LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvattavien kohteiden hallinta operatiivisen johtamisen näkökulmasta

Pohjola, Kari

2011 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvattavien kohteiden hallinta operatiivisen johtamisen näkökulmasta

Kari Pohjola
Turvallisuusosaamisen koulutus-ohjelma
Opinnäytetyö
Toukokuu, 2011

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusosaamisen koulutusohjelma
Ylempi ammattikorkeakoulututkinto

Kari Pohjola

Tietoturvattavien kohteiden hallinta operatiivisen johtamisen näkökulmasta

Vuosi 2011 Sivumäärä 93

Turvaamista tarvitsevia osa-alueita ja kohteita organisaatioissa on yleensä runsaasti ja ne sijaitsevat eri puolilla ja eri tasoilla organisaatiota. Vastaavasti myös vastuutahoja on useita – ja nekin eri puolilla ja eri tasoilla organisaatiota. Ellei turvattavaa omaisuutta ja muita kohteita tunnisteta, myös niihin liittyvät vastuut ja tarvittavat tietoturvatoimenpiteet ovat vaarassa jäädä epämääräisiksi ja sattumanvaraisiksi.

Valitussa tutkimustehtävässä tutkimusongelma rakentuu siitä, ettei tietoturvallisuuden hallinnan kannalta merkittävistä turvattavista kohteista ja niiden hallinnasta ole vakiintunutta käsitystä eikä turvattavien kohteiden hallinnasta löydy käytännöllistä kuvausta eikä työkalua. Tutkimuksen pääkysymyksenä on: Miten tietoturvallisuuden kannalta keskeisiä kohteita hallitaan? Pääkysymyksen ratkaisemiseksi tarvittavia apukysymyksiä tutkimuksessa ovat: Mitä tietoturvattavat kohteet ovat? Mitä tietoturvattavien kohteiden hallinta on?

Työn tarkoituksena on tuottaa malli, jota käyttämällä voidaan parantaa ja yhdenmukaistaa tietoturvattavien kohteiden hallintakäytäntöjä osana normaalin toiminnan ja samalla tietoturvallisuuden johtamista ja hallintaa. Tarkoituksen toteuttamiseksi analysoidaan keskeiset lähteet, täsmennetään käsitteet sekä kehitetään malli tietoturvattavien kohteiden hallintaan. Valmisteltavaa mallia ja annettavia suosituksia noudattamalla organisaatioissa voidaan parantaa todellista tietoturvatilannetta viemällä teoria työnläheiseksi käytännöksi, joka tavoittaa myös operatiivisesta toiminnasta vastaavat esimiehet.

Tutkimuksen teoreettisen taustan muodostamiseen sisältyy lähtötilanteen viitekehyksen määrittely käsitteineen sekä kohteiden ja omaisuuden hallinnan selvittäminen turvallisuuskontekstissa. Tästä jatketaan kohteiden ja omaisuuden hallinnan tarkasteluun turvallisuuskontekstin ulkopuolella ja selvittämällä kytkentämahdollisuudet organisaation johtamiseen ja toimintajärjestelmiin.

Tutkimus on toteutettu soveltavana tutkimushankkeena suunnittelutieteeseen kuuluvaa konstruktiivista tutkimusmetodia käyttämällä. Asteittaisten analysointi- ja kehittämisvaiheiden jälkeen on päädytty uuteen konstruktioon. Keskeiset esitettävät tulokset ovat uusi tietoturvattavien kohteiden hallinnan viitekehys ja käsitteistö, kohteiden hallinnan kytkentä normaaliin johtamis- ja toimintajärjestelmään sekä tietoturvallisuuden johtamis- ja hallintajärjestelmään, tietoturvattavien kohteiden hallinnan menettelytapakuvaus sekä tietoturvattavien kohteiden hallintaan käytettävän työkalun kuvaus. Myös tietoturva-alan peruskäsitteet (mm. tietoturvallisuus) ovat kriittisessä tarkastelussa ja niistä esitetään uudet perustellut määritelmät.

