Lappeenrannan teknillinen yliopisto
School of Business and Management
Tietotekniikan koulutusohjelma

Diplomityö

Joni Suomalainen

Tietoturvallisuuden hallintajärjestelmän käyttöönoton analyysi pk-yritysympäristöstä

Työn tarkastaja(t): Professori Jari Porras
Tutkijatohtori Ari Happonen

Työn ohjaaja(t): Tutkijatohtori Ari Happonen
Suunnittelupäällikkö Timo Storhammar

TIIVISTELMÄ

Lappeenrannan teknillinen yliopisto
School of Business and Management
Tietotekniikan koulutusohjelma

Joni Suomalainen

Tietoturvallisuuden hallintajärjestelmän käyttöönoton analyysi pk-yritysympäristöstä

Diplomityö

2018

57 sivua, 9 kuvaa, 2 taulukkoa

Työn tarkastajat: Professori Jari Porras
Tutkijatohtori Ari Happonen

Hakusanat: tietoturvallisuuden hallintajärjestelmät, VAHTI-ohje, ISO/IEC 27001, EU:n tietosuoja-asetus, tietoturva, tietosuoja

Tietoturvallisuuden hallintajärjestelmä on organisaation laatuinfrastruktuurin osa, jonka tehtävänä on kehittää ja lisätä organisaation tietoturvallisuutta sekä taata liiketoiminnan jatkuvuus. Tässä työssä esitellään tietoturvallisuuden ja tietosuojan merkityksestä organisaatioissa sekä erityisesti tietoturvallisuuden hallintajärjestelmän tärkeimpiä hallinta-alueita. Työn empiirisessä osassa esimerkkiorganisaatiolle implementoitiin tietoturvallisuuden hallintajärjestelmä. Hallintajärjestelmä toteutettiin teoriaosuudessa esitettyjen hallintajärjestelmien pohjalta. Hallintajärjestelmän toteutuksen tuloksena havaittiin, että projektisuunnittelussa tavoitteiden määrittäminen on tärkeässä roolissa implementointiprosessia, jotta toteutusvaiheessa ei tarvitse ryhtyä uudelleen suunnittelemaan hallintajärjestelmään tarvittavia hallinta-alueita. Lisäksi havaittiin, että hallintajärjestelmää toteuttaessa projektissa on osattava rakentaa tarvittavista hallintaosista looginen kokonaisuus, jotta kyseisen hallintajärjestelmän jalkauttaminen organisaatioon on mahdollisimman yksiselitteistä.

ABSTRACT

Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Joni Suomalainen

Analysis of the implementation of the information security management system for an SME environment

Master's Thesis

57 pages, 9 figures, 2 tables

Examiners: Professor Jari Porras
D.Sc. (Tech.) Ari Happonen

Keywords: information security management systems, VAHTI-instructions, ISO/IEC 27001, General Data Protection Regulation, information security, data protection

The information security management system is part of an organization's quality infrastructure, having the task to develop and increase the organization's information security and to ensure business continuity. This thesis will present the importance of information security and data protection in organizations and the most important management areas of the information security management system. In the empirical part of the work, an information security management system was implemented for the example organization. The management system was implemented based on the management systems presented in the theoretical part. As a result of the implementation of the management system, it was found that the design of objectives in project planning plays an important role in the implementation process so that during the implementation phase there is no need to re-design the management areas needed for the management system. In addition, it was found that when implementing a management system, the project must be able to build a logical entity for the necessary management components to make the management of the management system as unambiguous as possible.

ALKUSANAT

Tämä diplomityö on tehty Lappeenrannan teknillisen yliopiston LUT School of Business and Managementin Tietotekniikan koulutusohjelman päättötyönä. Haluan kiittää yliopistolta työni ohjaajaa Ari Happosta sekä työn laatijana toiminutta organisaatiota, jotka ovat kärsivällisesti jaksaneet odottaa työni valmistumista.

Erityskiitos kuuluu myös perheelleni, sukulaisille, työkavereille sekä ystäville jotka ovat jaksaneet tsempata minua tämän työn loppuunsaattamiseksi.

Lappeenrannassa 23.04.2018

Joni Suomalainen

SISÄLLYSLUETTELO

SYMBOLI- JA LYHENNELUETTELO

ISMS	Information Security Management System
ITSEC	Information Technology Security Evaluation Criteria
PDCA	Plan-Do-Check-Act
POA	Potentiaalisten ongelmien analyysi
TCSEC	Trusted Computer System Evaluation Criteria
VAHTI	Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä
VPN	Virtual Private Network

1 JOHDANTO

Tietotekniikasta johtuvien riskien määrät, joita ovat esimerkiksi virheellisten ohjelmien käyttö, hyökkäykset organisaatioiden verkkoa vastaan sekä laitteiden hajoaminen, vaihtelevat organisaatioissa merkittävästi liiketoiminta-alueesta riippuen. Tietoturva on myös yhtenä osana riskien toteuma-alueista. Huolehtimalla tietoturvan hallinnasta pätevästi, voidaan mahdollisista tietoturva- ja tietosuojariskeistä syntyvien uhkien toteutumisen todennäköisyyttä vähentää. Yrityksen organisoitu ja ohjeistettu toiminta, jolla vähennetään ongelmien toteutumistodennäköisyyttä, ovat osa organisaatioiden riskienhallinnan toimenpiteitä.

Tietoturvallisuuden hallintajärjestelmän tehtävänä on parantaa ja kasvattaa organisaation tietoturvallisuutta sekä taata liiketoiminnan jatkuvuus arvioimalla ja mittaamalla jatkuvasti riskejä sekä suorituskykyä. Hallintajärjestelmä koostuu monista eri tietoturvaan liittyvistä prosessien sekä politiikkojen kokoelmista, joista prosesseihin kuuluvan riskien hallinta- ja arviointiprosessin avulla organisaation oleellisimmat tietoturvaelementit; luottamuksellisuus, eheys, käytettävyys sekä saatavuus kyetään suojaamaan ja näin myös riskeihin voidaan varautua.

1.1 Tavoitteet ja rajaukset

Tämän työn tarkoituksena on esitellä teoriaosuus listaten keskeisimmät hallintajärjestelmän osat, jotka ovat havaittu tutkituista materiaaleista sekä esittää tiivistetysti kaksi kattavaa hallintajärjestelmämallia, joita voidaan käyttää referenssinä organisaation hallintajärjestelmän implementoinnissa. Teorialuvussa esitellään myös tulevan tietosuoja-asetuksen tuomia muutoksia ja sitä, mitä kaikkea tulee ottaa huomioon hallintajärjestelmää tehtäessä. Näitä muutoksia käsitellään konkreettisen yrityscasen ympärillä, ja siksi tarkastelussa on kontekstina mukana mm. energia-alan toimijat, joista lukuisat kuuluvat esimerkkiorganisaation sidosryhmiin. Teorialuvun lisäksi työhön on implementoitu käytännön osuus, jossa esitellään, kuinka esimerkkiorganisaatiolle toteutettiin ja jalkautettiin tietoturvallisuuden hallintajärjestelmä. Lopuksi tavoitteena on kertoa, mitä muut organisaatiot voivat tämän työn esimerkkiorganisaation tietoturvallisuuden

hallintajärjestelmän implementoinnista oppia. Eri hallintajärjestelmien kattavampi vertailu ei kuulu tämän diplomityön piiriin, vaan työ rajautuu esimerkkiorganisaatiolle tehdyn hallintajärjestelmän osien esittelyyn ja tämän toteutukseen.

1.2 Työn rakenne

Luvussa kaksi esitellään teoriaosuus, jossa ensimmäisenä kerrotaan tietoturvallisuuden sekä tietosuojan merkityksestä organisaatioissa sekä esitetään tiivistetysti kaksi julkista tietoturvan hallintajärjestelmämallia. Tämän jälkeen luvussa esitellään uuden tietosuoja-asetuksen (GDPR Portal, 2018) todennäköisistä muutoksista energiayhtiöiden toimenpiteissä, kuten millä ehdoilla henkilötietoja voidaan luovuttaa alihankkijoille sekä miten henkilötietojen syntyperäinen käyttötarkoitus voi rajoittaa tietojenkäsittelyä. Viimeisessä aliluvussa käsitellään tietoturvallisuuden hallintajärjestelmän olennaisimmat hallintaosat tarkemmalla tasolla. Kolmannessa luvussa kerrotaan, kuinka tietoturvallisuuden hallintajärjestelmä implementoitiin esimerkkiorganisaatiolle, joka edustaa tietotekniikan alaa.

Neljännessä luvussa analysoidaan sitä, kuinka hallintajärjestelmän implementointi esimerkkiorganisaatioon onnistui julkisiin tietoturvallisuuden hallintajärjestelmiin verrattuna sekä mitä kaikkea organisaatioiden olisi hyvä ottaa huomioon, jotta projekteista ei syntyisi mittavan pituisia sekä hallintajärjestelmän jalkauttaminen olisi mahdollisimman selkeää käyttöönotettaessa tietoturvallisuuden hallintajärjestelmää. Tällaisia ovat esimerkiksi erinäiset haasteet sekä hallintajärjestelmän valintaperusteet. Lisäksi luvussa pohditaan, mitä asioita toisin tekemällä hallintajärjestelmän jalkauttaminen olisi mahdollista onnistua ongelmitta. Viidennessä luvussa esitellään yhteenveto työstä.

2 TEORIAOSUUS

Teorialuku on laadittu kuvailevana teoriakatsauksena tutustumalla kyseisen aihepiirin tieteellisiin tutkimuksiin, valittujen aihepiirien kirjallisuuden teoksiin sekä muihin aihepiirien ajankohtaisiin julkaisutoimintoihin kuten eri standardeihin. Artikkeleita on haettu seuraavaksi lueteltujen hakusanojen avulla: tietoturvallisuuden hallintajärjestelmät, VAHTI-ohje, ISO/IEC 27001, EU:n tietosuoja-asetus, tietoturva sekä tietosuoja. Tutkimusten lisäksi tietoa on haettu kirjallisista teoksista sekä aiheisiin liittyvistä standardeista, jotka on haettu SFS-standardit -tietokannasta. Teorialuvun tarkoituksena on keskittyä tietosuoja-asetuksen tuomiin todennäköisiin muutoksiin sekä tietoturvallisuuden hallintajärjestelmän merkittävimpiin hallintaosiin konkreettisen yrityscasen ympärillä. Kokonaisuuden hahmottamiseksi luvussa tutustutaan aluksi tietoturvallisuuden merkitykseen organisaatioissa, esitetään tietoturvallisuuden ja tietosuojan erot sekä esitellään tiivistetysti kaksi hallintajärjestelmää, joita organisaatiot voivat käyttää implementoidessaan tietoturvallisuuden hallintajärjestelmää.

2.1 Tietoturvallisuus organisaatioissa

2.1.1 Tietoturvan hallinta

Nykytilanteessa tiedot ja tietojärjestelmät ovat jatkuvasti uhattuina ja organisaatioiden toiminnan varmistaminen edellyttää hyvää tietoturvapoikkeamiin ennaltavarautumista. Organisaatioiden toiminnassa tietoturvallisuuden hyvä taso ehkäisee tietoturvapoikkeamien toteutumista, vähentää poikkeamissa syntyviä vaurioita sekä edesauttaa niistä toipumista. Organisaation ylin johto on vastuussa tietoturvapoikkeamiin varautumisesta ja tietoturvastyön riittävästä resursoinnista. Vastuu on riippumatonta siitä, onko joitakin organisaation toimintoja ulkoistettu vai ei. (Valtiovarainministeriö 2009)

Tietoturvallisuus on kiinteä sekä keskeinen osa liiketoimintaa, ja liiketoiminta on lähes jokaisella organisaatiolla sidoksissa tietojärjestelmiin. Organisaation tehokkuus, toimivuus ja kehityskyky ovat merkittävästi riippuvaisia tietojärjestelmistä sekä niiden tietoturvallisuudesta. Tietoturvallisuus on osallisena koko organisaatiossa, eikä pelkästään tietotekniikan vastuullisessa osastossa. Tietoturvatason määrittely ei pelkästään synny teknisillä ja fyysisillä tietoturvaratkaisuilla vaan tietoturvallisen toimintaympäristön

rakentamisessa keskeisessä roolissa ovat ihmiset sekä heidän toimintatapansa. (Laaksonen ym., 2006, s. 19)

Yrityksen toiminta edellyttää ajan tasalla olevaa tietoa, joka tulisi olla työssään tarvitsevien henkilöiden sekä tahojen saatavilla. Saatavilla olevan tiedon tulee olla myös oikeaa ja luotettavaa. Organisaatiot ovat alkaneet käyttämään erilaisia tietoturvallisuuden organisoimiseen liittyviä hallintajärjestelmiä tai standardeja, jotta heidän toimintansa kannalta oleelliset tiedot vastaisivat liiketoiminnan vaatimuksia. Nämä vaatimukset usein linkittyvät myös organisaatioiden sidosryhmiin, joita ovat esimerkiksi alihankkijat. Organisaatioiden liiketoimintaympäristöjen jatkuvien muutosten myötä tietoturvavaatimuksia on mahdollista tulla organisaatioille monilta tahoilta. Näin ollen liiketoimintaympäristöjen seuraaminen on hyödyllistä tietoturvallisuuden kannalta. (Laaksonen ym., 2006, ss. 19-20)

Tietoturvallisuuden tavoitetason saavuttaminen on yleensä monivuotinen kehityshanke, jonka tavoitteet kuvataan talous- ja toimintasuunnitelmissa ja jaetaan useammalle vuodelle. Lisäksi hanke ositetaan niin, että vuositasolla kehitystoiminnalle voidaan asettaa mitattavat tavoitteet sekä osoittaa tarvittavat resurssit tavoitteiden saavuttamiseksi. (Valtiovarainministeriö 2007, ss. 42-43)

2.1.2 ISO 27k Standardiperhe

Lainsäädännöllinen kehys määrittelee ne oikeudet ja velvollisuudet, jotka tulee huomioida suunniteltaessa tietoturvallisuuden hallintajärjestelmää. Kyseinen malli toimii lähtökohtana koko organisaation tietoturvallisuuden suunnittelussa sekä toteutuksessa. Lainsäädännöllisen viitekehyksen käsittelyn jälkeen keskitytään yleensä tietoturvallisuuden hallinnan organisointiin, koska teknisillä ratkaisuilla ei päästä haluttuun lopputulemaan ilman, että hallinnollinen tietoturvallisuus on kunnossa. Siksi tietoturvallisuudenhallinnan suunnittelun apuna on hyvä käyttää erilaisia standardeja sekä toimintamalleja niihin liittyen. (Laaksonen ym., 2006, s. 83)

Organisaatiolla on mahdollista sitoutua käyttämään tietoturvan kehittämisessä tietoturvastandardien kuvaamia prosessimalleja, joista tunnetuin on ISO/IEC 27000 -

standardiperhe. ISO/IEC 27000 tarjoaa suosituksia tietoturvallisuuden hallintaan, riskeihin ja kontrollointiin.

Hallintajärjestelmän kehittämiseen luotu tietoturvastandardi ISO/IEC 27001 määrittelee tietoturvallisuuden hallintajärjestelmän vaatimukset ja näin ollen toimii tietoturvallisuuden yhtenä hallintajärjestelmän perustana (Laaksonen ym., 2006, s. 89). Standardi käsittää tietoturvallisuuden hallintajärjestelmän perustamisen, käyttöönoton, käyttämisen, ylläpidon, valvonnan, katselmusten sekä kehittämisen perusteet. Standardissa korostetaan hallintajärjestelmän kiinteää yhteyttä organisaation käytännön toimintamalleihin ja laatujärjestelmiin. (Hakala ym., 2006, s. 49) Hakalan mukaan varsinaisia toimintoja ohjaa standardissa seuraavat pykälät (Hakala ym., 2006, ss. 49-50):

1. Turvallisuuden hallintajärjestelmän (ISMS) perustaminen, käyttöönotto ja käyttö, valvonta ja katselmukset, ylläpito ja kehittäminen, dokumentointi ja dokumenttien hallinta.
2. Johdon vastuut (Management responsibility): Johdon sitoutuminen, tarvittavien resurssien varmistaminen, lainsäädännön ja sopimusten vaikutusten arviointi, katselmusten järjestäminen ja sen tuloksiin reagointi, turvallisuustietoisuuden edistäminen sekä koulutuksen järjestäminen ja sen tulosten kirjaaminen.
3. Sisäisen tietoturvallisuuden hallintajärjestelmän auditointi (Internal ISMS audits).
4. Johdon suorittama hallintajärjestelmän katselmus (Management review of the ISMS): Katselmuksen edellyttämät lähtötiedot ja sen tuloksena syntyvät tiedot.
5. Tietoturvallisuuden hallintajärjestelmän kehittäminen (ISMS improvement): jatkuva kehittäminen, korjaavat toimenpiteet sekä ehkäisevät toimenpiteet.

