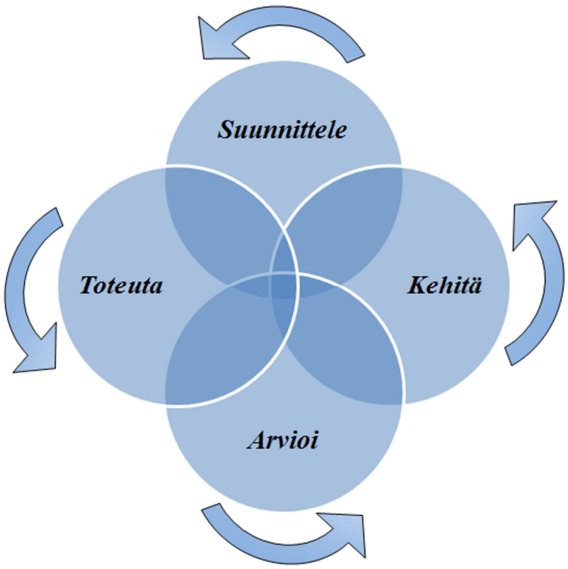
Aki Moilanen

TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

Sisältö ja kehittäminen valtionhallinnon organisaatiossa

Opinnäytetyö

Metsätalouden koulutusohjelma



KUVAILULEHTI

MIKKELIN AMMATTIKORKEAKOULU Mikkeli University of Applied Sciences	**Opinnäytetyön päivämäärä** 10.11.2012
Tekijä Aki Moilanen	**Koulutusohjelma ja suuntautuminen** Metsätalouden koulutusohjelma Metsätalous

Nimeke

Tietoturvallisuuden hallintajärjestelmä, Sisältö ja kehittäminen valtionhallinnon organisaatiossa

Tiivistelmä

Työn tavoitteena oli tutkia tietoturvan ja tietoturvallisuuden hallinnan teoriaa, yleisiä käytäntöjä, lainsäädäntöä, standardeja sekä erityisesti valtionhallinnon organisaatiolle kohdennettuja tietoturvavelvoitteita, -suosituksia ja -ohjeita.

Työn tavoitteena oli lisäksi selvittää miten valtionhallinto ohjaa alaisiaan organisaatioita tietoturvan hallintajärjestelmän sekä siihen liittyvän hallintaprosessin rakentamisessa, ylläpidossa ja kehittämisessä. Tavoitteena oli myös kuvata Suomen metsäkeskuksen tietoturvallisuuden hallinnan nykytila ja arvioida hallintajärjestelmään liittyviä kehittämistarpeita.

Työn teoreettinen tausta muodostuu lähtötilanteen viitekehyksen määrittelystä, johon sisältyvät keskeisinä osioina tietoturvallisuuden yleiset periaatteet, normiohjaus, standardit ja toimintamallit sekä tietoturvallisuuden johtaminen osana organisaatioturvallisuutta. Työssä käytetään viitekehyksenä pääasiassa valtiovarainministeriön antamia Vahti-tietoturvaohjeita sekä muita ministeriön linjauksia. Vahti-ohjeiden lisäksi työssä hyödynnetään muuta tietoturvadokumentaatiota ja -aineistoa, joka soveltuu käytettäväksi valtionhallinnon organisaation tietoturvatyössä ja joka tuo edelleen työvälineitä Suomen metsäkeskuksen tietoturvallisuuden kehittämistyöhön.

Valtionhallinnon organisaation tietoturvallisuuden hallintaa ohjaavat useat lait, asetukset, määräykset ja ohjeet, jotka sisältävät organisaatiota koskevia tietoturvavelvoitteita. Työssä selvitetään tämän kokonaisuuden hallinnan periaatteita ja miten ne viedään edelleen organisaatiota hyödyttäväksi tavoitteelliseksi tietoturvatoiminnaksi, mikä on tietoturvallisuuden hallintajärjestelmän sekä siihen liittyvän hallintaprosessin kehittämisen keskeinen päämäärä.

Työssä selvitetään tietoturvallisuuden hallintajärjestelmän sisältö, käydään läpi tarvittavat toimenpiteet tietoturvallisuuden hallintajärjestelmän luomiseksi sekä tuodaan esille hallintajärjestelmän kehittämisprosessin menetelmät tietoturvallisuuden jatkuvan toiminnan varmistamiseksi.

Työssä kuvataan Suomen metsäkeskuksen tietoturvallisuuden hallinnan nykytila ja arvioidaan tietoturvallisuuden hallintaan liittyviä kehittämistarpeita. Kehittämistarpeiden arvioinnissa otetaan huomioon Suomen metsäkeskuksen toiminnalliset tavoitteet, lainsäädäntö ja valtionhallinnon ohjaus sekä MMM:n hallinnonalalleen asettamat tavoitteet tietoturvallisuuden hallinnassa ja kehittämisessä.

Asiasanat (avainsanat)
Tieto, Tietoturvallisuus, Turvallisuusjohtaminen, Tietoturvallisuuden hallintajärjestelmä, Tietoturvallisuuden hallintaprosessi, Suomen metsäkeskus

Sivumäärä	**Kieli**	**URN**
86 s.	Suomi	URN:NBN:fi:mamk-opinn2012B6639

Ohjaavan opettajan nimi	**Opinnäytetyön toimeksiantaja**
Pasi Pakkala	Suomen metsäkeskus, Julkiset palvelut

DESCRIPTION

MIKKELIN AMMATTIKORKEAKOULU
Mikkeli University of Applied Sciences

Date of the bachelor's thesis

November 10, 2012

Author
Aki Moilanen

Degree programme and option
Degree Programme in Forestry

Name of the bachelor's thesis
Information security management system, Contents and developing in the organization of central government

Abstract

The objective of this work was to study the theory and control of information security and information security management, general practices, legislation, standards and especially information security obligations, recommendations and instructions that have been focused on the organization of central government.

The aim was also to find out how the government controls the subordinate organizations information security management system, as well as related management process building, construction, maintenance and development. The objective was furthermore to describe the present state of control of information security in Finnish Forest Centre and to estimate development needs which are related to the management system.

The theoretical background and start situation in this work consists of the definition of the frame of reference, which includes general principles of information security, norm control, standards and operation models and management of information security as a part of organization safety. Mainly the Vahti-government information security directives given by the Ministry of Finance and other definitions of policy are used as a frame of reference in the work. The work also utilize another collection of information security documentation and data which is suitable to be used in information security work of the organization of central government and which brings additional tools needed to be used in development of information security in Finnish Forest Centre.

Government organization's information security management is guided by a number of laws, regulations, orders and instructions, which include security obligations concerning the organization. This work clarifies the wholeness of management principles and how they are re-exported to benefit the organization as an objective information security activity, which is key targets for the development of information security management system, as well as the associated management process.

In the work the contents of information security management system were clarified, the necessary measures for the creation of information security management system were gone through and the methods of the developing process of management system for securing the constant operation of information security were brought out.

In the work the present state of the control of information security in Finnish Forest Centre is described and development needs which are related to the control of information security are estimated. In the evaluation of development needs of the functional objectives of Finnish Forest Centre, legislation and the control of the government and the objectives appointed by the Ministry of Agriculture and Forestry to its branch of administration were taken into consideration in the control and developing of information security.

Subject headings, (keywords)
Information, Information security, Security management, Information security management system, Information security management process, Finnish Forest Centre

Pages	**Language**	**URN**
86 p.	Finnish	URN:NBN:fi:mamk-opinn2012B6639

Tutor	**Employer of the bachelor's thesis**
Pasi Pakkala	Finnish Forest Centre, Public Services

SISÄLTÖ

1 JOHDANTO

Tietoturvatoiminnan perustana ja kivijalkana on Suomen lainsäädäntö. Valtionhallinnon organisaation tietoturvallisuuden hallintaa ohjaavat useat lait, asetukset, määräykset ja ohjeet, jotka sisältävät organisaatiota koskevia tietoturvavelvoitteita. Tämän kokonaisuuden hallinta ja vieminen organisaatiota hyödyttäväksi tavoitteelliseksi tietoturvatoiminnaksi on tietoturvallisuuden hallintajärjestelmän kehittämisen keskeisiä päämääriä.

Tämän opinnäytetyön motivaationa ja keskeisenä tavoitteena on selvittää tietoturvallisuuden hallintajärjestelmän sisältö ja kehittämisen menetelmät, ottaen huomioon vallitseva lainsäädäntö, normisto ja ohjeet sekä tietoturvallisuuden hallintaan kohdistuva valtionhallinnon ohjaus. Opinnäytetyön toimeksiantaja on Suomen metsäkeskuksen Julkiset palvelut.

Lisäksi tarve tähän työhön on osaltaan muodostunut toimeksiantajan organisaatiomuutoksen seurauksena, minkä johdosta 13 alueellista metsäkeskusta sekä osia Kehittämiskeskus Tapion toiminnoista yhdistyi vuoden 2012 alusta valtakunnalliseksi organisaatioksi, Suomen metsäkeskukseksi. Suomen metsäkeskuksen perustan muodostavat julkisia palveluja tuottava *Julkiset palvelut* ja asiakasrahoitteista palvelutoimintaa tuottava *Metsäpalvelut* (Laki Suomen metsäkeskuksesta 6.5.2011/418).

Tiedot ja tietoturvallisuus ovat ehdottomia edellytyksiä organisaation toiminnalle nykypäivän tietokeskeisessä yhteiskunnassa. Organisaation toiminnassaan ja päätöksenteossaan tarvitsemien keskeisten tietojen tulee olla saatavilla käytännössä jatkuvasti.

Mikäli toimintaympäristön tarvitsemien tietojen, tietojärjestelmien ja yhteyksien käyttö estyy, voi organisaation toiminta lamaantua täysin. Tietojen saatavuuden lisäksi täytyy huolehtia tietojen oikeellisuudesta ja luotettavuudesta sekä tietojen asianmukaisesta suojaamisesta. Organisaation tulee omaan toimintaan liittyvien tietojen salassapidon lisäksi huolehtia sidosryhmien ja erityisesti asiakkaiden tiedoista.

Organisaation tietoturvallisuustoimintaa ohjaa tietoturvallisuuden hallintajärjestelmä, joka yhdistää lainsäädännöstä, standardeista ja sopimuksista tulevat vaatimukset

(normiohjaus) yhdeksi kokonaisuudeksi. Tietoturvallisuuden hallintajärjestelmä toteuttaa organisaation strategiaa, joka kattaa tietoturvallisuuden yksityiskohtaisen organisoinnin, politiikat, suunnittelun, vastuut, menettelytavat, prosessit ja tarvittavat resurssit.

Tietoturvallisuuden hallintajärjestelmä on luonteeltaan viitekehys, joka on aina sovitettava organisaatiokohtaisesti riippuen tietoturvariskien merkityksestä ja tietoturvaasioiden kehitysvaiheesta organisaatiossa.

Valtiovarainministeriö (VM) on asettanut valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI), jonka keskeisenä tehtävänä on antaa tietoturvallisuuteen liittyviä ohjeita. Tämän toiminnan seurauksena valtionhallinnossa on pitkät perinteet tietoturvallisuuden hallinnasta osana hyvää tiedonhallintatapaa.

Tietoturvallisuuden hallintajärjestelmää ja sen olennaisimpia osia kuvataan alla olevissa Vahti-ohjeissa, jotka toimivat samalla tämän työn keskeisenä viitekehyksenä.

- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009.
- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010.
- Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007.
- Tietoturvatavoitteiden asettaminen ja mittaaminen 2006.
- Tietoturvallisuuden hallintajärjestelmän arviointisuositus 2003.

Tietoturvallisuuden hallintajärjestelmän kehittämiseen sekä yhteiskunnan tietoturvariskien hallitsemiseen ja tietoturvallisuuden kehittämiseen valtionhallinnossa vaikuttaa olennaisesti myös 1.10.2010 voimaan astunut tietoturvallisuusasetus (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681) sekä asetusta tukeva ohje (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010). Tietoturvallisuusasetuksen 23§ 3 mom. edellyttää viranomaisilta siinä kuvattujen tietoturvallisuuden perustason vaatimusten täyttämistä 30.9.2013 mennessä.

Tämän työn tavoitteena on tutkia tietoturvan ja tietoturvallisuuden hallinnan teoriaa, yleisiä käytäntöjä, lainsäädäntöä, standardeja sekä erityisesti valtionhallinnon organisaatiolle kohdennettuja tietoturvavelvoitteita, -suosituksia ja -ohjeita.

Työn keskeisenä tavoitteena on koostaa aineisto, joka antaa lukijalle selkeän kuvan valtionhallinnon organisaation tietoturvan hallinnasta sekä hallintajärjestelmän rakenteesta ja kehittämisprosessista. Tietoturvallisuuden hallintajärjestelmän kehittäminen on evoluutioprosessi, jossa organisaatiolle kehittyy valmiudet hallita systemaattisesti tietoturva-asioitaan.

Työn tavoitteena on lisäksi kuvata Suomen metsäkeskuksen tietoturvallisuuden hallinnan nykytila ja arvioida hallintajärjestelmään liittyviä kehittämistarpeita. Kehittämistarpeita arvioitaessa otetaan huomioon metsäkeskuksen toiminnalliset tavoitteet, lainsäädäntö ja valtionhallinnon ohjaus sekä MMM:n hallinnonalalleen asettamat tavoitteet tietoturvallisuuden hallinnassa ja kehittämisessä.

2 TIETOTURVALLISUUDEN MERKITYS

2.1 Tieto suojattavana kohteena

Tieto on informaatiota, jolla on arvoa ja merkitystä organisaation tavoitteiden toteutumisen kannalta. Tieto kuuluu aina jollekin, joten tiedonhallinnassa on olennaista määritellä tiedolle sekä *juridinen omistaja* sekä taho/henkilö, joka on siitä *hallinnollisessa vastuussa*. (Leppänen 2006, 66-67.)

Tiedolla on aina kohde ja se koskee aina jotakin asiaa. Se voi olla esimerkiksi laite tai tietokannassa oleva sähköinen informaatio. Tieto voi olla myös ajatus, joka on muodostunut työntekijän tietoisuuteen hänen työajallaan keräämän informaation pohjalta. (Leppänen 2006, 67.) Olennaista organisaation tiedon turvaamisessa on tiedostaa ja määritellä suojattava tieto kokonaistietomassasta.

Organisaation tulee aina määritellä ja arvioida ne asiat, jotka ovat erityisen tärkeitä toiminnan tavoitteiden saavuttamiseksi. Nämä kohteet ovat myös *suojattavia kohteita*,

joiden vahingoittumattomuuden varmistamiseen turvallisuus- ja riskienhallinta-toimenpiteet kohdistuvat. (Leppänen 2006, 61.)

Suojattavat kohteet voidaan määritellä sekä *organisatorisesta* että *riskinäkökulmasta*. Organisatorisesta näkökulmasta tarkasteltuna valinnat tehdään organisaatiokaavion, prosessimallien, omaisuusluettelon ja muiden organisaation tavoitteiden toteuttamiseksi valittujen toimintojen mukaisesti. Riskinäkökulmassa tarkastellaan suojattavaa kohdetta riskien näkökulmasta. (Leppänen 2006, 61-62.)

Jotta suojattavien kohteiden listaaminen vastaa muuta hallinnointi- ja raportointikäytäntöä, tulee ensimmäinen jaottelu tehdä organisaation näkökulmasta. Toisessa vaiheessa arvioidaan mitkä *tietoriskit* koskevat suojattavaa kohdetta ja kuinka vahingoittumattomana suojattavan kohteen täytyy säilyä. (Leppänen 2006, 64.)

Tiedon kohde on suojattava asia, jota esimerkiksi tietoturvamenetelmät suojaavat. Osaaminen voidaan suojata mm. sopimuksilla ja fyysinen tietomateriaali fyysisillä keinovalikoimilla. Suojattavana kohteena tieto on aina määriteltävä, sillä tiedon määrittelyn perusteella kehitetään turvallisuustoimenpiteet, joiden avulla varmennetaan tiedon turvallinen hyödyntäminen organisaation käyttöön. (Leppänen 2006, 67.)

Kaikki tieto ei voi olla tärkeää ja kuulua johonkin suojattavaan kohteeseen. Tämä on mahdotonta olemassa olevan tietomäärän vuoksi. Sellainen tieto, joka on organisaation toiminnan kannalta kriittistä ja joka täytyy suojata, voidaan määritellä *tietoturvallisuusluokituksen* avulla. Tällainen tieto on siis oltava tietyltä osin tai kokonaan vahingoittumatonta. (Leppänen 2006, 68.)

Organisaation *tietoresurssien* kautta voidaan jaotella suojattavat tiedot. Tietoresurssit muodostuvat henkisestä, organisatorisesta sekä asiakkaiden ja suhteiden pääomista. Suojattavia tietoja voidaan tarkastella esimerkiksi alla olevien tietoresurssien kautta. (Leppänen 2006, 68.)

- henkinen pääoma
- tietämys
- taidot

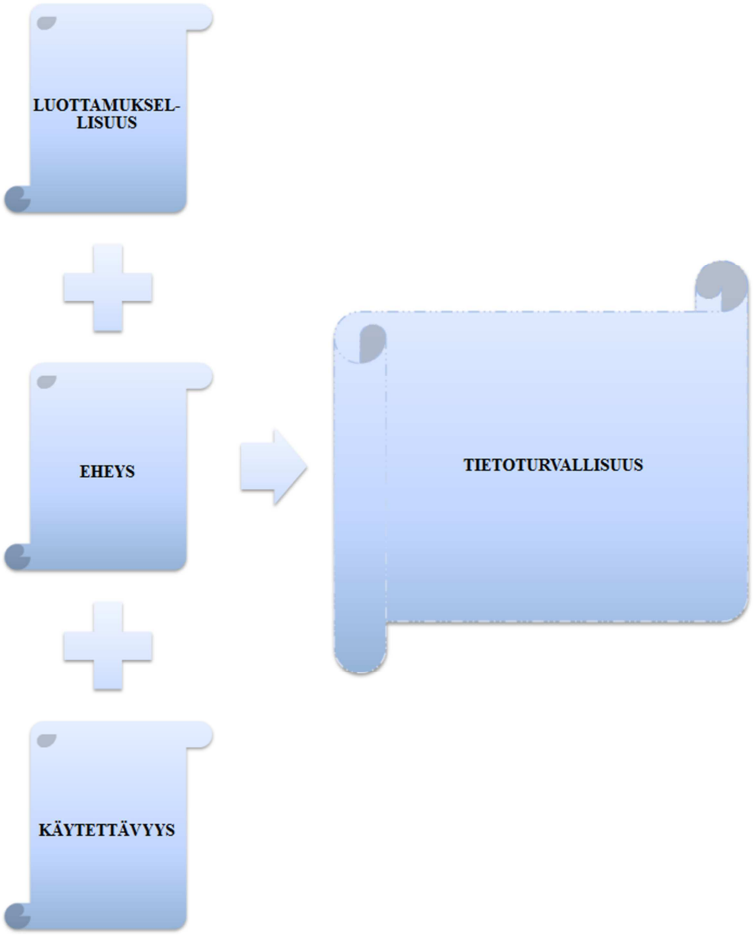
- motivaatio
- tehtävien hallinta
- organisatorinen pääoma
- liiketoimintaprosessin pääoma
- tietovirta
- tuotteiden ja palveluiden virta
- kassavirta
- yhteistyömuodot
- strateginen prosessi
- liiketoiminnan kehitys- ja uudistamispääoma
- erikoistuminen
- tuotantoprosessi
- uudet konseptit
- myynti ja markkinointi
- uudet yhteistyömuodot
- asiakkaat ja suhteiden pääoma
- asiakassuhteet
- sijoittajasuhteet
- tavaran hankkijoiden ja toimittajien suhteet
- yhteistyökumppaneiden suhteet

2.2 Tietoturvan määritelmä ja tietosuoja

Tietoturvallisuudella tarkoitetaan tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 13).

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010, 3 § 2 mom. määrittelee kyseisessä asetuksessa tietoturvallisuudella tarkoitettavan tietojen *salassapitovelvollisuuden* ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä.

Perinteisesti tietoturvallisuudella ymmärretään tiedon perusominaisuuksien (kuva 1.); *luottamuksellisuuden*, *eheyden* ja *käytettävyyden* turvaamista. Tietosuoja ja tietoturva ovat kaksi eri asiaa, vaikka niillä on yhteisiä piirteitä. Lisäksi niiden erottaminen käytännössä ei ole helppoa. (Laaksonen ym. 2006, 17.)



Kuva 1. Tiedon perusominaisuuksien turvaaminen.

Tietosuojalla suojataan erityisesti ihmisen yksityisyyttä sekä tiedollista itsemääräämisoikeutta (Laaksonen ym. 2006, 17). Tietosuojalla tarkoitetaan henkilötietojen suojaamista valtuudettomalta ja henkilöä vahingoittavalta käytöltä ja käsittelemiseltä. Tietosuojatoimien tavoitteena on tietojen valtuudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen. Tietosuoja on yksilön suojaa. (Tammisalo 2005, 6.)

Tietosuojaan kuuluvat ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Tietoturvallisuuden vaarantuessa vaarantuu myös tietosuoja. Henkilötietolaki (523/1999) edellyttää henkilötietojen käsittelyn suunnittelua

sekä hyvää *tietojenkäsittelytapaa*, johon sisältyvät henkilötietojen käsittelyä, tietojen laatua, arkaluonteisten henkilötietojen käsittelyä sekä tietoturvallisuutta koskevat periaatteet. Tällä perusteella tietojenkäsittelytapaa voidaan pitää osana hyvää *tiedonhallintatapaa*. Hyvän tiedonhallintatavan näkökulmasta tärkeää on henkilötietojen suojaaminen, henkilötietojen käsittelyn etukäteissuunnittelu, säilytysarvon määrittely sekä tarpeettomaksi käyneiden henkilötietojen hävittäminen. (Asianhallinnan tietoturvallisuutta koskeva ohje 2006, 36.)

Tietoturva tarjoaa erilaisia keinoja tai toimintamalleja tietosuojan ylläpitämiseen, eli sillä ikään kuin rakennetaan muuri suojattavan tiedon ympärille. Organisaation on kehitettävä ja hallinnoitava samanaikaisesti sekä tietoturvallisuutta että tietosuojaa, joten kokonaisuuden kannalta on olennaista tietää myös tietosuojaa koskevat perusasiat. (Laaksonen ym. 2006, 17.)

2.3 Tietoturvallisuuden perusulottuvuudet

Tietoturvallisuus -käsitettä voidaan tarkastella esimerkiksi ISO/IEC 27001 -standardin (2005, 12) kautta, jonka mukaan tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttämistä. Lisäksi standardissa todetaan, että tähän voi sisältyä myös muita ominaisuuksia, kuten *aitous, vastuullisuus, kiistämättömyys ja luotettavuus.*

Tietojen *luottamuksellisuus* täytyy taata; tietoja käyttävillä henkilöillä on oltava valtuudet käyttää tietoja. On myös määriteltävä, millaisin valtuuksin kukin käyttäjä tietoja käsittelee. Tämä edellyttää tietojen luokittelua, henkilöiden tunnistamista, todennusta ja valtuuksien määrittelyä sekä käsittelytapojen ja -sääntöjen määrittelyä. Henkilöiden tunnistaminen ja todennus tietojärjestelmien käytön yhteydessä voidaan toteuttaa lukuisilla eri menetelmillä, joista osa noudattaa heikkoja tai erittäin heikkoja tunnistamismenetelmiä (ryhmäkohtaiset tunnukset ja salasanat) ja osa vahvaa tunnistamista (toimikorttipohjainen todentaminen). Valtuudet ja oikeudet on tyypillisesti määritelty tietojärjestelmään. Erilaisia tietojen käsittelytapoja ovat esimerkiksi oikeus luoda, muuttaa tai tuhota asiakirja. (Tammisalo 2005, 8.)

Tietojen, joita käytetään, on oltava *eheitä* ja *oikeellisia.* Tiedot eivät saa olla vahingossa muuttuneet esimerkiksi ohjelmiston, tietokannan tai järjestelmän vioittumisen tai korruptoitumisen vuoksi. Tiedot eivät saa myöskään olla alttiina väärentämiselle. Tietojen eheyden rikkoutuminen on yleensä erittäin vaikeasti havaittavaa ja aiheuttaa mahdollisesti suuria haittavaikutuksia. Tästä syystä tietojen eheyden rikkoutuminen katsotaan usein yhdeksi vakavimmista tietoturvaloukkauksista. (Tammisalo 2005, 8.)

Käytettävyydellä (saatavuudella) tarkoitetaan, että tiedot ovat saatavissa silloin, kun niitä tarvitaan ja siellä, missä niitä tarvitaan. Jotta tiedot olisivat saatavilla, on tietojärjestelmien toimintakuntoisuus ja saavutettavuus turvattava. Toimintahäiriöihin voi varautua rakentamalla erilaisia turvamekanismeja, jotka estävät tietoturvaloukkauksia. Vika- tai ylikuormitustilanteista on kyettävä toipumaan mm. erilaisilla varajärjestelyillä, kahdennetuilla varajärjestelmillä, ohjelmilla ja varmistuskäytännöillä. (Tammisalo 2005, 7.)

Termiä *käytettävyys* käytetään usein synonyyminä *saatavuudelle*; tiedot ovat saatavissa eli käytettävissä. Käytettävyydellä tarkoitetaan myös *käyttökelpoisuutta* eli tietojen on oltava tallennettuina sellaisessa muodossa, että ne ovat yksiselitteisesti sekä luettavissa että ymmärrettävissä. Tällöin ei esimerkiksi muodostu turvariskiä sille, että tietojen tallennusformaatti olisi vanhentunut ja tiedot käyttökelvottomia eikä myös sille, että tietojen vaikea muoto voisi aiheuttaa virhetulkinnan. (Tammisalo 2005, 8.)

Usein tietojen olemassaoloon kytketään myös tekijä ja tekoaika, jolloin tietojen *aitous* ja *alkuperäisyys* voidaan tunnistaa. On olemassa menetelmiä, joilla asiakirjan tekijä voidaan *kiistämättömästi* todentaa ja joilla tietoihin voidaan liittää tekoajan tai muuttumishetken aikaleima. Teknisesti puhuttaessa tällaista menetelmää kuvataan usein termillä *sähköinen allekirjoitus*. Tietojärjestelmien sisäiseen tietojen käsittelyyn ja järjestelmien väliseen tietojen siirtoon on olemassa menetelmiä, joilla tietojärjestelmät ylläpitävät tietojen eheyttä ja tarkastavat käytettävien tietojen oikeellisuuden automaattisesti. Tekninen termi tällaiselle menetelmälle on *järjestelmäallekirjoitus* tai *organisaatioallekirjoitus*. Puhuttaessa sähköisestä allekirjoituksesta on yleensä syytä erottaa, tarkoitetaanko sähköistä allekirjoitusta sen teknisessä vai juridisessa merkityksessä. (Tammisalo 2005, 8.)