Asiasanat: tietoturvallisuus, tietoturvallisuuden hallinta, tietoturvallisuuden hallintajärjestelmä, turvattava kohde, suojattava kohde, tietoturvattava kohde, tietoturvattavan kohteen hallinta, operatiivinen johtaminen

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Master's Degree Programme in Security Management

Kari Pohjola

Information Security Asset Management within the Context of Operative Management

Year 2011 Pages 93

Usually there are plenty of assets needing protection in organizations. Those miscellaneous assets can reside in different places and levels. Accordingly the responsible ones can be found on many organizational levels and structures. If important assets are left unidentified, it is obvious that responsibilities relating to those assets will also be unclear and coincidental.

The main research problem in this study is based on the perception that there is neither integrated understanding of security critical assets, nor their management. There is also lack of practical procedures and tools. The main question in this thesis is how security critical assets should be managed. The supportive questions to be answered are: what are critical assets and what does asset management mean?

The purpose of this study is to produce a method to improve and integrate information security related asset management as part of an organization's operative management and information security management. To serve this goal the main informational sources will be analyzed, terms specified, and an asset management model developed. By using the new concept it is possible to look forward to improve the information security level where the theory becomes practice in the operative management.

The theoretical background in this thesis consists of preliminary specifications and terminology, and asset management study in the security context. This is broadened by studying the asset management models in a non-security context and ascertaining the possibilities to integrate with management and operational systems.

This study belongs to applied science and was conducted with a constructive research method resulting in a new construction. The main outcomes from the defined development phases are a new concept for information security asset management, specified terminology, and integration both with the operative management system and the information security management system. These include a documented procedure, or process description, and a tool to information security asset management. Also the terminological base (e.g. information security) is under a critical study, resulting in new definitions.

Key words: information security, information security management, information security management system, asset, asset management, security asset management, information security asset management, operative management

Sisällys

1 Johdanto

”Yritykseen pitäisi hankkia murtohälytys- ja kameravalvontajärjestelmä. Meille pitäisi laatia tietoturvaohjeet ja jatkuvuussuunnitelmat. Näille tiedoille pitäisi saada turvallinen säilytystila. Työasemiin tarvittaisiin salausohjelmistot.” Ratkaisut esimerkinomaisiin, organisaatioiden arkisiin tarpeisiin ovat varmasti löydettävissä. Ennen ratkaisujen hankintaan ja toimeenpanoon ryhtymistä on kuitenkin syytä pohtia tarkemmin, mitä varsinaisesti halutaan suojata ja miltä.

Turvallisuusjärjestelmien ja -mekanismien tarkoituksena on niiden syvällisyysasteesta ja sovellutusalueesta riippumatta suojata jotakin (mm. Curtis & McBride 2005; Fay 2002, 101; Johnson 2005, 2; Kovacich & Halibozek 2003, 25; Vellani 2007, 10; Virtanen 2002, 40). Tietoturvallisuuden johtamis- ja hallintajärjestelmät edustavat käsitteellisesti 2000-luvun näkemystä järjestelmällisistä menettelytavoista tietoturvallisuuden ja tietoturvatoiminnan suunnittelussa, toteutuksessa, arvioinnissa ja jatkuvassa parantamisessa. Näiden järjestelmien keskiössä on se, minkä vuoksi tietoturvatoimintaa ja -kontrolleja on olemassa — jotain on tarpeen turvata.

Alan kirjallisuudesta voidaan todeta, että riskienhallintamenettelyitä, turvamekanismeja ja turvallisuuden eri osa-alueilla huomioon otettavia asioita sinällään on pohdittu varsin laajasti. Tietoturvallisuuden hallintajärjestelmiä koskevassa standardissa ISO/IEC 27001 pidetään perustavanlaatuisena kiinnekohtana keskeisten suojattavien kohteiden tunnistamista ja ao. kohteiden asianmukaista huomioon ottamista tietoturvatoiminnassa. Mainitussa vaatimusstandardissa ja lisäohjeistusta tarjoavissa ISO/IEC 27002- ja 27003-standardeissa ei kuitenkaan määritellä tai neuvota, mitä kohteen hallinta tarkoittaa ja miten sitä toteutetaan käytännössä. Valtionhallinnon tietoturvallisuuden johtoryhmän tuottamissa VAHTI-ohjeistuksissa käytetään myös suojattava kohde ja turvattava kohde -terminologiaa varsin runsaasti, mutta myös tästä ohjeistuksesta puuttuu käytännölliset neuvot kohdekohtaiselle työlle.