Tämä standardi kuvasi vielä versiossa 2005 hallintajärjestelmän kehittämistoimintaa PDCA -prosessimallin avulla. PDCA -prosessimalli sisälsi erilaisia tehtäviä, jotka jaettiin neljään osaan:

- suunnittelun ja rakentamisen vaiheessa (Plan) prosessi käynnistetään, tehdään liiketoimintavaikutus- ja riskianalyysit sekä muodostetaan näiden pohjalta jatkuvuusstrategia
- toimeenpanon ja noudattamisen vaiheessa (Do) suunnitellut ratkaisut toteutetaan ja aloitetaan koulutus

- seurannan ja arvioinnin vaiheessa (Check) prosessin tilasta tuotetaan tietoa valvonnan, testauksen, katselmointien ja auditointien sekä raportoinnin avulla
- ylläpidon ja kehittämisen vaiheessa (Act) ratkaisuja parannetaan kerättyjen tietojen perusteella

Suomen Standardoimisliiton SFS:n tekemän esityksen mukaan PDCA-malli on kuitenkin poistettu nykyisestä versiosta (2013), mutta kuitenkin tehokkaat hallintajärjestelmät perustuvat vielä PDCA-malliin, jotta saavutettaisiin toivottuja tuloksia. (Suomen Standardoimisliitto SFS ry, 2015)

2.1.3 VAHTI-sovelluskehityksen tietoturvaohje

Valtiovarainministeriö ohjaa ja yhteensovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin. (Valtiovarainministeriö, 2000)

VAHTI:n tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tieto- ja kyberturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. VAHTI-ohjeistusta käytetään sovellettuna hallinnon lisäksi tietoturvallisuuden hallintajärjestelminä esimerkiksi yrityksissä, kansainvälisessä tietoturva- ja yhteistyössä sekä kunnissa (Valtiovarainministeriö, 2000).

VAHTI-ohjeistuksessa lisäksi keskitytään merkittävänä asiana tietoturvallisen sovelluskehityksen osa-alueisiin, joihin kuuluu:

- Strategia ja resursointi
- Politiikat
- Osaaminen ja koulutus
- Tekninen sovelluskehitysympäristö
- Jatkuvuuden hallinta

Nämä vaatimukset ovat jaettu kolmeen eri tietoturvatasoon, joiden mukaan esimerkiksi yritykset voivat toimia tietoturvallisesti sovelluskehityksissään:

- Perustaso,
- Korotettu taso sekä
- Korkea taso

Auditointinäkökulmasta organisaatiot saavat itse päättää, mitä kriteeristöä tullaan käyttämään heidän tietoturva-auditoinnissa. (Valtiovarainministeriö, 2013, s. 31)

2.2 Tietosuoja ja -lainsäädäntö

Tietosuoja on vakiintunut käytetyksi ilmaisuksi puhuttaessa henkilötietojen suojan oikeudellisesta sääntelystä. Tietosuojalla tarkoitetaan ihmisen yksityisyyden suojaa sekä muita sitä koskevia turvaavia oikeuksia joita ovat esimerkiksi tietojen valtuudettoman saannin estäminen sekä luottamuksellisuuden ylläpitäminen. Tietosuojan ideana on suunnata rekisterinpitäjiä hyviin henkilötietojen käsittelykäytäntöihin sekä varmistaa tiedon kohteen etujen, oikeuksien ja yksityiselämän turvaaminen (Ylipartanen, 2010, s. 18).

Tietosuoja on perusoikeus, jonka eri yksityiskohdista voidaan säätää lain tasolla. Kyseiseen lakiin lukeutuu mukaan henkilötietojen suojaan liittyviä rajoituksia, jotka osoittavat ne rajat, joissa rekisterinpitäjällä on oikeus käsitellä esimerkiksi arkaluonteisia tietoja. Andreassonin et al. mielestä filosofisemmin ajateltuna tietosuojaa voidaan katsoa suurimmassa määrin ihmisen ”tiedollisen kotirauhan” kunnioittamisena. (Andreasson ym., 2013, s. 14)

Tämä käsite ei siis tarkoita samaa asiaa kuin käsite **tietoturva**, millä tarkoitetaan toimenpiteitä, joilla rekisteröidyn etujen, oikeuksien ja yksityisyyden turvaamiseen sekä suojaamiseen pyritään (Andreasson ym., 2013, s. 14). Kyseisiä toimenpiteitä ovat tiedon laadun, luottamuksellisuuden ja eheyden säilyttäminen sekä suojaaminen teknisin keinoin. Toisin sanoen tietoturvalla tarkoitetaan käytännön toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen. (Ylipartanen, 2010, s. 18)

Tietosuojalainsäädännön ideana on luoda henkilötietoja luovuttaville henkilöille oikeuksia ja asettaa näiden henkilötietoa käsitteleville yrityksille velvollisuuksia. Tietosuojalainsäädäntö suojaa yksilöä ja hänen oikeuksiaan omiin tietoihinsa sekä yksilön henkilötietojen vahingollista käyttöä. Kyseinen lainsäädäntö ei siis suojaa itse tietoa. (Salminen, 2009, s. 15)

Informaatio- ja viestintäteknologian vauhdikkaan kehittymisen myötä tietosuojalainsäädäntö on saanut alkunsa ja tietosuojaan liittyviä kysymyksiä on ruvettu vasta ratkomaan suuremmalla kädellä viime vuosikymmeninä. Liiketoiminnan sähköistyessä liiketoiminnan raamit tulevat kehittymään sekä monipuolistumaan uusien teknologioiden käyttöönoton myötä liiketoiminnassa. Näistä syistä johtuen tietosuojalainsäädäntö on vielä nuorta verrattuna muihin lainsäädäntöihin ja vaikutus yritysten toiminnassa kasvaa sitä mukaan, mitä eri teknologioita otetaan käyttöön. (Salminen, 2009, ss. 19-20)

Yksityisyydensuoja on säädetty Suomen perustuslakiin perusoikeudeksi, jota on kunnioitettava sähköistä liiketoimintaa suunniteltaessa sekä eri tietojärjestelmien käytössä. Tämän lain mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu sekä laissa on myös maininta henkilötietojen suojasta, jota säädellään tarkemmin lailla. Toisin sanoen perustuslaki sisältää lainsäädäntötoimeksiannon, johon henkilötietolaki ja muu lainsäädäntö henkilötietojen suojaamisesta perustuu. (Salminen, 2009, s. 43)

2.2.1 Henkilötietolaki

Henkilötietolain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia käsiteltäessä henkilötietoja sekä edistämään tietojenkäsittelytapojen kehittämistä ja noudattamista. Henkilötietolakia sovelletaan yleislakina silloin, kun henkilötiedoista muodostuu tai on tarkoitus muodostua osa henkilörekisteriä esimerkiksi henkilötietojen käsittelyyn julkisen että yksityisen sosiaali- ja terveydenhuollon potilasrekistereissä. (Vanto, 2011, s. 22)

Lakia ei sovelleta henkilötietojen käsittelyyn, jos luonnollinen henkilö suorittaa näitä henkilökohtaisiin tai niihin verrattaviin yksityisiin tarkoituksiin. Tavoitteena on kuitenkin ehkäistä tietotekniikan ja uuden teknologian käyttöön kohdistuvia tietosuojariskejä sekä

ohjata ja varmistaa tietojenkäsittelytavan aikaansaamiseen. Henkilötietoja käsittelevän organisaation tulee ottaa huomioon lain velvoitteet sekä erityisesti suunnitelmallisuuden vaatimus, jos henkilötietojen käsittelyä aiotaan toteuttaa automaattisen tietojenkäsittelyn avulla. (Tietosuojavaltuutetun toimisto, 2013)

2.2.2 EU:n tietosuojauudistus

Euroopan Unionin tietosuojauudistuksella viitataan lainsäädäntöuudistukseen, johon kuuluvat yleinen tietosuoja-asetus ja direktiivi lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta. Euroopan komissio julkaisi vuonna 2012 lainsäädäntöuudistuksesta ehdotuksen, johon päästiin sopuun neljä vuotta myöhemmin vuoden 2015 lopulla. Uudet säädökset julkaistiin 4.5.2016, jonka mukaan asetus ja direktiivi astuvat käytäntöön 25.5.2018 kahden vuoden siirtymäajan jälkeen. (Valtiovarainministeriö, 2016, s. 6).

Tietosuoja-asetuksen tavoitteena on vastata teknologian nopeaan kehitykseen ja globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin päivittämällä tietosuojaan liittyvää käsittelyä. Tämän tarkoituksena on myös tukea digitalisaation kehittymistä sisämarkkina-alueilla yhdenmukaistamalla jäsenvaltioiden tietosuojaa koskevat säännökset sekä rakentamalla luottamusta. (Oikeusministeriö, 2017, s. 9)

Näiden lisäksi tietosuoja-asetuksen tavoitteena on kasvattaa henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa yksilön oikeuksia ja vapauksia. Näiden noudattamista varten on tehty asetukseen henkilötietolakia vakavammat seuraamukset henkiötietojen käsittelyn laiminlyönnistä, joihin kuuluu suuret hallinnolliset sakot sekä määräykset henkilötietojen käsittelyn korjaaviin toimenpiteisiin. (Oikeusministeriö, 2017, s. 9)

Tietosuoja-asetus koskee kaikkia sen soveltamisalaan kuuluvia henkilötietoja käsitteleviä organisaatioita niin rekisterinpitäjiä kuin henkilötietojen käsittelijöitä. Asetusta sovelletaan sekä yksityisellä että julkisella sektorilla riippumatta henkilötietojen käsittelyn laajuudesta, käsiteltävien henkiötietojen luonteesta tai käytetystä teknologiasta. Lisäksi asetusta

sovelletaan henkilötietojen automaattiseen sekä manuaaliseen käsittelyyn, kun henkilötiedot muodostavat rekisterin osan. (Oikeusministeriö, 2017, s. 9)

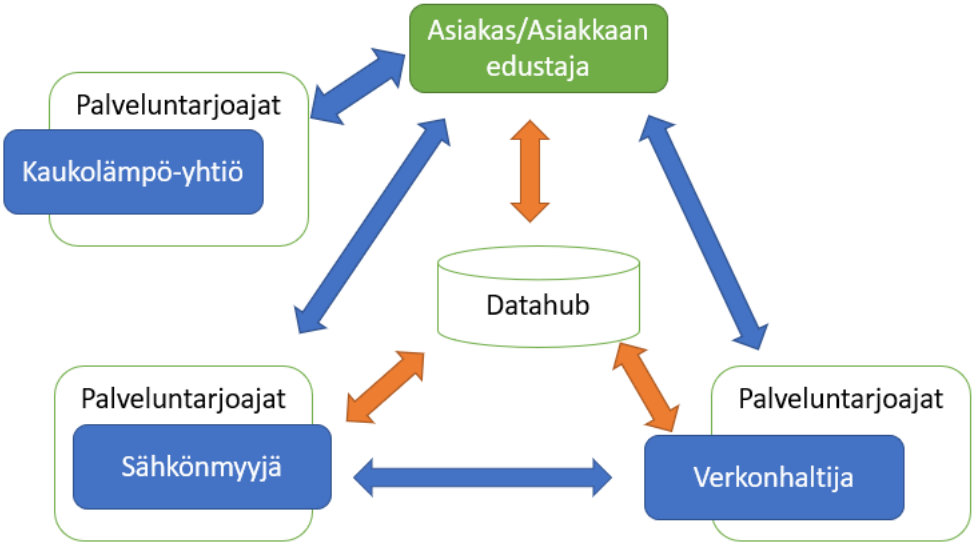
2.2.3 Tietosuojauudistuksen vaikutukset energiayhtiöihin

Uuden asetuksen astuessa tänä vuonna voimaan, on energiayhtiöiden oltava viimeistään silloin valmistautuneena asetuksen tuomiin uusiin muutoksiin nykyisissä toimenpiteissään korostaen henkilötietojen käsittelyn tapoja sekä piirteitä. Tässä luvussa kerrotaan, miten tietosuojasääntely tulee todennäköisimmin vaikuttamaan energia-alan toimijoihin sekä mitkä käytännöt voivat olla vastoin soveltuvaa tietosuojalainsäädäntöä. Syynä minkä takia tietosuoja-asetus joudutaan ottamaan huomioon myös energiayhtiöiden toiminnassa on tietointensiivisten palvelujen yleistyminen kuluttajille sekä energia-alan toimijoille, joiden avulla asiakkaista kerätään spesifisemmin ja enemmän tietoa lakisääteisiä velvoitteita, palvelujen tarjoamista sekä muita kaupallisia tarkoituksia varten (Energiateollisuus, 2016, s. 7).

Energiayhtiöt käsittelevät yleisimmin seuraavia asiakkaidensa tietoja päivittäisessä työssä:

- Yksittäiseen asiakkaaseen liittyvät tiedot kuten nimi, asiakkaan yksilöivät tiedot, hänen perhettään ja asuinpaikkaa koskevat tiedot sekä sopimussuhdetta koskevat tiedot
- Mittaustiedot, jotka koskevat henkilön tuotantoa ja kulutusta, joista esimerkkinä kotitalouksien tilastotiedot
- Käyttöpaikkaa ilmaisevat tiedot
- Yksittäistä palveluratkaisua koskevat tiedot kuten häiriötiedotejärjestelmiä koskevat tiedot
- Big data ja analytiikkaan perustuvat tiedot kuten sähkönkulutuksen analysoinnin avulla kerätyt tiedot

Tiedonvaihtoa toteutuu verkonhaltijoiden ja sähkönmyyjien sekä muiden sähkömarkkinaosapuolten välillä sähkömarkkinalain vaatimalla tavalla. Alla olevassa kuvassa (kuva 1) on esitetty, kuinka käytännössä tiedonvaihtaminen jakautuu asiakkaiden sekä energia-alan toimijoiden välillä.



Kuva 1. Asiakkaiden ja energia-alan toimijoiden välinen tiedonkulku (Energiateollisuus, 2016, s. 9)

Kaukolämpöyhtiön ja sähkönmyyjän välinen tiedonvaihto ei välttämättä ole aina automaattisesti lain osoittamaa ja sitä voivat hillitä esimerkiksi salassapitovelvoitteet sähkömarkkinalainsäädännössä. Lisäksi energiayhtiöt voivat ulkoistaa henkilötietojen käsittelyä ulkoisille palveluntarjoajille, jotka siis ovat toimeksiantosuhteessa energiayhtiöille ja ovat tämän vuoksi myös osallisena henkilötietojen käsittelyyn.

Energiateollisuuden tekemän selvityksen mukaan Tietosuoja-asetus tulee muuttamaan tai tarkentamaan alla listattuja asioita voimassaolevaan tietosuojasääntelyyn:

Keskeisiin käsitteisiin liittyvät muutokset

- *Henkilötieto*
    - Tuleva asetus tulee tarkentamaan henkilötiedon käsitettä, josta huomioonotettavana määrityksessä on se, että henkilötiedoksi voidaan luokitella myös verkko- ja muissa digitaalisissa palveluissa käytetyt käyttäjän yksilöivät tunnisteet. (Energiateollisuus, 2016, s. 14)
- *Rekisterinpitäjä*
    - Asetuksen mukaan reksiterinpitäjällä tarkoitetaan luonnollista henkilöä, joka yksin tai yhdessä muiden kanssa määrittelee henkiötietojen käsittelyn

ideat ja keinot. Tähän nojautuen energiayhtiöt luetaan rekisterinpitäjiksi, jotka vastaavat kaikkien tietosuoja-asetuksen velvoitteiden noudattamisesta. (Energiateollisuus, 2016, s. 16)

- *Arkaluonteinen henkilötieto*
    - Tietosuoja-asetuksen uuden määritelmän avulla voidaan mahdollisesti helpottaa sosiaalihuollon etuihin sekä tukitoimiin tarkoitettujen tietojen käsittelyä energiayhtiön toiminnassa, koska näiden tietoja ei luokitella arkaluonteisiksi uudessa asetuksessa, joten näiden käsittelyyn ei tarvita mitään erillistä perustetta. (Energiateollisuus, 2016, s. 21)
- *Suostumus*
    - Energiayhtiöt voivat joutua tilanteeseen, jossa henkilötietojen käsittelyä ei voida pohjata asiakassuhteesta tai lainsäädännöstä johtuvien velvoitteiden hoitamiseen. Tällainen tilanne syntyy esimerkiksi silloin, kun sähkö- ja kaukolämpöyhtiöt keräävät lakisääteisiä vaatimuksia ykityiskohtaisempia tietoja asiakkaan sähkön tai lämmön kulutuksesta (Energiateollisuus, 2016, s. 21). Tietosuoja-asetus määrittelee suostumukselle aiempaa niukemmat vaatimukset. Energiayhtiön tiedustellessa suostumusta henkilötietojen käsittelylle, on heidän noteerattava seuraavat asiat (Energiateollisuus, 2016, ss. 21-22):
        - Suostumus on annettava selkeästi yksityiskohtaistettuihin tietojenkäsittelytarkoituksiin
        - Kirjallisessa ilmoituksessa oleva suostumus, joka sisältää myös muita asioita, on suostumusta koskeva pyyntö esitettävä erillään muista asioista mahdollisimman selkeästi sekä saatavilla olevassa muodossa yksinkertaisesti kerrottuna. Suostumusta ei saa käytännössä kytkeä pelkästään osaksi sopimusehtoja.
        - Asetuksen vastaisesti pyydetty sopimus ei ole sitova.
        - Rekisteröidyllä on oikeus peruuttaa suostumus milloin tahansa. Lisäksi suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen sekä tästä asiasta on vastaanottajalle ilmoitettava.
        - Jos suostumus on palvelun tarjoamisen edellytyksenä, on kerättävien tietojen oltava tarpeellisia kyseistä palvelua varten. Jos tämän ohessa

tietoja kerätään muihin tarkoituksiin, on näihin tehtävä erillinen suostumus.