Tietojen käytön yhteydessä puhutaan myös *jäljitettävyydestä, tarkastettavuudesta* ja *tilivelvollisuudesta*. Näillä tarkoitetaan kaikkien tietojärjestelmässä tapahtuvien toimien kirjaamista, järjestelmien tietojen käytön seurantaa sekä valvontaa. Kaikista käyttäjien toimista ja järjestelmän automaattisesti suorittamista toimista täytyy jäädä sellainen tieto järjestelmään, että tilanteen myöhempi toteaminen on mahdollista. On rakennettava sopivat kontrollit tietojärjestelmien toiminnan turvallisuuden seurantaan sekä ohjelmistojen, laitteistojen että tietoliikenteen osalta. Vastaavasti, samanlaiset kontrollit on rakennettava käyttäjien toiminnan seurantaan. Kontrollit tukevat organisaation tietoturvasta vastaavien henkilöiden toimintaa ja ylläpitävät organisaatioiden prosesseissa käytettävien tietojen turvallisuutta. (Tammisalo 2005, 8.)

2.4 Tiedon turvaamisen merkitys

Organisaatiot ovat entistä haavoittuvampia tietoturvallisuutta uhkaaville tekijöille, sillä ne ovat yhä riippuvampia tietojärjestelmistä ja niiden avulla tarjottavista palveluista. Lisäksi julkisten ja yksityisten verkkojen yhdistäminen, hajautetun tietojenkäsittelyn yleistyminen sekä palveluiden ulkoistaminen ovat heikentäneet organisaatioiden mahdollisuuksia valvoa tehokkaasti tietoturvallisuuttaan. Organisaatiot ovat myös joutuneet hyväksymään sen, että monia tietojärjestelmiä ei ole suunniteltu turvallisiksi. (Suominen 2003, 79.)

Tekniikalla saavutetulla turvallisuudella on aina rajansa ja teknisiä ratkaisuja on tuettava erilaisilla *hallinnollisilla toimenpiteillä*. Näitä voivat olla esimerkiksi organisaation toimintatapojen muuttaminen, turvaohjeistuksen laatiminen, motivoivan koulutuksen järjestäminen ja toiminnan vakuuttaminen. (Suominen 2003, 79.)

Organisaatioiden toiminta ja päätöksenteko perustuvat tietoon, joka on entistä yksityiskohtaisempaa ja jota käsitellään prosesseissa sekä tallennetaan tietojärjestelmiin yhä enemmän. Tämä tieto on suurimmaksi osaksi *sähköisessä muodossa* ja se luodaan suoraan *sähköisiin järjestelmiin*, jolloin tietoja ei välttämättä ole olemassa paperimuodossa, vaan kaikki käsittely, säilytys ja arkistointi hoidetaan sähköisesti. (Tammisalo 2005, 6 - 7.)

Sähköinen tieto on paperilla olevaa tietoa alttiimpaa erilaisille tietoturvaloukkauksille. Tietoon voi päästä käsiksi ajasta ja paikasta riippumatta; maantieteellisellä etäisyydellä ei ole merkitystä verkossa tapahtuvaan tietojen hakkerointiin. Kaikki tieto on saavutettavissa ja kopioitavissa murto-osassa siitä ajasta, mikä kuluisi paperidokumenttien läpikäymiseen. Erilaiset vika- ja häiriötilanteet, kuten tietoliikenteen häiriöt ja tietojärjestelmien vioittuminen, voivat estää kaikkien tietojen käytön ja pahimmassa tapauksessa lamauttaa koko organisaation toiminnan. (Tammisalo 2005, 6 - 7.)

Tietojen sähkömuotoisuus asettaa mittavat vaatimukset turvallisuudelle. Toisaalta sähkömuotoisuus ja tietojärjestelmien hyödyntäminen tekevät mahdolliseksi monipuolisen ja varman käytön seurannan, valvonnan ja käyttäjien valtuuksien määrittelyn. Valtuudettomalta käyttäjältä estetään pääsy kaikkiin niihin tietoihin, joihin hänelle ei ole nimenomaisesti määritelty pääsyoikeuksia. Seuranta ja poikkeustilanteiden valvonta voidaan toteuttaa reaaliaikaisesti, jolloin ajantasaiset hälytykset esimerkiksi turvaloukkauksista ja virhetilanteista aikaansaavat erittäin nopean korjauksen ja paluun normaalitilanteeseen. (Tammisalo 2005, 7.)

Tietoturvallisuutta ja sen vaarantavia tekijöitä on tutkittu runsaasti. Yleisesti voidaan todeta, että *ihmisen toiminta*, joko tahallinen tai tahaton, on suurin yksittäinen turvallisuuden vaarantava tekijä. Eri organisaatioihin tehdyt kyselytutkimukset ovat myös osoittaneet, että suurin osa organisaatioista ei ole varautunut vakaviin riskeihin ja sellaisen kohdatessa vaikutus organisaation toimintaan on lamauttava ja vakavia seurauksia aiheuttava, olipa riski sitten ihmisen toiminnasta tai esimerkiksi teknisestä viasta aiheutuva. (Tammisalo 2005, 7.)

Tietoturvallisuus ja tietojen suojaaminen on muodostumassa yhteiskunnassamme yhä tärkeämmäksi osaksi myös viranomaisten toimintaa. Vaikka viranomaisten toiminta on julkista, ne käsittelevät toimissaan ja päätöksenteossaan usein salaista tai arkaluonteista tietoa, joka on suojattava asianmukaisesti. Toisaalta on myös välttämätöntä, että tietyt viranomaisen tarvitsemat tiedot ovat aina käytettävissä ja että tiedot ovat oikeellisia. (Tammisalo 2005, 7.)

Tiedon suojaamista on myös julkisen tiedon suojaaminen siten, että se on jokaisen saatavilla silloin, kun tiedon käytölle ilmenee tarpeita. Julkisen tiedon suojaaminen on

tosiallista toimintaa, joka luo tiedolle luottamuksellisuuden. Tiedon suojaamisella ei pyritä pelkästään luottamuksellisuuden säilyttämiseen vaan tiedon suojaaminen on myös sidoksissa tiedon eheyden säilyttämiseen sekä käytettävyyden varmistamiseen. (Voutilainen 2012, 120.)

Julkisen sekä salaisen ja arkaluonteisen tiedon käsittelyssä sekä tiedon luokittelussa tulee huomioida erityisesti *julkisuuslain;* Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621 sekä Valtioneuvoston 1.7.2010 julkisuuslain nojalla antaman *tietoturvallisuusasetuksen;* Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681) velvoitteet.

Julkisuuslain 18 §:n 4 kohdan mukaan asiakirjojen ja rekisterien tietorakenteet tulee suunnitella tietosisältöjen julkisuus maksimoiden siten, ettei julkisilla osilla paljasteta laissa salassa pidettäväksi säädettyjä tietoja. Tämän vuoksi viranomaisen tulee suunnitella asiakirjojensa laadinta ottaen huomioon *asiakirjan tietosisällön luonne*. Mikäli asiakirjaan sisältyy sekä julkisia että salassa pidettäviä tietoja, tulee ne pystyä erottelemaan helposti tiedonsaannin varmistamiseksi. (Voutilainen 2012, 113.)

Tietoturva-asetuksen 8§:ssä linjataan hyvän julkisuus- ja salassapitorakenteen ydinsisältö. Viranomaisen on arvioitava *asiakirjakohtaisesti* siinä olevien tietojen luonne sekä asiakirjan eri osien luonne tiedonsaantia koskevien rajoitusten kannalta. (Voutilainen 2012, 114.)

Valtionhallinnon tiedot, tietojärjestelmät ja palvelut ovat suomalaiselle yhteiskunnalle välttämättömiä, taloudellisesti korvaamattomia ja valtakunnan turvallisuuden ja toimintojen kannalta elintärkeitä. Tämän kokonaisuuden toimivuus edellyttää *riittävän tietoturvallisuuden tason varmistamista*. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 13.)

Turvallisuudessa ilmenevät puutteet vaikuttavat koko organisaation toimintaedellytyksiin. Toiminnan häiriintyminen tai suoranainen lamaantuminen, tietovuodot ja erilaiset muut häiriötekijät vievät organisaatiolta uskottavuutta ja voivat johtaa vakaviin ongelmiin, jotka estävät tuloksellisen toiminnan. Tietoturvallisuuden puutteet verkottuneessa yhteiskunnassa johtavat helposti myös organisaation asiakkaiden ja yhteistyö-

organisaatioiden toiminnan vaarantumiseen. Lisäksi kansalaisten luottamus hallintoon saattaa kärsiä toistuvien tietoturvaongelmien myötä. Ongelmat voivat johtaa myös juridisiin vastuisiin, koska organisaatiot ovat yhä enemmän vastuussa myös *sidosryhmiensä tietoturvallisuudesta*. (Tietoturvallisuus ja tulosohjaus 2004, 9.)

Nousevana haasteena on kehittää menettelytavat ja organisaatio, joka pystyy toimimaan uhkia kohtaan ennaltaehkäisevästi. Erityishaasteita aiheuttaa se, että tietoturvallisuus ei ole ainoastaan oman organisaation asia vaan myös alihankkijat ja yhteistyökumppanit ovat merkittävässä roolissa. (Karsisto 2007, s. 1)

Organisaation johdon täytyy päättää, minkä tasoista tietoturvaa se tarvitsee toimintansa tueksi ja mitä siitä ollaan valmiita maksamaan. Turvallisuusvaatimusten tunnistamisen apuna on Suomisen (2003, 83) mukaan kolme pääasiallista lähdettä:

1. Tietoriskien kartoitus, jossa tunnistetaan uhkat sekä arvioidaan uhkan toteutumisen todennäköisyys ja uhkan toteutumista seuraavat vahingot.
2. Lait, asetukset ja sopimukset, jotka velvoittavat organisaatiota.
3. Tietojenkäsittelyyn liittyvät periaatteet, jotka organisaatio on määritellyt toimintansa tueksi.

3 TIETOTURVALLISUUDEN OSA-ALUEET

3.1 Tietoturvallisuuden jaottelun periaatteet

Tietoturvallisuus on käsitteenä laaja kokonaisuus, josta on esitetty lukuisia määrittelyjä, riippuen tarkasteltavasta turvallisuuden osa-alueesta. Tietoturvallisuus ei koske käsitteenä vain teknisiä ratkaisuja, kuten laitteita ja ohjelmia, vaan siihen kuuluu keskeisesti myös ihmisten toimintaan ja turvatoiminnan yleisiin järjestelyihin liittyvät turvallisuustekijät. Tietoturvallisuuden vaikutukset ulottuvat koko organisaation toimintaan, kuten tuottavuuteen, taloudellisuuteen ja palvelujen laatuun. (Tietoturvallisuus ja tulosohjaus 2004, 15.)

Tiedot ja niiden käyttö liittyvät läheisesti organisaation kaikkiin toimintoihin ja osa-alueisiin. Riippuu organisaatiosta itsestään, mitä tietoturvan osa-aluetta se haluaa painottaa. Jakamalla tietoturva pienempiin osiin on kokonaisuuden käsitteleminen ja mahdollisten riskien tunnistaminen helpompaa. Jaottelun avulla pyritään saamaan kokonaisvaltainen kuva tietoturvasta sekä varmistetaan, ettei mitään osa-aluetta jätetä pois. (Suominen 2003, s. 82)

Tietoturvan osa-alueet ja niiden määritelmät vaihtelevat jonkin verran, riippuen mitä standardia tai viitekehystä käytetään. Yleisesti sovellettavia kansainvälisiä standardeja ovat brittiläistä alkuperää oleva BS7799, joka nykyään tunnetaan ISO27001 ja ISO27002 standardeina. Lisäksi on Internetistä ISF:n sivustolta saatavilla kansainvälisen Information Security Forumin ”Hyvien tietoturvakäytäntöjen standardi” (Information Security Forum 2007).

Tietoturvallisuuden osa-alueita on käsitelty esimerkiksi Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, Tietoturvallisuus ja tulosohjaus 2004 sekä Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007 -ohjeissa. Tietoturvallisuuden johtaminen ja hallinta on Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan (2007, 23 - 78) mukaan luokiteltu osa-alueisiin seuraavasti.

- hallinnollinen turvallisuus
- tietoturvallisuuden organisointi
- tietoaineistoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikennepalveluiden turvallisuus
- laitteistoturvallisuus
- käyttöturvallisuus
- ohjelmisto ja ohjelmistokehityksen turvallisuus
- jatkuvuuden ja erityistilanteiden hallinta

3.2 Hallinnollinen turvallisuus

Organisaation tietoturvatoiminnan lähtökohta ja *tietoturvallisuuden johtamistoiminto* on *hallinnollinen tietoturvallisuus*, joka muodostuu johdon hyväksymistä periaatteista, vastuunjaosta, tarkoitukseen varatuista resursseista sekä riskien arvioinnista. Varsinaiset toimenpiteet perustuvat hallinnollisiin ohjeisiin, joiden pohjana toimivat johdon määrittelemät periaatteet. Ilman kunnollisia tietoturvaperiaatteiden luomista, hallinnointia ja suunnittelua turvallisuusjärjestelyt voivat sisältää suuria puutteita tai ne voivat suuntautua vääriin asioihin. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 39.)

Hallinnollisen turvallisuuden kautta huolehditaan organisaation kokonaisriskienhallinnasta, jonka yhtenä osa-alueena on tietoturvallisuuden hallinta. Organisaation tietoturvallisuutta ohjataan riskienhallinta- ja tietoturvapolitiikan, tietoturvallisuuden johtamisen sekä laadun arvioinnin ja seurannan menetelmillä. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 23.)

Riskienhallintapolitiikka jäsentää hallinnan kokonaisuutta ja luo suuntaviivoja sen hoitamiseen ja kehittämiseen. Riskienhallintapolitiikan avulla riskienhallinta kytketään osaksi johtamisjärjestelmää ja sen vuosittaista aikataulutusta. Riskienhallintapolitiikka on organisaation ylimmän johdon hyväksymä ja sen lähtökohtana ovat säädökset ja ministeriöiden ohjeet. Johto määrittelee myös riskienhallinnan kattavuuden, vastuut ja sisäisen organisoinnin. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 24.)

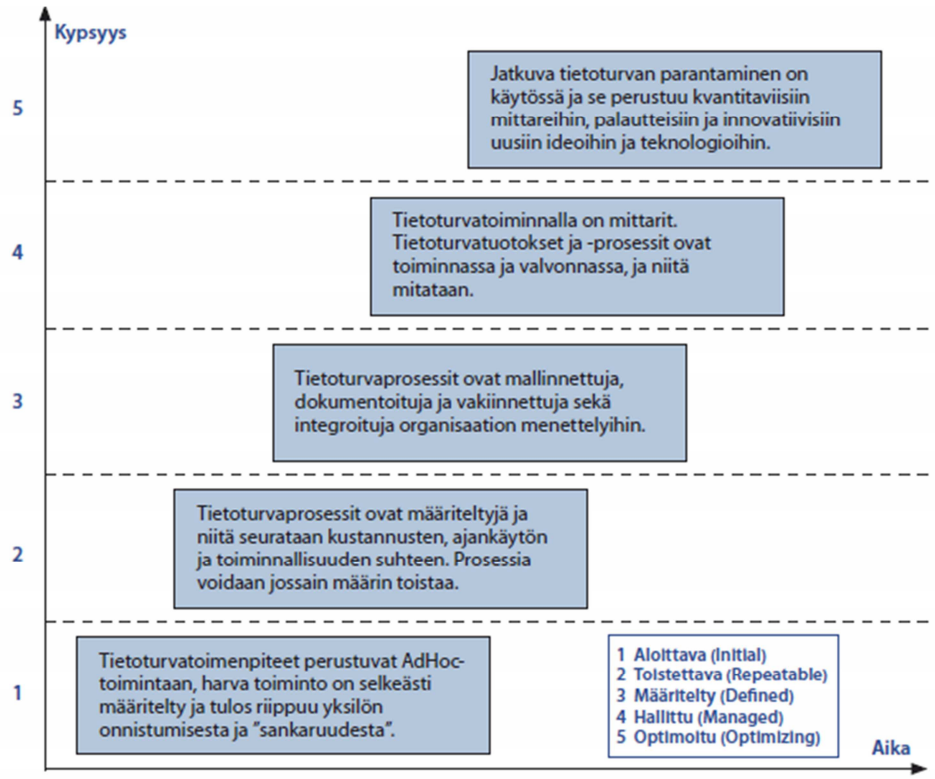
Tietoturvapolitiikan avulla johto määrittelee tietoturvatoiminnan tavoitteet, vastuut ja toimintalinjat. Tietoturvallisuuden merkityksen ja tietoturvatyön yleisperiaatteiden määrittely, dokumentointi ja viestintä jokaiselle organisaation työntekijälle on välttämätön perusta tietoturvakulttuurin luomiselle. Tietoturvapolitiikka toimii perustana, jonka varaan erilaiset tietoturvasuunnitelmat ja -ohjeistukset rakentuvat. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 25.)

Tietoturvallisuuden johtamisen perustana on ajantasainen tietoturvapolitiikka. Tietoturvallisuuden johtaminen on järjestettävä siten, että asetetut tavoitteet ovat oikeassa

suhteessa organisaation kokonaisturvallisuuteen ja tukevat eri strategioissa olevia turvallisuustavoitteita. Organisaatiossa tietoturvatoiminta ilmenee mm. säännöllisinä riskien arviointi- ja hallintatoimenpiteinä, uusien järjestelmien tietoturvatason määrittämisenä ja siitä huolehtimisena järjestelmän koko elinkaaren ajan. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 28.)

3.3 Tietoturvallisuuden organisointi

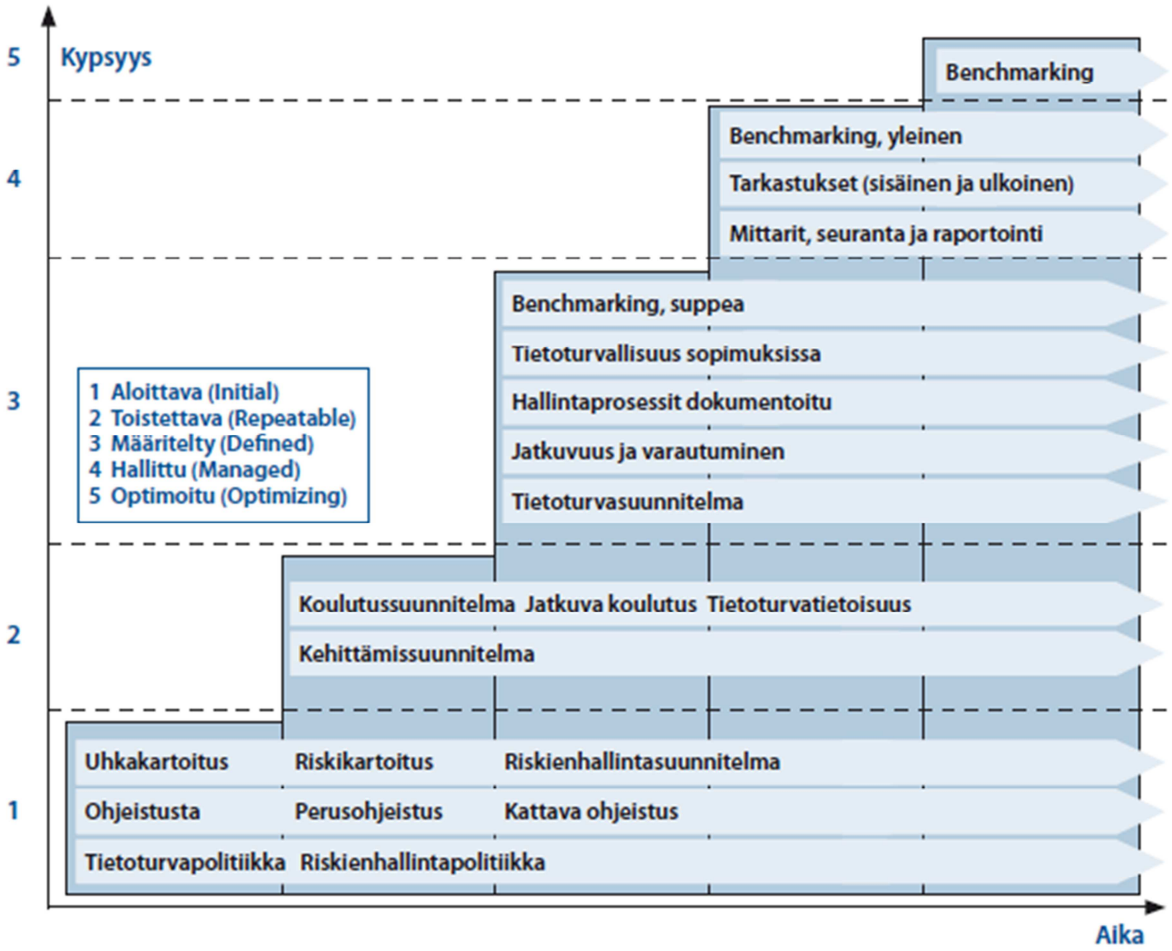
Tietoturvallisuus tulee sisällyttää osaksi *organisaation toimintaprosesseja*, jotta se toteutuisi käytännön toiminnassa. Sen sulauttaminen toimintaprosesseihin vaatii hyvää yhteistyötä tietoturvajohdolta, tietoturvallisuudesta vastaavasta operatiiviselta henkilöstöltä, palvelun omistajilta sekä sen tuottajilta. Turvallisuutta lisäävät toimenpiteet huomioidaan jo prosesseja suunniteltaessa, jotta turvallisuusvaatimukset täyttyvät. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 37.)



Kuva 2. Tietoturvallisuuden kypsyystasot (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 38).

Turvallisia prosesseja ylläpidettäessä ja kehitettäessä huomioidaan lisäksi organisaation prosesseille tavoitteeksi asetettu kypsyystaso (kuva 2) ja sen asettamat reunaehdot kehitykselle.

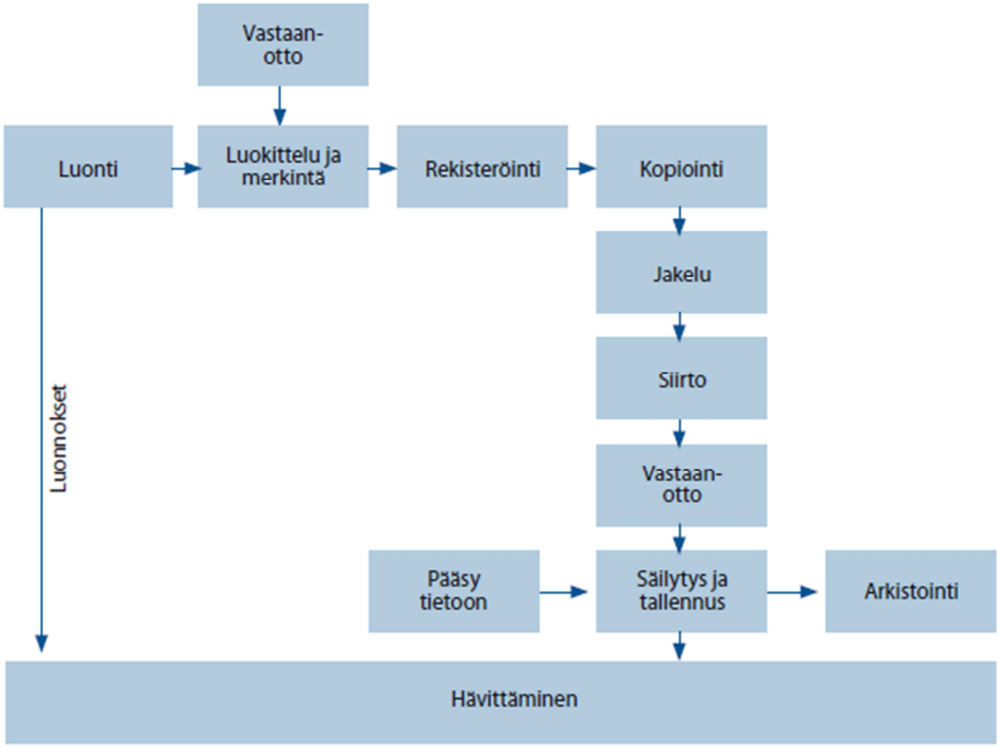
Kuvassa 3 on malli kypsyysajattelun soveltamisesta organisaation tietoturvallisuuden hallintajärjestelmän kehittämisessä. Kypsyysmallin avulla voidaan määritellä organisaation tietoturvatoiminnan nykytila ja asettaa sen kehittämiselle tavoitetaso, joka toteuttaa organisaation tietoturvallisuudelle linjatut vaatimukset. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 43.)



Kuva 3. Kypsyysajattelun soveltaminen tietoturvallisuuden hallintajärjestelmän kehittämisessä. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 42).

3.4 Tietoaineistoturvallisuus

Tietoaineistoturvallisuudessa on kyse eri talletusmuodoissa olevien tietojen suojauksesta. Se koskee paperiasiakirjoja, optisia ja magneettisia muistivälineitä, mikrofilmiä, äänitteitä sekä muita vastaavia teknisiä laitteita. Tietoaineistoturvallisuuden osa-alueessa keskitytään eri tallennusmuodoissa olevan tiedon järjestelmälliseen hallintaan läpi sen elinkaaren (kuva 4.), eli tietoaineistoturvallisuus kattaa käsittelysäännöt tietoaineiston synnystä sen tuhoamiseen asti. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 55.)



Kuva 4. Tietoaineiston elinkaari (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 55).

Tietoaineiston käsittelystä tarvitaan organisaatiokohtaiset ohjeet. Viranomaisen on huomioitava erityisesti laki viranomaisen toiminnan julkisuudesta (21.5.1999/621) ja sen nojalla annettu asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (12.11.1999/1030). Organisaation johto vastaa henkilöstön perehdyttämisestä tietoaineistojen käsittelyohjeisiin. Tietoaineistojen tietoturvallisuuden varmistaminen koskee koko henkilöstöä ja tietoaineiston koko elinkaarta. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 55.)

Viranomaisella tulee olla ajantasainen, kaikki tietoaineistot kattava arkistonmuodostussuunnitelma, josta ilmenee tietoaineiston käsittelysäännöt sekä eheyden ja käytettävyyden varmistaminen aineiston elinkaaren eri vaiheissa. Luokitellun tiedon käsittelyssä huomioidaan ko. turvaluokan edellyttämät suojaustoimenpiteet. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 55.)

3.5 Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöstöstä johtuvaa riskien hallintaa. Henkilöstöturvallisuuden perustana on osaava ja sitoutunut henkilöstö, jolle tietoturvavastuut ja -tehtävät on selkeästi kuvattu toimenkuvissa. Lisäksi tarvitaan riittävällä tasolla määriteltynä olevat henkilöstöhallinnon prosessit sekä muut prosessit, joissa kuvataan työtehtävät niin tarkasti, että *avainhenkilöriskien* syntyminen vältetään. Avainhenkilöriskien hallinnassa tunnistetaan toiminnan kannalta keskeiset avainhenkilöt sekä varmistetaan heidän käytettävyytensä organisaation palveluksessa eri tilanteissa. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 57.)

Henkilöstöturvallisuuden merkitys tietojen turvaamiselle on keskeinen. Haasteena henkilöstöturvallisuuden alueella on ihminen. Henkilöstö käsittelee tietoja vastaanottamalla, muokkaamalla, tallentamalla ja välittämällä niitä läpi prosessin. Varsinaisen käsittelyn päätyttyä henkilöstö huolehtii myös tiedon arkistoinnista tai tuhoamisesta. Lisäksi henkilöstöllä on keskeinen rooli tietovarastojen ja -järjestelmien ylläpidossa. (Tärkein tekijä on ihminen 2008, 12.)

Henkilöstöturvallisuus sisältää kaksi toisistaan riippuvaista vaatimusta; *käytettävyysvaatimus ja tietojen eheysvaatimus sekä salassapitovaatimus.* Kuvassa 5 havainnollistetaan tiedon suojauksen ja tiedon saannin turvaamisen haastetta.