1.1 Tutkimusongelman määrittely

Turvaamista tarvitsevia osa-alueita ja kohteita organisaatioissa on yleensä runsaasti ja ne sijaitsevat eri puolilla ja eri tasoilla organisaatiota. Vastaavasti myös vastuutahoja on useita – ja nekin eri puolilla ja eri tasoilla organisaatiota. Ellei turvattavaa omaisuutta ja muita kohteita tunnisteta, myös niihin liittyvät vastuut ja tarvittavat tietoturvatoimenpiteet ovat vaarassa jäädä epämääräisiksi ja sattumanvaraisiksi. Valitussa tutkimustehtävässä tutkimusongelma rakentuu siitä, ettei tietoturvallisuuden hallinnan kannalta merkittävistä turvattavista kohteista ja niiden hallinnasta ole vakiintunutta käsitystä eikä turvattavien kohteiden hallinnasta löydy käytännöllistä kuvausta eikä työkalua.

Tutkimuksen pääkysymyksenä on: Miten tietoturvallisuuden kannalta keskeisiä kohteita hallitaan? Pääkysymyksen ratkaisemiseksi tarvittavia apukysymyksiä tutkimuksessa ovat: Mitä tietoturvattavat kohteet ovat? Mitä tietoturvattavien kohteiden hallinta on?

1.2 Kehittämistyö, sen tavoite ja hyödyt

Tietoturvattavan kohteen vastuuhenkilönä on usein liiketoimintaprosessin omistaja tai substanssiyksikön päällikkö. Hän on samalla vain ani harvoin tietoturvallisuuden asiantuntija. Kun usein pyrkimyksenä on jalkauttaa tietoturvatoiminta yksiköihin ja prosesseihin (mm. ISO/IEC 27001:2005, 24; VAHTI 2/2010 7 - 9), tarvitaan juuri yksiköiden ja prosessien käyttöön soveltuvia malleja ja työkaluja.

Työn tarkoituksena on tuottaa malli, jota käyttämällä voidaan parantaa ja yhdenmukaistaa tietoturvattavien kohteiden hallintakäytäntöjä osana normaalin toiminnan ja samalla tietoturvallisuuden johtamista ja hallintaa. Tarkoituksen toteuttamiseksi analysoidaan keskeiset lähteet, täsmennetään käsitteet sekä kehitetään malli tietoturvattavien kohteiden hallintaan. Valmisteltavaa mallia ja annettavia suosituksia noudattamalla organisaatioissa voidaan parantaa todellista tietoturvatilannetta viemällä teoria työnläheiseksi käytännöksi, joka tavoittaa myös operatiivisesta toiminnasta vastaavat esimiehet. Koska esitettävät ratkaisut ovat johtamisjärjestelmään sovitettavia näkyviä menettelytapoja, voidaan samalla sivutuotteena tavoitella myös organisaation turvallisuuskulttuurin yleistä kehittämistä (Ruuhilehto & Vilppola 2000, 31 - 33).

1.3 Näkökulman valinta ja aiheen rajaus

Työn tulosten ensisijaisena kohderyhmänä ovat organisaation operatiivisesta toiminnasta vastaavat henkilöt. Tuloksia voivat hyödyntää myös tietoturvallisuuden johtamisesta ja hallinnasta kokonaisuutena vastaavat henkilöt sekä teemaan liittyvät kouluttajat, auditoijat ja tarkastajat. Tarkastelutavassa pitäydytään kohteiden luonteesta riippumattomissa hallinnollisissa menettelytavoissa – toisin sanoen asioissa, joilla turvattavia kohteita hallitaan ja joilla kohteen vastuuhenkilö ja henkilöstö voivat asiaa työstää. Vaikka laajasta turvallisuuskentästä tarkasteluun on valittu ensisijaisesti tietoturvallisuus, voi työn eri osia soveltaa käyttöön myös muilla turvallisuuden osa-alueilla.