- *Informointi*
    - Tietosuoja-asetus tulee laajentamaan rekisterinpitäjän ilmoitusvelvoitteita sekä se vaatii rekisterinpitäjää luovuttamaan rekisteröidylle rekisteriselosteen sisältövaatimuksia yksityiskohtaisemmat tiedot. Tämä tulee käytännössä edellyttämään energiayhtiöitä päivittämään sekä arvioimaan rekisteri- ja tietosuojaselosteensa tulevan asetuksen mukaisiksi. (Energiateollisuus, 2016, s. 26)
- *Viranomaiset ja viranomaisvelvoitteet*
    - Tietosuoja-asetus tulee antamaan valvontaviranomaisille uusia toimivaltuuksia sekä mahdollistamaan esimerkiksi lupien antamisen ja hallinnollisten sanktioiden langettamisen. Energiayhtiöiden tulee huomioida tulevan asetuksen vaikutukset Suomen lainsäädäntöön, jotka tullaan tekemään erikseen oikeusministeriön puolesta sekä sen, että muiden valtioiden näkemykset ja käytännöt voivat vaikuttaa tietosuoja-asetuksen tulkintaan Suomessa. Lisäksi ellei kansallisesti toisin säädetä, tietosuoja-asetus tulee lakkauttamaan nykyisen ilmoitusvelvollisuuden tietosuojavaltuutetulle, jonka tarkoituksena on kertoa, kuinka rekisterinpitäjän tietojenkäsittely toimii. (Energiateollisuus, 2016, s. 29)

Henkilötietojen käsittelyn perusteisiin liittyvät muutokset

- *Mitä arkaluonteisia tietoja voidaan käsitellä*
    - Jatkossa yhtiöt voivat myös käsitellä tietoja sosiaalihuollon tarpeesta, koska sitä ei enää katsota arkaluonteiseksi tiedoksi (Energiateollisuus, 2016, s. 42).
- *Millä ehdoilla tietoja voidaan luovuttaa alihankkijoille tai muille palveluntarjoajille*
    - Tietosuoja-asetus toimeenpanee tiukemmat määräykset alihankkijan käytölle henkilötietojen käsittelyssä. Näin ollen henkilötietojen käsittelijä ei saa esimerkiksi käyttää toisen henkilötietojen käsittelijän palveluita ilman rekisterinpitäjän kirjallista lupaa. Tästä syystä yhtiöiden on varmistettava,

että sen henkilötietojen käsittelyn ulkoistamisesta tekemät sopimukset ja alihankkijoita koskevat käytännöt vastaavat tietosuoja-asetuksen määräyksiä. (Energiateollisuus, 2016, s. 51)

- *DataHUB:in vaikutus asiakaskohtaiseen tiedon käsittelyyn*
    - DataHUB on sähkömarkkinoille suunnitteilla oleva keskitetyn tiedonvaihdon ratkaisu, jonka tarkoituksena on helpottaa tiedonvaihdon laatua, yhtenäistää toimintatapoja, optimoida resurssien käyttöä sekä selkeyttää myyjäyhtiön ja verkonhaltijan rooleja. DataHUB:iin tullaan käytännössä siirtämään jakeluverkko- ja myyntiyhtiöiden lähdejärjestelmien tiedot. Tämä ei tule kuitenkaan muuttamaan energiayhtiöiden vastuuta rekisterinpitäjän roolista, vaikka he luovuttaisivatkin tietoja DataHUB:iin. Itse sääntely sekä siihen perustuva henkilötietojen käsittely tullaan vielä arvioimaan tarkemmin tietosuoja-asetuksen näkökulmasta, kunhan DataHUB:iin liittyvä sääntely etenee. (Energiateollisuus, 2016, s. 52)
- *Miten henkilötietojen alkuperäinen käyttötarkoitus voi rajoittaa tietojenkäsittelyä*
    - Jos henkilötietojen käyttötarkoitus muuttuu alkuperäisestä johonkin muuhun käyttötarkoitukseen, on rekisterinpitäjän selvitettävä uuden ja vanhan käsittelyn tarkoituksen sekä asiayhteyden väliset komplikaatiot, henkilötietojen arkaluonteisuuden muuttuminen, mahdolliset seuraukset reksiteröidylle sekä hyväksyttävien suojaustoimien olemassaolo (Energiateollisuus, 2016, s. 54).

Rekisterinpitäjän velvollisuuksiin liittyvät muutokset

- *Mitä vastuita ja velvoitteita tietojen keräämisestä ja rekisterin ylläpitämisestä aiheutuu*
    - Yhtiöiden on osattava tulkita tietosuoja-asetuksen näkökulmasta se, kuinka ne käsittelevät asiakastietoja ja näin arvioitava erilaisten velvoitteiden sekä vaatimusten noudattaminen. Näihin vaatimuksiin sekä velvoitteisiin lukeutuvat riski- ja ilmoitusperusteiset velvoitteet sekä sisäänrakennetun ja oletusarvoisen tietosuojan vaatimus. Riskiperusteisiin velvoitteisiin liittyy henkilötietojen käsittelyn vaikutustenarviointi, jossa tulee huomioida tietosuoja-asetuksen vaatimukset suunniteltaessa tietojenkäsittelyä tai

esimerkiksi hankittaessa uusia tietojärjestelmiä. Toisena velvoitteena on tietosuojavastaavan nimittäminen organisaatioon edellyttäen sen, että tietosuojavastaavaan pystytään ottamaan vaivattomasti yhteyttä toimipaikasta riippumatta. Sisäänrakennetun ja oletusarvoisen tietosuojan vaatimuksessa rekisterinpitäjän tulee noudattaa sitä, että he toteuttavat asetusten mukaan tietosuojaperiaattensa sekä toteutettavat tekniset ja organisatoriset toimenpiteet on suunniteltu ainoastaan tarpeellisten henkilötietojen näkökulmasta. Näiden lisäksi tietosuoja-asetus suosittelee laatimaan sisäisen ohjeistuksen tietoturvaloukkausten ilmoittamisesta. (Energiateollisuus, 2016, ss. 55-57)

Tietojen säilyksiin liittyvät muutokset

- *Määritys henkilötietojen säilytysrajoille sekä milloin tiedot tulee poistaa*
    - Tietosuoja-asetus vaatii yhtiöitä määrittämään käsittelemilleen henkilötiedoille säilytysrajat tai vähintään kriteerit säilytysten toteutumiselle eikä minkäänlaisia minimiaikarajoja säilytyksille säädetä laissa. Säilytysajan jälkeen henkilötiedot tulee poistaa viimeistään silloin, kun niitä ei käytetä enään mihinkään tarkoitukseen. (Energiateollisuus, 2016, ss. 64-65)
- *Mitkä ovat yhtiön velvollisuudet poistaa tiedot asiakkaan vaatimuksesta*
    - Yhtiön ei tarvitse poistaa asiakkaansa henkilötietoja tämän pyydettäessä niitä, mutta jos tiedot eivät ole enään olennaisia niin tiedot pitää tällöin poistaa rekisteröidyn näin pyydettäessään (Energiateollisuus, 2016, s. 66).

Asiakkaan oikeuksiin liittyvät muutokset

- *Mihin tietoihin asiakkaan tarkastusoikeus ulottuu*
    - Asiakkaan tarkastusoikeus ulottuu oletuksena kaikkiin tietoihin, joita rekisteröidystä käytetään organisaatiossa (Energiateollisuus, 2016, s. 67).
- *Missä laajuudessa tiedot on toimitettava asiakkaalle*
    - Yhtiöiden on toimitettava jäljennös kaikista rekisteröidyn henkilötiedoista heidän näin pyydettäessä. Kustannuksia näistä voidaan periä ainoastaan silloin, jos rekisteröity pyytää useamman kuin yhden jäljennöksen

tiedoistaan. Yleisesti ottaen tiedot tulee lähettää sähköisessä muodossa ellei rekisteröity toisin pyydä. (Energiateollisuus, 2016, s. 69)

Seuraamuksiin liittyvät muutokset

- Asetus on syventänyt rekisterinpitäjien vastuuta vahingoista, joista tärkeimpänä uudistuksena ovat hallinnolliset sanktiot, joiden mukaan sanktioiden määrä on riippuvainen yrityksen koosta eli sanktiot voivat olla korkeimmillaan 4 % vuotuisesta kokonaisliikevaihdosta. Näin pyritään varmistua siitä, että yhtiöt noudattavat tietosuoja-asetusten velvoitteita. (Energiateollisuus, 2016, s. 77)

2.3 Tietoturvallisuuden hallintajärjestelmä

Tietototurvan hallintajärjestelmä on systemaattinen lähestymistapa, -menetelmä ja prosessi, jolla hallitaan organisaation tietoturvaa ja suojataan niitä tietoja, joiden on katsottu tarvitsevan suojausta (Tammisalo 2007, s. 10). Hallintajärjestelmä kattaa yksityiskohtaisen organisoinnin, politiikat, suunnittelun, vastuut, menettelytavat, prosessit ja tarvittavat resurssit. Hallintajärjestelmä koostuu erilaisista toimintamalleista ja dokumenteista, joihin sisältyvät VAHTI-ohjeen mukaan:

- Tietoturvapolitiikka ja -strategia
- Tietoturvakäytännöt
- Tietoturvallisuuden kehittämissuunnitelma
- Tietoturvallisuuden ohjeistus
- Tietoturvaraportointi johdolle
- Pelastus-, jatkuvuus- ja valmiussuunnitelmat
- Toimintaan liittyvät tietoturvaprosessit
- Auditointisuunnitelma

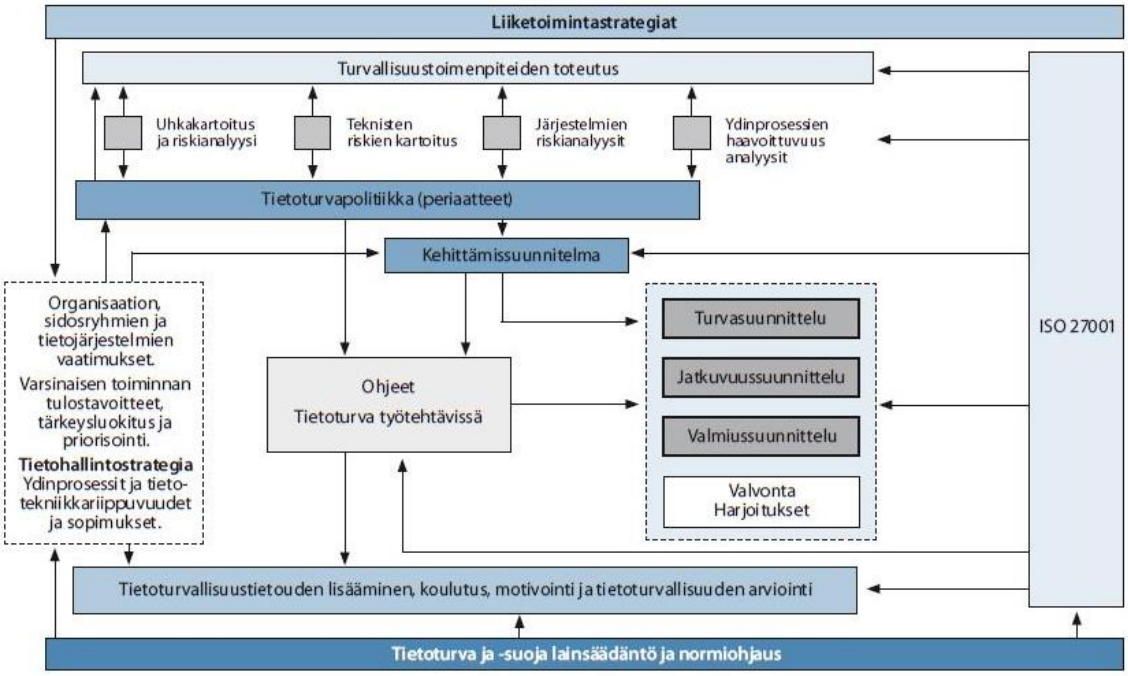
Susanto et al. puolestaan tulkitsevat tietoturvallisuuden hallintajärjestelmän koostuvan 11:sta eri hallinta-alueesta, jotka täyttävät vaatimuksen tietoturvallisuuden hallintajärjestelmänä kattaa koko organisaation toiminta perusteellisesti (Susanto et al, 2011):

1. **Tietoturvapolitiikka.** Hallintajärjestelmästä on löydyttävä vaatimus kirjallisen tietoturvapolitiikan olemassaololle ja sisällölle.

2. **Viestinnän ja operatiivinen johtaminen.** Hallintajärjestelmästä on löydyttävä se, miten tietojenhallintaympäristön operatiivinen johtaminen sekä myöskin johtamiseen liittyvä viestintä tulee toteuttaa.
3. **Pääsynhallinta.** Hallintajärjestelmästä on löydyttävä vaatimus kohteena olevan järjestelmän tai toiminnon autentikointi- ja käyttöoikeusjärjestelyille.
4. **Tietojärjestelmien hankinta, kehitys ja ylläpito.** Hallintajärjestelmästä on löydyttävä prosessikuvaus, joka määrittelee tietojärjestelmien täydellisen elinkaarehallinnan jossa on huomioitu sekä ulkoiset hankinnat, kehitys ja ylläpito.
5. **Tietoturvallisuuden organisointi.** Hallintajärjestelmässä edellytetään johdon sitoutuneisuutta tietoturvallisuuteen, tietoturvallisuuden koordinointikäytäntöjen toimeenpanoa sekä pääsynhallintaa tietojärjestelmän fyysiseen käyttöympäristöön.
6. **Omaisuudenhallinta.** Hallintajärjestelmässä edellytetään käytäntöjä tärkeimmän tuotanto-omaisuuden (mm. palvelimet sekä tuotantolaitteet) tunnistamiseksi, luokittelemiseksi ja omistajuusmäärittelyiksi.
7. **Tietoturvapoikkeamien hallinta.** Hallintajärjestemästä on löydyttävä käytännöt tietoturvallisuuden laatupoikkeamien havaisemiseksi ja käsittelemiseksi.
8. **Liiketoiminnan jatkuvuuden hallinta.** Hallintajärjestelmästä on löydyttävä käytännöt liiketoiminnan jatkuvuudesta huolehtimiseksi poikkeustilanteissa.
9. **Henkilöstöturvallisuus.** Hallintajärjestelmästä on löydyttävä käytännöt henkilöstön osaamisen varmistamiseksi, pääsyoikeuksien hallitsemiseksi sekä käyttäjäroolien määrittemiseksi.
10. **Fyysinen ja ympäristön turvallisuus.** Hallintajärjestelmästä on löydyttävä käytännöt järjestelmien, rakennusten ja niitä ympäröivän teknisen pohjan fyysiseksi suojelemiseksi vahingoilta ja vahingonteolta.
11. **Vaatimustenmukaisuus.** Hallintajärjestelmän on mukauduttava uusiin lakeihin, asetuksiin sekä muihin viranomaisten asettamiin vaatimuksiin.