Keskeisiä henkilöstöturvallisuuden alueella huomioitavia asioita ovat myös työhönottoon, toimenkuvien olennaisiin muutoksiin ja palvelussuhteen loppumiseen liittyvät prosessit ja niistä on tarpeen olla kaikilla osallisilla käytössään sovittu toimintamalli. Tehtävien vaativuudesta tai luottamuksellisuudesta riippuen rekrytoitavan henkilön

tausta, sopivuus ja osaaminen on selvitettävä ennen työhönottoa. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 57.)

Kuva 5. Henkilöstöturvallisuuden haaste on suojata tietoa ja turvata sen saanti (Tärkein tekijä on ihminen 2008, 12).

3.6 Fyysinen turvallisuus

Fyysisen turvallisuuden tarkoituksena on turvata organisaatioiden häiriötön toiminta kaikissa olosuhteissa, niiden erityistarpeet ja riskit huomioon ottaen. Kukin organisaatio vastaa itse fyysisestä suojauksestaan. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 59.)

Tähän tietoturvallisuuden osa-alueeseen kuuluvat mm. kulunvalvonta, kameravalvonta, muu tekninen valvonta ja vartiointi sekä palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta. Vähimmäisvaatimukset tilaturvallisuutta lisääville toimille ja järjestelmille määräytyvät turvallisuustarpeiden perusteella, jotka voi kohdistua alueeseen, rakennukseen, tilaryhmään tai tilaan. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 59.)

3.7 Tietoliikennepalveluiden turvallisuus

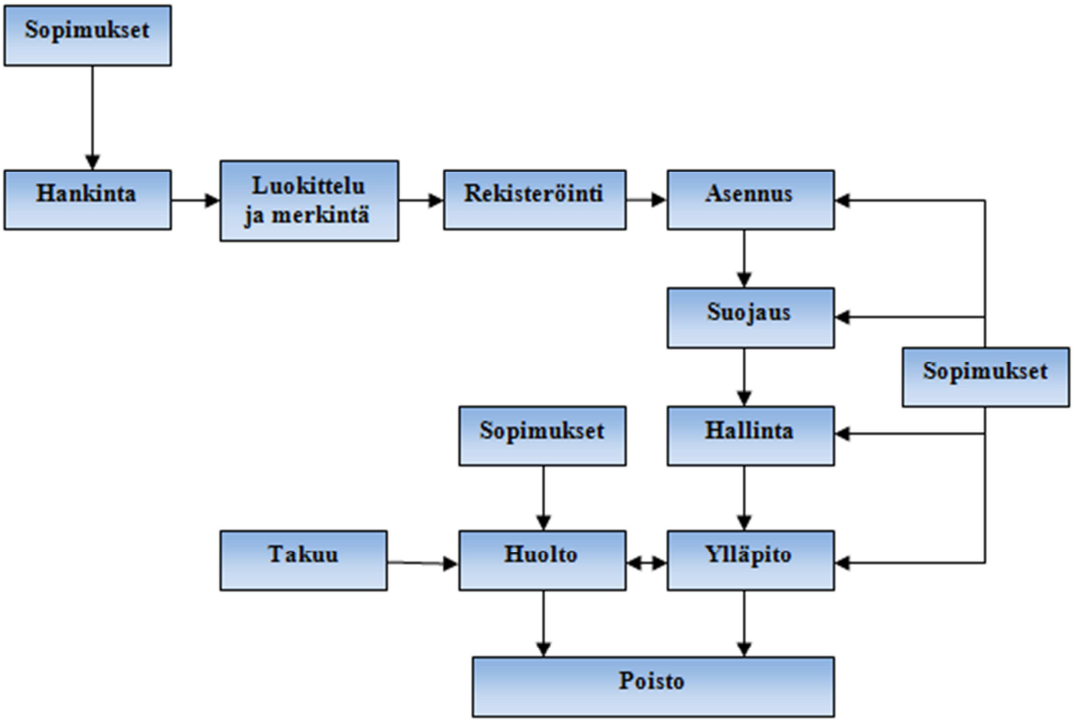
Organisaation *tietoliikennetoiminnot* ja niitä toteuttavat eri verkkojärjestelmät suunnitellaan ja rakennetaan hyvän tiedonhallintatavan mukaisesti siten, että valittu arkkitehtuuri tukee varautumista erilaisia uhkia vastaan. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 61.)

Tietoliikennepalveluiden turvallisuuteen sisältyvät mm. tietoliikennelaitteiston kokoonpano, luettelointi, ylläpito ja muutosten valvonta, ongelmatilanteiden kirjaus, käytön valvonta, verkon hallinta, viestinnän salaus ja varmistaminen, merkittävien tietoturvapoikkeamien tarkkailu, kirjaus ja selvittäminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 61.)

3.8 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 63.)

Laitteistoturvallisuudella turvataan laitteiston elinkaarta (kuva 6.), johon myös kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa. (Tietoturvallisuudella tuloksia / yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 63.)

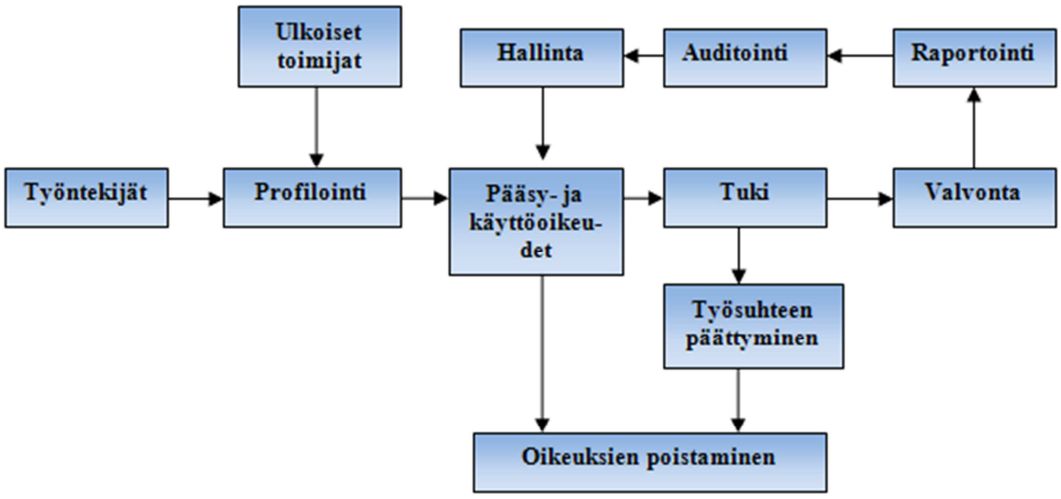


Kuva 6. Laitteiston elinkaari. Mukaillen hyödynnetty (Kokkala 2010, 11) kuvaa.

3.9 Käyttöturvallisuus

Käyttöturvallisuudella luodaan ja ylläpidetään tietotekniikan turvallisen käytön vaatimat toimintaolosuhteet. Tämä toteutetaan huolehtimalla mm. toimivuuden valvonnasta, käyttöoikeuksien hallinnasta, käytön ja lokien valvonnasta, ohjelmistotukeen, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvistä turvallisuustoimenpiteistä, varmuuskopioinnista sekä häiriöraportoinnista. Kuvassa 7 on malli käyttöoikeuksien hallinnan elinkaaresta, johon on sovellettu elinkaarenhallinnan ajattelumallia. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 65.)

Kaikkien tietojärjestelmien suojaaminen haittaohjelmilta (kuten sähköpostiviruksilta tai verkkomadoilta) on osa käyttöturvallisuutta. Järjestelmien käyttöturvallisuuden taso perustuu järjestelmässä olevien *tietojen luokitukseen*. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 65.)



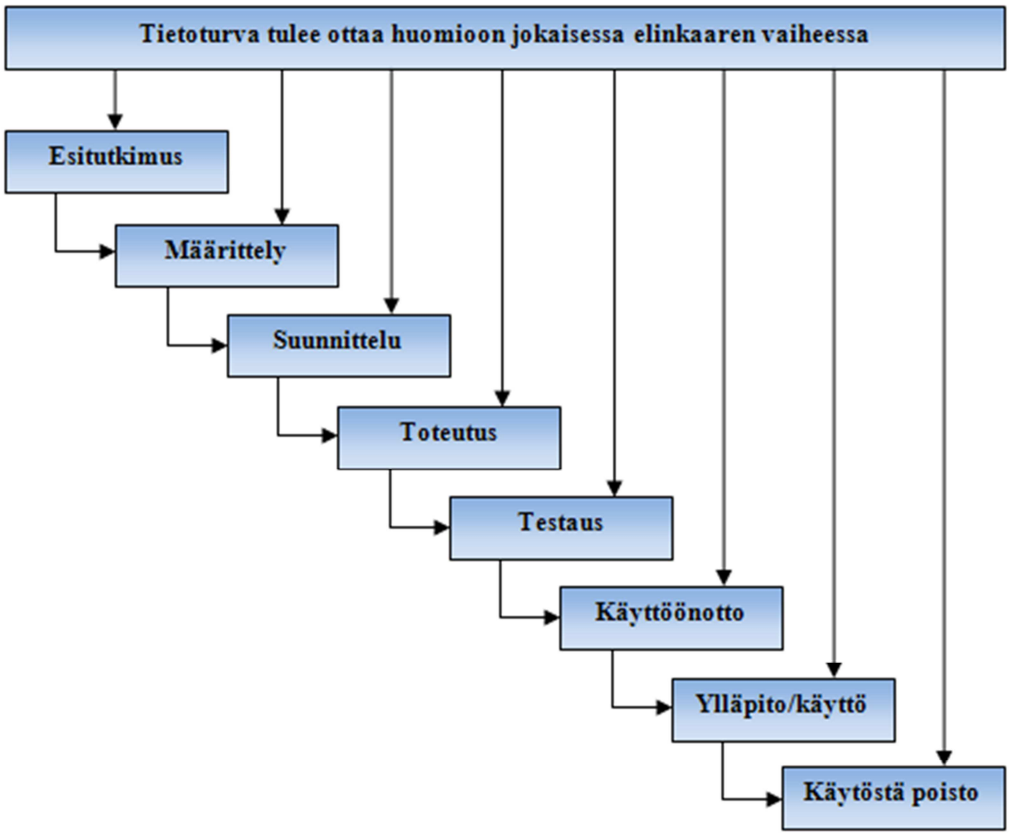
Kuva 7. Käyttöoikeuksien hallinnan elinkaari. Mukaillen hyödynnetty (Kokkala 2010, 12) kuvaa.

3.10 Ohjelmisto ja ohjelmistokehityksen turvallisuus

Ohjelmisto ja ohjelmistokehityksen turvallisuudella tarkoitetaan käyttöjärjestelmien, varus- ja työkaluohjelmistojen sekä muiden ohjelmistojen ja sovellusten tunnistamis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ohjelmistojen ylläpitoon ja päivitykseen liittyviä turvallisuustoimenpiteitä. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 69.)

Ohjelmistojen turvallisuuteen vaikuttavat ohjelmistokehityksessä käytetyt prosessit, ohjelmiston käytönaikaiset asetukset ja ohjelmiston palvelualustan (käyttöjärjestelmän ja mahdollisten väli- ja apuohjelmistojen) asetukset sekä käyttäjien saama koulutus ja ohjeistus. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 69.)

Kuvassa 8 perinteisessä sovelluskehitysprosessin, hyvien käytäntöjen mukaisessa prosessissa tietoturva määritellään ja suunnitellaan projektin alkuvaiheessa ja toteutetaan myöhemmissä vaiheissa (Sovelluskehityksen tietoturvaohje, luonnos 2012, 10).



Kuva 8. Ohjelmiston elinkaari. Mukaillen hyödynnetty (Sovelluskehityksen tietoturvaohje, luonnos 2012, 10) kuvaa.

3.11 Jatkuvuuden ja erityistilanteiden hallinta

Poikkeusoloilla tarkoitetaan alueellisesti tai valtakunnallisesti vaikeutuneita toimintaolosuhteita, jolloin tilanteen hallitsemiseksi ei voida tukeutua enää säännönmukaisiin toimivaltuuksiin. Poikkeusolot on määritelty *valmiuslaissa ja puolustustilalaissa.* (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 73.)

Organisaation on kyettävä valmistautumaan siten, että *poikkeusolojen ja normaaliaikojen häiriötilanteiden* aikana toimintakyky säilytetään suunnitellusti. Nämä tilanteet ovat yllättäviä tai äkillisiä tapahtumia, jotka voivat lamaannuttaa organisaation tai sen ylläpitämien keskeisten toimintojen turvallisuuden ja keskeisten järjestelmien toiminnan. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 73.)

Jokaisen organisaation on itse tunnistettava ne tietojärjestelmät, jotka ovat keskeisiä oman organisaation tai valtion toiminnan kannalta. Keskeiset järjestelmät on toteutettava siten, että niiden toiminnan jatkuvuus on turvattu kaikissa olosuhteissa. Häiriötilanteissa joudutaan erityistoimenpiteisiin normaalin tilanteen palauttamiseksi. Häiriötilanteet voivat aiheuttaa merkittävää resurssien uudelleen ohjaustarvetta. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 73.)

Varautumisen painopiste on uhkien tunnistamisessa ja ennalta ehkäisyssä sekä välttämättömän tietojenkäsittelyn varmistamisessa. Suunnitelmien avulla pyritään toimimaan poikkeuksellisissa olosuhteissa ensisijaisesti olemassa olevalla organisaatiolla ja resursseilla. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 73 - 75.)

4 TURVALLISUUSJOHTAMINEN

4.1 Tietoturvallisuus osana organisaatioturvallisuutta

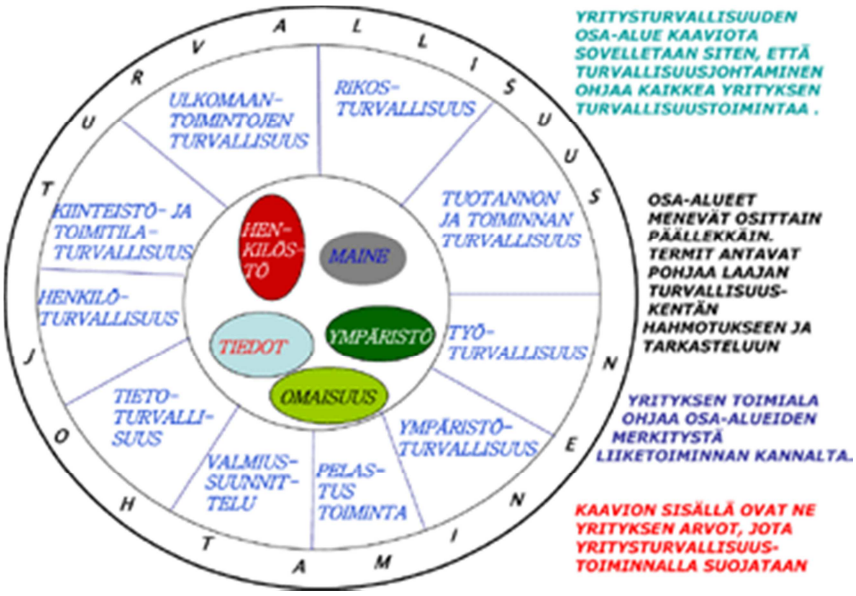
Turvallisuusjohtamisen perinteisiä osa-alueita ovat henkilöturvallisuus, työturvallisuus, palo- ja pelastustoiminta, *tietoturvallisuus*, valmiustoiminta, ympäristöturvallisuus, tuotannon ja toiminnan turvallisuus, toimitilaturvallisuus, ulkomaantoimintojen turvallisuus sekä vakuuttaminen. (Leppänen 2006, 57.)

Uuden näkemyksen mukaan turvallisuusjohtaminen sisältää kaikki ne osa-alueet ja toiminnot, joiden avulla varmistetaan organisaation tavoitteiden saavuttaminen ja suojattavien kohteiden vahingoittumattomuus. (Leppänen 2006, 57.)

Turvallisuusjohtamisen yhteydessä on käytetty käsitettä *yritysturvallisuus*. Yritysturvallisuudella tarkoitetaan yrityksen kaikkien turvallisuusasioiden yhtenäistä, tulostavoitteita tukevaa kokonaishallintaa. Sillä pyritään takaamaan yrityksen lailliset toimintaedellytykset, tuotannon ja toiminnan häiriöttömyys sekä suojaamaan yrityksen henkilöstöä, omaisuutta, tietoa ja ympäristöä onnettomuuksilta, vahingoilta ja rikolliselta toiminnalta. (Kerko 2001, 21.)

Koska turvallisuusjohtamisen kenttä on laajentunut myös valtionhallintoon, kuntiin, järjestöihin sekä eri verkostoihin ja organisoitumismuotoihin, on alettu käyttää yritysturvallisuuden sijasta käsitettä *organisaatioturvallisuus*. Organisaatioturvallisuuteen liittyvät toiminnot jakaantuvat suojattavien kohteiden määrittelyyn, riskien arviointiin, riskien hallinta- ja turvallisuustoimenpiteiden suunnitteluun ja toteutukseen sekä jatkuvaan arviointiin ja parantamiseen. (Leppänen 2006, 59.)

Organisaatioturvallisuuden kokonaisuus on määriteltävä aina tapauskohtaisesti, joskin lähtökohtana voidaan kuitenkin pitää yleisesti tunnettuja kokonaisuuksia (Leppänen 2006, 59). Kuvassa 9 on Yritysturvallisuuden neuvottelukunnan toimesta kehitetty malli yritysturvallisuuden kokonaisuudesta.

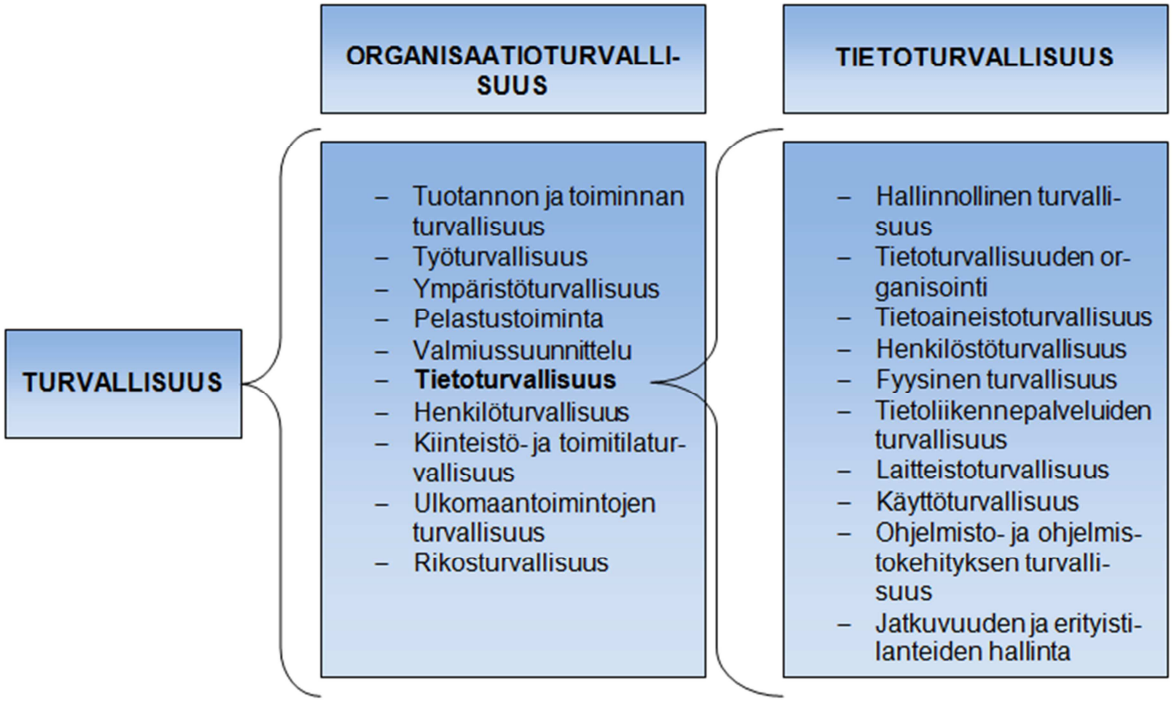


Kuva 9. Yritysturvallisuuden kokonaisuus (Yritysturvallisuus EK Oy 2009).

Kerko (2001, 225) toteaa, että ehkä enemmän kuin missään muussa yritysturvallisuuden osa-alueessa on tietoturvallisuudessa järkevää toteuttaa yhtenäistä, suunnitelmallista hallintajärjestelmää yksittäisten ja hajanaisten ja usein kalliiden investointiluontoisten turvallisuusjärjestelyjen asemasta.

Kuvassa 10 on esimerkki organisaatioturvallisuuden ja tietoturvallisuuden välisestä suhteesta. Kuvassa on käytetty taustatietona luvun 3 mukaisia tietoturvallisuuden osa-alueita sekä Yritysturvallisuus EK Oy 2009 kuvassa esitettyjä yritysturvallisuuden osa-alueta. Samoja komponentteja esiintyy kummassakin lohkossa, joskin niiden mer-

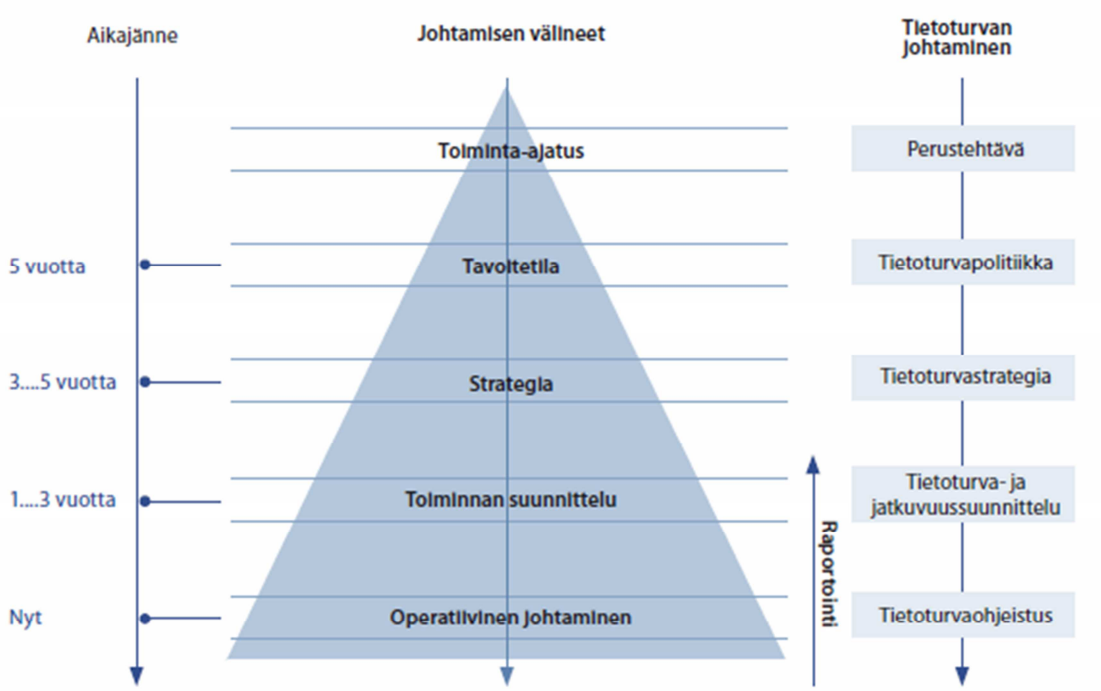
kitykset ovat kummallekin lohkolle ominaisia ja asettavat näin ollen haasteita turvallisuusjohtamisen kokonaisuuden hallintaan.



Kuva 10. Organisaatioturvallisuuden ja tietoturvallisuuden suhde. Kuvassa on mukaillen hyödynnetty (Yritysturvallisuus EK Oy 2009) kuvan tietoa.

4.2 Tietoturvallisuuden johtaminen

Tietoturvallisuuden johtaminen on osa kaikkea johtamistoimintaa ja johdon lisäksi tietoturvallisuudesta huolehtiminen kuuluu osaltaan jokaisen organisaatiossa työskentelevän toimintavastuisiin. Johto tarvitsee kokonaisnäkemyksen organisaation eri tasojen toiminnasta, prosesseista, henkilöstön osaamisesta sekä toimintaan liittyvistä keskeisistä riskeistä. Lisäksi tietoturvallisuuden johtaminen on järjestettävä siten, että asetetut tavoitteet ovat oikeassa suhteessa organisaation kokonaisturvallisuuteen ja tukevat eri strategioissa olevia turvallisuustavoitteita. Kuvassa 11 on malli johtamisjärjestelmän ja tietoturvallisuuden välisestä suhteesta. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 27.)



Kuva 11. Johtamisjärjestelmän ja tietoturvallisuuden välinen suhde (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 27).

Perustavoitteena tietoturvallisuuden tulosjohtamisessa on kehittää *tietoturvakulttuuria* osana organisaation riskienhallintaa. Tietoturvatoiminnan päämääränä on vähentää toimintaan kohdistuvia tietoriskejä ja häiriöitä sekä aikaansaada toiminnallista laatua. Tietoturvallisuuden johtamisella toteutetaan organisaation kokonaisvaltaista riskien- ja laadunhallintaa. Tavoitetaso asettuu ja määräytyy sen mukaan, mikä on tietotekniikan ja tiedonhallinnan merkitys organisaation palvelutuotannolle ja muulle toiminnalle. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 16.)

Päivittäisessä kielenkäytössä tietoturvallisuus ja sen johtaminen ovat laajoja käsitteitä, joilla on lukuisia merkityksiä. Tietoturvallisuuden johtaminen voi suppeimmillaan tarkoittaa tietoturvallisuudesta huolehtimista lain vähimmäisvaatimusten edellyttämällä tavalla, ilman selkeää suunnitelmaa tai vastuuta. Laajemmin käsitettynä se tarkoittaa nimettyä tietoturvapäällikköä, jonka tehtävänä on tietoturvan kokonaisuuden hallinnointi. Tietoturvan johtaminen voi laajimmillaan mieltää johdon uudeksi tehtäväkokonaisuudeksi, joka koskettaa koko organisaation johtamista. (Laaksonen ym. 2006, 115.)

Tietoturvallisuus on johdon näkökulmasta hierarkkista politiikan ja toimintaohjeiden laatimista, tavoitteiden asettamista sekä jatkuvaa valvontaa ja toiminnan kehittämistä. Tietoturvallisuuden johtaminen perustuu määrätietoiseen ja organisoituun toimintaan ja se on samanlaista johtamista kuin muiden toimintojen johtaminen. *Asetetaan tavoitteet, määritetään vastuut ja osoitetaan riittävät resurssit*. Lopputulosta verrataan asetettuihin tavoitteisiin ja pohditaan jatkotoimenpiteitä, joita mahdolliset poikkeamat vaativat. (Laaksonen ym. 2006, 117.)

Tietoturvallisuuden johtamiseen on laadittu erilaisia viitekehyksiä, malleja ja standardeja, joita kutsutaan *alan parhaiksi käytännöiksi*. Lisäksi on olemassa lukuisia dokumentteja ja muistilistoja, jotka auttavat hallitsemaan tietoturvallisuuden osa-alueet. Malleilla tuodaan määrämuotoisuutta tietoturvallisuuden hallintaan liittyviin käytäntöihin, mutta nämä apuvälineet ovat tehottomia, mikäli tietoturvallisuutta johdetaan organisaation muusta johtamisesta irrallisena toimintona. Tietoturva on otettava huomioon organisaation kaikissa yksiköissä osana päivittäistä johtamista sekä saatava osaksi jokaisen työntekijän päivittäisiä toimia. (Laaksonen ym. 2006, 115.)