Tässä työssä tietoturvattavan kohteen elinkaarta tarkastellaan kokonaisuutena. Työn tarkoituksena ei kuitenkaan ole syventyä turvattavien kohteiden hallinnan elinkaarella oleviin yksittäisiin osa-alueisiin, kuten esimerkiksi riskienhallintaan. Näitä yksittäisiä osa-alueita käsitellään tässä työssä ns. valmisosina (Järvinen & Järvinen 2004, 111), joiden käyttämiseen tarvittavat rajapinnat määritellään toimintamallissa ja työkalussa. Tämä ratkaisun tarkoituksena on

tehdä mallista laajasti sovellettavissa oleva, koska riskienhallintaesimerkkiä jatkaen jokaisessa mallin käyttäjäorganisaatiossa voidaan käyttää juuri sitä riskien arviointi- ja hallintamallia, jota siinä jo entuudestaan on totuttu käyttämään.

Tietoturvattavien kohteiden hallinta on osa organisaation toimintaa. Tarkoituksena ei ole tämän työn kautta rakentaa organisaatioon uutta johtamisjärjestelmää, vaan pikemminkin sovittautua jo olemassa oleviin rakenteisiin. Tämä näkökulma ja rajaus on otettu huomioon siten, että tietoturvattavien kohteiden hallintaan määritellään rajapinnat johtamisjärjestelmään. Useat johtamisjärjestelmät tarkastelevat organisaation toimintaa varsin laaja-alaisesti, joten tehdyllä rajauksella pyritään samalla välttämään turhia päällekkäisyyksiä.

1.4 Tutkimusraportin rakenne

Luvussa 2 käsitellään tutkimuksen teoreettinen tausta. Se sisältää lähtötilanteen viitekehyksen käsitteineen sekä kohteiden ja omaisuuden hallinnan turvallisuuskontekstissa. Lisäksi luvussa käsitellään kohteiden ja omaisuuden hallintaa turvallisuuskontekstin ulkopuolella ja tehdään kytkentä organisaation johtamiseen.

Kolmannessa luvussa selostetaan käytetyt tutkimus- ja kehittämismenetelmät. Aluksi esitetään tutkimuskirjallisuuteen pohjautuva menetelmällinen perusta. Tämän jälkeen käydään läpi, miten menetelmällistä perustaa on sovellettu käytännön kehittämistyöhön tavoitetilanteen, määrittelyvaiheen, toteutuksen ja lopputilanteen työkuvauksina.

Neljännessä luvussa esitetään varsinaiset tutkimustulokset. Niihin sisältyvät uusi tietoturvattavien kohteiden hallinnan viitekehys, tarvittavien käsitteiden määritelmät sekä kytkentä organisaation varsinaiseen toimintaan ja tietoturvallisuuden hallintajärjestelmään. Kehittämistyön tuloksiin sisältyvät tietoturvattavien kohteiden hallinnan menettelytapakuvaus sekä menettelyyn soveltuvan työkalun kuvaus.

Raportin lopussa esitetään tutkimuskokonaisuuteen liittyvä yhteenveto sekä esitetään johtopäätökset ja arviointi niin tutkimuksesta kuin saavutetuista tuloksistakin. Kuvauksia ja tuloksia on raportissa käsitelty siten, että todellisen kohdeorganisaation yksilöivät nimet, erikoistermit ja salassa pidettävät tiedot on joko jätetty pois tai muutettu yleisempään muotoon. Tällä seikalla ei ole määrällistä tai laadullista vaikutusta esitettyyn sisältöön. Menettelyn tarkoituksena on osaltaan tehdä esityksestä mahdollisimman yleiskäyttöinen ja hyödynnettävä organisaatiotyypistä riippumatta.

2 Teoreettinen tausta

Tutkimustyötä aloitettaessa ja tehtäessä on valittava ja käytettävä tutkimustehtävään ja -ongelmiin soveltuvia menetelmiä (Aaltola & Valli 2007, 10). Tutkimusongelman ratkaisemisessa eräänä mahdollisena lähtökohtana on selvitys siitä, mitä muut ovat aiheesta kirjoittaneet, millaisia käsitteitä he ovat käyttäneet ja millaisia tutkimusongelmia he ovat nostaneet esille. Kirjallisuuskatsaukseen voidaan koota lähteitä monipuolisesti. Tässä työssä käsitteitä työstetään aloittaen turvallisuus- ja tietoturva-alan lähteistä ja jatkamalla vastaavien käsitteiden pohdintaa turvallisuusalan ulkopuolella. Valittu lähestymistapa tarjoaa mahdollisuuden arvioida näkemysten välisiä eroja.