Koska hallintajärjestelmä on luonteeltaan kuitenkin viitekehys, voivat organisaatiot toteuttaa haluamallaan tavalla hallintajärjestelmää heidän tarpeiden mukaisiksi. (Valtiovarainministeriö, 2007, s. 40)

Tietoturvallisuuden hallintajärjestelmän olennaisimmat osat ovat **ajantasainen tietoturvapolitiikka** ja siihen liittyvät asiakirjat sekä **säännöllinen riskienhallinta**, joka koskee sekä nykyistä toimintaa että suunniteltuja muutoksia. Niiden pohjalta tulee laatia **tietoturvastrategia ja suunnitelmat**, joiden avulla **tietoturvakäytännöt** toteutetaan tietoturvavaatimusten mukaisesti. Hallintajärjestelmä sisältää myös tietoturvatoiminnan tehokkuuden ja tarkoituksenmukaisuuden säännöllisen mittaamisen ja arvioinnin eli **auditoinnin**. Kuvassa 2 on esitetty perusmalli hallintajärjestelmästä. (Valtiovarainministeriö, 2007, s. 42)



Kuva 2. Tietoturvallisuuden hallintajärjestelmän malli. (Valtiovarainministeriö, 2007, s. 41)

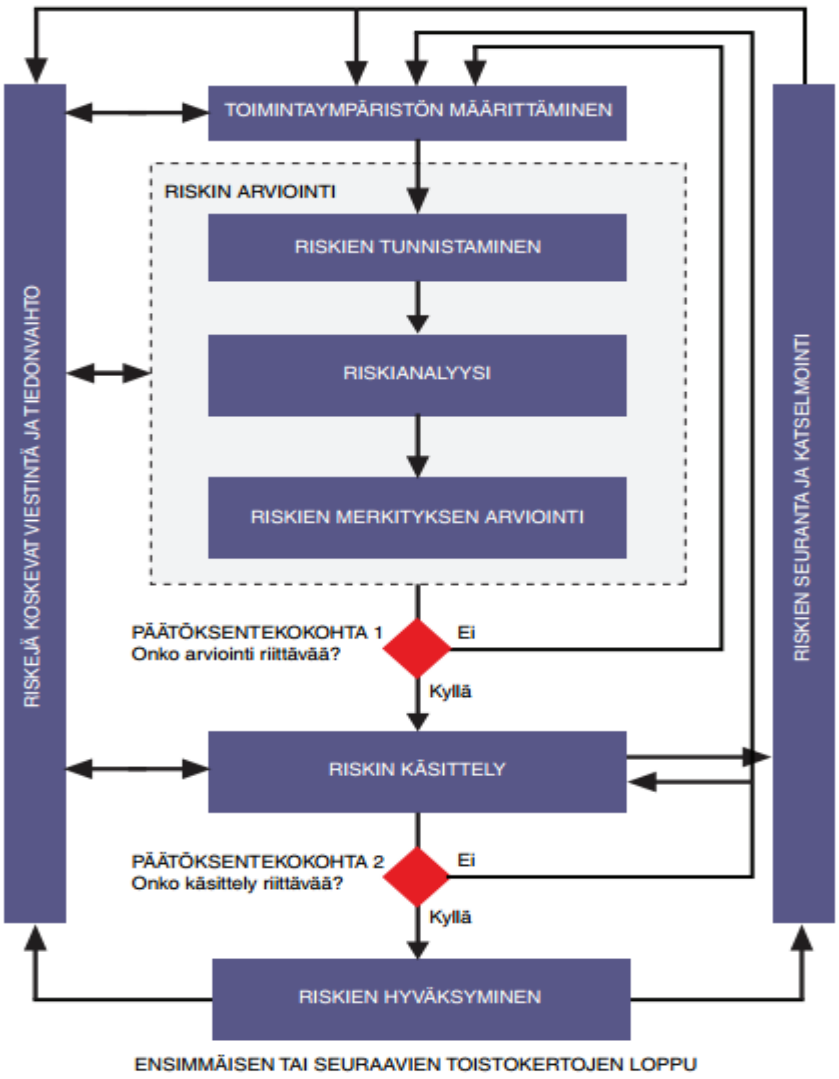
2.3.1 Riskienhallintaprosessi

Organisaation tietoturvan hallintajärjestelmän luomiseen liittyvien tarpeiden tunnistamiseen edellytetään järjestelmällistä tietoturvariskienhallintaa. Tämän täytyy olla olennainen osa tietoturvallisuuden hallintatoimintoja, ja sitä tulisi osata soveltaa tietoturvan hallintajärjestelmän käyttöönotossa sekä sen jatkuvassa prosessissa. Riskienhallinnassa analysoidaan, mitä voi tapahtua sekä minkälaisia seurauksia näihin voi kohdistua ennen kuin on päätetty, kuinka näitä riskejä tultaisiin ehkäisemään. Riskienhallintaa voidaan soveltaa organisaation eri osa-alueisiin kuten esimerkiksi yhteen palveluun, johonkin

tietojärjestelmään tai erityisiin valvonnan osa-alueisiin kuten toiminnan jatkuvuussuunnitteluun. (Suomen standardoimisliitto SFS ry, 2013, ss. 18-20)

Standardi ISO/IEC 27001 määrittelee, että tietoturvallisuuden hallintajärjestelmän puitteissa toteutettujen hallintakeinojen tulee perustua riskien arviointiin. Näin ollen kyseinen vaatimus voidaan täyttää organisaatioissa siten, että organisaatio valitsee itselleen toimintamallin, kuinka riskienhallintaprosessia ryhdytään toteuttamaan ja joka myös parhaiten sopisi organisaation olosuhteisiin kaikissa tilanteissa, joissa tätä prosessia tullaan käyttämään. (Suomen standardoimisliitty SFS ry, 2013, s. 24) Kuvassa 3 on esitetty kansainvälisen standardin mukaan sovellettu riskienhallintaprosessimalli, jota voidaan hyödyntää organisaatioissa.

Riskienhallintaprosessi koostuu toimintaympäristön määrittämisestä, riskien arvioinnista, riskien käsittelystä, riskien hyväksymisestä, riskien seurannasta sekä katselmoinnista ja riskejä koskevasta viestinnästä sekä tiedonvaihdosta. Riskienhallintaprosessin ”kulmakivenä” pidetään riskien käsittelyä, koska tämän vaikuttavuus riippuu riskien arvioinnin tuloksista. Jos riskien arvioinnin tulokset eivät ole riittäviä, kyseinen arviointiprosessi toistetaan uudelleen niin pitkään, kunnes riskit saavuttavat hyväksytyn tason. (Suomen standardoimisliitto SFS ry, 2013, s. 24)



Kuva 3. Riskienhallinnan prosessimalli (Suomen standardoimisliitto SFS ry, 2013, s. 22)

2.3.1.1 Riskien arviointi

Ensimmäisenä tehtävänä riskienhallinnan prosessimallissa organisaation tulee määrittää toimintaympäristö, jossa tällä mallilla tullaan vaikuttamaan. Toimintaympäristön määrittämisen lopputuloksena tulisi olla määriteltynä peruskriteereistä muodostunut toimintamalli, toimintaympäristön laajuus sekä rajaukset ja riskienhallintaprosessin organisointi (Suomen standardoimisliitto SFS ry, 2013, s. 26). Tämän jälkeen arvioidaan riskit. Riskien arviointi sisältää kolme vaihetta:

- Riskien tunnistaminen
- Riskianalyysi
- Riskin merkityksen arviointi

Riskien tunnistamisen tavoitteena on määrittää asiat, joita voisi tapahtua, mikä voisi aiheuttaa tappioita sekä kerätä tietoa siitä, miten, missä ja miksi tällainen tappio voisi syntyä (Suomen standardoimisliitto SFS ry, 2013, s. 32).

Riskien analysoinnin tavoitteena on luoda perusta tietoturvapolitiikan oikeille päätöksille, ja jotta analysointia voidaan käyttää toimivasti, on määriteltävä selkeät sekä konkreettiset tavoitteet. Ilman selkeitä määrityksiä lopputulos tulee olemaan joko pinnallinen tai jopa harhaanjohtava ja näistä seuraa helposti virhearviointeja. Riskien analysointia varten on monia eri lähestymistapoja, joita ovat esimerkiksi tarkistuslistat, haavoittuvuusanalyysi sekä potentiaalisten ongelmien analyysi (POA). (Miettinen & Kajava, 1994, ss. 10-11) Lähdettäessä analysointia toteuttamaan jollain näistä edellämainituista esimerkeistä, on työryhmän kyettävä arvioimaan lähestymistavan soveltuvuus kyseiseen riskienhallintaprosessiin (Miettinen & Kajava, 1994, s. 23).

Tarkistuslistat sisältävät lyhyen kuvauksen siitä, minkälaisia mahdollisia vaaroja tiettyihin riskikartan riskeihin kohdistuu. Tarkistuslistoja on luotu yleiseen käyttöön, joita voidaan käyttää apuna organisaatioissa oman tarkistuslistan luonnissa. Lisäksi Leppänen toteaa, että valmiiden tarkistuslistojen lisäksi olisi suotavaa käyttää myös ulkopuolista asiantuntijaa tarkistuslistojen ja riskianalyysimenetelmien käytössä, koska ulkopuolinen voi havaita sellaisia asioita, jotka ovat organisaation toimintoja, eivätkä siten voi olla organisaation erityisriskien asiantuntijoita. Tarkistuslistojen sisältö tulee olla hyvistä käytännöistä koostuva tiivis kokonaisuus. Tällöin tarkistuslista toimii samalla turvallisuusohjeena sekä auttaa määrittelemään toiminnan tavoitetason. (Leppänen, 2006, s. 133)

Haavoittuvuusanalyysi on tunnetuin riskianalyysimenetelmä, jolla on samanlainen periaate kuin tarkistuslistoissa. Lähtökohtaisesti tällä tarkastellaan koko organisaation toimintaa yleisellä tasolla. Tästä siirrytään seuraavaan vaiheeseen tarkastelemaan yhä pienempiä kokonaisuuksia silloin kun toiminnassa havaitaan haavoittuvuuksia ja samalla analyysistä rakentuu selkeä hierarkkinen kokonaisuus. Leppäsen mukaan (Leppänen, 2006, ss. 134-135) organisaation toimintaa voidaan jakaa esimerkiksi seuraaviin kokonaisuuksiin:

- henkilöstö

- talous, rahoitus ja johtaminen
- tuotanto, tuotteet
- alihankinta, ostot, kuljetukset ja varastointi
- myynti, markkinointi ja asiakkaat
- kilpailijat ja suhdanteet
- investoinnit
- normit, julkinen valta ja sidosryhmät

Haavoittuvuusanalyysin tuloksena syntyy karkea kokonaiskuva organisaation tai sen osien haavoittuvuudesta. Haavoittuvuusanalyysiin kirjataan riskin pääotsikko, vahinkoesimerkki ja lisäksi siihen merkitään riskin nykytila (ei riskiä – riski hallinnassa – hoidettava kuntoon – ei koske meitä) karkealla arvinoinnilla (3x3 menetelmällä) sekä kirjataan kehittämistoimenpiteiden suunnittelu, toteutus ja seuranta.

Näiden lisäksi analyysissä voidaan kuvata tavallisimpia riskejä, riskien toteutumisen todennäköisyyttä ja seurausten vakavuutta. Arvioinnin yhteydessä tehdään yleensä yksityiskohtaisempia kuvauksia riskistä tai siihen liittyvistä muista tekijöistä. Tärkein osa haavoittuvuusanalyysissä on se, että riskit herättäisivät keskustelua ja näin ollen mahdollistaisi erilaisten näkökulmien esiin tuomisen prosessin aikana. Riskin arvioiminen voi siis johtaa parhaimmassa tapauksessa uudelleen arviointiin työskentely- ja toimintatavoista. Syntyneestä haavoittuvuusanalyysistä laaditaan vielä yhteenveto, johon kootaan alla luetellut asiat:

- riski tai ongelma
- riskin syyt
- pahimmat seuraukset
- riskin suuruus (asteikolla 1-5)
- toimenpiteet
- toteutusaikataulu ja vastuuhenkilö
- seuranta (asia hoidettu).

(Leppänen, 2006, s. 135)

Potentiaalisten ongelmien analyysin (POA) tarkoituksena on kartoittaa erilaisia onnettomuusvaaroja identointimenetelmään tarkoitetulla analysoinnilla. Menetelmänä malli on yksinkertainen, eikä kyseinen malli kohdistu tietylle sektorille vaan se kykenee toimimaan monenlaisissa ongelmien analysoimisessa. Lisäksi POA perustuu erilaisille tarkistuslistoille, joiden laajuus voi olla menetelmän heikkous että vahvuus. POA:n prosessin ensimmäisenä tehtävänä on rakentaa asiantuntiaryhmä, joka tulee työskentelemään tässä prosessissa. Ryhmän tehtävänä on toteuttaa arvioinnit sekä tehdä korjausehdotukset. Asiantuntijaryhmän on koostuttava jokaisen tarkastelukohteeseen vaikuttavista henkilöryhmistä. Jokaisella kohteella on oltava toiminnasta vastaava henkilö, perustason käyttäjä, erityisriskialueiden asiantuntija sekä johdon asiantuntija, joka tietää parhaiten, miten olemassa olevia resursseja käytetään. Lisäksi työryhmään tulee kuulua asiantuntijasihteeri, joka hankkii analysointiprosessille taustatietoja ja koordinoi prosessia. (Leppänen, 2006, s. 140)

Potentiaalisten ongelmien arvioinnin aloittaa ryhmän sihteeri, jonka tehtävän on tehdä tarkkaa taustatietoa, jotta hän on kykeneväinen valitsemaan sekä rajaamaan tarkasteltavan kohteen. Liian laajan alueen arvioiminen koituu yleensä sekavaan, epäyhtenäiseen ja pintapuoliseen tarkasteluun. Taustaselvityksen jälkeen ryhmän puheenjohtaja käy läpi järjestelmällisesti läpi kohteeseen kohdistuvat sihteerin listaamat riskit. Lopputuloksena tästä pitäisi syntyä luettelo vaaratilanteista, joissa on käsiteltynä ainoastaan suurimmat ja keskeisimmät riskit. Analysointiryhmä työskentelee ensiksi itsenäisesti käymällä listat läpi sekä listaten samalla tulevia mahdollisia ongelma- ja riskitilanteita. Jokaisella tulisi olla listattuna kolmesta viiteen eri tilannekuvausta. Tämän jälkeen listoja kierrätetään ja muut ryhmän jäsenet täydentävät tai lisäävät muiden tekemiä tilannekuvauksia. Kun listat ovat käyneet jokaisella asiantuntijalla, jokainen listojen kohta käydään yksitellen läpi ryhmässä keskustellen. Tämän vaiheen tarkoituksena on saada jokaisen ryhmänjäsenen panos näkyviin ongelmien löytämiseksi sekä ratkaisemiseksi. Tästä aivoriihistä sihteeri rakentaa yhteenvedon, johon hän tekee alustavan ongelmatilanteiden kokoamisen sekä luokittelun. Ongelmat jaetaan kolmeen luokkaan (Leppänen, 2006, s. 142):

- A) jatkokäsittelyä edellyttävät riskit, jotka tullaan siirtämään arviointivaiheeseen
- B) ”vanhat” ja luotettavasti hoidossa olevat riskit, joille on määritelty vastuuhenkilö

- C) merkityksettömät riskit, joiden hallitseminen on lähes mahdotonta

Leppäsen mukaan POA:n rajoitus on se, ettei se ole systemaattinen, koska se ei tarjoa kattavaa tai johdonmukaista menetelmää riskienarviointiin, vaan se perustuu enemmän tarkistuslistojen laatijan kykyyn muodostaa kattava ja riittävän syvä analysointimenetelmä. Lisäksi tämä ei kata riittävän hyvin organisaatioon ja tiedonkulkuun liittyviä ongelmia. (Leppänen, 2006, s. 143)

Riskien merkityksen arviointivaiheessa suoritetaan riskin taloudellisen vaikutuksen arviointi (Leppänen, 2006, s. 123). Tunnistetuista riskeistä arvioidaan, mitä vaikutuksia näillä on todellisuudessa sekä kuinka todennäköinen riski on, kun uhkatekijät ja haavoittuvuudet on otettu huomioon. Lopputulemana tulisi syntyä selkeä käsitys riskitasosta, jonka perusteella päätetään riskienhallinnan toimenpiteistä. (Hakala ym., 2006, s.108.) Tämän kokonaisuuden perusteella syntyy perusta riskienhallinnalle sekä todennäköiselle turvallisuusjohtamiselle. Lisäksi Leppäsen mukaan riskien merkityksen arivointivaiheessa on huomioitava organisaatioon vaikuttavien todennäköisten riskien seuranta, joka antaa myös perusteet riskienhallintatoimenpiteille. (Leppänen, 2006, ss. 123–124)

Kun arvioitu riski on saavuttanut hyväksytyn tason, niin seuraavaksi siirrytään riskin käsittelyyn. SFS-ISO/IEC 27005 standardin mukaan riskien käsittelyyn on neljä erilaista vaihtoehtoa: riskin muokkaaminen, riskin säilyttäminen, riskin välttäminen ja riskin jakaminen (Suomen standardoimisliitto SFS ry, 2013, s. 46). Riskin käsittelyn vaihtoehdot tulisi valita vaihtoehtojen toteuttamisesta odotettavissa olevien kustannusten, näistä vaihtoehdoista odotettavissa olevien hyötyjen sekä riskin arvioinnin tulosten perusteella. Vaihtoehdoksi valikoituu tällöin mahdollisimman alhaisin kustannuksin toimiva menetelmä, jolla pystytään samalla myös pienentämään merkittävästi riskejä. Riskin käsittelyssä on myös mahdollista yhdistellä vaihtoehtoja, esimerkiksi seurausten vähenemisestä, todennäköisyyden pienentämisestä ja jäännösriskien jakamisesta tai säilyttämisestä. Vaihtoehtojen tarkastelussa on otettava huomioon se, millainen käsitys riskistä on osapuolilla, joihin riski kohdistuu sekä se, mikä on toteutettava tapa viestiä kyseisten osapuolten kanssa. (SFS ISO/IEC 27005, 2013, s. 48).