Toimivan tietoturvallisuuden perustana on täsmällinen johtaminen sekä tietoturvallisuuden liittäminen tiiviisti organisaation jokapäiväiseen toimintaan. Tietoturvallisuus on mahdollista saada osaksi työntekijän jokapäiväistä toimintaa, kun se sisällytetään itsestäänselvyytenä henkilöiden rutiineihin. Tietoturvallisuus voidaan esimerkiksi liittää henkilön työhön liittyviin ohjeisiin, perehdytykseen sekä työnohjaukseen. Erillistä tietoturvakoulutusta ei välttämättä tarvitse järjestää henkilöille, koska tietoturvallinen toiminta voidaan liittää osaksi muita ohjeita ja koulutuksia. (Laaksonen ym. 2006, 116.)

4.3 Tietoturvallisuuden johtamisjärjestelmän laajuus

Organisaation on saatava kokonaiskuva siitä, minkälainen ja miten laaja johtamisjärjestelmä tietoturvallisuuden hallinnointiin on syytä rakentaa. Edesauttaakseen tietoturvallisuuteen kohdistettavien resurssien määrittelyä sekä siihen liittyvän päätöksenteon tueksi organisaatio voi pohtia vastauksia oheisiin kysymyksiin. (Laaksonen ym. 2006, 118.)

1. Minkälaista tietoa organisaatio käsittelee? Voiko joku hyötyä esimerkiksi taloudellisesti organisaation tiedoista? Onko tiedon tuottaminen vaatinut suuria taloudellisia tai muita panostuksia? Kuinka helposti ja nopeasti tieto voidaan tuottaa uudelleen ja onko siitä enää tuolloin hyötyä?

2. Kuka on kiinnostunut organisaation tiedoista ja miten tämä pyrkii tietoihin käsiksi?

3. Miten tietoa voidaan viedä organisaatiosta ulos ja minkälaisia tapoja tietojen havittelijat käyttävät?

4. Kuinka laajaa ja monimuotoista organisaation toiminta on ja miten monimutkainen on nykyisin käytössä oleva johtamisjärjestelmä? Voidaanko tietoturvan johtaminen yhdistää nykyiseen johtamisjärjestelmään?

5. Millainen on organisaation ulkoinen vaatimusympäristö ja miten sen uskotaan kehittyvän? Miten organisaatio vastaa ulkopuolelta tuleviin tietoturvavaatimuksiin?

6. Onko organisaatiolla käsitystä sitä velvoittavasta yleisestä lainsäädännöstä tai erityisestä organisaatioon kohdistetusta säännöstelystä?

Tieto, jonka organisaatio omistaa tai hallitsee voi olla monella tavalla kiinnostavaa ja syyt tiedon hankkimiseen tai tuhoamiseen voivat olla esimerkiksi *taloudellisia, poliittisia tai henkilökohtaisia*. Esimerkiksi henkilökohtaiset syyt voivat olla oman organisaation henkilöstön motiivina. Taloudelliset syyt ovat usein rikollisten motiiveja ja poliittiset syyt voivat olla esimerkiksi merkittävien innovaatioiden tai keksintöjen tutkimus- ja kehitystietojen anastamisen takana. (Laaksonen ym. 2006, 118 - 119.)

4.4 Tietoturvallisuuden johtamisen kehittämiskohteet

Valtioneuvosto on valtioneuvoston ohjesäännön (262/2003) 3§:n 11 kohdan mukaan päättänyt tietoturvallisuuden kehittämisperiaatteista, jotka linjataan Vahti-ohjeessa

7/2009, Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä.

Periaatepäätöksellä ohjataan valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa. Periaatepäätös edistää valtion ja erilaisten yhteisöjen tietoturvallisuuden sekä kansalaisten perusoikeuksien ja tietosuojan toteutumista julkisissa palveluissa ja viranomaisten tietojärjestelmissä. (Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009, 25.)

Periaatepäätöksellä ohjataan kokonaisuutta ja sen keskeisiä rajapintoja sidosryhmiin sekä vahvistetaan tietoturvayhteistyötä. Lisäksi periaatepäätöksessä päätetään kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat jokaisen viranomaisen tietoturvatyölle. (Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009, 8.)

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä (2009, 10) mukaan tietoturvallisuuden johtamisen kehittämiskohteita ovat:

1. Tietoturvatoiminnan kattava sisällyttäminen tulosohjaukseen.
2. Selvitys tietoturvallisuuden johtamisesta, raportoinnista ja tarkastustoiminnasta.
3. Resurssien priorisointi tietoturvallisuuden varautumisen kannalta keskeisiin kohteisiin.
4. Tietoturvamittareiden kehittäminen ja käyttö johtamisessa.

4.5 Organisaation johdon keskeiset tietoturvavelvoitteet

Organisaation johto on keskeisessä asemassa tietoturvallisuuden kehittämisessä ja ylläpitämisessä. Tietoturvatyölle tulee nimetä *vastuuhenkilö* sekä osoittaa hänelle riittävät resurssit hoitaa ja toteuttaa organisaation tietoturvavelvoitteita organisaation toimintaympäristön ja ulkoisten vaatimusten edellyttämällä tavalla. Tietoturvallisuus tulee organisoida ja kohdentaa vastuut erityisesti riskienhallintatoimessa, tietohallintotoimessa, sopimus- ja hankintatoimessa sekä lainmukaisuuden valvonnassa. Ilman

johdon tukea tietoturvatyölle asetettuja tavoitteita ei voi saavuttaa lainsäädännön velvoitteiden osalta eikä tietoturvatyö voi tuottaa tavoiteltuja hyötyjä. (Johdon tietoturvaopas 2011, 14.)

Johdon tietoturvaopas (2011, 14) mukaan organisaation keskeiset tietoturvavelvoitteet voidaan tiivistää seuraaviin kohtiin:

- lainmukaisuuden varmistaminen
- riskienhallinnan- ja hallintajärjestelmän toteuttaminen
- tietoturvapolitiikkaan sitoutuminen.
- tietoturvajohtaminen.
- tietoturvavastuuhenkilön nimeäminen
- tietoturvallisuuden organisointi
- tietoturvallisuuden toteutumisen varmistaminen
- tietoturvallisuuden TTS-suunnitteluedellytysten luonti
- poikkeama- ja erityistilanteiden hallinta
- tietoturvaraportointivelvollisuuksista huolehtiminen

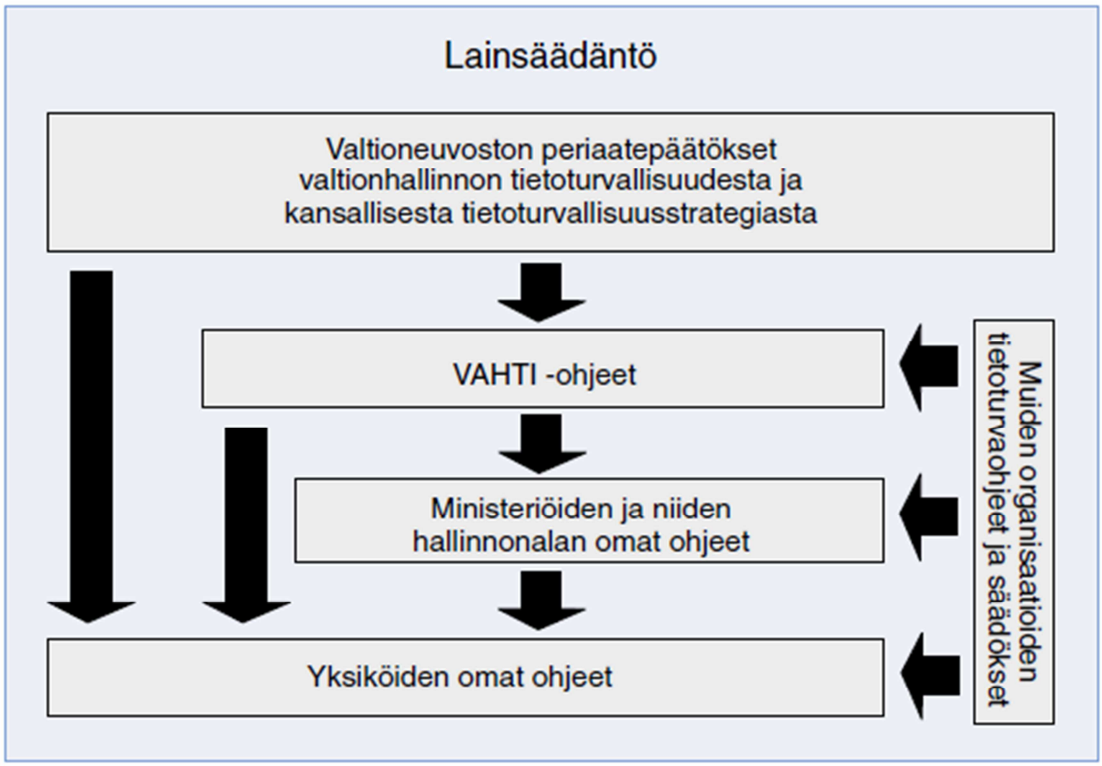
5 NORMIOHJAUS

5.1 Lainsäädännön rooli

Kotimainen ja kansainvälinen lainsäädäntö asettaa organisaatioille suoria ja epäsuoria velvoitteita tietoturvallisuudesta huolehtimiseksi. Nämä määritellyt velvoitteet ovat yleisluontoisia ja käytännön toteutus sekä riittävän tietoturvallisuuden tason määritteleminen on jätetty organisaatioiden vastuulle. (Laaksonen ym. 2006, 18.)

Organisaation kannalta on keskeistä kartoittaa pakottavat yksittäiset säädökset, jotka ohjaavat yrityksen tietoturvan suunnittelua, ylläpitoa ja kehittämistä. Lainsäädännön lisäksi tulee tunnistaa sopimuksiin perustuvat tietoturvavelvoitteet. (Laaksonen ym. 2006, 18.)

Kaiken tietoturvan perustana on *Suomen lainsäädäntö*. Useat lait, asetukset ja määräykset sekä ohjeet sisältävät viranomaisia koskevia tietoturvavelvoitteita. Lainsäädäntö on myös huomioitu valtioneuvoston periaatepäätöksissä valtionhallinnon tietoturvallisuudesta ja kansallisesta tietoturvastrategiasta. Kuvassa 12 havainnollistetaan tätä kokonaisuutta. (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 20.)



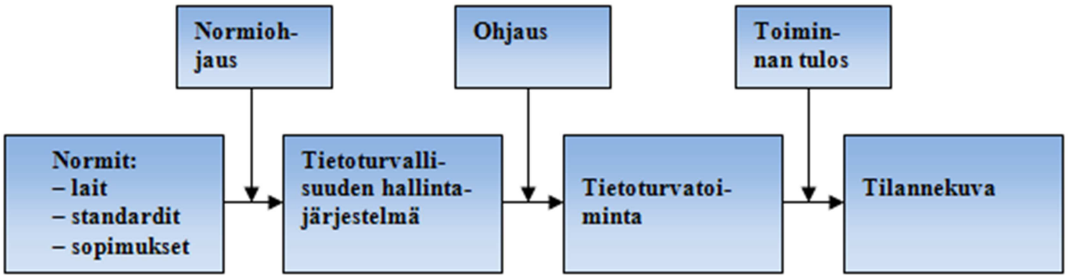
Kuva 12. Lainsäädäntö, normit ja ohjeet valtionhallinnossa (Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003, 20).

Valtioneuvoston periaatepäätös kansallisesta tietoturvastrategiasta hyväksyttiin 4.12.2008. Edellinen periaatepäätös oli ollut voimassa vuodesta 2003. *Kansallisen tietoturvastrategian* avulla pyritään luomaan suomalaisille (kansalaiset, yritykset, viranomaiset ja muut toimijat) turvallinen arki tietoyhteiskunnassa. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen tieto- ja viestintäverkoissa sekä niihin liittyvissä palveluissa. Yleisen tietototuturvaosaamisen täytyy olla korkealla tasolla ja yhteiskunnan eri tahot toimivat saumattomassa yhteistyössä tietoturvan edistämiseksi. (Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi 2008, 1.)

Kansallisessa tietoturvastrategiassa on kolme painopistettä:

1. Perustaidot arjen tietoyhteiskunnassa.
2. Tietoihin liittyvien riskien hallinta ja toimintavarmuus.
3. Kilpailukyky ja kansainvälinen verkostoyhteistyö.

Valtionhallinnossa on pääsääntöisesti toteutettu *normiperustaista* tietoturvallisuuden ohjausta, jossa otetaan huomioon lainsäädännöstä tulevat velvoitteet ja tietoturvatoiminnan perusteet. Hallinnan toteuttamisen välineitä ovat *standardit, hallintamallit ja suositukset*. Kuvassa 13 esitetään normiohjaus valtionhallinnon tietoturvallisuuden hallintajärjestelmän tietoturvatoiminnassa.



Kuva 13. Normiohjaus tietoturvallisuuden hallinnassa. Mukaillen hyödynnetty (Kalander 2007, 3) kuvaa.

Tietoturvallisuuden merkittävyydestä huolimatta viranomaisten toiminnassa on tietoturvatoimenpiteitä suunniteltaessa sovellettava *suhteellisuusperiaatetta*, sillä raskaat tietoturvajärjestelyt voivat hidastaa viranomaisen toimintaa perusteettomasti. Usein voidaan kevyemmillä ratkaisuilla turvata tietojenkäsittely normaalioloissa sekä ennustettavissa olevissa poikkeusoloissa; järjestelyissä on otettava huomioon suojattava kohde ja suhteutettava järjestelyt sen mukaan. (Voutilainen, 2012, 125.)

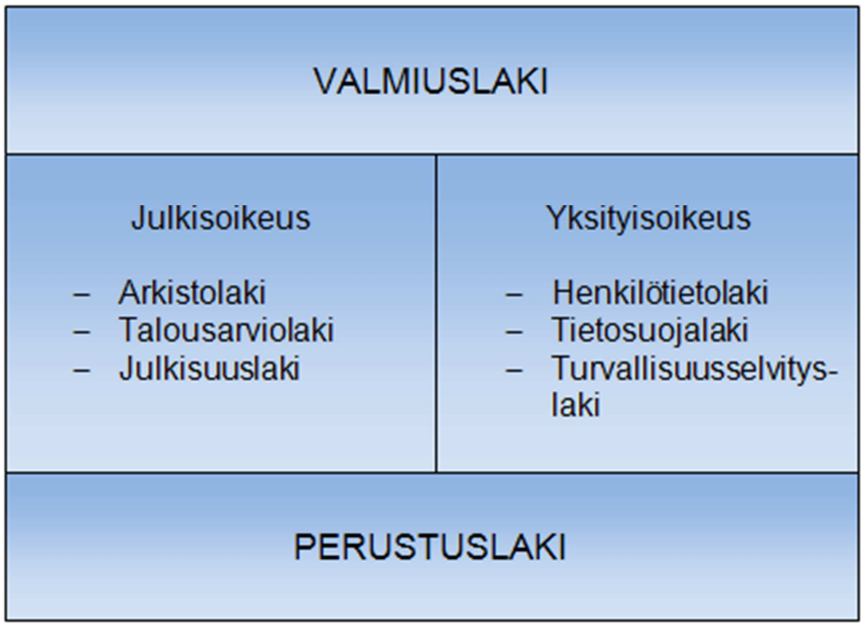
5.2 Lainmukaisuus valtionhallinnossa

Tietoturvallisuuden eräänä tarkoituksena on luoda hallinnon asiakkaisiin luottamus hallinnon toimivuuteen. *Tietoturvallisuudella on sidos kaikkiin viranomaisten tietojenkäsittelyä koskeviin säädöksiin* ja se on yksi niistä elementeistä, joilla mahdolliste-

taan viranomaisen lainmukainen toiminta tietojenkäsittelyn yhteydessä. Tietoturvallisuus voidaan nähdä oleellisena osana palvelujen ja toiminnan piirteitä ja ominaisuuksia, joilla täytetään asetetut tai odotetut tarpeet, joten se on siten *keskeinen viranomaistoimintojen laatuvaatimus*. (Voutilainen, 2012, 125.)

Lainsäädännön perusta on *perusoikeuksissa*, jotka on kuvattu *perustuslaissa*. Muu lainsäädäntö rajaa ja tarkentaa perustuslain säädöksiä. Poikkeusoloja varten on säädetty *valmiuslaki*, jossa osa lainsäädännöstä rajataan ja tarkennetaan poikkeusoloihin sopivaksi.

Lainsäädäntö antaa raamit tietoturvallisuuden tavoitetason toteuttamiselle. Osa lainsäädännöstä sisältää selkeitä tietoturvallisuusvelvoitteita, kuten henkilötietolaki. Rajaavasti vaikuttava on esimerkiksi sähköisen viestinnän tietosuojalaki ja välillisesti vaikuttaa esimerkiksi sopimuslaki. Vaikuttavan lainsäädännön suhteita esitetään kuvassa 14. (Kalander 2007, 4.)



Kuva 14. Lainsäädännön suhteet. Mukaillen hyödynnetty (Kalander 2007, 4) kuvaa.

Tietoturvallisuus on valtionhallinnossa voimakkaassa muutostilassa, mikä johtuu yhteiskunnan keskeisten toimintojen ja tarjottavien palveluiden sähköistymisestä sekä kasvavasta tietoteknisestä riippuvuudesta. Lisäksi turvallisuusuhkat kohdentuvat yhä

enemmän tietoverkkoihin, tietojärjestelmiin ja organisaatioiden arkaluonteisiin tietoihin sekä avainhenkilöihin, kansalaisiin ja asiakkaisiin. Tähän uhkien muodostamaan kokonaisuuteen valtionhallinnossa on pyritty vastaamaan lainsäädännön keinoin, *velvoittamalla organisaatioita tietoturvallisuuden kehittämiseen*. (Johdon tietoturvaopas 2011, 15.)

Johdon tulee varmistaa, että organisaatiossa on tunnistettu sitä koskeva keskeinen tietoturvallisuuden lainsäädäntö. Organisaation on täytettävä sille asetetut tietoturvavelvoitteet, erityisesti tietoturva-asetuksen ja sen perusteella annetut tietoturvatasojen vaatimukset. (Johdon tietoturvaopas 2011, 15.)

5.3 Perustuslain perusoikeussäännökset

Suomen perustuslain perusoikeussäännökset määrittelevät yksityiselämän suojan, sananvapauden ja julkisuuden. Perustuslakia tarkentavia lakeja ovat esimerkiksi henkilötietolaki, julkisuuslaki, laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän tietosuojalaki. (Suomen perustuslaki 11.6.1999/731, 2 luku.)

5.4 Laki viranomaisten toiminnan julkisuudesta

Laissa säädetään oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisessa toimivan vaitiolovelvollisuudesta, asiakirjojen salassapidosta ja muista tietojen saantia koskevista yleisten ja yksityisten etujen suojaamiseksi välttämättömistä rajoituksista, samoin kuin viranomaisten velvollisuuksista tämän lain tarkoituksen toteuttamiseksi. (Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621, 2 §.)

Laissa säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. (Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621, 3 §.)

5.5 Asetus viranomaisten toiminnan julkisuudesta

Asetuksessa (julkisuusasetus) säädetään menetelmistä, miten viranomainen selvittää ja arvioi asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys, samoin kuin asiakirja- ja tietohallintonsa. (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030.)

Julkisuusasetuksen 1. §:n mukaan toimenpiteiden tarvetta arvioitaessa on kiinnitettävä huomiota siihen, kuinka toteutetaan:

1. Oikeus sada tietoja viranomaisen julkisista asiakirjoista.
2. Velvollisuus tuottaa ja jakaa tietoja sekä antaa tietoja keskeneräisistä asioista.
3. Henkilötietojen, erityisesti arkaluonteisten tietojen, suojaaminen.
4. Salassa pidettäviksi säädettyjen tietojen suojaaminen.
5. Tietojen käyttötarkoituksia koskevat rajoitukset.
6. Tietojen käytettävyys, eheys ja laatu viranomaisen tehtävän hoidossa ja viranomaisten yhteistyössä.
7. Tietojen laatu erityisesti käytettäessä niitä yksilöitä ja yhteisöjä koskevan päätöksenteon pohjana tai oikeuksien ja velvollisuuksien osoittajina.

Hyvän tiedonhallintatavan toteuttamiseksi on lisäksi selvitettävä ja arvioitava tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaan sekä tietojärjestelmien turvallisuuteen vaikuttavat uhat sekä niiden vähentämiseksi ja poistamiseksi käytettävissä olevat keinot ja niiden kustannukset sekä muut vaikutukset. (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030, 1 §.)

5.6 Valtion virkamieslaki

Virkamiehen vaitiolovelvollisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) ja muussa laissa säädetään. (Valtion virkamieslaki 19.8.1994/750, 17 §).

5.7 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä

Periaatepäätöksellä ohjataan valtionhallintoa kehittämään tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä ja toimintaa. Riittävä resursointi tietoturvallisuuden kehittämiseen ja ylläpitoon on välttämätön edellytys toiminnalle sekä sen tehostamiselle ja tuottavuuden parantamiselle. (Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009, 7-8.)

Periaatepäätöksellä ohjataan valtionhallinnon tietoturvallisuuden kokonaisuutta ja sen keskeisiä liittymäpintoja sidosryhmiin sekä vahvistetaan tietoturvayhteistyötä. Siinä päätetään kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat jokaisen viranomaisen tietoturvatyölle. (Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009, 7-8.)

5.8 Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa

Asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvavaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvavaatimuksista. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 1 §.)

Valtionhallinnon viranomaisen on pidettävä huolta, että tietoturvallisuuden suunnittelu hyvän tiedonhallintatavan mukaisesti perustuu viranomaisen selvityksiin ja arvioihin sen hallussa olevista asiakirjoista sekä niihin talletettujen tietojen merkityksestä. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 4 §.)

Tietoturvallisuuden suunnittelussa otetaan huomioon vaatimus hyvän julkisuus- ja salassapitorakenteen toteuttamisesta tietojärjestelmissä ja että tietoturvallisuustoimenpiteet mitoitetaan ottamalla huomioon suojattavien tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 4 §.)

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 5 §:n mukaan valtionhallinnon viranomaisen on tietoturvallisuuden perustason toteuttamiseksi huolehdittava seuraavista tehtävistä:

1. Viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan.
2. Viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään.
3. Asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään.
4. Tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi.
5. Asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi.
6. Tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä.
7. Asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja.
8. Henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla.
9. Henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä.
10. Annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Lisäksi tietoturvallisuustoimenpiteet on suunniteltava ja toteutettava siten, että ne kattavat asiakirjan kaikki käsittelyvaiheet niiden laatimisesta tai vastaanottamisesta arkistointiin tai hävittämiseen mukaan lukien asiakirjan luovuttaminen ja siirtäminen sekä käsittelyn valvonta. Suunnittelussa on pidettävä huolta siitä, että tietojenkäsittelyä

koskevia velvoitteita noudatetaan myös silloin, kun tietojenkäsittelytehtävää hoidetaan viranomaisen toimeksiannosta. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 6 §.)

5.9 Henkilötietolaki

Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. (Henkilötietolaki 22.4.1999/523, 1 §.)

Henkilötietolakia sovelletaan henkilötietojen automaattiseen käsittelyyn sekä muuhun henkilötietojen käsittelyyn silloin, kun henkilötiedot muodostavat tai niiden tarkoitus on muodostaa henkilörekisteri tai sen osa. Lakia ei sovelleta henkilötietojen käsittelyyn, jonka luonnollinen henkilö suorittaa yksinomaan henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin. (Henkilötietolaki 22.4.1999/523, 2 §.)

Henkilötietolain 2. luvussa säädetään henkilötietojen käsittelyä koskevista yleisistä periaatteista, joita ovat:

- huolellisuusvelvoite
- henkilötietojen käsittelyn suunnittelu
- käyttötarkoitussidonnaisuus
- käsittelyn yleiset edellytykset
- tietojen laatua koskevat periaatteet
- rekisteriseloste

5.10 Laki sähköisestä asioinnista viranomaistoiminnassa

Tämän lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä. (Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13, 1 §.)

Lain 5 §:n mukaan viranomaisen velvollisuuksiin kuuluu järjestää mm. sähköiset asiointipalvelut seuraavasti:

- Viranomaisen, jolla on tarvittavat tekniset, taloudelliset ja muut valmiudet, on niiden rajoissa tarjottava kaikille mahdollisuus lähettää ilmoittamaansa sähköiseen osoitteeseen tai määriteltyyn laitteeseen viesti asian vireille saattamiseksi tai käsittelemiseksi.

- Tällöin on lisäksi kaikille tarjottava mahdollisuus lähettää sähköisesti viranomaiselle sille toimitettavaksi säädettyjä tai määrättyjä ilmoituksia, sen pyytämiä selvityksiä tai muita vastaavia asiakirjoja taikka muita viestejä.

- Viranomaisen on pyrittävä käyttämään asiakkaan kannalta teknisesti mahdollisimman yhteensopivia ja helppokäyttöisiä laitteistoja ja ohjelmistoja. Viranomaisen on lisäksi varmistettava riittävä tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa.

Lain 6 §:n mukaan viranomaisen on turvattava saavutettavuus seuraavasti:

- Viranomaisen tulee huolehtia siitä, että sen sähköiset tiedonsiirtomenetelmät ovat toimintakunnossa ja mahdollisuuksien mukaan käytettävissä muulloinkin kuin viraston aukioloaikana.

Lain 7 §:n mukaan viranomaisen on ilmoitettava yhteystietonsa seuraavasti:

- Viranomaisen tulee sopivalla tavalla ilmoittaa sähköisessä asioinnissa käytettävät yhteystietonsa.

- Jos oikaisuvaatimus tai valitus voidaan tehdä viranomaiselle myös sähköisesti, tällainen yhteystieto on ilmoitettava oikaisuvaatimus- tai valitusosoituksessa.

5.11 Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. (Sähköisen viestinnän tietosuojalaki 16.6.2004/516, 1 §.)

Laissa määritellään myös tietoturvavelvoitteita sen soveltamisalaan kuuluville tahoille sekä viestinnän tietoturvaan liittyvien velvollisuuksien huolehtimisesta ja toimenpiteistä tietoturvan toteuttamiseksi. Viestintävirasto on ohjaava viranomainen, joka täydentää lakia määräyksillään (Sähköisen viestinnän tietosuojalaki 16.6.2004/516, 19-21 §.)

5.12 Laki yksityisyyden suojasta työelämässä

Lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. (Laki yksityisyyden suojasta työelämässä 13.8.2004/759, 1-2 §.)

5.13 Arkistolaki

Arkistolaissa säädetään arkistolaitoksesta ja arkistotoimesta ja sen järjestämisestä, asiakirjojen laatimisesta, säilyttämisestä ja käytöstä, sekä yksityisistä arkistoista. Arkistolaki määrää mm. mitkä asiakirjat ovat säilytettävä (arkistoitava) pysyvästi. Keskeisiä käsitteitä ovat käytettävyys, eheys, luottamuksellisuus, tietosuoja ja tietoaineiston hävittäminen. Arkistolaitos ohjaa määräyksillään arkistolain toteutumista. (Arkistolaki 23.9.1994/831, 3-21 §.)

