosessin tietojen luokittelun (luotamuksellinen, salainen jne.)?				
Tietääkö työntekijä mistä löytyy prosessin tietoturvaohjeistus?				
Työsuhteen päättyminen				
Onko prosessin tietojärjestelmien käyttöoikeudet poistettu työsuhteen päättyessä/muuttuessa?				
Onko työntekijä palauttanut kaikki hallussaan olleet tallennusvälineet ja muut laitteet (kannettava tietokone, puhelin, muistitikut jne.) poistuessaan prosessista?				
PROSESSI JA FYYSINEN TURVALLISUUS (turvamekanismi A9)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Prosessin turva-alueet ja laiteturvallisuus				
Liittyykö prosessiin tietoteknisiä tiloja (palvelinhuoneet ym.), joihin on kulunvalvonta ja kulkuoikeudet määritelty?				
Onko kulkuoikeudet dokumentoitu?				
Onko prosessiin liittyvien tietoteknisten tilojen avainten hallinnointi järjestetty?				
Onko avainten haltijat dokumentoitu?				
Onko prosessiin liittyvät tietotekniset laitteet ja välineet suojattu asianmukaisesti murtojen ja varkauksien varalta?				
Onko prosessiin liittyvät tietotekniset laitteet ja välineet suojattu asianmukaisesti vesivahinkojen varalta? varalta?				

Onko prosessiin liittyvät tietotekniset laitteet ja välineet suojattu asianmukaisesti tulipalon varalta?				
Onko prosessiin liittyvät tietotekniset laitteet ja välineet suojattu asianmukaisesti sähkökatkon varalta?				
Liittyykö prosessiin julkisia tiloja, joissa sijaitsee tietoteknisiä välineitä (verkkopisteet, tietokoneet jne.)?				
Onko julkisten tilojen tietoteknisten välineiden valvonta ja suojaus hoidettu asianmukaisesti?				
Onko prosessiin liittyvät tietotekniset laitteet ja järjestelmät huollettu asianmukaisesti?				
Onko prosessista poistuvien tietoteknisten laitteiden sisältämän tiedon tuhoaminen järjestetty asianmukaisesti?				
PROSESSIN TIETOLIIKENNE JA KÄYTTÖTOIMINNOT (turvamekanismi A10)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Onko prosessiin liittyvien tietoteknisten sovellusten ja laitteiden menettelyohjeet dokumentoitu?				
Onko prosessiin liittyvien tietoteknisten sovellusten ja laitteiden menettelyohjeet niitä tarvitsevien saatavilla?				
Onko prosessin tietojenkäsittelypalveluiden ja -järjestelmien muutosten hallinta valvottua ja dokumentoitua?				
Onko prosessin tietojenkäsittelypalveluiden ja -järjestelmien testausympäristöt erotettu tuotantokäytöstä?				
Onko varmistettu, että prosessiin liittyvä ulkopuolinen palveluntarjoaja seuraa sovittuja toimitustasoja ja palvelumäärittelyjä?				
Seurataanko ja hallitaanko ulkopuolisen palveluntarjoajan tekemiä muutoksia prosessin tietojärjestelmiin?				
Seurataanko prosessin käyttämien tietojärjestelmien kapasiteetin riittävyyttä säännöllisesti?				
Onko luotu prosessiin liittyville tietojärjestelmien uusille versioille ja päivityksille hyväksyntäkriteerit?				
Prosessi ja haittaohjelmat				
Onko prosessin työntekijöillä ohjeet miten toimitaan, kun havaitaan haittaohjelma työasemalla?				
Onko prosessin työntekijöillä ohjeet miten internetissä toimitaan turvallisesti?				
Onko prosessiin liittyvät tietotekniset laitteet ja järjestelmät suojattu haittaohjelmia vastaan?				
Onko prosessiin liittyvät tietojärjestelmät varmuuskopioitu asianmukaisesti?				
Onko prosessissa käytettävien siirrettävien tietovälineiden käyttö ohjeistettu asianmukaisesti?				
Onko prosessiin liittyvien tietojärjestelmien tapahtumalokien seuranta säännöllistä?				
Onko prosessiin liittyvien tietojärjestelmien häiriötilanteet dokumentoitu ja analysoitu?				
PROSESSI JA PÄÄSYOIKEUKSIEN HALLINTA (turvamekanismi A11)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Onko prosessiin liittyvien tietojärjestelmien käyttöoikeudet dokumentoitu				
Onko prosessiin liittyvien tietojärjestelmien käyttöoikeuksien hallinnasta tehty menettelyohjeet?				
Onko prosessin käyttäjiä ohjeistettu tietojärjestelmien salasanojen hallinnasta?				
Onko prosessiin liittyvien tietojärjestelmien käyttöoikeudet katselmoitu säännöllisesti?				
Onko prosessin käyttäjiä opastettu työaseman lukitsemisesta poistuttaessa työpisteeltä?				