Viimeisenä vaiheena riskienhallinnan prosessissa ovat riskien hyväksyminen sekä näitä koskeva viestintä ja tiedonvaihto. Lopputuloksena hyväksymisvaiheessa tulisi olla luettelo hyväksytyistä riskeistä sekä perustelut sellaisille riskeille, jotka eivät ole organisaation tavanomaisten riskien hyväksymiskriteerien mukaisia. Riskien hyväksymiskriteerit voivat kuitenkin olla monimuotoisempia kuin sen määrittäminen, onko jäännösriski jotakin yksittäistä kynnysarvoa suurempi vai pienempi. Riskien viestinnän ja tiedonvaihdon tavoitteena on päästä päätöksentekijöiden sekä muiden sidosryhmien kanssa päätökseen siitä, miten riskejä hallitaan. Tehokas viestintä sidosryhmien kanssa on olennaista, koska se vaikuttaa merkittävästi tehtäviin päätöksiin. Viestintä varmistaa riskienhallinnasta vastaavien tahojen ymmärryksen siitä, mihin päätökset perustuvat sekä mistä syistä tiettyjä toimenpiteitä tarvitaan. (SFS ISO/IEC 27005, 2013, s. 54)

Tässä kontekstissa puhutusta prosessimallista toimintaympäristön määrittäminen, riskien arviointi, riskienkäsittelysuunnitelman laadinta ja riskien hyväksyminen kuuluvat tietoturvan hallintajärjestelmässä suunnitelmavaiheeseen. Tietoturvan hallintajärjestelmän toteutusvaiheessa aloitetaan toteuttamaan riskienkäsittelysuunnitelman mukaiset toimenpiteet ja hallintakeinot, joita käytetään pienennettäessä riskejä halutulle tasolle. Arviointivaiheessa johtajat määrittelevät olosuhteiden muutosten perusteella, onko toteutettua riskienarviointia sekä käsittelyä tarvetta muuttaa. Viimeisenä toimintavaiheessa toteutetaan kaikki halutut toimenpiteet sekä tietoturvariskien täydentäviä vaiheita. SFS ISO/IEC 27005, 2013, s. 24)

2.3.2 Tietoturvapolitiikka

Tietoturvapolitiikka on yrityksen tietoturvan hallintajärjestelmään kuuluva dokumentaatio, jonka tehtävänä on luoda perustaa tietoturvallisuutta edistävälle toiminnalle. Tietoturvapolitiikkaa ei ainoastaan kehitetä tietoturvallisuuden vuoksi, vaan myös tukemaan yritystä liiketoiminnallisten tavoitteiden saavuttamisessa. Tietoturvapolitiikan tärkeimpänä tehtävänä on määrittää liiketoiminnan tavoitteita tukevat tietoturvallisuuden tavoitteet. (Bacik, 2008, s. 22)

Tietoturvapolitiikan ideana on siis toteuttaa johdon kanssa päätetyt linjaukset, joissa otetaan kantaa tietoturvan peruskysymyksiin eli mitä suojataan, miksi suojataan ja miten suojataan. Tietoturvapolitiikasta näin ollen ei tule yksityiskohtaista tietoturvan toteutusdokumentaatiota, vaan korkeammalla tasolla esitetty dokumentaatio. Politiikan omistajana on yrityksen ylin johto, esimerkiksi toimitusjohtaja tai hallituksen puheenjohtaja. Johdon avulla koko organisaatio kykenee toimimaan todennäköisimmin samalla tavalla, eikä esimerkiksi liiketoimintayksiköiden välillä ole työ hankaloittavia ristiriitaisuuksia. (Barman, 2002, s. 4)

Laaksosen mukaan Tietoturvapolitiikassa otetaan yleisimmin kantaa seuraaviin asioihin (Laaksonen ym., 2006, s. 147):

- Tietoturvallisuuden tavoitteisiin sekä niihin liittyviin toimintoihin
- Tietoturvallisuuden rooleihin ja vastuisiin
- Tietoturvallisuuskoulutukseen
- Tietojenkäsittelyn suojaamiseen
- Yleisiin linjauksiin
- Seurauksiin tietoturvapolitiikan laiminlyönnistä

Tietoturvallisuuden tavoitteet ilmenevät politiikassa siten, kuinka tietoturvallisuus vaikuttaa organisaation toimintaan ja miten organisaatioissa tietoturva-asioihin tulee suhtautua. **Rooleista ja vastuista** kertovat määriteltävät vastuuhenkilöt, joiden tehtävänä on vastata asetettujen tavoitteiden saavuttamisesta (Laaksonen ym., 2006, s. 147). Vastuut eivät saa olla ristiriidassa työntekijöiden päivittäisten töiden kanssa, vaan näiden tulisi tukea toinen toistaan. Lisäksi tietoturvapolitiikassa tulee määritellä organisaation linjaus, miten tietoturvallisuus otetaan huomioon sopimuksissa sekä muissa juridisissa kysymyksissä. **Tietoturvallisuuskoulutuksesta** tulee olla määriteltynä politiikassa koulutuksen vaatimukset. Koulutuksen avulla henkilöstö kykenee ymmärtämään ja sisäistämään politiikan tavoitteet ja toimenpiteet, joilla tavoitteet saavutetaan. Ilman koulutusta tietoturvallisuus jäisi todennäköisimmin toteuttamatta tai se toteutettaisiin vain teknisellä tasolla politiikan mukaisesti. **Tietojenkäsittelyn suojaamiseen** liittyen politiikassa määritellään suuntaviivat, joita suojaamisessa noudatetaan. Näitä ovat esimerkiksi päätös tietosisällön luokittelusta sekä laitteiden ja sovellusten suojaaminen

viruksilta. **Yleisiä linjauksia** määritellään politiikassa yleisimmin vain liittyen liiketoiminnan jatkuvuus- ja toipumissuunnittelun toteuttamiseen. **Tietoturvapolitiikan laiminlyönnin seurauksiin** vastataan myös politiikan sisällössä. Seurauksissa otetaan kantaa siihen, minkälaisia kurinpitotoimenpiteitä tehdään, jos joku laiminlyö tietoturvaohjeiden noudattamisen. (Laaksonen ym., 2006, s. 147)

Tietoturvapolitiikalle ei ole olemassa valmista mallia, koska organisaatioiden liiketoimintamallit eroavat toisistaan hyvinkin paljon eikä näin ollen mallit ole soveltuvaisia keskenään. Yritysten tietoturvapolitiikka tulisi syntyä edellisessä kappaleessa mainituista asioista keskustellen johdon kanssa sekä näistä laatia kirjallinen dokumentti. Tietoturvapolitiikan lähtökohtana pidetään tietoturvallisuuden tarpeiden tunnistamista, ja jotta nämä voidaan tunnistaa, on tiedettävä hyvin yrityksen liiketoimintaprosessit sekä sen tietoarkkitehtuuri. Jos organisaatio käyttäisi valmista tietoturvapolitiikkaa, johdon sitoutuneisuus ei olisi välttämättä ehdotonta eikä tämän sisältöä olisi tällöin täysin ymmärretty. Politiikka on pidettävä erittäin ymmärrettävänä sekä lyhyenä, jotta kaikki lukijat ymmärtävät lukemansa, koska politiikan on mahdollista kyettävä jakaa myös ulkopuoliselle kuten asiakkaille tai alihankkijoille. Näistä syistä politiikassa ei luetella tarkempia kuvauksia tietoturvakäytännöistä tai muista yksityiskohtaisemmista asioista. (Laaksonen ym., 2006, s. 148)

2.3.3 Tietoturvakäytännöt

Thomaksen mukaan tietoturvakäytäntöjen luominen on ydinasia verkon suojaamisessa sekä turvaamisessa. Korkealla tasolla tarkasteltaessa tietoturvakäytäntöjen tehtävänä on luoda perussäännöt hyväksyttävälle käyttäytymiselle organisaatiossa sekä verkossa. Käytännöistä syntyy ”oikeusohje”, johon kaikkea muuta verrataan. Perustehtävänä käytäntöjen tulee määritellä ne asiat, jotka ovat soveliaita erilaisia työtehtäviä tehdessä organisaatioissa. (Thomas, 2005, s. 47)

Lisäksi Thomas luettelee tietoturvakäytäntöjen käyttökelpoisuudelle olevia perusteluja, joissa tietoturvakäytäntö

- Luo menettelytapoja koskevat muutokset
- Määrittelee soveliaan käyttäytymisen

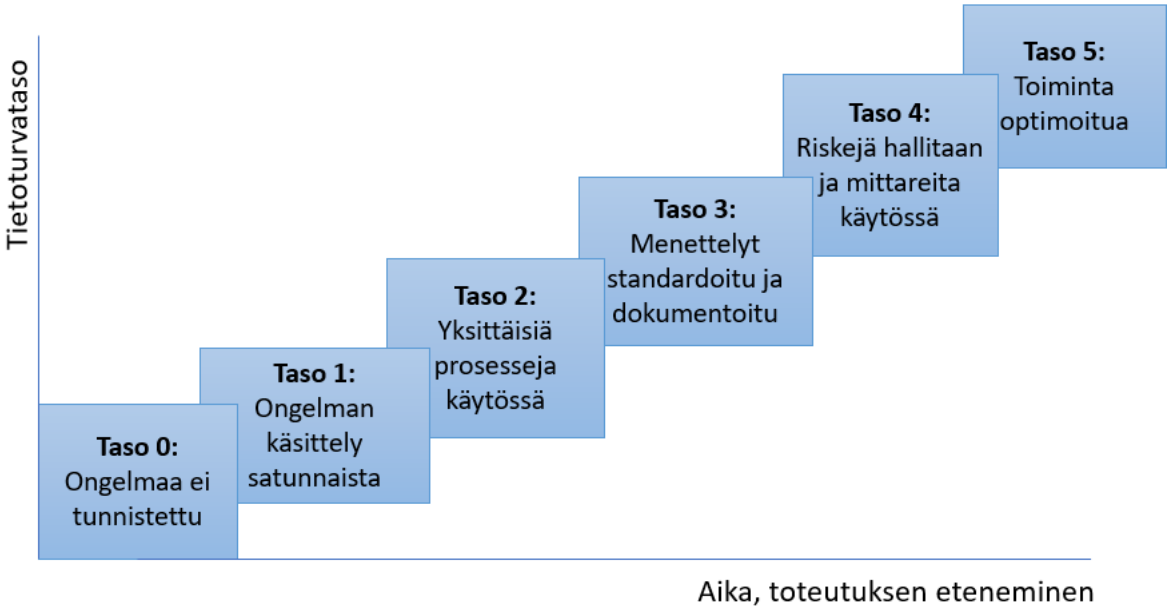
- Kuvaa toiminnalliset ja liiketoiminnalliset periaatteet
- Toimii väärinkäytöstapauksissa perustana henkilöstöhallinnon toimenpiteille
- Määrittelee eri ryhmien roolit ja vastuut turvallisuuden takaamisessa
- Toimii väärinkäyttötapauksissa tukena mahdollisille juridisille toimenpiteille
- Määrittelee verkon tietoturvassa tarvittavat käsitteet ja mallit
- Määrittelee mitä työkaluja tietoturva edellyttää ja toimii perusteena niiden hankintakustannuksille

(Thomas, 2005, ss. 47-48).

Syntyneestä tietoturvakäytännöstä käy selväksi se, mitä vastuualueita kullakin työntekijällä on organisaatiossa. Käytäntöjen tulisi määritellä organisaation jokaisen osaston käytännöt sekä prosessit, jotta esimerkiksi asiakaspalvelu tietäisi, kuinka arkaluonteisia asiakastietoja tulisi suojata. Tärkein tietoturvakäytantöjen tulos on se, mitä tämä tarkoittaa tietohallinnon kannalta. Tietohallinto esimerkiksi pystyy tämän avulla tekemään erilaiset asennukset palvelimille sekä määrittelemään virtuaalisen erillisverkon eli VPN:n asetukset tai palomuurien säännöt. (Thomas, 2005, s. 48)

2.3.4 Tietoturvan kehittämisuunnitelma

Tietoturvan kehittämissuunnitelman tarkoituksena on pyrkiä hallinnoimaan organisaation määrittelemää tietoturvaa jatkuvana toimintana (Tammisalo, 2007, s. 10). Se muodostaa tietoturvapolitiikan ja tietoturvan arvioinnin kanssa johdonmukaisen kokonaisuuden, joka ilmaisee toiminnon suunnitelmallista kehittämistyötä. Tämä ei siis tarkoita samaa kuin tietoturvasuunnitelma, vaan näiden ero on se, että kehittämissuunnitelmassa tulisi kuvata tietoturvasuunnitelmassa myöhemmin käyttöön otettavat ratkaisut (Valtiovarainministeriö, 2007, s. 46). Kehitämissuunnitelman tulisi myös toimia implementoinnin ohjaajana toimenpiteille, joilla tulisi korjata tietoturvan arvioinnissa havaitut puutteet ja joiden avulla pyritään hallitusti kehittämään tietoturvan kypsyystasoa tavoitetasolle. (Valtiovarainministeriö, 2007, s. 47) Tammisalo on kuvannut eri kypsyystasoja esittävän kypsyysmallin, jonka tarkoituksena on ilmentää tietoturvatason paranemista, joka hänen mukaan saavutetaan tietoturvaongelmien hallinnoinnin ja käsittelyn menettelytapojen kehittämisellä sekä suunnittelulla (Tammisalo, 2007, s. 25). Kypsyysmalli on esitetty alla olevassa kuvassa 4.



Kuva 4. Tietoturvan kehittämissuunnitelman kypsyysmalli (Tammisalo, 2007, s. 25)

Kypsyysmallissa tarkemmin ottaen mitataan, missä määrin organisaatio on saavuttanut sen tietoturvatoiminnalle asetetut tavoitteet eli kuinka kehittämisuunnitelma vastaa tietoturvatoimintaan kohdistuviin vaatimuksiin. Tammisalon esittämässä kypsyysmallissa on kuusi eri tasoa tietoturvaongelmien ratkaisussa (Tammisalo, 2007, s. 26):

- **Taso 0**: Organisaatio ei ole havainnut ongelman olemassaoloa, mistä johtuen minkäänlaisia toimintaperiaatteita, prosesseja tai mittareita ei ole luotu tai käytössä.
- **Taso 1**: Ongelma on alustavasti tunnistettu, mutta käsittely on harvinaista tai epäloogista, toimintakäytännöt ovat summittaisia ja ratkaisuja tuotetaan tapauskohtaisesti vain yksitäisiin tarpeisiin. Seurantaa harjoitetaan vain reaktiivisesti.
- **Taso 2**: Ongelma on tiedostettu koko organisaatiossa, ja toimintaperiaate tälle on luotu. Ongelman hoitamista varten organisaatiossa on luotu prosessit, mutta ne eivät ole kokonaislaajuisesti käytössä, vaan ainoastaan yksittäisten henkilöiden vastuulla. Mittaamisen tarve on periaatetasolla tunnistettu, mutta mittaaminen on satunnaista ja kehitysasteella.
- **Taso 3**: Ongelman selvittämisen tarve on ymmärretty ja hyväksytty, sekä käytännöt on linjattu yhteensopiviksi organisaation muiden toimintakäytäntöjen kanssa. Toiminnan mittareita on kehitetty ja seurataan, mutta seurannassa ei analysoida tapahtumien syitä eikä seurantatietoja oteta huomioon prosessien kehityksessä. Lisäksi menettelyt ja toimintatavat on standardoitu, dokumentoitu sekä toteutettu

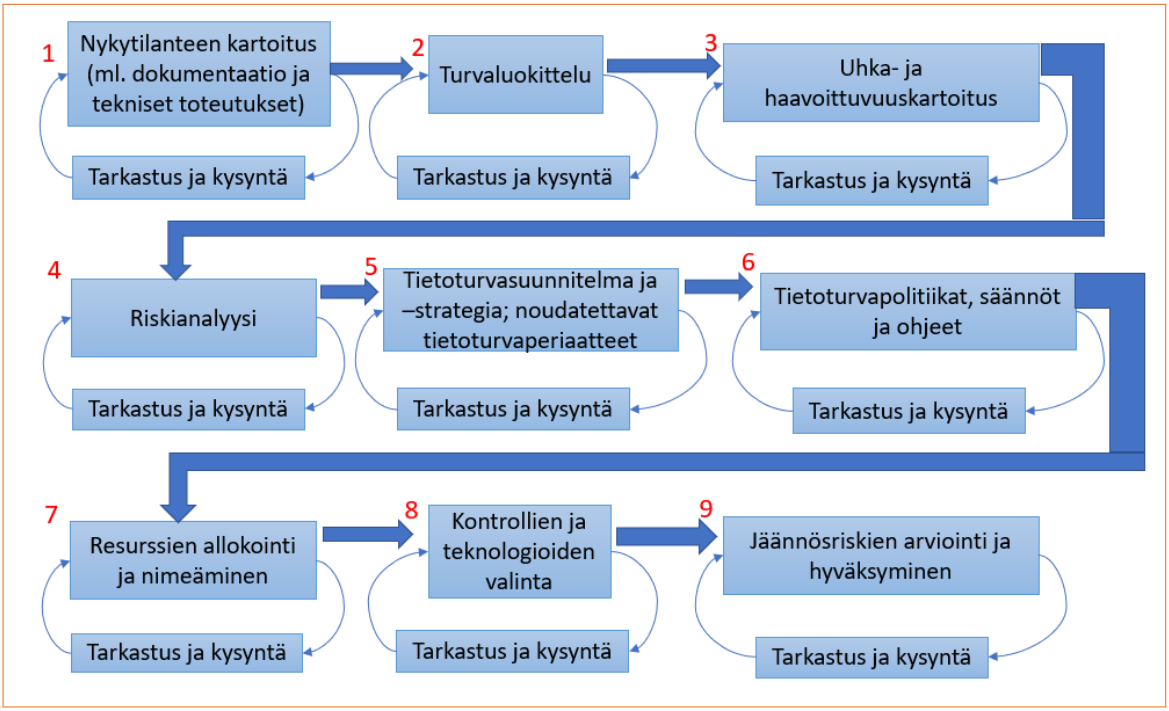
koko organisaatiossa. Näistä syistä koulutusta on myös mahdollista järjestää tarvittaessa työntekijöille.