Arkistolain 1 §:n mukaan arkistonmuodostajia ovat:

1. Valtion virastot, laitokset, tuomioistuimet sekä muut lainkäyttöelimet ja valtion viranomaiset.
2. Kunnalliset viranomaiset ja lainkäyttöelimet.
3. Suomen Pankki, Kansaneläkelaitos sekä muut itsenäiset julkisoikeudelliset laitokset ja yliopistolaissa tarkoitetut säätiöyliopistot.
4. Valtion ja kunnan liikelaitokset.
5. Ortodoksinen kirkkokunta ja sen seurakunta.
6. Muut yhteisöt, toimielimet ja henkilöt niiden suorittaessa julkista tehtävää lain tai asetuksen tai lain tai asetuksen nojalla annetun säännöksen tai määräyksen perusteella siltä osin kuin niille tämän tehtävän johdosta kertyy viranomaisen toiminnan julkisuudesta annetussa laissa tarkoitettuja asiakirjoja.

5.14 Laki valtion talousarviosta

Valtionhallinnon toimintaa ohjataan tulosohjausperusteisesti ja näin myös tietoturvatoimintaa. Lain keskeisiä käsitteitä ovat tiedon eheys ja luotettavuus, riskienhallinta ja sisäinen valvonta. Viraston ja laitoksen on huolehdittava siitä, että taloudenhoidon ohjaus ja sisäinen valvonta on asianmukaisesti järjestetty sen omassa toiminnassa sekä toiminnassa, josta virasto tai laitos vastaa. Ohjaava viranomainen on Valtiokonttori. (Laki valtion talousarviosta 13.5.1988/423, 24 b §.)

5.15 Valmiuslaki

Valmiuslain tarkoituksena on poikkeusoloissa suojata väestöä sekä turvata sen toimeentulo ja maan talouselämä, ylläpitää oikeusjärjestystä, perusoikeuksia ja ihmisoikeuksia sekä turvata valtakunnan alueellinen koskemattomuus ja itsenäisyys. (Valmiuslaki 29.12.2011/1552, 1 §).

Keskeinen lain kohta on varautumisvelvollisuus, jonka mukaan valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan

toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa. (Valmiuslaki 29.12.2011/1552, 12 §.)

Varautumista johtaa ja valvoo valtioneuvosto sekä kukin ministeriö toimialallaan. Lisäksi kukin ministeriö yhteensovittaa varautumista omalla toimialallaan. Valtioneuvostossa säädetään erikseen varautumisen yhteensovittamisesta. (Valmiuslaki 29.12.2011/1552, 13 §.)

5.16 Valtioneuvoston periaatepäätös yhteiskunnan turvallisuusstrategiasta

Periaatepäätöksellä ylläpidetään osaltaan valtiollista itsenäisyyttä, yhteiskunnan turvallisuutta sekä väestön elinmahdollisuuksista kaikissa turvallisuustilanteissa. (Johdon tietoturvaopas 2011, 16). Periaatepäätös yhteiskunnan turvallisuusstrategiasta antaa perusteet näiden tavoitteiden saavuttamiseksi. Strategia on valtioneuvoston ohjausasiakirja ministeriöille ja antaa perusteita myös alue- ja paikallishallinnolle. (Yhteiskunnan turvallisuusstrategia 2012, 5.)

Periaatepäätöksellä yhtenäistetään ministeriöiden varautumista, noudattaen valtioneuvoston ohjesäännön toimialajakoa ja yhteensovittamissäännöksiä. Yhteiskunnan turvallisuus perustuu normaaliolojen aikaisiin järjestelyihin. Ministeriöt johtavat hallinnonalansa varautumista ja sisällyttävät periaatepäätöksen edellyttämät toimenpiteet hallinnonalansa toiminnan ja talouden suunnittelu- sekä toimeenpanoasiakirjoihin. Tässä kehittämisessä otetaan huomioon myös alue- ja paikallishallinnon sekä elinkeinoelämän ja järjestöjen toiminta. (Yhteiskunnan turvallisuusstrategia 2010, 3.)

5.17 Laki kansainvälisistä tietoturvallisuusvelvoitteista

Laissa säädetään viranomaisten toimenpiteistä kansainvälisten tietoturvavelvoitteiden toteuttamiseksi. Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana. (Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588, 1 §.)

Laissa säädetään myös turvallisuusviranomaisista sekä niiden välisestä yhteistyöstä ja tietojen vaihdosta. Lisäksi laissa säädetään mm. viranomaisen tietoturvallisuustoimenpiteistä liittyen salassapitovelvollisuuteen ja tiedon käyttöön, vaitiolovelvollisuuteen ja hyväksikäyttökieltoon, turvallisuusluokan merkitsemiseen, turvallisuusluokkaa vastaaviin käsittelyvaatimuksiin, tilojen turvallisuusvaatimuksiin, henkilöturvallisuusselvityksiin ja -arvioihin sekä yhteisöturvallisuusselvityksiin ja -arvioihin. (Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588, 6 - 12 §.)

6 SERTIFIKAATIT, STANDARDIT JA TOIMINTAMALLIT

6.1 Tietoturvallisuuden hallinnoinnin apuvälineet

Lainsäädännöllinen kehys määrittelee oikeudet ja velvollisuudet, jotka tulee ottaa huomioon suunniteltaessa tietoturvallisuuden hallintamallia. Tämä malli toimii perustana organisaation tietoturvallisuuden suunnittelussa ja toteutuksessa. Hallintamallin suunnittelun hyvänä apuna ovat erilaiset tietoturvallisuuden hallinnan standardit ja toimintamallit. (Laaksonen ym. 2006, 83.)

Tietoturvallisuuden hallinnoinnin ja kehittämisen avuksi on kehitetty useita *standardeja, viitekehyksiä ja toimintamalleja*, joista tässä työssä esitetään yleisimmät ja laajimmalle levinneet. Esitettävien standardien ja toimintamallien pyrkimyksenä on käsitellä tietoturvallisuutta kokonaisuutena, mutta ne keskittyvät kuitenkin pääsääntöisesti tietoturvallisuuden hallinnointiin. Malleilla on erilaisia vahvuuksia ja soveltamiskohteita, joiden perusteella organisaatio voi valita itselleen sopivimman tietoturvallisuuden viitekehyksen tai yhdistellä eri mallien parhaita puolia. (Laaksonen ym. 2006, 83.)

Riippumatta siitä valitaanko tietoturvallisuuden kehittämisen perustaksi jokin kansainvälinen malli tai standardi vai kehitetäänkö jokin sisäinen toimintamalli itse, merkittävin hyöty joka voidaan saavuttaa, on tietoturvallisuuden integroiminen osaksi jokapäiväistä toimintaa ja organisaation toimintaprosesseja sekä toiminnan saattaminen määrämuotoiseksi. Toissijainen, mutta kuitenkin merkittävä hyöty on kyky osoittaa ulkopuolisille tahoille, kuten asiakkaille tai auditoijille, toiminnan olevan ennalta määrätyn tason ja vaatimusten mukaista. (Laaksonen ym. 2006, 104.)

6.2 Sertifikaatit

Tietoturvallisuuteen liittyy useita sertifikaatteja, jotka voidaan Laaksonen ym. (2006, 84) mukaan jaotella seuraavasti:

- *Palvelusertifikaatit* ovat sertifikaatteja, joita voidaan tietoturvallisuuden osalta myöntää palveluille, jotka täyttävät sertifikaatin myöntäjän tai jonkun muun tahon ennalta asettamat tietoturvallisuusvaatimukset ja jotka todetaan auditoinnilla näiden vaatimusten mukaisiksi.

- *Tuotesertifikaatit* ovat sertifikaatteja, joita voidaan tietoturvallisuuden osalta myöntää tuotteille, jotka täyttävät sertifikaatin myöntäjän tai jonkun muun tahon ennalta asettamat tietoturvallisuusvaatimukset ja jotka todetaan auditoinnilla näiden vaatimusten mukaisiksi.

- *Järjestelmäsertifikaatit* ovat sertifikaatteja, joita voidaan myöntää organisaation toiminnassa käytettävälle järjestelmälle (esimerkiksi tietoturvallisuuden hallintajärjestelmä) tai prosessille, jotka täyttävät kansainvälisen standardin, sertifikaatin myöntäjän tai jonkun muun tahon ennalta asettamat tietoturvallisuusvaatimukset ja jotka todetaan auditoinnilla näiden vaatimusten mukaisiksi.

- *Henkilösertifikaatit* ovat sertifikaatteja, joita voidaan myöntää henkilöille, jotka täyttävät tietoturvallisuuden alalla sertifikaatin myöntäjän tai jonkun muun tahon ennalta asettamat edellytykset ja jotka todennetaan näiden edellytysten mukaisiksi. Henkilösertifikaatit ovat tuoteriippuvaisia tai tuoteriippumattomia.

Sertifikaateista hyödyllisimpiä ja vakuuttavampia ovat sellaiset, jotka perustuvat johonkin *tunnettuun standardiin* ja sen *akkreditoituun sertifiointiin*. Läheskään kaikki markkinoilla olevat tietoturvallisuuteen liittyvät sertifikaatit eivät ole tällaisia. Liikenne- ja viestintäministeriö on selvittänyt osana kansallista tietoturvastrategiaa, tietoturvallisuuteen liittyvät sertifikaatit. Selvitystyön tulokset ovat luettavissa kansallisen tietoturvastrategian Sertifikaatit -työryhmän loppuraportista. (Laaksonen ym. 2006, 84-85.)

Tietoturvallisuuden sertifiointi tarkoittaa käytännössä *tietoturvallisuuden hallintajärjestelmän sertifiointia*. Tietoturvallisuuden hallintajärjestelmä on johtamisjärjestelmän osa, joka perustuu riskien arviointiin ja hallintaan. Sen tarkoituksena on suunnitella, toteuttaa, noudattaa, seurata, arvioida, ylläpitää ja kehittää tietoturvallisuutta. Sertifiointi on tuotteen tai toiminnan *vaatimuksenmukaisuuden* osoittamista. (Laaksonen ym. 2006, 105.)

Tietoturvallisuuden sertifioinnin voi suorittaa vain akkreditoitu taho. Akkreditointi tarkoittaa pätevyyden toteamista ja se on kansainvälisiin kriteereihin perustuva menettelytapa, jonka avulla toimielimen, esimerkiksi yrityksen tai organisaation pätevyys ja sen antamien todistusten uskottavuus voidaan todeta luotettavasti. Aikaisemmin organisaation tietoturvallisuuden sertifiointi oli mahdollista esimerkiksi standardin BS 7799 vaatimusten mukaan. Nykyisin sertifiointi suoritetaan ISO/IEC 27001-standardiin perustuen, eli ISO-standardi on korvannut BS 7799-standardin. (Laaksonen ym. 2006, 105-106.)

6.3 Standardit

Standardisointi on yhteisten toimintatapojen laatimista ja sen tarkoitus on helpottaa viranomaisten, elinkeinoelämän ja kuluttajien elämää. Lisäksi standardisoinnilla lisätään tuotteiden yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa. (Suomen Standardisoimisliitto SFS, 2012.)

Standardit laaditaan yhteistyönä työryhmissä ja komiteoissa, joihin voi osallistua viranomaisten, teollisuuden, kaupan, käyttäjien, kuluttajien sekä korkeakoulujen, tutkimuslaitosten ja järjestöjen edustajia. Kaikkien osapuolten näkökannat pyritään ottamaan valmistelussa huomioon sekä pääsemään yhteisymmärrykseen sisältökysymyksissä. (Pohjola 2011, 14.)

Standardit julkaistaan asiakirjoina, joita kuka tahansa voi hankkia ja käyttää. Standardien käyttö ja hyödyntäminen on maksutonta, joskin standardien hankinta on maksullista. Näin rahoitetaan huomattava osa SFS:n ja sen toimialayhteisöjen standardisointityöstä. (Suomen Standardisoimisliitto SFS, 2012.).

Keskeisimmät tietoturvastandardit ovat nykyisin *ISO-standardeja*. Näiden standardien perustana on usein käytetty kansallisia standardeja, jotka ovat saavuttaneet alkuperämaata laajemman suosion. ISO:n jäseninä ovat noin 150 maan kansalliset standardoimiselimet, minkä johdosta ISO-standardit ovat laajasti levinneitä ja tunnustettuja. (Laaksonen ym. 2006, 85.)

Tietoturvastandardeilla voi olla suuri merkitys organisaatioiden ja yritysten välisen liiketoiminnan ja kumppanuuden kannalta. Mikäli organisaatio noudattaa tiettyä standardia omassa toiminnassaan, on mahdollista, että potentiaaliselta yhteistyökumppanilta vaaditaan samanlaista laatutasoa tietoturvallisuuden osalta. (Laaksonen ym. 2006, 85.)

6.3.1 ISO/IEC 17799

ISO/IEC 17799 on kenties parhaiten tunnettu standardi BS 7799 standardin jälkeen, ja se on pyritty suunnittelemaan soveltuvaksi sekä pienien, että suurien yritysten käyttöön. ISO/IEC 17799 laadittiin BS 7799-standardin osan yksi pohjalta vuonna 2003 ja siitä julkaistiin uudistettu versio vuonna 2005. Standardin nimi on ISO/IEC 17799:2005 (Information technology-Security techniques-Code of practise for information security) ja se tarjoaa ohjausta tietoturvallisuuden hallinnoimiseksi. Standardia ei ole tarkoitettu sertifioinnin perustaksi, eikä organisaatio voi siten olla ISO 17799/IEC -sertifioitu, vaikka tällaisia väitteitä voi kohdata. (Laaksonen ym. 2006, 86.)

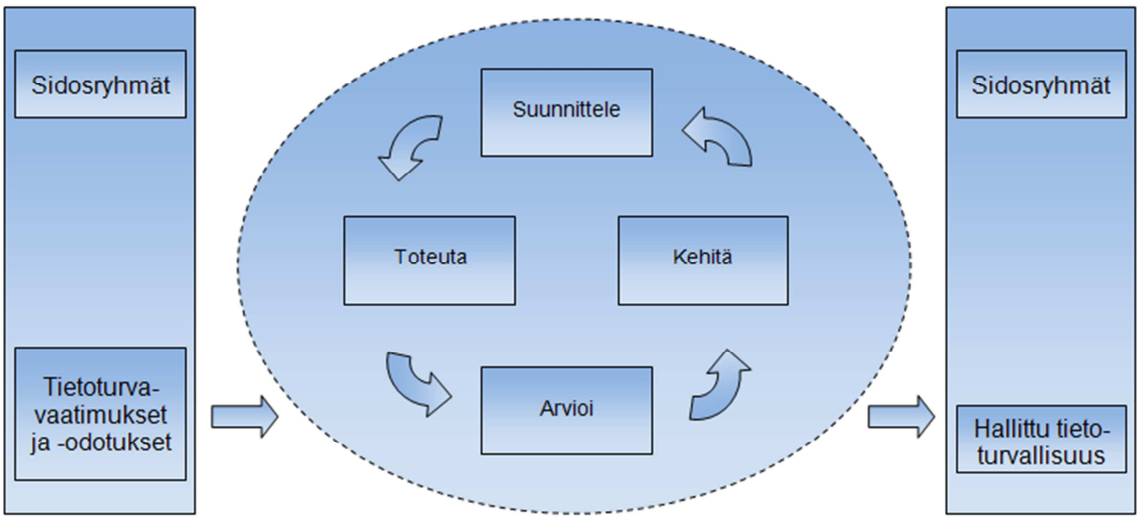
ISO/IEC 17799 ottaa huomioon OECD:n ohjeistuksen tietojärjestelmien ja tietoverkkojen tietoturvaperiaatteista. Ohjeistus laadittiin vuonna 1992, minkä jälkeen sitä päivitettiin vuonna 2002, jolloin esitettiin myös käsite tietoturvallisuuskulttuuri. (Laaksonen ym. 2006, 86.)

6.3.2 ISO/IEC 27001

ISO/IEC 27001 on kansainvälinen standardi, joka kattaa kaikentyyppiset organisaatiot, kuten kaupalliset yritykset, valtion virastot ja ei kaupalliset organisaatiot. Tämä kansainvälinen standardi määrittelee ne vaatimukset, jotka koskevat dokumentoidun

tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, käyttämistä, valvontaa, katselmointia, ylläpitoa ja parantamista ottaen huomioon organisaation yleiset liiketoimintariskit. Standardi määrittelee vaatimukset turvamekanismien toteuttamista varten yksittäisen organisaation tai sen osien yksilöllisten tarpeiden mukaisesti. (ISO/IEC 27001:2005, 10-11.)

ISO/IEC 271001 -standardissa esitetyt vaatimukset ovat yleisiä ja tarkoitus on, että ne soveltuvat kaikille organisaatioille niiden tyypistä, koosta tai luonteesta riippumatta. (ISO/IEC 27001:2005, 10-11). Lisäksi tässä kansainvälisessä standardissa *viittaukset liiketoimintaan tulisi tulkita laajasti tarkoittamaan niitä toimintoja, jotka ovat organisaation olemassaolon ydintarkoitus* (Suomen Standardisoimisliitto SFS, tuotetiedot ISO/IEC 27001:fi). ISO/IEC 27001-standardissa hyödynnetään ”suunnittele-toteuta-arvioi-kehitä -mallia (PDCA-malli), jonka mukaan jäsennetään kaikki standardin hallintaprosessit (kuva 15).



Kuva 15. Tietoturvallisuuden hallinnan PDCA-sykli (ISO/IEC 27001:2005, 8-9).

6.3.3 ISO/IEC 27002

ISO/IEC 27002 -standardi on tietoturvallisuuden hallintaa koskeva menettelyohje. Standardissa tietoa pidetään erittäin tärkeänä suojattavana kohteena muiden liiketoiminnallisten kohteiden tavoin, minkä vuoksi tietoa on suojattava asianmukaisesti. Standardin mukaan systemaattisessa ja toistuvassa turvallisuusriskien arvioinnissa on

otettava huomioon erilaiset muutokset, kuten muutokset suojattavissa kohteissa. (Pohjola 2011, 15.)

6.3.4 ISO/IEC 27003

ISO/IEC 27003 -standardissa keskitytään tietoturvallisuuden hallintajärjestelmän rakentamiseen. Standardin tarkoituksena on tuoda esille seikat, jotka auttavat järjestelmän suunnittelussa ja toimeenpanemisessa. *Suojattavien kohteiden tunnistamis- ja luokittelutarve* otetaan standardissa esille osana tarvittavan vaatimustason määrittelyä. Standardin tehtäväohjeistuksessa neuvotaan keräämään seuraavaa tietoa; prosessien yksilöidyt nimet, prosessien kuvaukset, prosessien kriittisyys organisaatiolle, prosessien omistajat, input- ja output -liittymäprosessit, prosesseja tukevat tietotojärjestelmät sekä tietoaineistot turvallisuustarpeiden mukaisesti luokiteltuina. Nämä tiedot ovat syötteenä tietoturvallisuuden rakentamisen seuraavalle vaiheelle, jossa arvioidaan riskit. (Pohjola 2011, 16.)

6.3.5 ISO/IEC 27005

ISO/IEC 27005 -standardi on tietoturvallisuuden hallintajärjestelmäkontekstiin sovellettu *riskienhallintastandardi*. Se on luonteeltaan ohjaava ja käsittelee riskienhallinnassa huomioon otettavia näkökohtia, ottamatta kantaa varsinaisiin menetelmiin ja työkaluihin. Standardin mukaan kaikki asiaankuuluvat suojattavat kohteet on otettava huomioon riskien arvioinnissa. Standardissa suojattava kohde määritellään kaikeksi, jolla on arvoa ja mikä tämän johdosta vaatii suojausta. Lisäksi standardissa muistutetaan, että kohteiden tunnistaminen on tehtävä soveltuvalla yksityiskohtaisuuden tasolla riskien arvioimiseksi. Edelleen pidetään tärkeänä tunnistaa jokaiselle kohteelle omistaja vastuun ja tilivelvollisuuden toteamiseksi. Lisäksi omistajalla on usein paras näkemys kohteen arvosta ja vaikutuksista. (Pohjola 2011, 16.)

6.3.6 BSI-standardit

Saksan tietoturvavirasto, Bundesamt für Sicherheit in der Informationstechnik (BSI) on julkaissut tietoturvallisuuden hallintaan liittyviä standardeja kansallisen julkishal-

linnon käyttöön sekä laajemmin hyödynnettäväksi. Standardit ovat pääosin ISO/IEC 27001 -sarjan standardeista johdettuja. (Pohjola 2011, 17.)

BSI-standard 100-1 kuvaa, miten tietoturvallisuuden hallintajärjestelmä määritellään ja suunnitellaan. Standardia käytetään myös sertifioinnin vaatimuslähteenä. BSI-standard 100-2:ssa neuvotaan ensimmäisen osan mukaisen hallintajärjestelmän rakentaminen. Esitetyn mallin lähtötilanteen kartoituksessa ja rakenneanalyysissä tarvitaan tiedot organisaatiosta, infrastruktuurista, tietojärjestelmistä, sovelluksista ja työntekijöistä. (Pohjola 2011, 17.)

6.3.7 SoGP-standardi

The Standard of Good Practise (SoGP) for information Security on kansainvälisen Information Security Forum (ISF) -järjestön tuottama yhtenäinen kuvaus tietoturvallisuuteen liittyvistä hyvistä käytännöistä. Tässä yhteydessä standardi tarkoittaa järjestön itse määrittämää suositusta jäsenilleen ja järjestön ulkopuolisille tahoille. (Pohjola 2011, 18.)

SoGP-mallin tietosisältö pohjautuu foorumin puitteissa tehtyyn tutkimukseen, jäsenistöltä selvitettyyn käytännön kokemukseen sekä aiheeseen liittyvien keskeisten standardien, viitekehysten ja mallien analysointiin ja integrointiin. (Pohjola 2011, 18.)

Nimensä mukaisesti standardi tarjoaa tietoturvallisuuden parhaita käytäntöjä ja se lähtee perusajatuksesta, että kaikki sen suositukset tulisivat ottaa käyttöön, ellei joidenkin suositusten poisjättämiselle ole liiketoiminnallisesti perusteltua syytä (Laaksonen ym. 2006, 90).

6.4 KATAKRI-kriteeristö

Kansallisen turvallisuusauditointikriteeristön päätavoitteena on yhtenäistää viranomaistoimintoja silloin, kun viranomainen toteuttaa yrityksessä tai muussa yhteisössä kohteen *turvallisuustason todentavan* tarkastuksen, auditoinnin. Viranomainen voi tarpeen mukaan täydentää auditointia arvioinneilla. Nämä toimet eivät kuitenkaan kuulu itse auditoinnin, eivätkä tämän kriteeristön piiriin. Tämä kriteeristö toimii kan-

sallisesti velvoittavana asiakirjana silloin, kun suomalaisten yritysten turvallisuustaso varmennetaan kansallisen turvallisuusviranomaisen toimesta kansainväliseen viranomaispyyntöön pohjautuen ja *yritysturvallisuustodistuksen* myöntämiseen tähdäten. (KATAKRI 2011, 3.)

Turvallisuusauditointikriteeristön toinen päätavoite on auttaa yrityksiä ja muita yhteisöjä sekä myös viranomaisia sidosryhmineen omassa sisäisessä turvallisuustyössään. Kriteeristö sisältää tästä syystä erilliset, viranomaisvaatimusten ulkopuoliset ”elinkeinoelämän suositukset”, joista toivotaan voitavan poimia kulloinkin käyttökelpoisia turvallisuuskäytänteitä ja edetä tätä kautta tarvittaessa viranomaisvaatimusten tasolle. (KATAKRI 2011, 3.)

Turvallisuusauditointikriteeristö jakautuu neljään pääosioon: hallinnolliseen turvallisuuteen (turvallisuusjohtaminen), henkilöstöturvallisuuteen, fyysiseen turvallisuuteen ja tietoturvallisuuteen. Auditointitapahtumassa tulee huomioida näiden kaikkien neljän osion vaatimukset, eli osioita ei ole rakennettu itsenäisiksi kokonaisuuksiksi. (KATAKRI 2011, 3.)

Viranomaisvaatimukset noudattavat kolmiportaista luokittelua, joka vastaa valtionhallinnon tietoturvallisuusasetuksen mukaisia turvallisuustasokäsitteitä; *perustaso, korotettu taso, korkea taso*. Näitä täydentävät elinkeinoelämän suositukset. (KATAKRI 2011, 3.)

6.5 Toimintamallit

Tietoturvallisuuden hallinnointiin on kehitetty useita erilaisia malleja. Osa malleista käsittelee yksin tietoturvallisuutta ja osa keskittyy liiketoiminnan kokonaisuuden tukemiseen. (Laaksonen ym. 2006, 91.)

Toimintamalleja ei sellaisenaan voi pitää velvoittavina vaatimuksina. Virastoissa on harkittava ja arvioitava oman toiminnan kannalta mahdollista tarvetta sitoutua yleisiin malleihin tai standardeihin esimerkiksi keskinäisen luottamuksen rakentamiseksi. Toimintamalleista löytyy kuitenkin tarpeellista lisätietoa ja hyvää arviointikriteeristöä

virastokohtaiseen työskentelyyn. (Tietoturvallisuuden hallintajärjestelmän arviointisuositus 2003, 22.)

6.5.1 COBIT-Tietojärjestelmien hallinnoinnin viitekehys

COBIT (Control Objectives for Information and related Technology) on *viitekehys*, jota organisaatio voi hyödyntää määritellessään tietojenkäsittelyn liiketoiminnallisia vaatimuksia ja tavoitteita. Sen on kehittänyt kansainvälinen asiantuntijajärjestetö ISACA (Information System Audit and Control Association). COBIT auttaa hahmottamaan, mitä asioita ja toimintoja organisaation tietojenkäsittely sisältää. (Laaksonen ym. 2006, 92.)

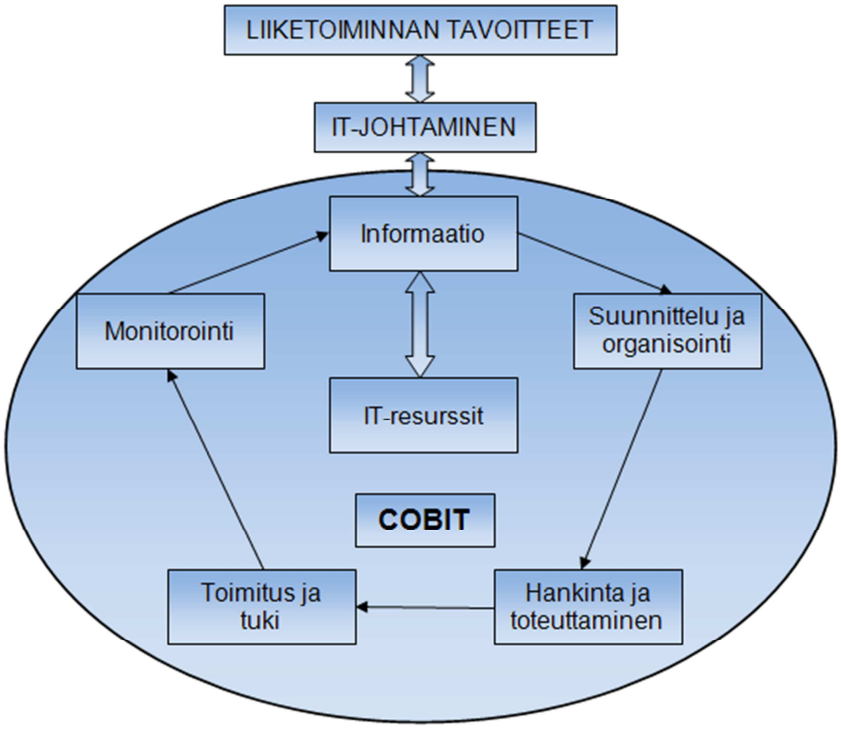
COBIT on teknologiasta riippumaton viitekehys, mikä tekee siitä myös hyvin yleisluontoisen mallin, joka ei ota kantaa siihen, miten asiat tulee hoitaa käytännössä. Se toimii parhaiten yleisen tason mallina, jonka avulla voi varmistua siitä, että toiminnan organisoinnissa on otettu huomioon kaikki toimintaan liittyvät tietojenkäsittelytarpeet. Organisaation tulee käyttää yksityiskohtaisten ohjeiden laatimiseen muita lähteitä, kuten aiemmin esitettyjä standardeja tai esimerkiksi Vahti-ohjeita. (Laaksonen ym. 2006, 92.)