Onko prosessiin liittyvien etähuoltoyhteyksien käyttöoikeudet dokumentoitu?				
Onko prosessiin liittyvät etähuoltoyhteydet rajoitettu ja valvottu fyysisesti palomuuritekniikalla?				
Onko prosessiin liittyvien verkkolevyalueiden käyttöoikeudet asianmukaiset?				
Onko prosessiin liittyvien verkkolevyalueiden käyttöoikeudet katselmoitu säännöllisesti?				
Onko prosessiin liittyvien verkkolevyalueiden käyttöoikeudet dokumentoitu?				
Onko prosessiin liittyvän tietojärjestelmän käyttöoikeudet poistettu irtisanoutuneilta henkilöiltä?				
Onko prosessiin liittyvän tietojärjestelmän pääkäyttäjäoikeudet rajoitettu vain tietyille henkilöille?				
PROSESSI JA UUDEN TIETOJÄRJESTELMÄN HANKINTA, KEHITYS SEKÄ YLLÄPITO (turvamekanismi A12)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Onko prosessin liiketoiminnan vaatimukset määritelty tietoturvan osalta?				
Onko prosessin tuotantokäytössä olevien tietojärjestelmien osalta määritelty menettelytavat, kun asennetaan uusi versio tai ohjelmisto?				
Onko prosessiin liittyvien tietojärjestelmien testiaineisto suojattu asianmukaisesti?				
Onko prosessiin liittyvien tietojärjestelmien lähdekoodi suojattu ja siihen pääsy rajoitettu asianmukaisesti?				
Onko prosessiin liittyvien tietojärjestelmien tehtävät muutokset valvottu asianmukaisesti?				
Onko prosessiin liittyvien tietojärjestelmien tehtävät muutokset dokumentoitu asianmukaisesti?				
Onko prosessiin liittyvien tietojärjestelmien tehtävät muutokset testattu asianmukaisesti?				
PROSESSIN TIETOTURVAHÄIRIÖIDEN HALLINTA (turvamekanismi A13)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Onko prosessiin liittyvien tietojärjestelmien tekniset haavoittuvuudet päivitetty säännöllisesti?				
Onko prosessiin liittyvien tietojärjestelmien havaitut heikkoudet (viat) raportoitu?				
Onko prosessiin liittyvien tietojärjestelmien hallintavastuut ja menettelytavat tietoturvahäiriöiden osalta määritelty ja dokumentoitu?				
PROSESSI JA LIIKETOIMINNAN JATKUVUUDEN HALLINTA (turvamekanismi A14)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Onko prosessille tehty toipumissuunnitelma tietotekniikan osalta?				
Onko toipumissuunnitelma testattu säännöllisesti?				
Onko toipumissuunnitelma koulutettu prosessin avainhenkilöille?				
PROSESSI JA VAATIMUSTENMUKAISUUS (turvamekanismi A15)	KYLLÄ	EI	En tiedä	Ei kuulu prosessiin
Liittyykö prosessiin lakisääteisiä vaatimuksia tietotekniikan/tietojärjestelmien osalta?				
Onko prosessiin liittyvät lait, määräykset ja sopimukset dokumentoitu ja ajan tasalla?				
Liittyykö prosessiin sidosryhmien vaatimuksia tietoturvan osalta?				
Onko prosessiin liittyvät sidosryhmien vaatimukset dokumentoitu ja ajan tasalla?				
Onko prosessiin liittyvien henkilötietojen tietosuoja hoidettu lain vaatimalla tavalla?				
Onko prosessin työntekijöiltä estetty tietojärjestelmien väärinkäyttö asianmukaisesti?				

Onko prosessin esimies varmistanut tietoturva-asioiden noudattamisen ja turvamekanismien asianmukaisen käytön prosessissa?				
Onko prosessi auditoitu säännöllisesti tietoturva-asioiden osalta?				