- **Taso 4**: Ongelman selvittämisen tarve on myös tällä tasolla ymmärretty sekä hyväksytty, sekä käytännöt ja toteutus on käytössä koko organisaatiossa. Lisäksi riskien hallinta on otettu huomioon hallinnoinnissa, ongelmien käsittelyssä sekä prosessin kehittämisessä. Ne henkilöt, jotka ovat osallisena prosessiin, ovat koulutettuja sekä tietoisia uhkista, riskeistä ja vaihtoehdoista. Prosesseja parannetaan mittareiden tuottamiin tuloksiin pohjautuen, poikkeamat ja tulosten raja-arvot on määritelty.
- **Taso 5**: Edellisen tason 4 toteuman lähtökohdasta organisaation tietoturvan kehittämissuunnitelman kehitystyö kohdistuu tulevaisuuteen. Käytäntöjen, toimintatapojen sekä prosessien kehityksen tukena käytetään vertailua myös kolmansiin osapuoliin, joiden mukaan optimoidaan omaa toimintaa. Ulkoisia asiantuntijoita käytetään tällä tasolla vertailukohtien saamiseksi.

2.3.4.1 Tietoturvan kehittämissuunnitelman vaiheet

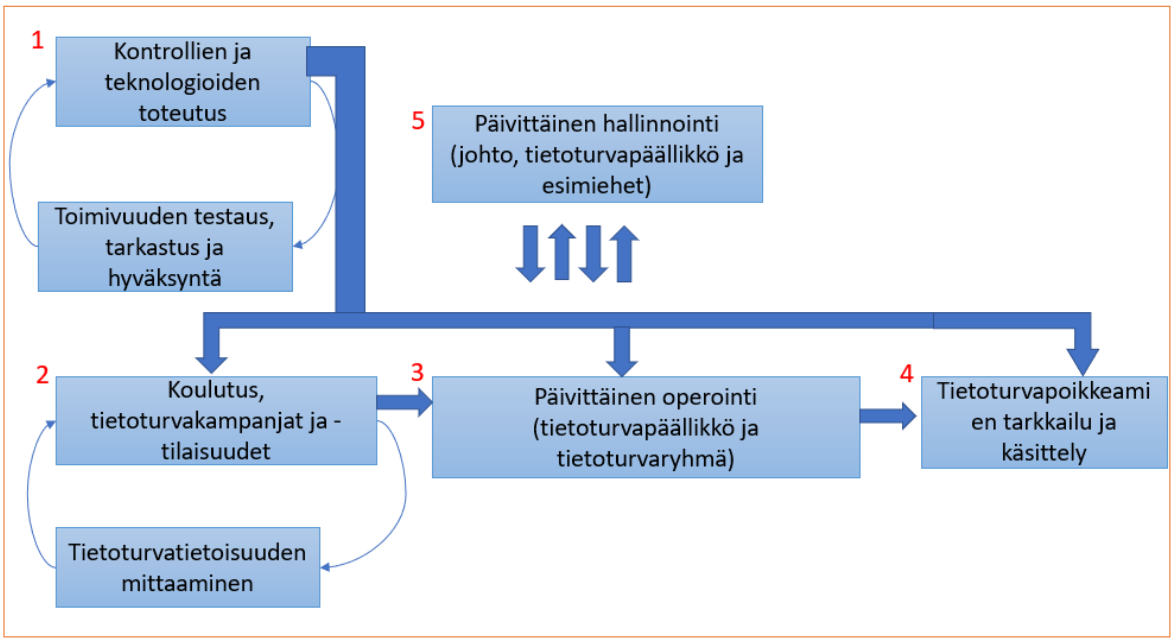
Tammisalon mukaan tietoturvan kehittämissuunnitelman vaiheet koostuvat PDCA-malliin pohjautuen suunnittelusta, toteutuksesta, tarkastuksesta sekä kehityksestä. Jokaiseen vaiheeseen kuuluu erilaisia alitehtäviä, jotka olisi tarkoitus suorittaa järjestelmällisesti päästäkseen kehittämissuunnitelmassa seuraavaan vaiheeseen (Tammisalo, 2007, s. 26).

Suunnitteluvaiheessa organisaation tehtävänä on luoda raamit ja säännöt tietoturvan hallinnalle. Suunnitteluvaihe koostuu yhdeksästä eri alitehtävästä, joista syntyneitä periaatteita ryhdytään toteuttamaan seuraavassa vaiheessa. Jotta toteutus vaiheeseen voi siirtyä, on jokainen alitehtävä oltava tarkastettu huolellisesti sekä hyväksytty. Suunnitteluvaiheen alitehtävän on kuvattu alla olevassa kuvassa 5. (Tammisalo, 2007, ss. 26-28)



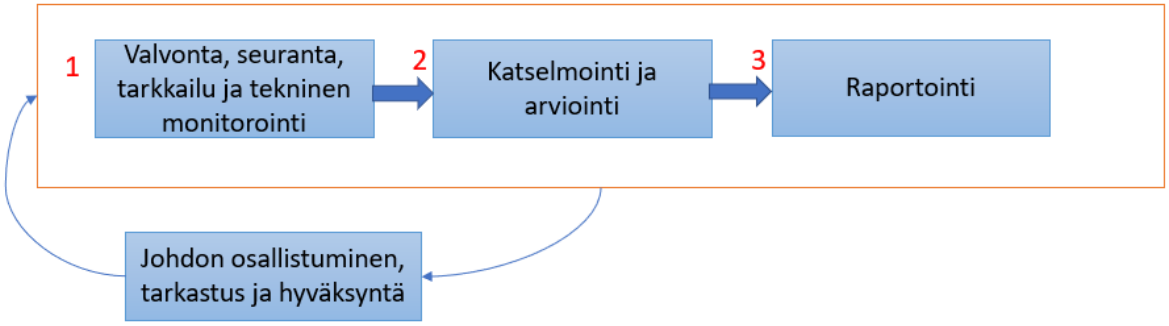
Kuva 5. Suunnitteluvaiheen alitehtävät (Tammisalo, 2007, s. 28)

Seuraavissa vaiheissa suoritetaan organisaation normaaliin rutiiniin kuuluvat tietoturvatoimet. Tälle toiminnalle on jo luotu pohja valmiiksi tietoturvakäytännöissä, joten tämä vaihe on olemassa olevien raamien mukaista toimintaa. Tästä syystä toteutusvaihe on itseohjautuva, jossa esimerkiksi erilaisissa poikkeamatilanteissa noteeratut asiat voivat aikaansaada päivityksiä teknologioiden toteutukseen, jos nämä päivitykset noudattavat organisaation käytössä olevaa toimintasuunnitelmaa eikä näitä tästä syystä tarvitse hyväksyttää erikseen tietoturvaryhmässä. Alla olevassa kuvassa 6 on vielä tarkemmin kuvattuna prosessi, joka käydään toteutusvaiheessa läpi, ja jonka jälkeen siirrytään tarkastusvaiheeseen. (Tammisalo, 2007, ss. 35-36)



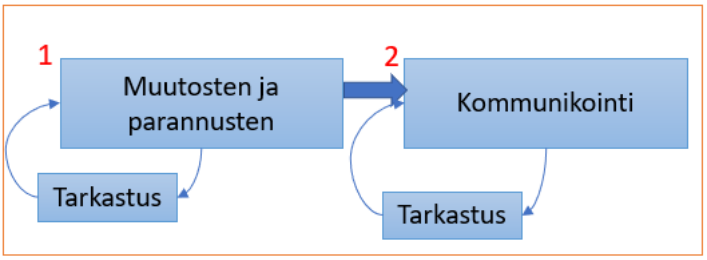
Kuva 6. Toteutusvaihe (Tammisalo, 2007, s. 36)

Tarkastusvaiheessa tarkoituksena on valvoa sekä arvioida organisaation tietoturvallisuuden tilaa kokonaisuudessaan, dokumentoida tietoturvasta tarvittavassa kokonaisuudessa ja hankkia tietoturvatoiminnalle valittu sertifiointi. Lopputuloksena arvioinnissa tulisi tietää organisaation tietoturvahallinnoinnin toimintakyky ja sopivuus toteutettujen vaatimusten mukaan ja tämän perusteella kyetä suunnittelemaan ja toteuttamaan tarvittavat muutokset hallinnointiprosessiin. (Kuva 7.) (Tammisalo, 2007, s. 40)



Kuva 7. Tarkastuvaihe (Tammisalo, 2007, s. 40)

Viimeisessä vaiheen eli kehityksen ideana on tarkentaa tietoturvahallinnoinnin syklisen prosessin kehä. Vaiheessa evaluoidaan organisaation muutos- ja kehitystarpeet hallinnointiprosessiin ja -menettelyihin. Tarpeiden muutosten käsittely sekä niiden toteuttaminen aloittaa uuden hallinnointisyklin suunnitteluvaiheesta aloittaen. (Kuva 8.) (Tammisalo, 2007, s. 41)



Kuva 8. Kehitysvaihe (Tammisalo, 2007, s. 41)

2.3.5 Auditointisuunnitelma

Tietoturva-auditointi on puolueetonta tietoturvan testaamista niin, että saadaan selkeä käsitys siitä, onko organisaation tietoturva riittävä sen etuuksien suojaamiseen, ja mitä tietoturvan osa-alueita pitää vielä mahdollisesti parantaa. Auditoinnin aikana selvitetään organisaation tietoturvariskit sekä varmistetaan, että niiltä on suojauduttu oikealla tavalla. (Kokkarinen, 2012, s. 3)

Eri teknologien avulla kyetään pienentämään tietoturvariskejä, mutta ainoastaan silloin, kun niitä käytetään oikein ja oikeissa paikoissa. Tietoturva-auditoijan tehtäviin kuuluu selvittää organisaatiota koskevat tietoturvariskit, niiden toteutumismahdollisuudet sekä niiden mahdollisesta toteutumisesta koituvat kustannukset ja tarkistaa, onko niihin varauduttu tarpeeksi hyvin ottaen huomioon riskien toteutumismahdollisuudet ja niiden toteutumisesta aiheutuvat tappiot. Lisäksi auditoijan tulee raportoida havaituista puitteista sekä esittää puitteille korjausehdotuksia. Ilman kattavaa auditointia ei tiedetä, onko tietoturva toteutettu organisaatiossa onnistuneesti. (Kokkarinen, 2012, s. 3)

Auditoija voi olla joko organisaation sisäinen vastuutettu henkilö tai vastapuolen hankkima auditoija, joka voi tehdä satunnaisesti auditointeja tai sovitusti esimerkiksi kerran vuodessa. Ulkoisten ja sisäisten auditoijien välillä on kuitenkin eroja ja sen takia onkin harkittava tarkkaan, kumpaa vaihtoehtoa organisaatiossa halutaan ensisijaisesti käyttää vai riittääkö resurssit jopa molempien hankintaan. Ulkoistetut auditoijat ovat saaneet kattavan koulutuksen ammattiinsa, voivat todistaa pätevyytensä sertifikaattien avulla sekä jatkuvalla prosessilla parantavat osaamistaitojaan tietoturvassa ja auditoinnissa (Hämäläinen, 2004). Näistä syistä johtuen ulkoiset auditoijat ovat ammattitaitoisempia ja tehokkaampia kuin sisäiset auditoijat, joilla auditointi voi olla pahimmassa tapauksessa vain sivutehtävä heidän muiden päätehtävien ohella. Lisäksi ulkoiset auditoijat ovat pääasiallisesti

puolueettomia, joka vaikuttaa myös suuresti auditoinnin toteutukseen ja arviointiin. (Kokkarinen, 2012, ss. 4-5)

SFS-EN ISO 19011 mukaan organisaatiossa nimetyn pääauditoijan tulisi laatia auditointisuunnitelma auditointiohjelmaan sisältyvien tietojen sekä auditoitavan tahon toimittamien asiakirjojen perusteella. Auditointisuunnitelman tavoitteena on helpottaa auditointitoimien tehokasta aikatauluttamista ja koordinointia, jotta tavoitteet pyrittäisiin saavuttamaan vaikuttavasti. Suunnitelman tarkkuus voidaan määrittää auditoinnin soveltamisalan sekä monimutkaisuuden mukaan, ja siinä tulisi ottaa huomioon epävarmuuden vaikutus auditoinnin tavoitteiden saavuttamiseen. Pääauditoijan olisi oltava tietoinen myös soveltuvista näytteenottomenetelmistä, auditointiryhmän kokoonpanosta ja sen kokonaispätevyydestä sekä auditoinnin organisaatiolle aiheuttamista riskeistä. Auditointisuunnitelma on mahdollista katselmoittaa sekä hyväksyttää auditoinnin asiakkaalle sekä lisäksi valmis suunnitelma tulisi näyttää auditoitavalle taholle. (Suomen standardoimisliitto SFS ry, 2011, ss. 42-44)

3 HALLINTAJÄRJESTELMÄN TOTEUTUS ORGANISAATIOLLE

Tässä luvussa on kuvattu esimerkkiorganisaatiossa tehdyn tietoturvallisuuden hallintajärjestelmän projektin prosessivaiheista. Luvussa 3.1 on kerrottu projektin taustasta eli miksi hallintajärjestelmää ryhdyttiin esimerkkiorganisaatiolle toteuttamaan. Luku 3.2 sisältää toteutuksen suunnittelun lähtökohdat. Luvussa 3.3 kerrotaan projektin kohteista ja miksi nämä ovat valikoituneet projektissa suojeltaviksi kohteiksi. Luvussa 3.4 esitellään uhkien analysointimenetelmä. Viimeisissä luvuissa 3.5-3.7 on esitelty tietoturvapolitiikan, tietoturvakäytäntöjen sekä tietoturvan kehittämissuunnitelman toteutumista.

3.1 Toteutuksen lähtökohdat

Toteutuksen aihe lähti liikkeelle esimerkkiorganisaation kanssa pidetystä palaverista, jossa keskusteltiin esimerkkiorganisaation järjestelmien tietoturvakuvauksista. Esimerkkirganisaatiolla ei aiemmin ollut yksityiskohtaisempaa tietoturvapolitiikkaa luotuna ja monet asiakkaat olivat alkaneet vaatia tarkempia tietoturvakuvauksia järjestelmistä. Näistä syistä esimerkkiorganisaatiossa ryhdyttiin toteuttamaan tietoturvan hallintajärjestelmää. Toteutukseen vaikuttivat myös erilaiset mahdolliset tietomurrot, jotka voisivat aiheuttaa huonoa julkisuutta ja lisäksi hallintajärjestelmän luominen parantaisi esimerkkiorganisaation valmiuksia hallita systemaattisesti tietoturva-asioita. Tietoturvan hallintajärjestelmän toteuttamisen jälkeen tavoitteena oli saada hallintajärjestelmästä sovitut käytännöt jalkautetuksi mahdollisimman nopeasti. Lisäksi tarkoituksena on tulevaisuudessa toteuttaa kehittämisuunnitelman mukaiset muutokset jatkuvaa prosessina. Hallintajärjestelmän toteuttamista varten luotiin esimerkkiorganisaatiossa oma projekti, jossa tämä kokonaisuus toteutettiin järjestelmällisesti vaiheittain. Projekti aloitettiin 08.09.2016 ja päätettiin 23.12.2016.

3.2 Toteutuksen suunnittelu

Ensimmäisenä vaiheena esimerkkiogrnisaatiossa projektiin luotiin projektisuunnitelma, jossa määriteltiin projektille projektiryhmä vastaamaan hallintajärjestelmän toteutumisesta sekä ohjausryhmä, jonka tehtävänä projektissa oli varmistaa projektin toimintaedellytykset ja projektin hyötyjen oleellisuuden sekä hyötyodotusten riskit. Lisäksi ohjausryhmässä hyväksyttiin kaikki dokumentaatiot, mitä projektin aikana syntyi eri workshopeissa.

Projekti rersursoitiin siten, että projektiryhmä muodostettiin viidestä henkilöstä sekä ohjausryhmä kolmesta henkilöstä. Projektille määriteltiin toteutettavat tehtäväalueet, jotka muodostuivat hallintajärjestelmän eri toimintamalleista ja dokumentaatioista:

- Suojeltavien kohteiden määrittely
- Uhkien määrittely
- Tietoturvapolitiikka
- Tietoturvakäytännöt
- Tietoturvan kehittämissuunnitelma

Näiden pohjalta jokaiselle osa-alueelle luotiin omat pienryhmät, joissa toteutettiin omat vastuualueet. Pienryhmien vastuualueisiin kuuluivat käytännössä osa-alueensa suunnittelu sekä toteutus ja tästä workshoppeja varten sekä dokumentaation tekeminen että esitysten teko projektiryhmälle esitettäväksi ja hyväksyttäväksi. Toteutettavat osa-alueet tehtiin porrastetusti aloittaen suojeltavista kohteista ja päätettiin tietoturvan kehittämissuunnitelmaan.

3.3 Suojeltavien kohteiden määrittely

Projektissa ensimmäisenä tehtävänä oli määritellä tietoturvasuunnitelman mukaisesti esimerkkiorganisaation suojeltavat kohteet. Suojeltavat kohteet jaettiin ryhmittelemällä suojeltavat tuotetiedot sekä tietojärjestelmät, joissa tietoja käsitellään. Tietojen ja tietojärjestelmien lisäksi suojeltavaksi kohteeksi nostettiin myös tietoliikenne, sillä sen suojaaminen liittyy erottamattomana osana tietojärjestelmien tietoturvaan esimerkkiorganisaatiossa.