COBIT-mallissa tarkastellaan kohdetta kaikista valvonnan näkökulmista mukaan lukien tietoturvallisuus, mutta toisaalta se ei käsittele kaikkia tietoturvallisuuteen liittyviä osa-alueita, kuten asiakirjaturvallisuutta tai tietosuojaa. Mallin keskeisiä osia ovat kohdealueen määritellyt *valvontatavoitteet, arviointiohjeet ja kypsyystasomalli*. COBIT on suunnattu johdolle, tietohallintohenkilöstölle, tietotekniikkapalvelujen hankkijoille ja arvioijille. (Tietoturvallisuuden hallintajärjestelmän arviointisuositus 2003, 22.)

COBIT auttaa tunnistamaan ja määrittelemään monia tietoturvallisuuden kannalta keskeisiä prosesseja ja sen mukaan IT-resursseja tulee johtaa prosesseina, jotka tuottavat organisaation toiminnalle tärkeää ja tarpeellista tietoa. Mallin avulla pyritään löytämään organisaatiolle *tärkeät valvonnan kohteet* sekä mittaamaan, miten tietojenkäsittely vastaa odotuksia. Lisäksi se auttaa tietohallinnon toimintojen vertailemisessa organisaatioiden välillä. COBIT on linkitetty sisäisen tarkastuksen viitekehykseen

COSO:on, ISO 17799 - tietoturvastandardiin sekä tietojenkäsittelyn parhaisiin käytäntöihin *ITIL:iin*. (Laaksonen ym. 2006, 92.)

COBIT malli sisältää menettelyn organisaation tietohallinnon ja -tekniikan toteuttamiseksi liiketoimintatavoitteisiin tukeutuen. Siinä on neljä hallinnollista aluetta, jotka kattavat kaikkiaan 34 prosessia. Lisäksi toteutumisen tasoa mitataan kypsyysmallilla, jonka selvittämiseksi on annettu mittaristo. Kuvassa 16 on havainnollistettu COBIT-prosessi. (Kalander 2007, 8.)



Kuva 16. COBIT-prosessi. Mukaillen hyödynnetty (Kalander 2007, 8) kuvaa.

6.5.2 ITIL

ITIL (Information Technology Infrastructure Library) on kokoelma tietojenkäsittelyn palvelutuotantoon liittyvistä parhaista käytännöistä. ITIL:n ensimmäinen versio on laadittu 1980-luvun lopussa ja sitä on aktiivisesti kehitetty kattamaan tärkeimmät IT-palvelutuotannon toimintatavat. ITIL on vapaasti saatavalla, vaikka se on suojattu tekijänoikeudella. Vapaan käytön ansiosta ITIL on levinnyt laajalti tietotekniikan palveluyritysten suosimaksi viitekehykseksi, jota käytetään *palvelujen standardoimiseen*. (Laaksonen ym. 2006, 95.)

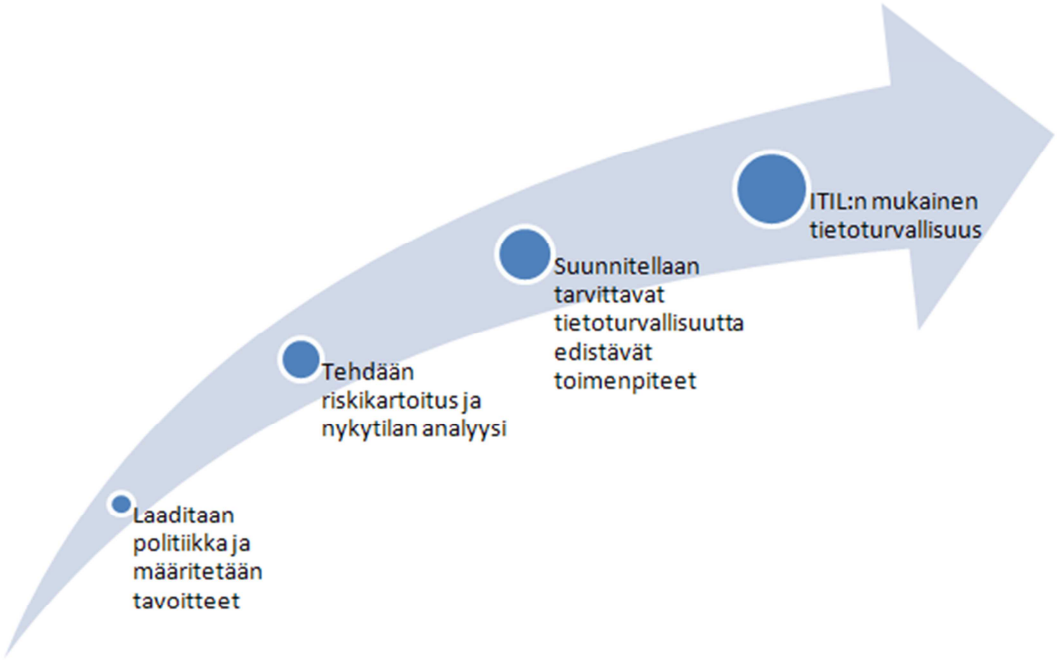
ITIL ei ole vaatimusmäärittely, joten organisaation toiminnan ei voida sanoa olevan ITIL:n vaatimuksen mukaista. ITIL on kokoelma hyväksi havaittuja toimintatapoja, joita voi soveltaa omassa toiminnassa ja se sopii kaikenkokoisille organisaatioille. ITIL koostuu seitsemästä osasta, joista tärkein, *palvelujen hallinta*, on jaettu kahteen kokonaisuuteen; palvelujen tukeen ja palvelujen tuottamiseen (Laaksonen ym. 2006, 95-97.)

Käytännössä ITIL on nimensä mukaisesti kirjasarja, joka sisältää seitsemän teosta, joista kukin teos käsittelee yhtä asiakokonaisuutta Laaksonen ym. (2006, 97) mukaan seuraavasti:

1. IT-palvelujen tuottaminen.
2. IT-palvelujen tuki.
3. IT-palvelujen toteutuksen suunnittelu.
4. Turvallisuuden hallinta.
5. Infrastruktuurin hallinta.
6. IT-toimintojen liiketoiminnallinen näkökulma.
7. Sovellusten hallinta.

ITIL määrittelee tietoturvallisuuden johtamisen periaatteet, joiden mukaan tietoturvallisuus tulee ottaa huomioon palveluiden suunnitteluvaiheessa. ITIL:n mukaan tietoturvallisuuden johtaminen on prosessi, jonka avulla määritetään organisaation tietoturvallisuuden taso. Lisäksi tietoturvallisuuden johtamisella varmistutaan siitä, että organisaatiolla on *riittävä määrä kontrolleja*, joilla ehkäistään uhkatilanteita, havaitaan mahdolliset vaaratilanteet ja korjataan aiheutuneet vahingot. (Laaksonen ym. 2006, 98-99.)

ITIL edellyttää myös tietoturvallisuuden säännöllistä tarkastamista ja raportointia tietoturvallisuuden nykytilasta. ITIL:n perusajatus ei juuri poikkea esimerkiksi ISO-27001 standardin vaatimuksista tai ISO 17799-standardin suosituksista. Kuvassa 17 havainnollistetaan ITIL:n mukaisia tietoturvatoimenpiteitä. (Laaksonen ym. 2006, 98-99.)



Kuva 17. ITIL:n mukaiset tietoturvatoimenpiteet. Mukaillen hyödynnetty (Laaksonen ym. 2006, 99) kuvaa.

6.5.3 GASSP, GAISP

GASSP (Generally Accepted System Security Principles) perustuu Amerikan Yhdysvaltojen kansallisen tutkimuskeskuksen vuonna 1990 julkaisemaan raporttiin, *Vaaralle alttiit tietokoneet (Computer at risk).* Raportin pohjalta laadittiin yleiset *järjestelmäturvallisuuden periaatteet* eli GASSP. Nykyisin GASSPia kehittää kansainvälinen järjestö ISSA (Information System Security Association), jonka tukena toimivat kansainvälinen tietoturvasertifiointiyhteenliittymä ISC2 sekä kansainvälinen standardoimisorganisaatio ISO. (Laaksonen ym. 2006, 100.)

GASSP:n nimi on vaihtunut ja nykyään se tunnetaan nimellä GAISP (Generally Accepted Information Security Principles). Se toimii kattavana viitekehyksenä tietoturvatyössä riippumatta siitä, mitä periaatteita, standardeja tai menetelmiä organisaatiossa käytetään. GAISP:n johtavat periaatteet on jaettu kolmeen osaan Laaksonen ym. (2006, 100-103) mukaan seuraavasti:

1. Organisaation kaikille toiminnan tasoille tarkoitettuja periaatteita on yhdeksän. Nämä periaatteet ovat kokonaisuuden kannalta olennaisia ja perustavaa laatua olevia ja ne on tarkoitettu organisaation johdon sovellettavaksi.

2. Yleisluontoisia toiminnallisia periaatteita on neljätoista. Ne kuuluvat yleisten perusperiaatteiden alle ja ovat luonteeltaan kuvailevampia. Ne on tarkoitettu operatiivisen johdon sovellettavaksi.

3. Yksityiskohtaiset periaatteet on suunnattu tietoturvasta vastaaville henkilöille. Näitä periaatteita on runsaasti ja ne antavat yksityiskohtaisempia ohjeita ylemmän tason periaatteiden toteuttamiseksi.

7 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

7.1 Johdanto

Tietoturvallisuuden hallintajärjestelmä, ISMS (Information Security Management System) on systemaattinen lähestymistapa -menetelmä ja prosessi, jolla hallitaan organisaation tietoturvaa ja suojataan niitä tietoja, joiden on katsottu tarvitsevan suojausta (Tammisalo 2007, 10.)

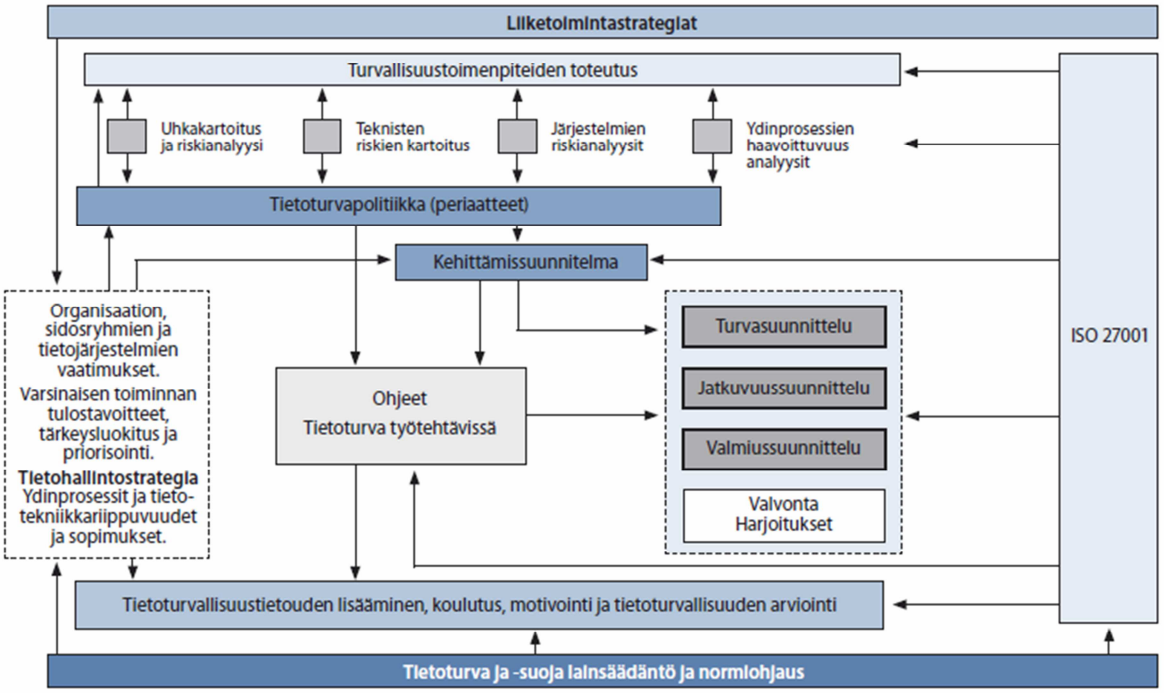
Tietoturvallisuuden hallintajärjestelmä toteuttaa *organisaation strategiaa*. Hallintajärjestelmä kattaa tietoturvallisuuden yksityiskohtaisen organisoinnin, politiikat, suunnittelun, vastuut, menettelytavat, prosessit ja tarvittavat resurssit. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 40.)

Tietoturvallisuuden hallintajärjestelmä on Pohjola (2011, 65) mukaan toimintamalli tietoturvallisuuden kehittämiseen, toteuttamiseen, valvontaan, katselmointiin, ylläpitämiseen ja parantamiseen. Sen lähtökohtina ovat mm. tietoturvatarpeet, -vaatimukset ja odotukset, toiminnan ja tietoturvallisuuden kannalta tärkeiden turvattavien kohteiden määrittely, riskien tunnistaminen ja arviointi sekä siihen pohjautuvat suunnitelmalliset kehittämistoimenpiteet, aikataulut ja vastuut, resurssit, seuranta, mittaaminen sekä jatkuva parantaminen.

Tietoturvallisuuden hallintajärjestelmän avulla seurataan tietoturvatoimien tehokkuutta ja tarkoituksenmukaisuutta. Järjestelmän jatkuva kehittäminen parantaa organisaation valmiuksia hallita *systemaattisesti tietoturva-asioitaan*. Tietoturvallisuuden hallintajärjestelmä on luonteeltaan viitekehys, johon sisältyy mm. Tietoturvallisuuden hallintajärjestelmän arviointisuositus (2003, 13-14) sekä Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan (2007, 40) mukaan seuraavat toimintamallit ja asiakirjat:

- tietoturvapolitiikka ja -strategia
- tietoturvakäytännöt ja -periaatteet, joka kuvaa käytössä olevat turvakäytännöt
- tietoriskien arviointi
- tietoturvallisuuden kehittämissuunnitelma
- tietoturvallisuuden toteutustapa, organisaatio ja vastuut
- toimintaan liittyvät tietoturvaprosessit
- tietoturvallisuuden perus- ja lisäohjeistus
- tietoturva-arkkitehtuurit (topologia ja ratkaisujen periaatekuvaukset)
- tietoturvallisuuden tulosohjaus
- auditointisuunnitelma
- pelastus-, jatkuvuus- ja valmiussuunnitelmat
- vuosisuunnitelmat ja budjetit
- tietoturvaraportointi johdolle

Tietoturvallisuuden hallintajärjestelmän olennaisimmat osat ovat ajantasainen *tietoturvapolitiikka* ja siihen liittyvät asiakirjat sekä säännöllinen *tietoriskien hallinta*, joka koskee sekä nykyistä toimintaa että suunniteltuja muutoksia. Näiden pohjalta laaditaan *tietoturvastrategia* ja *suunnitelmat*, joiden avulla tietoturvaratkaisut toteutetaan tietoturvavaatimusten mukaisesti. Hallintajärjestelmä sisältää myös *tietoturvatoiminnan tehokkuuden* ja tarkoituksenmukaisuuden *säännöllisen mittaamisen ja arvioinnin*. Kuvassa 18 esitetään tietoturvallisuuden hallintajärjestelmän malli. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 42.)



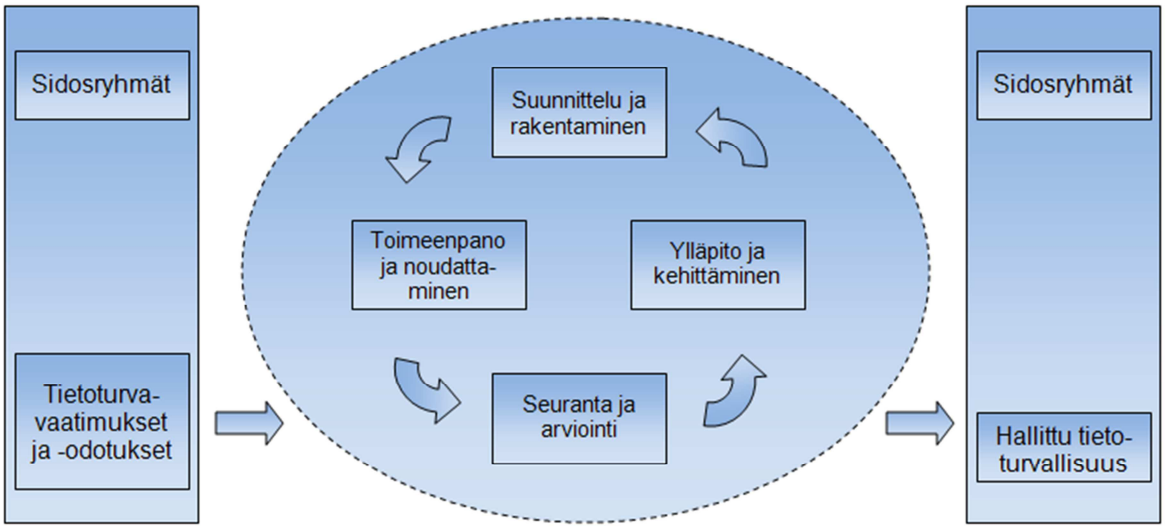
Kuva 18. Tietoturvallisuuden hallintajärjestelmän malli. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 41).

Tietoturvallisuuden hallintajärjestelmän kehittämisessä voidaan käyttää apuna erilaisia *kypsyysmalleja* (esimerkiksi luku 3.2, kuva 2 ja 3), joiden avulla *tietoturvatoiminnan nykytila* voidaan määrittää ja asettaa sen kehittämiselle *tavoitetaso*, joka toteuttaa organisaation tietoturvallisuudelle linjatut vaatimukset. Organisaatio voi myös sitoutua noudattamaan *tietoturvastandardien kuvaamia prosessimalleja* tietoturvallisuuden kehittämisessä. Kuvassa 19 on havainnollistettu ISO/IEC 27001 mukaisen prosessimallin soveltamista tietoturvallisuuden hallintajärjestelmän kehittämisessä.

Tietoturvastandardi ISO/IEC 27001 mukaisen kehittämisen PDCA (Plan, Do, Check, Act) -prosessimallin sisältämät tehtävät voidaan (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 38) mukaan jakaa 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



Kuva 19. PDCA-mallin soveltaminen tietoturvallisuuden hallintajärjestelmän kehittämisessä (ISO/IEC 27001:2005, 8-9).

Kuvan 19 mukainen *tietoturvallisuuden hallintaprosessi* eli tietoturvallisuuden hallintajärjestelmän kehittämisen ja ylläpitämisen prosessi kuvaa olennaisin osin myös *tietoturvallisuuden johtamisjärjestelmän*. Prosessin tavoitteena on tuottaa hallittu tietoturvakokonaisuus, joka osaltaan mahdollistaa organisaation tavoitteiden toteutumisen ja toiminnan luotettavuuden. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 39.)

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. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 42.)

7.2 Tietoturvallisuuden hallintaprosessin viitekehys

Tässä työssä tietoturvallisuuden hallintajärjestelmän kehittäminen esitetään PDCA -prosessimallin mukaan. Viitekehyksenä käytetään Vahti-ohjeita, joista keskeisimmät on mainittu tämän työn johdanto -sivulla. Lisäksi PDCA-syklin kokonaisuuden hahmottamisessa hyödynnetään Tammisalon (2007, 27) dokumentissa esitettyä hallinnointiprosessin mallia. Hallintaprosessin kutakin vaihetta kuvaavia kuvia tulee tulkita PDCA-syklin mukaisesti jatkumona, vaikka prosessivaiheen edelliseltä osalta tulevia ja prosessivaiheesta lähteviä nuolia ei ole merkitty erikseen tietoturvallisuuden hallintaprosessin kuviin (kuvat 20, 22-24).

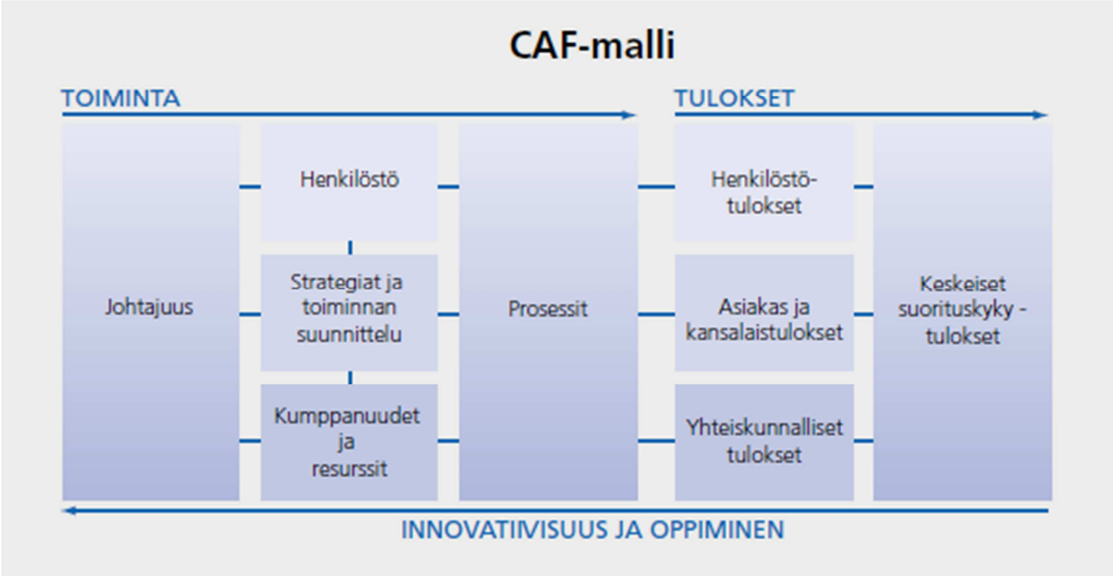
Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (2010, 45) -asiakirjassa esitetään hallinnollista tietoturvallisuutta koskevien vaatimusten yhteydessä *CAF-laatumalli* (Common Assessment Framework), joka on EU-jäsenmaiden yhteistyönä kehitetty *julkisen sektorin organisaatioiden laadunarviointimalli*. CAF-mallin uudistettu versio CAF 2006 julkistettiin Tampereella järjestetyssä Euroopan unionin julkisen sektorin laatukonferenssissa. CAF- itsearviointimalliin on Suomessa tehty erillisiä liitteitä, joita voi käyttää joko varsinaisen CAF-mallin lisänä tai erillisenä arviointivälineenä. (CAF-yhteinen arviointimalli 2006.)

CAF on tarkoitettu helppokäyttöiseksi työkaluksi julkisen sektorin organisaatioiden suorituskyvyn arviointiin ja kehittämiseen. Yhteinen arviointimalli CAF (2006, 4) mukaan arviointimallilla on neljä päätavoitetta:

1. Helpottaa laatujohtamisen menetelmien käyttöönottoa julkisella sektorilla. Lisäksi itsearviointi on keskeinen osa perinteistä PDCA- kehittämissykliä.
2. Auttaa paikantamaan julkisen sektorin organisaatioiden vahvuuksia ja parantamisalueita.
3. Yhdistää erilaisia käytössä olevia laadunhallintamenetelmiä.
4. Edesauttaa julkisen sektorin organisaatioiden välistä vertailukehittämistä.

CAF on tarkoitettu kaikille julkisen sektorin organisaatioille valtionhallinnossa ja kunnissa. Mallia voi hyödyntää osana laajempaa kehittämistyötä tai sitä voi käyttää

kohdennetusti tiettyyn kehittämistarpeeseen. CAF soveltuu (kuva 20) koko organisaation tai sen osien arviointiin. (Yhteinen arviointimalli CAF 2006, 5.)



Kuva 20. CAF-mallin rakenne. (Yhteinen arviointimalli CAF 2006, 5).

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta -asiakirjassa (2010, 45-46) käsitellään tietoturvallisuuden hallinnan vaatimuksia CAF-laatumallista johdettujen *osatoimintojen avulla*. CAF-mallin mukaan kullekin tietoturvallisuustason ympäristölle asetetaan *hallinnolliset ja tekniset* vaatimukset ao. alakohtien mukaan.

- johtajuus
  - strateginen ohjaus
  - resursointi ja organisointi
  - yhteystyön koordinointi
  - raportointi ja viestintä sidosryhmille
  - johtaminen erityistilanteissa
  - raportointi johdolle

- strategiat ja toiminnan suunnittelu
  - toimintaympäristön vaikutus
  - tavoitteiden määrittely
  - toiminnan kehittäminen riskien arvioinnilla

- toimintaverkoston hallinta
- erityistilanteiden hallinta

– henkilöstö
  - osaamisen ja tietoisuuden kehittäminen ja sanktiot
  - henkilöresurssien ja tehtävien hallinta
  - erityistilanteissa toimiminen

– kumppanuudet ja resurssit
  - sopimusten hallinta
  - toiminnan varmistaminen erityistilanteissa

– toiminnan prosessit
  - tietoaineistojen hallinta

– mittaaminen
  - toiminnan arviointi ja kohdentaminen

CAF-mallin mukaan asetettujen hallinnollisten ja teknisten tietoturvavaatimusten liittäminen tietoturvallisuuden hallintajärjestelmään ja sen kehittämiseen kohdistuu pääasiassa PDCA-syklin *seurannan ja arvioinnin* sekä edelleen jatkumona *suunnittelu ja -rakentaminen* prosessivaiheisiin, joissa tarkastellaan mm. organisaation tietoturvastrategiaa ja tietoturvallisuuden toiminnan suunnittelua. Tämä tulee huomioida valtionhallinnon organisaation tietoturvallisuuden hallintajärjestelmässä, sillä Valtiovarainministeriön antaman Vahti 2/2010 ohjeen Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010 tavoitteena on tehostaa ja yhdenmukaistaa lain viranomaisen toiminnan julkisuudesta (621/1999) perusteella 1.7.2010 annetun ja 1.10.2010 voimaantulleen tietoturvallisuusasetuksen (681/2010) täytäntöönpanoa.