ESIMERKKI ISO 27001 standardin sisällöstä

LIITE 5

ISO 27001 VALVONTATAVOITTEET JA TURVAMEKANISMIT

Valvontatavoite = päämäärä miten asia tulisi hoitaa
Turvamekansimi = keinot millä tavoite saavutetaan

A.5 Turvallisuuspolitiikka	Turvamekanismi
A.5.1 Tietoturvapolitiikka *Tavoite: Tarjota johdon ohjaus ja tuki tietoturvallisuudelle liiketoimintatavoitteiden ja asiaankuuluvien lakien ja asetusten*	
A.5.1.1 Tietoturvapolitiikan määrittelyasiakirja	Tietoturvapolitiikan määrittelyasiakirjan tulee olla johdon hyväksymä, se tulee julkaista ja siitä tulee tiedottaa kaikille työntekijöille ja merkittäville ulkopuolisille tahoille.
A.5.1.2 Tietoturvapolitiikan katselmointi	Tietoturvapolitiikka tulee katselmoida suunnitelluin aikavälein tai mikäli merkittäviä muutoksia tapahtuu, jotta varmistetaan sen jatkuva soveltuvuus, asianmukaisuus ja vaikuttavuus.

A.6 Tietoturvallisuuden organisoiminen	Turvamekanismi
A.6.1 Sisäinen organisaatio *Tavoite: Organisaation tietoturvallisuuden hallinta.*	
A.6.1.1 Johdon sitoutuminen tietoturvallisuuteen	Johdon tulee aktiivisesti tukea turvallisuutta organisaatiossa osoittamalla selkeää suuntaa, näkyvää sitoutumista ja tietoturvavastuiden yksiselitteistä jakamista ja tunnustamista.
A.6.1.2 Tietoturvallisuuden koordinointi	Organisaation eri osien edustajien, joilla on asiaankuuluvia rooleja ja työtehtäviä, tulee koordinoida tietoturvallisuuteen liittyvät toimet.
A.6.1.3 Tietoturvallisuutta koskevien vastuiden jako	Kaikki tietoturvavastuut tulee määritellä selvästi.
A.6.1.4 Tietojenkäsittelypalveluja koskeva hyväksyntäprosessi	Tulee määritellä ja ottaa käyttöön uusia tietojenkäsittelypalveluja koskeva johdon hyväksyntäprosessi.
A.6.1.5 Salassapitositoumus	Salassapito- tai vaitiolositoumukset, jotka kuvastavat organisaation tarpeita

	suojata tietoa, tulee yksilöidä ja niitä tulee katselmoida säännöllisesti.
A.6.1.6 Yhteydet viranomaisiin	Asiaankuuluvien viranomaisten kanssa tulee pitää asianmukaista yhteyttä.
A.6.1.7 Yhteydet erityisintressiryhmiin	Tulee ylläpitää asianmukaisia yhteyksiä erikoisintressiryhmiin tai muihin turvallisuusasiantuntijaryhmiin ja ammatillisiin järjestöihin.
A.6.1.8 Tietoturvallisuuden riippumaton arviointi	Organisaation tietoturvallisuuden toimintamallille ja sen toteuttamiselle (eli tietoturvallisuuteen liittyville valvontatavoitteille, turvamekanismeille, periaatteille, prosesseille ja menettelytavoille) tulee suorittaa riippumaton katselmus suunnitelluin väliajoin, tai kun turvallisuuden toteuttamisessa tapahtuu merkittäviä muutoksia.

RISKIEN ARVIOINTITAULUKKO

LIITE 6

OHJE: Voit arvioida allaolevan taulukon mukaan eri tietoturvariskien todennäköisyyttä ja vakavuutta liiketoiminnan kannalta. Mitä todennäköisempi ja vakavampi riski on, sitä nopeammin tulisi turvamekanismit riskin osalta saattaa kuntoon.

Vakavuus → Todennäköisyys ↓	1. lievästi haitallinen liiketoiminnalle	2. haitallinen liiketoiminnalle	3.erittäin haitallinen liiketoiminnalle
1.hyvin epätodennäköinen	**I merkityksetön riski**	**II siedettävä riski**	**III kohtalainen riski**
2. epätodennäköinen	**II siedettävä riski**	**III kohtalainen riski**	**IV merkittävä riski**
3. todennäköinen	**III kohtalainen riski**	**IV merkittävä riski**	**V sietämätön riski**