3.3.1 Tuotetiedot

Tuotetietoihin liittyviin suojeltaviin kohteisiin lukeutui allaolevat listatut asiat:

- Tuotteen ominaisuudet
- Tekninen toteutus ja ympäristö
- Tuotekehitysideat

Tuotteen ominaisuudet ovat osittain julkista, osittain yhteistyökumppanien ja asiakkaiden välistä ja osittain sisäistä tietoa. Tuotetietoja on saatavilla myynnin ja markkinoinnin välityksellä, asiakassuhteista sekä asiakkaan ympäristöön asennetuista tuotteista. Asiakassuhteissa on solmittu salassapitosopimus, joka velvoittaa molempia osapuolia. **Tekninen toteutus** on myös kokonaisuus, joka haluttiin suojata säilymisen sekä teknisen tietoturvan vuoksi. **Tuotekehitysideat** eivät yleensä näy suoraan tuotteessa, mutta näiden suojaaminen kilpailijoilta on myös tärkeää. Myynnillisestä näkökulmasta tuotekehitysideat ovat myös myyntivaltti, eikä näiden suojelu ole siis yksiselitteinen asia ja näin ollen nämäkin otettiin mukaan osaksi suojeltavia kohteita.

3.3.2 Asiakkaan tieto-omaisuus

Asiakkaan tieto-omaisuuden tarkemmat suojeltavat asiat koostuivat alla mainituista asioista:

- Asiakkaiden yhtiökohtainen tietosisältö
- Asiakkaiden toimintamallit
- Loppuasiakkaiden tiedot

Nämä asiat päätyivät mukaan suojeltaviin kohteisiin, koska asiakkaan tiedot ovat luottamuksellisia, elleivät ne muutoin ole julkisesti saatavilla. Lisäksi kun puhutaan sähkökauppa-toimialoista, ovat näiden toimintamallinsa hyvin toistensa kaltaisia. Lisäksi yhtiöiden loppuasiakkaiden tiedot ovat henkilötietolain mukaan salassa ja vaitiolovelvollisuuden piirissä pidettäviä tietoja jotka oli huomioitava esimerkkiorganisaation työprosessien eri vaiheissa.

3.3.3 Tietojärjestelmät

Tietojärjestelmien suojeltavat asiat koostuivat alla mainituista asioista:

- Palvelutuotanto (esim. Asiakkaiden omat ympäristöt)
- Tuotekehitys (esim. Sisäiset kehitysympäristöt)
- Dokumentaatio (esim. järjestelmät, missä ylläpidetään sisäistä dokumentaatiota)
- Esimerkkiorganisaation toimintaan liittyvät tietojärjestelmät

Eri tietojärjestelmät sisältävät liityntäpinnan tietoihin, joten itse tietojärjestelmät pitää huomioida suojauksessa. Tietojärjestelmien tietoturvan tulee ottaa huomioon tietojen salassa pysyminen sekä estää niiden tahallinen tai tahaton katoaminen.

3.3.4 Tietoliikenne

Tietoliikenteen suojeltaviin asioihin kuuluu:

- Integraatiot
- Etäyhteydet
- Sisäverkko

Tämä osa suojeltavista kohteista on yksi tärkeimmistä sen haavoittuvuuden takia operatiivisessa toiminnassa ja palvelutuotannossa. Salaamaton tietoliikenne sekä liian laajat käyttöoikeudet eri järjestelmiin voivat romuttaa hetkessä koko muun järjestelmän tietoturvan.

Jotta projektista ei olisi tullut liian suurta kokonaisuutta hallita, suojeltavien kohteiden osalta tehtiin rajaukset, joissa päädyttiin keskittymään ainoastaan palveluiden toteuttamiseen ja tarjoamiseen. Rajauksen ulkopuolelle jäivät esimerkkiorganisaation operatiivisen toiminnan tiedot, päätelaitteet sekä henkilöstö. Rajauksesta huolimatta yhtenäinen politiikka, henkilöstön toiminta sekä työvälineet kuuluvat jatkuvan toiminnan piiriin.

3.4 Uhkien määrittely

Projektin toisessa vaiheessa keskityttiin suojeltavien kohteiden uhkien määrittelyyn sekä tunnistamiseen. Uhkien tunnistamista varten pienryhmässä valittiin ensimmäisenä menetelmä, kuinka suojeltavien kohteiden uhkia ryhdyttiin tunnistamaan. Menetelmää valittaessa pienryhmä huomioi menetelmän sopivuuden, yksiselitteisyyden, selkeyden, käyttöhelppouden, raportointimahdollisuuden ja kuinka se sopeutui heidän ympäristön ominaisuuksiin sekä kuinka uhkat tultiin ymmärtämään. Nämä asiat huomioon ottaen menetelmäksi valikoitui potentiaalisten ongelmien analyysi (POA) tunnistusmenetelmä.

POA:ssa aloitettiin valitsemalla tarkasteltavat kohteet, jotka olivat määritelty projektin ensimmäisessä vaiheessa (tuotantoympäristö, kehitysympäristö, dokumentaatio, henkilöstö

ja päätelaitteet). Näistä ylemmän tason määrittelyistä pienryhmä tarkensi jokaisen tason alle siihen kuuluvat osat, jotka esimerkkiorganisaatiolla kuului kuhunkin tasoon. Näistä alettiin keräämään aivoriihien avulla mahdollisia ongelmia ja uhkia, jotka listattiin sitten omaksi dokumentaatioksi. Aivoriihien jälkeen listatut ideat järjesteltiin ja luokiteltiin ensimmäiseksi suojeltavien kohteiden ylätasojen mukaan, ja tämän jälkeen kustakin ryhmästä rajattiin pois sellaiset ideat, joita ei haluttu tarkasteltavan jatkokäsittelyssä yksityiskohtaisemmin tai jotka olivat lähes mahdottomina pidettäviä tapauksia.

Seuraavassa vaiheessa jatkokäsiteltäviksi valittuja uhkia alettiin käsittelemään yksityiskohtaisemmin. Yksityiskohtaisessa tarkastelussa luotiin lomake, johon kirjattiin sarakkeittain uhkien kohde, kohteiden tarkenne, itse uhkat, näiden seuraukset, riskiluvut jotka koostuivat annetusta todennäköisyydestä sekä vakavuudesta, uhkien nykyinen varautuminen sekä toimenpide-ehdotukset taulukko 1 mukaisesti. Tästä muodostuneen lopullisen lomakkeen jälkeen ohjausryhmälle sekä projektiryhmälle laadittiin erillinen dokumentaatio tiivistettynä tämän projektiosuuden toteutuksesta sekä myös liitteenä kaikkien uhkien tunnistamisesta toteutunut raportti.

Taulukko 1, Esimerkkiorganisaation raportointimalli uhkien määrittelyssä

Kohde	Tarkenne	Uhka	Seuraukset	Tod.näk	Vakavuus	Riski	Nykyinen varautuminen	Toimenpide-ehdotukset
K1	T1	Uhka1	Selitys	3	4	12	Selitys	Selitys
K2	T2	Uhka2	Selitys	2	3	6	Selitys	Selitys

3.5 Tietoturvapolitiikka

Uhkien määrittelyn jälkeen tehtävänä oli toteuttaa dokumentoitu tietoturvapolitiikka.
Pienryhmän tavoitteena oli toteuttaa dokumentoitu toimintamalli, joka ohjaisi esimerkkiorganisaation henkilöiden toimintaa, soveltavin osin esimerkkiorganisaation asiakkaita sekä sidosryhmiä. Pienryhmään valikoitui työskentelemään projektiryhmästä myyntipuolen sekä tuotannon puolen edustajia, koska politiikan ymmärtämiseen tarvittiin tietoa esimerkkiorganisaation liiketoimintaprosesseista sekä tietoarkkitehtuurista. Politiikan sisällöstä rajattiin pois tietoturvan teknisen toteutuksen näkökulma, koska tietoturvapolitiikan ideana on pitää dokumentti sellaisessa muodossa, jotta

esimerkkiorganisaation ylin johtokin tämän dokumentin sisällön ymmärtäisi. Politiikan sisältöä lähdettiin suunnittelemaan ennalta määriteltyjen kysymysten pohjalta, eli mitä suojataan, miksi suojataan sekä miten suojataan. Näihin kysymyksiin nojautuen pienryhmä määritteli politiikan laajuuden sekä itse politiikan, johon kohdistettiin mukaan sidosryhmiin vaikuttava tietoturvapoliittinen toiminta.

3.6 Tietoturvakäytännöt

Tietoturvakäytäntöjen toteuttaminen luotiin tietoturvapolitiikan sekä uhkien pohjalta. Käytäntöjen tavoitteena oli luoda esimerkkiorganisaatiolle dokumentaatio, jonka avulla esimerkkiorganisaation työntekijät havainnollistavat sovelluksen kehitys- sekä tuotantoympäristön uhkakuvat, ja kuinka toimia esimerkkiorganisaatiossa tietoturvallisesti molemmissa ympäristöissä. Dokumentaatio päätettiin toteuttaa esimerkkiorganisaatiossa käytettävään Confluence-wikiin, mikä on www-sivusto, joka tarjoaa erilaisille materiaaleille luonti- ja ylläpitomahdollisuuden verkossa helpolla ja turvallisella tavalla (Atlassian, 2018). Wikiin voi luoda vapaasti sisältöä, joille voidaan jakaa oikeuksia vain esimerkiksi esimerkkiorganisaation henkilöiden käyttöön (Atlassian, 2018).

Dokumentaation yksityiskohtainen sisältökokonaisuus muodostettiin vastuussa olevan pienryhmän toimesta yhteisissä palavereissa. Tekstin tuottaminen toteutettiin jakamalla jokaiselle pienryhmän jäsenelle oma osa-alue, josta tuli kirjoittaa itsenäisesti materiaalipaketti. Nämä materiaalipaketit käytiin ennen varsinaista workshoppia läpi pienryhmän palaverin yhteydessä, jossa vielä keskusteltiin analysoitiin sitä, oliko materiaaleissa puutteita tai korjattavia asioita. Viimeisenä osana tätä projektin vaihetta koko dokumentaatio esitettiin pienryhmän toimesta workshop:ssa projektiryhmälle, jossa tämä tuotos hyväksyttiin esitettäväksi myös ohjausryhmälle. Materiaalipaketit muodostuivat neljästä eri osasta:

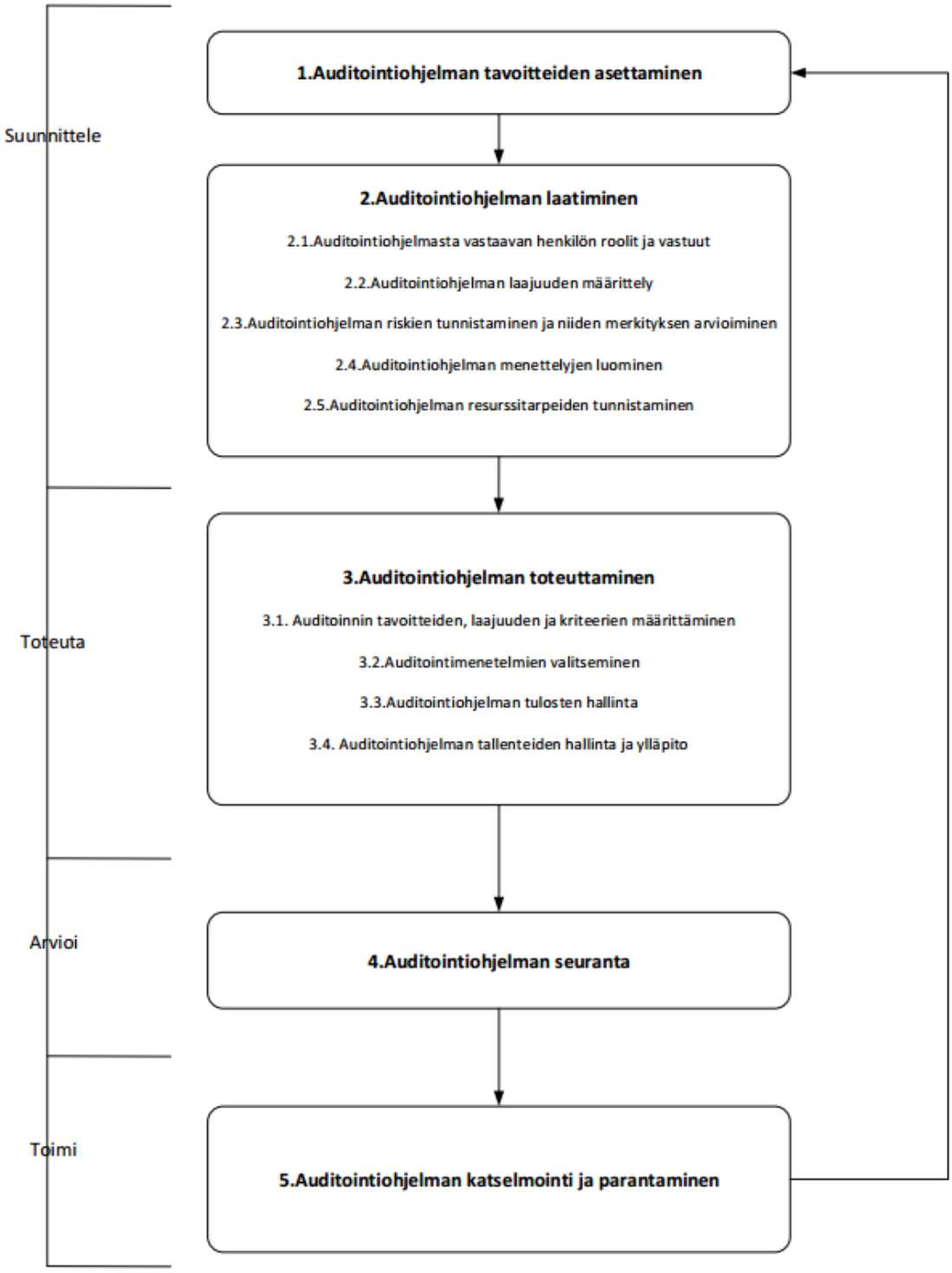
- Kehitysympäristö
- Kehitysympäristön kehitysohjeet
- Tuotantoympäristö
- Tuotantoympäristön operointiohjeet

Kehitysympäristöstä tarkoituksena oli esitellä esimerkkiorganisaatiossa eniten käytettäviä kehitysvälineitä, näiden erilaisia tietoturvauhkia, joita näihin kohdistuu sekä kuinka työntekijän tulisi näihin uhkiin varautua omassa ohjelmistokehityksessään. Näiden lisäksi itse kehitysympäristölle luotiin tietoturvavaatimukset nojautuen Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) laatimaan ohjeistukseen. Kyseiset tietoturvavaatimukset luovat pohjan esimerkkiorganisaation kehitysympäristölle tehtyyn tietoturvaan. Tämä ohjeistus edesauttaa myös uusien työntekijöiden kouluttamisessa, jonka uudet työntekijät voivat varsinkin töiden aloittamisen ohella käydä läpi. Kehitysympäristölle luotiin myös kehitysohjeet, jotka opastavat sovelluskehittäjiä työskentelemään kehitysympäristössä eri tilanteissa tietoturvavaatimusten mukaisesti. Tuotantoympäristöstä kuvattiin uhka-analyysin sekä tietoturvapolitiikan pohjalta tietoturvavaatimukset, jotka liittyivät palvelinten, tietokantojen sekä käyttöoikeuksien käyttöön, joista dokumentoitiin eri uhkakuvat jokaiselle osa-alueelle, sekä kuinka näitä voidaan omalla toiminnalla ennaltaehkäistä.

3.7 Tietoturvan kehittämissuunnitelma

Projektin viimeisessä vaiheessa tarkoituksena oli toteuttaa projektille jatkuvan prosessin malli sekä kehittämissuunnitelma, jonka avulla jatkuvan prosessin mallia tullaan suorittamaan. Näiden avulla esimerkkiorganisaation tietoturvalle taataan se, että tietoturvasta huolehditaan sekä sitä päivitetään jatkuvasti, eikä näin ollen tietoturva jäisi vain projektitasolle esimerkkiorgansaatiossa.

Jatkuvan prosessimallin tärkeimpänä osa-alueena oli toteuttaa esimerkkiorganisaatiolle sisäinen auditointisuunnitelma, jonka avulla tietoturvapäällikkö kykenee tekemään sisäisen tietoturva-auditoinnin esimerkkiorganisaation palveluille sekä kehitysympäristöille. Auditointimalli suunniteltiin esimerkkiorganisaatiolle PDCA-mallin mukaisesti SFS-ENO ISO 19011 standardia apuna käyttäen. Kuvassa 9. on esitetty esimerkkiorganisaatiolle toteuttettu sisäisen audioinnin prosessivuokaavio.



Kuva 9. Yrityksen sisäisen auditoinnin prosessivuokaavio

Jokaiselle kohdalle on määritelty tarkemmat kuvaukset kehittämissuunnitelmassa, mitä kukin kohta sisältää, ja jonka kuvausten pohjalta tietoturvapäällikön tulisi kyetä tekemään sisäinen auditointi tuote- ja sovelluskehitykselle.