Käytännössä valtionhallinnon organisaatioiden tulee saattaa kuntoon vähintään hallinnollisten ja teknisten tietoturvavaatimusten perustason mukaiset toimenpiteet omassa toiminnassaan. Hallinnolliset ja tekniset tietoturvavaatimukset on kuvattu Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010 -

asiakirjan liitteessä 5, joiden pohjalta on tehty kaksi erillistä Excel-taulukkoa (Tietoturvatasot, organisaatioiden arviointi -taulukko, Tietoturvatasot, IT-arviointi -taulukko) organisaatioiden tietoturvallisuuden kypsyystasoihin liittyvän arvioinnin pohjaksi.

Valtioneuvoston 1.7.2010 julkisuuslain nojalla antamaa tietoturvallisuusasetusta sovelletaan valtionhallinnon viranomaisiin. Näillä tarkoitetaan valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia. (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 3 § 1 kohta)

Tietoturvallisuusasetus ja em. asetusta tukeva Vahti-ohje ovat tärkeä osa valtionhallinnon tietoturvallisuuden kehittämistä koskevan valtioneuvoston periaatepäätöksen 26.11.2009 toimeenpanoa. Ohjeen mukaisella toiminnalla viranomainen voi saavuttaa toiminnassaan ja yhteistyössään vähintään *tietoturvallisuusasetuksen 5 §:n mukaisen tietoturvallisuuden perustason*, joka tasapainottaa organisaation riskienhallintaa ja kustannustehokkuutta. Viranomaisen tietojenkäsittely on saatettava vastaaman 5 §:ssä säädettyjä perustason tietoturvallisuusvaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 23 § 3 mom.).

7.3 Tietoturvallisuuden hallintaprosessi

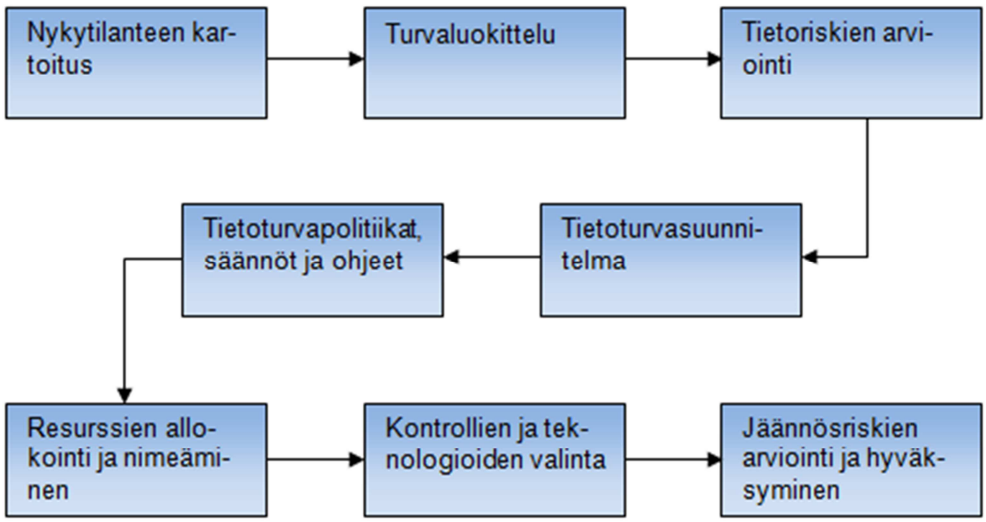
Mikäli organisaatiolla ei ole riittävää tietoturvallisuuden organisaatiota, ensimmäisenä tehtävänä tietoturvallisuuden hallintajärjestelmän kehittämistyössä tulee toimeenpanna *kehittämisprojekti tai esiselvitys* tarvittavan tietoturvatoiminnan aikaansaamiseksi. Siinä selvitetään, millaisella organisaatiolla ja menettelytavoilla organisaation tietoturvatoiminta voidaan perustaa ja miten sitä voidaan kehittää. Varsinainen toiminta on jatkuva prosessi, jonka omistaa ja jota valvoo organisaation johto.

Esiselvityksen yhteydessä tulee tarkasteltavaksi organisaation *tietoturvallisuuden tilannekuva*, jonka yhteydessä arvioidaan tietoturvatoiminnan *nykytila ja kypsyystaso sekä tavoitetila*, joiden mukaan voidaan arvioida reunaehdot tietoturvallisuuden kehit-

tämiselle. Kypsyystason määrittämisessä voi hyödyntää esimerkiksi aikaisemmin luvussa 3.2 esitettyjä kuvien 2 ja 3 mukaisia kypsyystason malleja.

7.3.1 Suunnittelu ja rakentaminen

Tietoturvallisuuden PDCA-mallin mukaisen hallintaprosessin suunnittelun ja rakentamisen vaiheessa (kuva 21) määritetään raamit ja säännöt organisaation tietoturvallisuuden hoitamiselle.



Kuva 21. Tietoturvallisuuden hallintaprosessin suunnittelu ja rakentaminen -vaihe. Mukaillen hyödynnetty (Tammisalo 2007, 27) kuvaa.

Suunnitteluvaihe sisältää Tammisalon (2007, 27) mukaan seuraavat prosessivaiheet:

1. *Nykytilan kartoitus*

   Nykytilan kartoituksessa selvitetään organisaation nykytila ja tavoitteet. Nykytilan kuva luodaan esimerkiksi katsastamalla organisaation toiminta olemassa olevien dokumenttien, lokien ja erikseen tehtävien haastattelujen perusteella. Lopputuloksena syntyy organisaatiolle *tietoturvallisuuden nykytilaa kuvaava dokumentti*, jota hyödynnetään erityisesti tietoturvatoimenpiteiden suunnittelussa. Nykytilan kartoitus tehdään erityisesti organisaation toimintaan kohdistuneiden muutosten tai vaatimusten (lainsäädäntö) yhteydessä/jälkeen, jolloin tietoturvaan liittyviin asiakirjoihin voi kohdistua päivittämistarpeita.

2. *Turvaluokittelu*

   Turvaluokittelussa luokitellaan tiedot ja järjestelmät sekä määritellään niiden tärkeys. Näiden toimenpiteiden pohjalta voidaan myöhemmin suunnitella tietojen riittävät suojaustoimet. Tietojen turvaluokittelussa tunnistetaan keskeiset suojattavat tiedot ja tietojärjestelmät, kuvataan kunkin suojattavan kohteen ominaisuudet sekä nimetään *suojattavalle kohteelle omistaja*.

3. *Tietoriskien arviointi (uhka- ja haavoittuvuuskartoitus, riskianalyysi)*

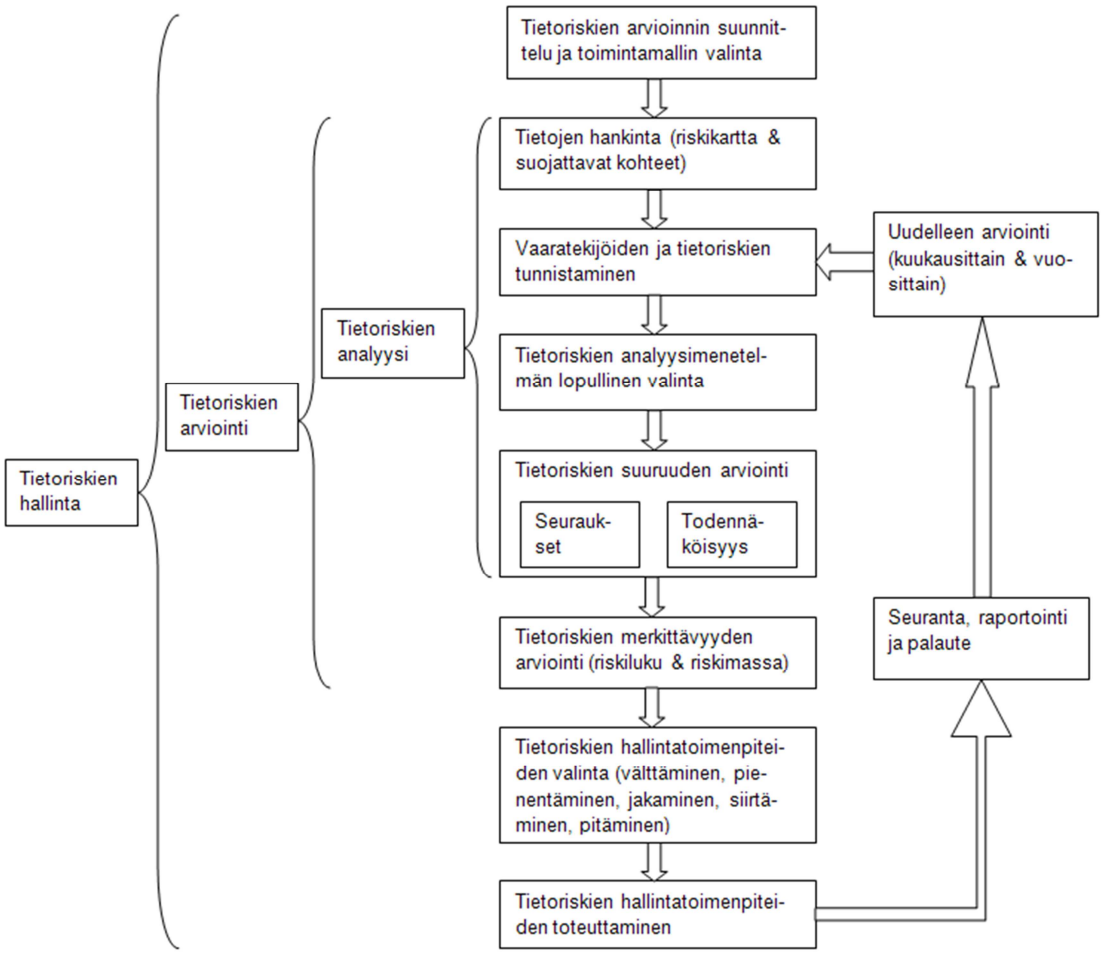
   Organisaatiossa tietoturvatoiminta ilmenee mm. säännöllisinä *tietoriskien arviointi- ja hallintatoimenpiteinä*. Riskienhallinnan periaatteisiin kuuluu riskien hallintajärjestelmän käyttöönotto, ylläpitäminen ja päivittäminen. Toimiva tietoriskien hallinta vähentää ja lievittää organisaatiota uhkaavia menetyksiä ja muita vahinkoja, jolloin se on suunnitelmallista ja jatkuvaa kehittämistoimintaa uhkien tunnistamiseksi, arvioimiseksi ja hallitsemiseksi.

   Organisaation tietoturvallisuuden hallintajärjestelmän olennaisimmat osat ovat ajantasainen tietoturvapolitiikka sekä säännöllinen tietoriskien hallinta. Tietoriskien hallinnan kokonaiskuvan sisäistämiseksi on tärkeää tiedostaa *tietoriskien hallintaprosessin* vaiheet, jotka Moilasen (2011, 11) mukaan muodostavat kuvan 22 mukaisen kokonaisuuden.

4. *Tietoturvasuunnitelma*

   Tietoturvasuunnitelma laaditaan organisaatioon kohdistuvien vaatimusten, suojattavien tietojen sekä tiedossa olevien tietoriskien perusteella. Tietoturvasuunnitelman laadinnassa käytetään apuna mm. tietoriskien arvioinnin tuloksia. Tietoturvasuunnitelmassa linjataan mm. ne toimenpiteet, joilla suojaudutaan riskeiltä, jotka tietoriskien arvioinnissa on nostettu esille.

   Tietoturvallisuuden hallinnan kehittämiseen liittyvät muutokset tehdään käytännössä tässä prosessissa. Myös organisaation *tietoturvatavoitteet ja noudatettavat periaatteet* päivitetään tarvittaessa. Lisäksi tässä prosessissa laaditaan tai päivitetään dokumentit, ”tietoturvasuunnitelma” ja ”tietoturvastrategia”.



Kuva 22. Tietoriskien arviointi- ja hallintaprosessi. Moilasen (2011, 11) kuvassa on mukaillen hyödynnetty Leppäsen (2006, 124) sekä Riskianalyysien laatu (2007, s.7) kuvia.

5. *Tietoturvapolitiikat, säännöt ja ohjeet*

   Tässä prosessissa laaditaan organisaation tietoturvallisuuteen liittyvät politiikat, säännöt ja ohjeet, joita tarvitaan tietoturvan hoitamisessa suunnitellussa laajuudessa ja sovitulla tasolla tietoturvasuunnitelman mukaan. Arvioitavaksi tulevat voimassa olevat politiikat ja sääntöjen kelpaavuus. Lisäksi laaditaan suunnitelmat ja muut tarvittavat dokumentit, joilla *hallinnointiprosessia tarkastetaan ja arvioidaan.*

6. *Resurssien allokointi ja nimeäminen*

   Johdon toimia ovat tietoturvallisuuteen liittyvien vastuiden määrittäminen sekä resurssien varaus ja nimeäminen. Budjetoinnin suunnittelussa on otettava huomioon mm. *henkilöresurssit* ja työntekijöiden tietoturvaan käyttämä aika,

tietoturvan hoidossa tarvittavat *työkalut* sekä aineettomat resurssit, kuten *koulutus ja osaamisen ylläpitäminen*.

7. *Kontrollien ja teknologioiden valinta*
   Käytettäviä kontrolleja ja turvamekanismeja voivat olla esimerkiksi valvonta- ja seurantamenettelyiden sekä hälytysten menettelyt. Valittujen kontrollien ja teknologioiden avulla *suojaudutaan tietoturvauhkilta*. Lisäksi niillä seurataan, valvotaan ja raportoidaan tietoturvauhkista ja toteutuneista loukkauksista. Niitä käytetään myös korjaus- ja toipumistilanteissa.

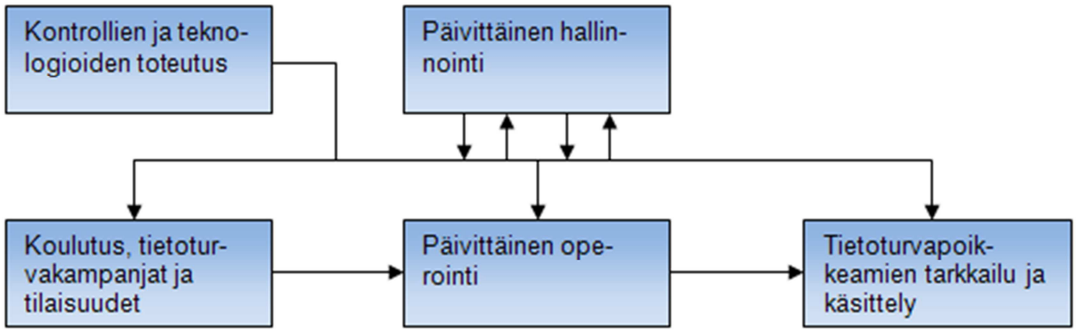
   Erityistä huomiota on kiinnitettävä ulkoisista toimijoista ja alihankkijoista aiheutuvien riskien torjuntaan ja kontrollien valintaan sekä omaan *ohjelmistokehitystoimintaan*, mikäli organisaatiossa sellaista tehdään. Esimerkkejä kontrolleista on runsaasti; organisaatio voi hyödyntää tietoturvatoiminnassaan lukuisia erilaisia standardeja, ohjeita, suosituksia, malleja sekä muita julkaisuja.

8. *Jäännösriskien arviointi ja hyväksyminen*
   Tämän prosessin vaiheessa arvioidaan, kirjataan ja hyväksytään tietoriskit, joihin valitut kontrollit eivät vaikuta ja joita vastaan valituilla kontrolleilla ei voida suojautua. Jäännösriskien tunnistaminen ja hyväksyminen on oleellinen osa tietoriskien hallintaa.

7.3.2 Toimeenpano ja noudattaminen

Toimeenpanon ja noudattamisen vaiheen yhteydessä suoritetaan organisaation päivittäiset ja säännölliset tietoturvatoimenpiteet. Koska kehykset toiminnalle on määritelty aiemmin, tämä vaihe toteuttaa kuvan 23 mukaan, olemassa olevien raamien mukaista toimintaa.

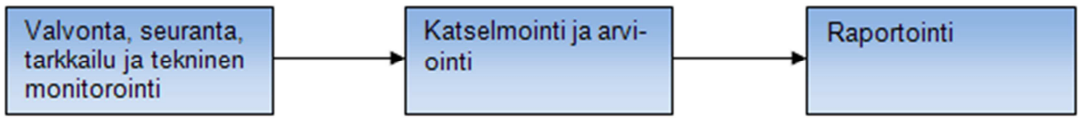
Toimeenpanon ja noudattamisen -vaihe voi olla itseohjautuva, jolloin poikkeamien käsittelyssä havaitut epäkohdat voivat saada aikaan muutoksia teknologioiden toteutukseen. Mikäli nämä muutokset ovat sellaisia, että ne noudattavat voimassa olevaa toimintasuunnitelmaa, niitä ei tarvitse hyväksyttää erikseen esimerkiksi tietoturvaryhmässä.



Kuva 23. Tietoturvallisuuden hallintaprosessin toimeenpano ja noudattaminen -vaihe. Mukaillen hyödynnetty (Tammisalo 2007, 27) kuvaa.

7.3.3 Seuranta ja arviointi

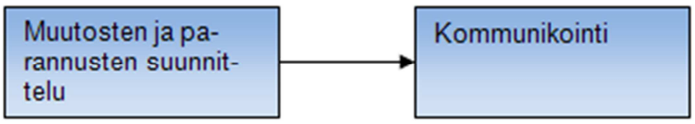
Seurannan ja arvioinnin yhteydessä valvotaan ja arvioidaan *tietoturvallisuuden tilaa, raportoidaan tietoturvasta* tarvittavassa laajuudessa sekä hankitaan tarvittaessa tietoturvatoiminnalle valittu *sertifiointi*. Arvioinnin lopputuloksena tiedetään organisaation tietoturvallisuuden hallintajärjestelmän kelpaavuus ja toimintakyky asetettuihin vaatimuksiin nähden. Tuloksen perusteella voidaan suunnitella ja toteuttaa tarvittavat muutokset hallintaprosesseihin. Kuva 24 esittää seurannan ja arvioinnin prosessivaiheet.



Kuva 24. Tietoturvallisuuden hallintaprosessin seuranta ja arviointi -vaihe. Mukaillen hyödynnetty (Tammisalo 2007, 27) kuvaa.

7.3.4 Kehittäminen

Kehittäminen -vaihe täydentää tietoturvallisuuden hallinnan syklisen prosessikehän. Tässä prosessivaiheessa arvioidaan *muutos- ja kehitystarpeet* organisaation tietoturvallisuuden hallintaprosessiin ja menettelyihin. Mikäli tulee muutostarpeita, niiden käsittely ja muutosten toteuttaminen aloittaa uuden hallintasyklin prosessista ”Suunnittelu” alkaen. Kuva 25 esittää kehittämisen -prosessivaiheet.



Kuva 25. Tietoturvallisuuden hallintaprosessin kehittäminen -vaihe. Mukaillen hyödynnetty (Tammisalo 2007, 27) kuvaa.

8 TIETOTURVALLISUUDEN HALLINTA SUOMEN METSÄKESKUKSESSA

8.1 Johdanto

Vuoden 2012 alusta 13 alueellista metsäkeskusta sekä osia Kehittämiskeskus Tapion toiminnoista yhdistyi valtakunnalliseksi organisaatioksi, Suomen metsäkeskukseksi. Suomen metsäkeskuksen perustan muodostavat julkisia palveluja tuottava Julkiset palvelut ja asiakasrahoitteista palvelutoimintaa tuottava Metsäpalvelut.

Valtakunnallisen organisaation muodostuminen tuo yhtälailla omat kehittämistavoitteet tietoturvallisuuden hallintaan ja suunnitteluun samoin kuin organisaation muuhun kehittämistyöhön. Uusi yhtenäinen toimintatapa antaa mm. aikaisempaa paremmat mahdollisuudet ottaa käyttöön suunnitelmallinen ja yhtenäinen tietoturvallisuuden hallintajärjestelmä.

Metsäkeskuksien tietoturvallisuuden organisointi on perustunut johtajien hyväksymään tietoturvapolitiikkaan, jonka periaatteiden mukaan metsäkeskuksissa toimii mm. *tietoturvaryhmät ja tietoturvavastaavat* sekä muu *tietoturvallisuuden vastuuhenkilöstö*. Lisäksi metsäkeskukset ovat käyttäneet tietoturvallisuuden ylläpidossa ja kehittämisessä *yhteisiä tietoturvaohjeita*.

Metsäkeskusten tietoturvatyön tehostamiseksi perustettiin 2010 yhteinen tietoturvaryhmä. Tietoturvaryhmän keskeisiä tehtäviä ovat mm:

- vuositoimenpideohjelman laadinta ja seuranta
- tietoturvan ja tietoturvadokumentaation kehittäminen
- tietoturvapoikkeamien seuranta

- parannustoimenpiteistä tiedottaminen
- tietoturva-asetuksen velvoitteiden työstäminen
- osallistuminen MMM:n hallinnonalan tietoturvallisuuden ja ICT-varautumisen koordinaatioryhmän kokouksiin

Keskeisesti metsäkeskusten tietoturvan kehittämiseen vaikuttaa 1.10.2010 voimaan tullut *tietoturvallisuusasetus* (*Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681).* Asetuksen tavoitteena on asettaa valtion virastoja sitovat *perustietoturvatason vaatimukset* tietoturvallisuuden kehittämiseksi sekä *yhtenäistää menettelyt* käsiteltäessä salassa pidettäviä ja käytöltään rajoitettuja tietoaineistoja. Kaikkia valtionhallinnon viranomaisia koskeviin tietoturvallisuusvaatimuksiin kuuluu myös mm. toimintaan liittyvien tietoturvallisuusriskien kartoittaminen ja vastuiden määrittely.

Voutilaisen (2012, 124) mukaan *tietoturvallisuusasetuksessa säädettyjen perustason vaatimusten* voidaan katsoa koskevan myös kuntia *ja muita julkisuuslain piiriin kuuluvia toimijoita,* koska asetuksen 5 §:n säännökset on johdettavissa joko *julkisuuslaista tai henkilötietolaista* suoraankin sovellettavaksi myös muihin kuin valtion viranomaisiin.

Metsäkeskuksen tavoitteena on saattaa toimintansa ja tietojenkäsittelynsä vastaamaan asetuksessa säädettyjä perustason (minimivelvoite) tietoturvavaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä; kuten asetus velvoittaa (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681, 23 § 3 mom.). Perustason saavuttamiseksi on julkaistu useita ohjeita koskien sekä hallinnollista, että teknistä tietoturvaa (esimerkiksi Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010).

8.2 Tietoturvallisuuden nykytila

Lähtökohta tietoturvallisuuden nykytilan arvioinnissa, on vuoden 2012 alusta voimaan astunut organisaatiomuutos. Itsenäisistä metsäkeskuksista ja osista Kehittämiskeskus Tapion toiminnoista muodostettiin valtakunnallinen organisaatio, jonka perustan

muodostavat julkisia palveluja tuottava Julkiset palvelut ja asiakasrahoitteista palvelutoimintaa tuottava Metsäpalvelut.

Julkisen palvelun yksikössä on viisi palvelua: metsävaratieto-, metsäalan edistämis-, rahoitus ja tarkastus-, asiakkuus- ja hallintopalvelut. Toimintaa johdetaan keskusyksiköstä, joka toimii Lahdessa ja johon henkilöstö on siirtynyt valtaosin aikaisemman organisaation palveluksesta.

Organisaatiomuutoksen jälkeen metsäkeskuksen tietoturvallisuuden yhteistä kehittämistyötä on suunnattu mm. johdanto -luvussa 8.1 mainitun tehtävälistan mukaisesti toimeksiannolla metsäkeskuksen yhteiselle tietoturvaryhmälle. Viimeaikaiset tehtävät ovat kohdistuneet pääasiassa tietototurvallisuusasetuksen velvoitteiden työstämiseen.

Suomen metsäkeskuksen tietoturvallisuuden organisointi on vielä kesken, joten alueyksiköissä toimitaan tietoturvallisuuden hallinnan osalta samoilla periaatteilla kuin ennen organisaatiomuutosta. Käytännössä metsäkeskuksen alueyksiköiden tietoturvaryhmät ja tietoturvallisuuteen liittyvät vastuukäytännöt ovat voimassa ja toimivat samoilla ehdoilla ja toimintalinjoilla kuin aikaisemmin. Nykyinen toiminta on väliaikaista kunnes metsäkeskuksen tietoturvallisuus ja vastuut on organisoitu uudelleen vastaamaan valtakunnallista organisaatiomallia.

Tietoturvallisuuden nykytilan arvioinnissa pitäydytään *hallinnollisen tietoturvallisuuden* suunnittelu- ja strategiatasolla, joten tietoturvallisuuden hallintaan liittyvät yksityiskohdat jäävät tässä työssä käsittelyn ulkopuolelle. Tietoturvallisuuden nykytila arvioidaan aikaisemmin tämän työn luvussa 7.1 mainittujen ohjeiden; Tietoturvallisuuden hallintajärjestelmän arviointisuositus (2003, 13-14) sekä Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan (2007, 40) mukaan:

1. *Tietoturvapolitiikka ja -strategia*
   Aikaisemmassa organisaatiorakenteessa metsäkeskuksilla on ollut käytössä yhteinen tietoturvapolitiikka, jonka toimintaperiaatteen mukaan tietojen ja tietojen käsittelyn turvaaminen perustuu säädösten ja muiden ulkoisten velvoitteiden noudattamiseen sekä metsäkeskuskohtaiseen riskien analysointiin ja sen pohjalta tehtävään tarkempaan suunnitteluun ja ohjeistamiseen.

Vanha tietoturvapolitiikka on edelleen voimassa ja alueyksiköt toimivat sen mukaan. Kun Suomen metsäkeskuksen tietoturvallisuuden kokonaisuutta organisoidaan uudelleen, tulee tietoturvapolitiikka päivittää samassa yhteydessä vastaamaan uutta organisaatiorakennetta.

2. *Tietoturvakäytännöt ja -periaatteet, joka kuvaa käytössä olevat turvakäytännöt*
   Käytössä olevat tietoturvaohjeet ja -suunnitelmat ovat edelleen voimassa ja alueyksiköiden käytössä vastaavalla periaatteella kuin tietoturvapolitiikka. Tietoturvaohjeet päivitetään uuden tietoturvapolitiikan käyttöönoton yhteydessä/jälkeen.

   Alla on tällä hetkellä keskeisimmät yhteisessä käytössä olevat tietoturvaohjeet ja -suunnitelmat:

   - henkilöstön tietoturvallisuusohjeet
   - esimiesten tietoturvallisuusohjeet
   - atk-henkilöstön tietoturvallisuusohjeet
   - tietoturvallisuussuunnitelma
   - tietoturvallisuusvelvoitteet
   - riskienhallinta- ja tietoturvallisuus metsäkeskuksessa

3. *Tietoriskien arviointi*
   Tietoriskien hallinta pohjautuu samoihin johdon asettamiin ja hyväksymiin menettelytapoihin kuin muu metsäkeskuksen riskienhallinta. *Riskienhallinta* on osa metsäkeskuksen johtamisjärjestelmää, toimintajärjestelmää ja kunkin toiminnon prosesseja normaalin toiminnan suunnittelun yhteydessä.

   Riskikartoituksilla tunnistetaan ja arvioidaan riskejä, niiden todennäköisyyksiä ja vaikutuksia sekä määritellään *priorisoiduille riskeille* hallintakeinoja. Tehtyjen kartoitusten perusteella riskienhallintaa kehitetään edelleen ja varmistetaan jatkuvuus.

   Riskienhallinnan onnistumisen edellytyksenä on *johdon ja henkilöstön sitoutuminen, selkeät vastuut, säännöllinen raportointi, seuranta ja konkreettisten*

toimenpiteiden johtaminen todetuista kehittämiskohteista. Kuvassa 26 on metsäkeskuksen riskienhallinnan vuosikello.

Tietoriskien arviointi suoritetaan toistaiseksi alueyksiköiden tietoturvaryhmissä (kunnes otetaan käyttöön uusi toimintatapa). Ryhmässä tulee olla riittävä edustus eri toiminnoista. Arvioinnissa otetaan huomioon *yhteiset tietoturvaohjeet, riskienhallintaa koskeva lainsäädäntö sekä voimassa olevat Vahti-ohjeet*, kuten Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003, jossa on liitetiedostona mm. luettelo riskien arviointia ohjaavasta lainsäädännöstä.

Kuva 26. Metsäkeskuksen riskienhallinnan vuosikello.

Tietoriskien analyysimenetelmänä on metsäkeskuksessa käytetty esimerkiksi *Potentiaalisten ongelmien analyysimenetelmää (POA),* jonka yhteydessä on hyödynnetty Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003 -asiakirjan käytäntöjä. Lopulliset tietoriskien analyysimenetelmät (mahdolliset lisäanalyysit ja niiden tarvitsemat henkilö- ja aikaresurssit) on sovittu tietoturvaryhmässä vaaratekijöiden ja tietoriskien tunnistamisen jälkeen.

4. *Tietoturvallisuuden kehittämissuunnitelma*
   Tietoturvallisuuden jatkokehittäminen on pääsääntöisesti liittynyt riskienarvioinnin lopputulokseen ja mahdollisiin korjaaviin tietoturvatoimenpiteisiin sekä tietoturvallisuuden kehittämistoimenpiteisiin.

5. *Tietoturvallisuuden toteutustapa, organisaatio ja vastuut*
   Tietoturvapolitiikassa on määritelty mm. tietoturvallisuuden tavoitteet, toimintaperiaatteet, organisointi, vastuut sekä valvonta ja raportointi.

6. *Tietoturvallisuuden perus- ja lisäohjeistus*
   Metsäkeskuksen alueyksiköt ovat ottaneet käyttöön ja toteuttaneet tietoturvallisuussuunnitelmaan, jatkuvuus- ja toipumissuunnitelmaan sekä valmiussuunnitelmaan liittyviä alueyksikkökohtaisia lisäohjeita. Nämä perustuvat ennen organisaatiomuutosta käyttöönotettuihin yhteisiin suunnitelmiin.

7. *Auditointisuunnitelma*
   Auditointisuunnitelma on käytössä ja tietoturvallisuuden auditointia toteutetaan muun organisaatioon kohdistuvan auditoinnin yhteydessä. Lisäksi on tehty erikseen sisäisiä tietoturva-auditointeja ja ristiinauditointeja sekä tietojärjestelmiin liittyviä auditointeja.

8. *Pelastus-, jatkuvuus- ja valmiussuunnitelmat*
   Metsäkeskuksen alueyksiköt ovat ottaneet käyttöön ja toteuttaneet jatkuvuus- ja toipumissuunnitelmaan sekä valmiussuunnitelmaan liittyviä alueyksikkökohtaisia lisäohjeita. Nämä perustuvat ennen organisaatiomuutosta käyttöönotettuihin yhteisiin suunnitelmiin.

Suomen metsäkeskuksen yhteinen tietoturvaryhmä on työstänyt tietoturva-asetuksen vaatimuksia sekä toimenpanoon liittyviä Vahti-ohjeiden velvoitteita. Metsäkeskuksen tietoturvallisuuden tavoitetaso on *perustaso, joka on myös MMM:n hallinnonalalle määritelty vähimmäistaso* ja jonka toimeenpanoon sisältyy hallinnollisen ja teknisen tietoturvan osalta tiedon käsittelyyn ja turvaamiseen liittyviä vaatimuksia, jotka on lueteltu Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010 -asiakirjan (Vahti 2/2010) liitteessä 5.

Metsäkeskuksen yhteinen tietoturvaryhmä on kartoittanut alueyksiköiden tietoturvallisuuden nykytilaa, lähettämällä alueyksiköille läpikäytäväksi ja täytettäväksi valtioneuvoston sivustoilta löytyvät *Tietoturvatasot, organisaation arviointi sekä Tietoturvatasot, IT-arviointi -taulukot,* joiden kysymyksenasettelu vastaa Vahti 2/2010 -ohjeen liite 5 mukaista tietosisältöä.

Metsäkeskuksen tietototuturvaryhmän työtä ohjaa metsäkeskuksen johto. Lisäksi tietoturvallisuuteen liittyvää tiedottamista ja ohjausta tapahtuu osaltaan myös *MMM:n hallinnonalan tietoturvallisuuden ja ICT-varautumisen -koordinaatioryhmän* kautta, jonka kokouksissa tietoturvaryhmällä on edustus.

Metsäkeskuksen yhteisen tietoturvaryhmän keskeisiä tehtäviä on mm. tuoda esille tarvittavat toimenpiteet riittävän tietoturvatason saavuttamiseksi. Tarkoituksena on saada tietoturvallisuuden kehittämiseen liittyvät jatkotoimenpiteet käyntiin yhteistyössä asiasta vastuullisen tahon kanssa (tietojärjestelmän tai prosessin omistaja ym.).

8.3 Tietoturvallisuuden hallinta ja kehittämisen toimenpiteet

8.3.1 Hallintakäytännön taustaa

Metsäkeskuksen tietoturvallisuuden hallinta ja kehittäminen on perustunut ennen organisaatiomuutosta käyttöönotettuun tietoturvapolitiikkaan ja sen mukaisiin toimintatapoihin, ohjeisiin ja suunnitelmiin. Organisaatiomuutoksen jälkeen tietoturvallisuuden organisointi järjestetään prosessien määrittelyn yhteydessä/jälkeen, minkä vuoksi nykyinen toimintatapa jatkuu toistaiseksi ennallaan.

Metsäkeskuksessa (entisissä metsäkeskuksissa) ei ole ollut käytössä erikseen määriteltyä ja dokumentoitua yhteistä tietoturvallisuuden hallintajärjestelmää ja hallintaprosessia. Tietoturvallisuuden kehittäminen on perustunut metsäkeskusten yhteiseen tietoturvapolitiikkaan sekä tietoturvadokumentteihin ja suunnitelmiin, jotka on esitetty aiemmin luvussa 2, nykytilan arvioinnin yhteydessä.

Edellä mainittuja dokumentteja on tarvittaessa päivitetty yhteisten periaatteiden mukaan ja viety edelleen metsäkeskusten tietoturvaryhmien jatkokäsiteltäväksi ja metsäkeskuskohtaisten ohjeiden rungoksi.

Metsäkeskuksissa toimineet tietoturvaryhmät ovat kokoontuneet säännöllisesti, suorittaneet riskienarviointia ja muita tietoturvallisuussuunnitelmassa mainittuja tehtäviä, vieneet tarvittavat tietoturvallisuuden kehittämistyöt tietoturvallisuuden toimenpidesuunnitelmaan sekä raportoineet tietoturvallisuuden tilasta sovitulla tavalla.

Suomen metsäkeskuksen tietoturvallisuuden jatkokehittämiseksi yhteinen tietoturvaryhmä on tehnyt toimeksiannosta esityksen metsäkeskuksen tietoturvallisuuden järjestämisestä. Esityksessä tietoturvaryhmä mm. katsoo, että uuden organisaatiomallin mukaisen tietoturvallisuuden hallinnan ja kehittämisen järjestämisessä ensimmäisiä toimenpiteitä ovat keskeisten tietoturvaan liittyvien tehtävien määrittely ja vastuiden kohdentaminen.

8.3.2 Esiselvitys

Tietoturvaan liittyvien tehtävien määrittelyn ja vastuiden kohdentamisen jälkeen on tarpeen tehdä tietoturvallisuuden esiselvitys, jonka yhteydessä voi hyödyntää luvun 7.3 mukaisia toimenpiteitä. Olennaista on selvittää *millaisilla menettelytavoilla organisaation tietoturvatoiminta voidaan perustaa ja miten sitä voidaan kehittää*. Varsinainen toiminta on jatkuva prosessi, jonka omistaa ja jota valvoo organisaation johto.

Esiselvityksen yhteydessä tulee tarkasteltavaksi metsäkeskuksen tietoturvatoiminnan *nykytila ja kypsyystaso sekä tavoitetila*, joiden mukaan voidaan arvioida reunaehdot tietoturvallisuuden kehittämiselle. Kypsyystason ja tavoitetilan määrittämisessä voi hyödyntää esimerkiksi aikaisemmin luvussa 3.2 esitettyjä kuvien 2 ja 3 mukaisia kypsyystason malleja.

Esiselvityksen yhteydessä tulee mietittäväksi myös metsäkeskuksessa käytettävä *tietoturvallisuuden hallintamalli*. Kysymys on organisaation tietoisesta tietoturvallisuuden hallinnan kiinnittämisestä hallintajärjestelmään ja sen hallintaprosessiin. Periaatteessa organisaation tietoturvallisuuden kehittäminen hoituu jonkinasteisen hallintajärjestel-

män puitteissa, mikäli toiminta on määritelty tietoturvapolitiikassa, jonka käytänteissä on otettu huomioon tietoturvaan liittyvät vastuut, tietoriskien hallinta, tietoturvaan ja tietosuojaan liittyvä lainsäädäntö sekä asiakkaiden ja yhteistyökumppaneiden tietoturvallisuuden hallintaan ja tietosuojaan kohdistetut vaatimukset.

Tietoturvallisuuden hallintajärjestelmän suunnitelmallinen käyttöönotto sekä tietoturvallisuuden hallinnan prosessien liittäminen siihen esimerkiksi luvun 7.3 mukaan, vastaa kuitenkin parhaiten valtionhallinnon organisaatiota kohtaan asetettuja tavoitteita ja on luontevin ratkaisu, mitä suuremmasta organisaatiosta on kysymys.

8.3.3 Metsäkeskuksen tietoturvallisuuden hallintajärjestelmän kehittäminen

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (2010, 45) -asiakirjan mukaan *viranomaisen tulee kehittää ja ylläpitää tietoturvallisuuden hallintajärjestelmää*, joka rakentuu viranomaiselle asetettujen tehtävien toteuttamisen mahdollistamiseksi hyvää tiedonhallintatapaa noudattaen.

Tietoturvallisuuden hallintajärjestelmän avulla voidaan varmistaa tietoturvallisuuden toteutuminen *kaikissa toimintaprosesseissa*. Hallintajärjestelmän avulla seurataan prosessien nykytilaa ja mahdollisia ongelmia sekä ohjataan *korjaavien toimenpiteiden* toteutumista. Lisäksi hallintajärjestelmän avulla voidaan *ohjata tietojärjestelmien ja palvelujen kehittämistyötä* tietoturvallisuuden vaatimusten osalta. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 45.)

Metsäkeskuksen tietoturvallisuuden hallintajärjestelmän suunnittelussa ja kehittämisessä voi hyödyntää tämän työn lukua 7, jossa on esitelty tietoturvallisuuden hallintajärjestelmä ja hallintaprosessi valtionhallinnon organisaation tietoturvallisuuden kehittämisen näkökulmasta.

Tässä työssä tietoturvallisuuden hallintajärjestelmän kehittäminen -osion viitekehyksenä on käytetty mm. Tietoturvallisuuden hallintajärjestelmän arviointisuositus (2003, 13-14) sekä Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan (2007, 40) -ohjeita. Lisäksi tietoturvallisuuden hallintaprosessissa on käytetty viitekehyksenä Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen

täytäntöönpanosta (2010, 45) -asiakirjaa, jossa esitetään hallinnollista tietoturvallisuutta koskevien vaatimusten yhteydessä CAF-laatumalli.

Metsäkeskuksen tietoturvallisuuden hallintajärjestelmän ja hallintaprosessin käynnistämisessä tulee määritellä *tavoitteet ja runko*, jotta suunnitelmallinen tietoturvatoiminta on ylipäätään mahdollista. Tavoitteita ovat esimerkiksi:

- tietoturvallisuuden organisointi (tietoturvavastuut, tehtäväkuvat, tietoturvan hallintaorganisaatio, muut tarvittavat resurssit)
- tietoturvatoiminnassa tarvittavien asiakirjojen laatiminen ja käyttöönotto (tavoitteet, strategia, toimintasuunnitelma ja politiikat)
- tietoturvatoiminnassa suoritettavien toimenpiteiden, turvamekanismien ja tarvittavien teknisten välineiden määrittely
- aikaansaada koko henkilöstölle tarvittava tietoturvan ymmärrys ja sitoutuminen valittujen toimintatapojen noudattamiseen
- hallintaprosessin ja menettelyiden määrittely metsäkeskuksen tietoturvallisuuden hallinnoimiseksi

Kun tietoturvallisuuden hallintajärjestelmän toimintatapa on määritelty toivotulla tavalla ja metsäkeskuksen tietoturvallisuuden järjestämiseksi asetetut tavoitteet on saavutettu, saadaan esimerkiksi ao. lopputulos, jossa tarvittavat dokumentit on laadittu, keskeiset resurssit on varattu, tietoturvatehtävät on tunnistettu ja lueteltu sekä hallintamenettelyt on laadittu.

- tarvittavat dokumentit on laadittu tai päivitetty
    - tietoturvapolitiikka
    - tietoturvastrategia
    - tietoturvatavoitteet
    - tietoturvasuunnitelma
    - toimenpidesuunnitelma
- tarvittavat henkilöresurssit on varattu
    - tietoturvavastaava nimetty
    - tietoturvallisuuden hallintaorganisaatio (tietoturvaryhmä) nimetty

    - muu tietoturvallisuuden erityisvastuuta vaativat tehtävät ja resurssit on varattu
- resurssit on varattu
    - budjetti laadittu
    - tarvittavat hankinnat tehty tai suunniteltu
- päivittäiset tietoturvatehtävät on tunnistettu ja lueteltu
    - seuranta- ja raportointimenettelyt
- tietoriskien hallintamenettelyt on laadittu
- tietoturvallisuuden hallintajärjestelmän ja hallintaprosessin kuvaukset on laadittu
    - tietoturvallisuuden hallintaprosessi on valmis käynnistymään

Tietoturvallisuuden hallintajärjestelmän ja hallintaprosessien toiminnan tarkoituksena on ehkäistä *metsäkeskusta kohtaavia tietoturvauhkia*, mikä vaatii riittävässä määrin myös henkilötyötä. Asianmukaisen tietoturvatyön mahdollistamiseksi sekä tavoitteenmukaisen tietoturvallisuuden toteuttamiseksi on tietoturvatyöhön osallistuville henkilöille varattava *riittävästi työaikaa*. Lisäksi on panostettava *osaamiseen* ja varattava tarvittaessa resursseja lisäkoulutukseen, mikäli tarpeellista. Tässä yhteydessä tulee mietittäväksi myös koko henkilöstölle suunnattu koulutus, johon liittyy tavanomaisiin työtehtäviin liittyvät tietoturvavelvoitteet sekä mahdolliset erityisvastuut ja -velvoitteet koskien työtehtäviä, joihin kohdistuu suurempia tietoriskejä.

9 POHDINTA

9.1 Tietoturvallisuuden kehittäminen

Metsäkeskuksen tietoturvallisuuden kehittäminen pohjautuu pääosin lainsäädännön asettamiin velvoitteisiin sekä valtionhallinnon normiperustaiseen tietoturvallisuuden ohjaukseen, minkä lisäksi maa- ja metsätalousministeriöllä on omat tietoturvallisuuteen liittyvät tavoitteet hallinnonalalleen suuntaamassaan ohjauksessa.

Metsäkeskuksen tietoturvallisuuden kypsyystaso voidaan jatkossa joutua tarkastuttamaan esimerkiksi ulkoisen auditoijan toimesta ennen erilaisten valtionhallinnon orga-

nisaatiolle tarkoitettujen palveluiden käyttöönottoa, millä varmistetaan, että palvelua käyttävällä organisaatiolla on riittävä tietoturvallisuuden taso (perustaso tai korkeampi), ennen kuin palvelu on käytettävissä.

Suomen metsäkeskuksen tietoturva pohjautuu vanhassa organisaatiorakenteessa käyttöönotettuun tietoturvapolitiikkaan, jonka mukaan tietoturvallisuus on osa metsäkeskusten toiminnan laatua ja myös toiminnan perusedellytyksiä. Metsäkeskukset haluavat pysyä luotettavana ja myös luotettavaksi koettuna palvelujen tarjoajana ja toimittajana. Asiakkaiden ja henkilökunnan lisäksi luotettavuutta odottavat ja myös valvovat mm. maa- ja metsätalousministeriö sekä EU:n komissio.

Tietoturvapolitiikassa kuvatuista ohjeista ja suunnitelmista tärkeimpiä on tietoturvallisuussuunnitelma-asiakirja. Siinä ohjeistetaan (silloisten) metsäkeskusten yhteiset suunnitelmalliset toimenpiteet tietoturvallisuuden kehittämiseksi ja ylläpitämiseksi omassa toiminnassaan. Suunnitelmassa ei viitata minkään yksittäisen metsäkeskuksen, toiminnon, toimipaikan tai tietojärjestelmän tietoturvallisuusjärjestelyihin, vaan esitetyt menettelyt ovat metsäkeskuksissa yleisesti sovellettavissa tietoturvaryhmien ja -vastaavien tietoturvallisuuden kehittämistyössä.

Suomen metsäkeskuksen yhteistä tietoturvan kehittämistyötä on myös tehnyt metsäkeskuksen yhteinen tietoturvaryhmä, jonka toiminta on viime aikoina kohdistunut pääosin tietoturvallisuusasetuksen velvoitteiden työstämiseen. Tietoturvaryhmälle ei ole asetettu varsinaista vastuuta ja velvollisuutta tietoturva-asioiden toimeenpanoon liittyen, vaan ryhmän tehtävänä on ollut toimia koordinoijana ja tiedonantajana niille tahoille, joille esitettyjen toimenpiteiden täytäntöönpano kuuluu esimerkiksi järjestelmien tai prosessien omistajuuteen liittyvien velvoitteiden mukaan.

Suomen metsäkeskuksen tietoturvallisuuden jatkokehittämisessä keskeiset tehtävät liittyvät *tietoturvallisuuden hallintajärjestelmän ja hallintaorganisaation sekä tietoturvapolitiikan ja sitä tukevien ohjeiden ja suunnitelmien työstämiseen*. Kehittämistyön välittömiä tehtäviä on lisäksi hajautetun tietoturvallisuuden hallintamallin suunnitelmallinen muuttaminen kohti yhdenmukaista ja keskitettyä, valtakunnallisen organisaatiorakenteen mukaista hallintamallia.

9.2 Kohti tietoturvallisuuden hallintajärjestelmää

Tässä opinnäytetyössä on koostettu kokonaisuus, jota Suomen metsäkeskuksen tietoturvallisuuden hallintaorganisaatio (esimerkiksi tietoturvaryhmä) voi hyödyntää metsäkeskuksen tietoturvallisuuden kehittämistyössä. Työn alkuosassa käydään läpi tietoturvallisuuden teoriatietoa ja perusteita sekä tuodaan esille tietoturvallisuuden johtamisen periaatteet ja tietoturvallisuuden merkitys osana organisaatioturvallisuutta. Tämän kokonaisuuden hahmottaminen auttaa tietoturvallisuuteen liittyvien toimenpiteiden priorisoinnissa ja kohdentamisessa sekä tehostaa tietoturvallisuuden hallintajärjestelmässä käytettävien työvälineiden käyttöä.

Tietoturvallisuuden teoriatiedon ja perusteiden lisäksi normiohjauksen, sertifikaattien, standardien ja toimintamallien periaatteiden sekä tietoturvatyössä käytettävien politiikkojen, ohjeiden ja muun tietoturvadokumentaation muodostaman kokonaisuuden hallitsemiseksi tarvitaan järjestelmää *(tietoturvallisuuden hallintajärjestelmä)*, johon kukin asiakokonaisuus asetetaan. Tietoturvallisuuden hallintajärjestelmän päivittäiseen ylläpitämiseen tarvitaan systemaattinen prosessi *(tietoturvallisuuden hallintaprosessi)*, jotta metsäkeskuksessa tapahtuvat ja/tai metsäkeskusta koskevat tietoturvaan liittyvät muutokset ja toimenpiteet ovat hallittavissa.

Toistaiseksi metsäkeskuksen käytössä on vanhan organisaatiomallin mukainen tietoturvallisuuden hallinnan järjestelmä. Vuodenvaihteessa 2012 tapahtunut organisaatiomuutos antaa hyvän mahdollisuuden ottaa suunta kohti valtakunnallista ja yhtenäistä tietoturvallisuuden hallintajärjestelmää sekä siihen implementoitua hallintaprosessia.

Työssä on käyty läpi tarvittavat toimenpiteet tietoturvallisuuden hallintajärjestelmän luomiseksi, ylläpitämiseksi ja kehittämiseksi. Työn viitekehyksenä on käytetty pääasiassa valtiovarainministeriön antamia Vahti-tietoturvaohjeita sekä muita ministeriön linjauksia. Vahti-ohjeiden lisäksi työssä hyödynnetään muuta tietoturvadokumentaatiota ja -aineistoa, joka soveltuu käytettäväksi valtionhallinnon organisaation tietoturvatyössä; päämääränä lisätiedon ja tarvittavien työvälineiden saattaminen Suomen metsäkeskuksen tietoturvallisuuden kehittämistyöhön.

LÄHTEET

Arkistolaki 23.9.1994/831.
http://www.finlex.fi/fi/laki/ajantasa/1994/19940831

Asianhallinnan tietoturvallisuutta koskeva ohje 2006. Vahti 5/2006.

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030.
http://www.finlex.fi/fi/laki/ajantasa/1999/19991030

CAF-yhteinen arviointimalli 2006.
http://www.vm.fi/vm/fi/13_hallinnon_kehittaminen/03_palvelujen_laatu/03_caf/index.jsp

Henkilötietolaki 22.4.1999/523.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Information Security Forum, (2007), *"Standard of Good Practice for Information Security"*, Information Security Forum, saatavana verkossa.
https://www.securityforum.org/?page=downloadsogp

ISO/IEC 27001:2005. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki. Suomen Standardisoimisliitto SFS.

Johdon tietoturvaopas 2011. Vahti 2/2011.

Kalander, Juha 2007. Tietoturvallisuuden hallinta: palautejärjestelmän vaatimukset ja toteutustavat. Diplomityö. Teknillinen korkeakoulu. Elektroniikan, tietoliikenteen ja automaation tiedekunta.

Karsisto, Timo 2007. Tietoturvariskianalyysin tehostaminen työkalun avulla. Diplomityö. Teknillinen korkeakoulu. Sähkö- ja tietoliikennetekniikan osasto

KATAKRI 2011. Kansallinen turvallisuusauditointikriteeristö. Versio II, 2011

Kerko, Pertti 2001. Turvallisuusjohtaminen. Jyväskylä: PS-kustannus.

Kokkala, Rami 2010. Tietoturvariskien hallinta pelastustoimessa. Diplomityö. Tampereen teknillinen yliopisto. Tietotekniikan koulutusohjelma.

Laaksonen, Mika, Nevasalo, Terho & Tomula, Karri 2006. Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588.
http://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki Suomen metsäkeskuksesta 6.5.2011/418.
http://www.finlex.fi/fi/laki/ajantasa/2011/20110418

Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13.
http://www.finlex.fi/fi/laki/ajantasa/2003/20030013

Laki valtion talousarviosta 13.5.1988/423.
http://www.finlex.fi/fi/laki/ajantasa/1988/19880423

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.
http://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Leppänen, Juha 2006. Yritysturvallisuus käytännössä. Jyväskylä: Gummerus Kirjapaino Oy.

Moilanen, Aki 2011. Tietoriskien hallinta ja hallintajärjestelmän suunnittelu. Oulun seudun ammattikorkeakoulu. Turvallisuusjohtamisen erikoistumisopinnot.

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 2003. Vahti 7/2003.

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010. Vahti 2/2010.

Opas julkishallinnon tietoturvakoulutuksen järjestämisestä 2003. Vahti 6/2003.

Pohjola, Kari 2011. Tietoturvattavien kohteiden hallinta operatiivisen johtamisen näkökulmasta. Laurea Leppävaara, Turvallisuusosaamisen koulutusohjelma, Ylempi ammattikorkeakoulututkinto.

Riskianalyysien laatu: vaatimukset tilaajalle ja toteuttajalle. TUTKIMUSRAPORTTI VTT-R-03718-07. VTT, Tampere 2007.

Sovelluskehityksen tietoturvaohje, luonnos 2012. Vahti X/2012.

Suomen perustuslaki 11.6.1999/731.
http://www.finlex.fi/fi/laki/ajantasa/1999/19990731

Suomen Standardisoimisliitto SFS, 2012.
http://www.sfs.fi/julkaisut_ja_palvelut/standardi_tutuksi/

Suomen Standardisoimisliitto SFS, tuotetiedot, ISO/IEC 27001:fi.
http://sales.sfs.fi/sfs/servlets/ProductServlet?action=productInfo&productID=184396

Suominen, Arto 2003. Riskien hallinta. Helsinki: WSOY.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516.
http://www.finlex.fi/fi/laki/ajantasa/2004/20040516

Tammisalo, Tero 2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Ohje sosiaali- ja terveydenhuollon

organisaatioille tietojärjestelmien tietoturvan ja tietosuojan kehittämiseksi. Helsinki: Stakes.

Tammisalo, Tero 2007. Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. Periaatteet ja menetelmät. Helsinki: Stakes.

Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007. Vahti 3/2007.

Tietoturvallisuuden hallintajärjestelmän arviointisuositus 2003. Vahti 3/2003.

Tietoturvallisuus ja tulosohjaus 2004. Vahti 2/2004.

Tietoturvatavoitteiden asettaminen ja mittaaminen 2006. Vahti 6/2006.

Tärkein tekijä on ihminen 2008. Vahti 2/2008.

Valmiuslaki 29.12.2011/1552.
http://www.finlex.fi/fi/laki/ajantasa/2011/20111552

Valtioneuvoston ohjesääntö 3.4.2003/262.
http://www.finlex.fi/fi/laki/ajantasa/2003/20030262

Valtioneuvoston periaatepäätös kansalliseksi tietoturvastrategiaksi 2008. Liikenne- ja viestintäministeriö.

Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009. Vahti 7/2009.

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681.
http://www.finlex.fi/fi/laki/ajantasa/2010

Valtion virkamieslaki 19.8.1994/750.
http://www.finlex.fi/fi/laki/ajantasa/1994/19940750

Voutilainen, Tomi 2012. Oikeus tietoon. Informaatio-oikeuden perusteet. Helsinki: Edita.

Yhteinen arviointimalli CAF 2006. Organisaation kehittäminen itsearvioinnin avulla. Valtiovarainministeriö. Edita Prima Oy.
http://www.vm.fi/caf

Yritysturvallisuus EK Oy 2009. Yritysturvallisuuden osa-alueet. Turvallisuusjohtaminen ohjaa kaikkea yritysturvallisuustyötä. Turvallisuusjohtaminen.
http://ek2.ek.fi/ytnk08/fi/yritysturvallisuus.php

Yhteiskunnan turvallisuusstrategia 2012. Valtioneuvoston periaatepäätös 16.12.2012.