4 ANALYYSIT JA POHDINTA

Luvussa 4.1 on vertailtu esimerkkiorganisaatiolle toteutettua hallintajärjestelmän kattavuutta kahteen tässä työssä jo aiemmin mainittuun hallintajärjestelmään eli VAHTI-ohjeisiin sekä ISO/IEC 27001 -standardiin. Toisessa luvussa 4.2 kerrotaan, mitä muiden organisaatioiden tulisi ottaa huomioon ryhtyessään implementoimaan tietoturvallisuuden hallintajärjestelmää sekä mitä yleisimpiä haasteita voidaan näissä projekteissa kohdata.

4.1 Hallintajärjestelmän toteutuksen onnistuminen versus yleiset määrittelyt

Projektin suunnittelussa korkeimpana prioriteettina oli toteuttaa hallintajärjestelmä, joka tulisi kattamaan koko organisaation toiminnan. Tästä syystä tietoturvallisuuden hallintajärjestelmä toteutettiin esimerkkiorganisaatiolle VAHTI-ohjeisiin perustuen ja lisäksi apuna käyttäyen myös ISO/IEC 27001 -standardia. Nämä kaksi soveltuvat paremmin organisaationlaajuisen, perusteellisen hallintajärjestelmän toteutukseen kuin esimerkiksi TCSEC-hallintajärjestelmä (United States Department of Defense, 1985), ITSEC-hallintajärjestelmä (Gehrke et al, 1992) sekä Common Criteria-hallintajärjestelmä (The Common Criteria Portal, 2018), jotka kohdistuvat ainoastaan tuotekehitystoimintaan, jolloin hallittavana kohteena ovat tuotannossa olevat järjestelmät, tuotteet ja lisäksi tekniset ympäristöt. Esimerkkiorganisaatioon valmistuneen hallintajärjestelmän kattavuutta on analysoitu tässä työssä aikaisemmin mainittuun Susanto et al:n määrittelemään 11 kohdan hallinta-alue listaan taulukossa 2. Taulukko on laajennettu kuvaamaan myös sen matriisimuodossa, mitä kaikkia hallinta-alueita tässä työssä esitetyt tietoturvallisuuden hallintajärjestelmät kattavat.

Taulukko 2. Tietoturvallisuuden kattavuusvertailu esimerkkiorganisaatiossa.

Hallinta-alueet	**Esimerkkiorganisaation hallintajärjestelmä**	**VAHTI**	**ISO27001**
1. Tietoturvapolitiikka	x	x	x
2. Viestinnän ja operatiivinen johtaminen	-	x	x
3. Pääsynhallinta	x	x	x
4. Tietojärjestelmien hankinta, kehitys ja ylläpito	-	x	x
5. Tietoturvallisuuden organisointi	x	x	x
6. Omaisuudenhallinta	-	x	x
7. Tietoturvapoikkeamien hallinta	x	x	x
8. Liiketoiminnan jatkuvuudenhallinta	x	x	x
9. Henkilöstöturvallisuus	x	x	x
10. Fyysinen ja ympäristön turvallisuus	x	x	x
11. Vaatimustenmukaisuus	x	x	x
Kattavuus hallinta-alueista (11)	**8**	**11**	**11**

Tämän kattavuusvertailun perusteella havaitaan, että esimerkkiorganisaatiolle tehty hallintajärjestelmä kattaa yhdestätoista hallinta-alueesta kahdeksan, joten kattavuuden näkökulmasta projekti oli onnistunut. Kuten huomataan, VAHTI-ohjeistus sekä ISO27001 kattavat jossain laajuudessa kaikki esitetyt hallinta-alueet ja näin ollen esimerkkiorganisaatiolle pystytään myöhemmin toteuttamaan täysin kattava hallintajärjestelmä, koska valmistunut hallintajärjestelmä perustuu VAHTI:in sekä ISO27001:seen.

4.2 Tietoturvallisuuden hallintajärjestelmän implementointiprosessista opittua

Tietoturvallisuuden hallintajärjestelmän käyttöönotto on oltava perusteltua, joten organisaatiossa on tunnistettava tämän tarpeellisuus. Tarpeellisuuteen vaikuttavia tekijöitä voivat olla esimerkiksi organisaation muutostilanne, organisaation toimintaan liittyvät erityistarpeet, yhteistyökumppaneiden kautta tulevat vaatimukset tai nykyisen tietoturvallisuuden hallintajärjestelmän puuttellisuus. Muutostilanne voi syntyä silloin, kun organisaation strategia sekä asiakaskunta muuttuvat. Tällöin on mahdollista, että näihin liittyvät muutokset tuovat uusia tietoturvallisuushaasteita. Organisaation toimintaan

liittyvissä erityistarpeissa kyseessä useasti on kyseisen organisaation toimiala, jotka voivat asettaa omia vaatimuksia tietoturvallisuudelle, kuten terveydenhuolto ja tämän potilastietojärjestelmä. Yhteistyökumppanitkin voivat velvoittaa organisaatiota toimimaan tiettyjen tasovaatimusten mukaan, sillä jos näitä ei pystytä noudattamaan niin yhteistyökumppani ei välttämättä halua kyseistä palvelua enään samalta organisaatiolta ostaa tai huonoimmassa tapauksessa ei ole mahdollista edes päästä tarjouskilpailuun mukaan. Lisäksi organisaation tämän hetkinen hallintajärjestelmä voi sisältää puutteita esimerkiksi liiketoiminnan jatkuvuuden kannalta, jota voidaan pitää hyvänä syynä tietoturvallisuuden hallintajärjestelmän käyttöönotolle.

Kun tietoturvallisuuden hallintajärjestelmän tarpeellisuus on perusteltua, organisaation tulisi pohtia, millä eri kriteerein valitaan käytettävä hallintajärjestelmä. Tässä työssä esimerkkiorganisaation kriteereiksi muodostuivat prioteettijärjestyksessä hallintajärjestelmän kattavuus, mukautuvuus sekä sidosryhmiltä tulleet tietoturva ja -suojavaatimukset. Kattavuuden näkökulmasta organisaation tulisi arvioitava se, mitä kaikkia organisaation osia tietoturvallisuuden hallintajärjestelmässä halutaan määritellä. Jos kattavuutta halutaan rajoittaa vain esimerkiksi tuotteen tietoturvaominaisuuksien määrittelyyn, tällöin ei välttämättä tarvita kokonaisvaltaista VAHTI-ohjetta hallintajärjestelmän kehittämiseen, vaan silloin kannattaa kääntyä esimerkiksi Common Criterian puoleen. Mukautuvuuteen on myös hyvä kiinnittää huomiota hallintajärjestelmän valinnassa, eli kuinka hyvin kyseinen hallintajärjestelmän määrittely sopisi organisaatiolle. Esimerkiksi pienessä organisaatiossa kattavan hallintajärjestelmän vaatiman oheistyöryhmien toteuttaminen voi vaatia huomattavasti enemmän resursseja suhteessa henkilöstön määrään. Lisäksi jos hallintajärjestelmän struktuuri sekä siihen liittyvät toimintaprosessit ovat hyvinkin kankeita, voi se syödä paljon enemmän resursseja, mitä siihen alunperin oli suunniteltu. Näiden valintakriteerien lisäksi kannattaisi ottaa huomioon myös eri hallintajärjestelmien julkinen ylläpito, eli mitkä julkaistuista hallintajärjestelmistä kehittyvät aktiivisesti, jotta organisaatiossa ei tarvitsisi ryhtyä vaihtamaan hallintajärjestelmää ainoastaan tämän takia.

Hallintajärjestelmän toteuttamisprojektissa kannattaa muistaa myös erinäiset haasteet, joita syntyi myös esimerkkiorganisaatiossa hallintajärjestelmän implementointiprojektissa.

Yhtenä suurimpana haasteena kyseisessä projektissa oli alkuperäisen tavoitteen tarkentuminen projektin toteutuksen aikana ja sen seurauksena projektin laajentui määritellystä. Projektin suunnittelussa tulisi tiedostaa mahdolliset poikkeamat ja näin asettaa selkeät tavoitteet, jotta hallintajärjestelmää toteuttaessa ei tarvitsisi käyttää liikaa resursseja siihen, että mitä kaikkea haluttu tietoturvallisuuden hallintajärjestelmä pitäisi pitää sisällään. Lisäksi toisena oleellisena havaintona ilmeni hallintajärjestelmässä tehtyjen käytäntöjen jalkauttamisprosessin huomiointi organisaatiossa. Jotta ohjeistuksen jalkauttaminen olisi mahdollisimman esteetöntä sekä yksinkertaista, on projektissa tähdättävä mahdollisimman loogiseen dokumentaatiokokonaisuuteen, josta käy ilmi jokaisen hallintajärjestelmän hallinta-alueen osat ja siihen perustuen jokainen organisaation jäsen pystyy hallintajärjestelmän oleellisimmat osat sisäistämään. Näin ollen valmiista hallintajärjestelmistä ei kannata kopioida suoraan valmiita kokonaisuuksia, vaan suositeltavaa on, että nämä osataan selkeyttää käytännön tasolle organisaation arvoja vasten.

5 YHTEENVETO

Tämän diplomityön tarkoituksena oli toteuttaa esimerkkiorganisaatiolle kattava tietoturvallisuuden hallintajärjestelmä. Hallintajärjestelmän toteutuksen pohjaksi työssä esiteltiin tietoturvallisuuden hallintajärjestelmän keskeisimmät hallintaosat esimerkkiorganisaation näkökulmasta sekä lyhyesti kaksi hallintajärjestelmämallia, VAHTI-ohjeistus (Valtiovarainministeriö, 2017) sekä ISO/IEC 27001-standardi (Noticebored, 2018). Lisäksi työssä esiteltiin tietoturvallisuuden merkityksistä organisaatioissa sekä tulevan tietosuoja-asetuksen oleellisimmista ja merkittävimmistä muutoksista. Työssä syntyi esimerkkiorganisaatiolle hallintajärjestelmä, jota vertailtiin työssä Susanto et al:n tutkimuksessa käytettyyn yhdentoista kohdan hallinta-alue kokonaisuuteen. Vertailussa tarkasteltiin hallintajärjestelmän kattavuutta, joka osoitti, että Susanto et al:n määrittelemän hallintajärjestelmän kokonaisuudesta esimerkkiorganisaatiolle toteutettu hallintajärjestelmä saavutti kahdeksan kohtaa. Työn alussa asetetut tavoitteet saavutettiin melko onnistuneesti.

Hallintajärjestelmän toteutuksessa ilmeni myös asioita, joita muidenkin organisaatioiden tulisi ottaa huomioon ryhtyessään implementoimaan tietoturvallisuuden hallintajärjestelmää. Jotta implementointiprosessista syntyy mahdollisimman selkeä ja hyvin määritelty kokonaisuus, tulisi organisaatioiden muistaa peruslähtökohdat toteutukselle, jotka tässä työssä konkretisoituivat hallintajärjestelmän tarpeellisuuden analysointiin, kriteerien määrittämiseen hallintajärjestelmän valinnassa sekä mahdollisten haasteiden tunnistamiseen käyttöönotossa.

Tulevan tietosuoja-asetuksen myötä organisaatioiden kannattaa osata varautua oikealla tavoin mahdollisiin muutoksiin, mitkä koskevat omaa organisaatiotaan henkilötietojen käsittelyssä. Tämä tarkoittaa sitä, että organisaatioiden on kyettävä arvioimaan, miten henkilötietoja käsitellään heillä nyt, miten niitä halutaan käsitellä sekä lopuksi suunniteltava, miten henkilötietojen käsittelyssä asetusten vaatimukset toimeenpannaan käytäntöön. Lisäksi kyseisestä prosessista syntyvää dokumentaatiota kannattaa pohtia, pystytäänkö tätä liittämään osaksi organisaation tietoturvallisuuden hallintajärjestelmää.

LÄHTEET

1. GDPR Portal. 2018. https://www.eugdpr.org/ [Verkkosivusto]. [Viitattu 08.04.2018].
2. Valtiovarainministeriö 2009. *Tietoturvapoikkeamiin varautuminen.* https://www.vahtiohje.fi/web/guest/tietoturvapoikkeamiin-varautuminen [Verkkosivusto]. [Viitattu 22.01.2017].
3. Laaksonen, M., Nevasalo, T., Tomula, K. 2006. *Yrityksen tietoturvakäsikirja.*
4. Valtiovarainministeriö 2007. *Tietoturvallisuudella tuloksia. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan.* https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229 [Verkkodokumentti]. [Viitattu 22.01.2017].
5. Hakala, M., Vainio, M., Vuorinen, O. 2006. *Tietoturvallisuuden käsikirja.*
6. Suomen Standardisoimisliitto SFS ry. 2015. *Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. ISO/IEC 27000 -standardiperhe* [Kalvosarja]. [Viitattu 22.01.2017].
7. Valtiovarainministeriö. 2000. *VM, VAHTI ja tietoturvallisuus.* https://www.vahtiohje.fi/web/guest/vm-vahti-ja-tietoturvallisuus [Verkkosivusto]. [Viitattu 22.01.2017].
8. Valtiovarainministeriö. 2013. *Sovelluskehityksen tietoturvaohje.* https://www.vahtiohje.fi/c/document_library/get_file?uuid=03c32520-f3f8-4621-b0d4-ec4ca8edafb3&groupId=10128&groupId=10229 [Verkkodokumentti]. [Viitattu 22.01.2017].
9. Ylipartanen, A. 2010. *Tietosuoja terveydenhuollossa. Potilaan asema ja oikeudet henkilötietojen käsittelyssä.*
10. Andreasson, A., Koivisto, J., Ylipartanen, A. 2013. *Tietosuojavastaavan käsikirja.*
11. Salminen, M. 2009. *Tietosuoja sähköisessä liiketoiminnassa.*
12. Vanto, J. 2011. *Henkilötietolaki käytännössä.*

13. Tietosuojavaltuutetun toimisto. 2013. *Henkilötietolaki.* http://tietosuoja.fi/fi/index/lait/Henkilotietolaki.html [Verkkodokumentti]. [Viitattu 02.04.2018].
14. Valtiovarainministeriö. 2016. *EU-tietosuojan kokonaisuudistus.* https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128 [Verkkodokumentti]. [Viitattu 02.04.2018].
15. Oikeusministeriö. 2017. *Miten valmistautua EU:n tietosuoja-asetukseen?* http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf [Verkkodokumentti]. [Viitattu 02.04.2018].
16. Energiateollisuus. 2016. *Tietosuojaselvitys.* Pääsy tietoon rajoitettu, lupaa voi kysyä Energiateollisuudelta.
17. Tammisalo, T. 2007. *Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi*. https://julkari.fi/bitstream/handle/10024/76251/R5-2007-VERKKO.pdf?sequence=1 [Verkkodokumentti]. [Viitattu 22.01.2017].
18. Susanto, H., Almunawar, M.N., Tuoan, Y.C. 2011. *Information Security Management System Standards: A Comparative Study of the Big Five.* International Journal of Electrical & Computer Sciences IJECS-IJENS. Vol. 11 No. 05. pp. 23-29
19. Suomen standardisoimisliitto SFS ry (2013). 27005 2013. *Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta.*
20. Miettinen, J. & Kajava, J. 1994. *Tietoriskien arviointi Risk Analysis and Risk Assesment: an overview of basic ideas and commonly used techniques.* [Väitöskirja]
21. Leppänen, J. 2006. *Yritysturvallisuus käytännössä.*
22. Bacik, S. 2008. *Building an effective information security policy architecture.*
23. Barman, S. 2002. *Writing information security policies.*

24. Thomas, T. 2005. *Verkkojen tietoturva.*
25. Kokkarinen, L. 2012. *Tietoturvan auditointi*. [Progradu-tutkielma]
26. Hämäläinen, P. 2004. *Auditointi tarkastaa tietoturvan tason.* http://www.tivi.fi/Arkisto/2004-11-30/Auditointi-tarkastaa-tietoturvan-tason-3089436.html [Verkkodokumentti]. [Viitattu 22.01.2017].
27. Suomen standardisoimisliitto SFS ry (2011). 19011 2011. *Johtamisjärjestelmän auditointiohjeet.*
28. Atlassian. 2018. *Confluence document collaboration.* https://www.atlassian.com/software/confluence [Verkkosivusto]. [Viitattu 02.04.2018].
29. The Common Criteria Portal. 2018. https://www.commoncriteriaportal.org/ [Verkkosivusto]. [Viitattu 04.04.2018].
30. United States Department of Defense. 1985. *Department of Defense Standard - Department of Defense Trusted Computer System Evaluation Criteria.* http://csrc.nist.gov/publications/history/dod85.pdf [Verkkodokumentti]. [Viitattu 4.4.2018].
31. Gehrke, M. et al. 1992. *Information Technology Security Evaluation Criteria (ITSEC) - a Contribution to Vulnerability?* Information Processing 92 - Proceedings from IFIP 12th World Computer Congress Madrid Spain 7-11 Sept 1992. Vol 2. pp 579-587
32. Valtiovarainministeriö. 2017. *Vahti-ohjeet.* https://www.vahtiohje.fi/web/guest/home [Verkkosivusto] [Viitattu 08.04.2018]
33. Noticebored. 2018. ISO/IEC 27001. http://www.iso27001security.com/html/27001.html [Verkkosivusto]. [Viitattu 08.04.2018]