2.1 Lähtötilanteen viitekehys

Toikon ja Rantasen (2009, 36 - 37) mukaan ihmiset tekevät tulkintoja todellisuudesta ja myös rakentavat todellisuutta puheen ja sanojen kautta. Kehittämistoiminnassa ei yleensä voida pitäytyä pelkässä kielenkäytön analysoinnissa, mutta konstruktiivisella lähestymistavalla voi heidän mukaansa olla annettavaa myös käytännön kehittämistoimintaan. Toikko ja Rantanen toteavat myös kehittämistodellisuuden kompleksisuuden. Käytännössä on esimerkiksi mahdollista, että kehittämisprosessin osapuolilla on erilaisia käsityksiä niin käsitteistä kuin tavoitteistakin, joten tarkoituksenmukaista on määritellä käsitteet ainakin alustavasti jo työn alussa.

Tämän työn aiheista käytetään vaihtelevasti erilaisia ilmaisuja, kuten omaisuus, turvattava kohde ja suojattava kohde. Vakiintunutta yhtä käsitettä niillä tarkoitetulle asialle ei suomenkielellä ole, mikä näkyy siinä, että myös englanninkielinen ilmaisu *asset* käännetään asiayhteydestä riippuen hieman eri tavoin. Tässä luvussa käytetään tarkoituksellisesti ”sekaisin” eri lähteissä olevia tai niistä tulkittavia termejä lähteiden esittelyn yhteydessä, sillä kulloinkin käytetty termi kuvannee parhaiten kunkin kirjoittajan käsitystä asiassa.

Tämän työn tulosten keskeisenä kohderyhmänä ovat organisaation varsinaisesta operatiivisesta toiminnasta vastaavat yksiköiden päälliköt ja esimiehet. He eivät siten juuri koskaan ole tietoturvallisuuden ja siihen liittyvän ammattiterminologian asiantuntijoita. Käsitteiden tarkastelu onkin tässä tilanteessa kiintoisaa aloittaa yleiskielestä ja aiheen tärkeimpien viitekehysten angloamerikkalaisesta taustasta johtuen erityisesti englanninkielestä.

Oxford Advanced Learner’s Dictionary of Current English -sanakirjoista on jatkuvan ylläpitämisen kautta kehittynyt maailmanlaajuisesti levinnyt työkalu englannin opetukseen ja opiskeluun. Sanastosta on sitä kautta tullut myös liike-elämässä laajasti hyödynnetty lähde haetta-

essa englanninkielisten sanojen merkityksiä. Sanakirjan nykyinen Oxfordin yliopiston toimittama verkkoversio Oxford Advanced Learner's Dictionary 2011 määrittelee tämän työn otsikossa esiintyvät avainsanat yleiskielen kautta seuraavasti:

> *Information = 1) facts or details about somebody/something*
>
> *Security = 1) the activities involved in protecting a country, building or person against attack, danger, etc; 2) the department of a large company or organization that deals with the protection of its buildings, equipment and staff; 3) protection against something bad that might happen in the future; 4) the state of feeling happy and safe from danger or worry; 5) a valuable item, such as a house, that you agree to give to somebody if you are unable to pay back the money that you have borrowed from them; 6) (pl.) documents proving that somebody is the owner of shares, etc. in a particular company*
>
> *Asset = 1) a person or thing that is valuable or useful to somebody/something; 2) a thing of value, especially property, that a person or company owns, which can be used or sold to pay debts*
>
> *Management = 1) the act of running and controlling a business or similar organization; 2) the people who run and control a business or similar organization; 3) the act or skill of dealing with people or situations in a successful way*

Tämän työn konstruoinnin kannalta merkittäviä käsitteitä ovat turvattava kohde ja turvattavien kohteiden hallinta. Alustavasti nämä käsitteet voidaan edellä olevasta johtaen määritellä seuraavasti:

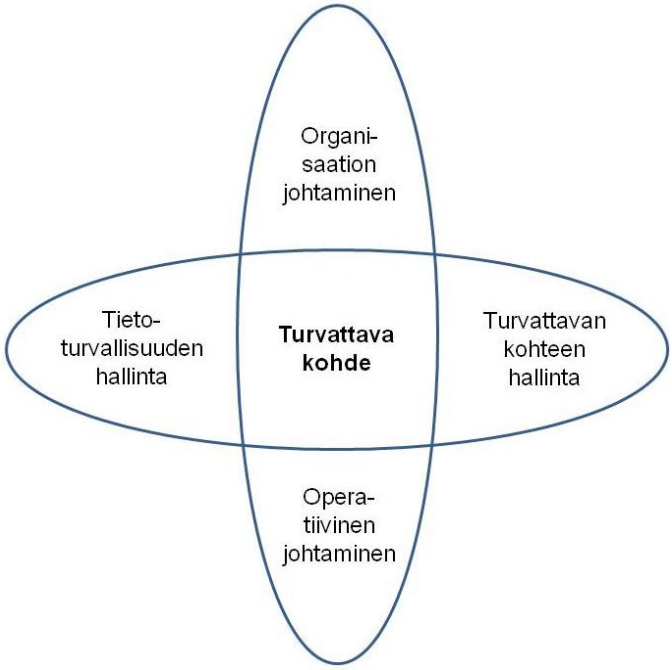
> **Turvattavalla kohteella** tarkoitetaan asiaa, toimintaa, omaisuutta tai ihmistä, joka on arvokas tai hyödyllinen jollekin tai johonkin.
>
> **Turvattavan kohteen hallinnalla** tarkoitetaan menettelyjä, joilla menestyksekkäästi ohjataan, toimeenpannaan ja valvotaan arvokkaan ja hyödyllisen (tietoa sisältävän) asian, toiminnan, omaisuuden tai ihmisen suojaamista.

Turvattavien kohteiden tietoturvanäkökulmaan voidaan kiinnittyä tietoturvallisuus -käsitteen kautta. ISO/IEC 27001 -standardin (2005, 12) mukaan tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttämistä. Lisäksi mainitussa standardissa todetaan, että tähän voi sisältyä myös muita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus.

Tuokon ja Rantasen (2009, 130 - 131) mukaan tutkimuksellinen ajattelu on käsitteellistä. Käsitteellistäminen voi kohdistua esimerkiksi kehitettävän toiminnan jäsentämiseen ja täsmentämiseen. Tarkoituksena on tukea toiminnan tavoitteen määrittelyä ja arviointia ja auttaa siten fokusoimaan kehittämistä mahdollisimman olennaisiin toiminnan piirteisiin. Tuokon ja

Rantasen (2009, 131 - 132) mukaan käsite, jonka merkitystä pohditaan, on luonteva lähtökohta käsiteanalyysille. Käsitekartan he puolestaan näkevät hieman laajempana loogisena ja systemaattisena kokonaisuutena, jossa kuvataan tutkimus- tai kehittämistoiminnan kannalta olennaisimmat käsitteet ja niiden väliset suhteet.

Turvattavat kohteet ja niiden hallinta eivät ole organisaatioissa muusta toiminnasta irrallisia, vaan ne ovat normaalin toiminnan ja sen johtamisen tiedostettu tai tiedostamaton osa. Olennaiset käsitteet ovat konstruoinnin tässä vaiheessa kolmella eri tasolla. Ylätasolla ovat käsitteet organisaation johtaminen ja tietoturvallisuuden hallinta. Keskimmäisellä tasolla edellisiä kavennetaan käsitteisiin operatiivinen johtaminen ja turvattavien kohteiden hallinta. Näiden tasojen läpileikkausta ja suhdetta turvattavaan kohteeseen havainnollistetaan kuviossa 1.



Kuvio 1: Käsitekartan perusta

Keskimmäisellä ja sitä alemmalla käsitetasolla tarvitaan lisäksi joukko muita käsitteitä. Niiden kautta voidaan lähestyä ja avartaa tutkimusongelmaa sekä sen ratkaisua. Käsitekartoissa tarkoituksena on kuitenkin keskittyä tärkeimpiin käsitteisiin, eikä kuvata kaikkia mahdollisia alakäsitteitä.

2.2 Kohteiden ja omaisuuden hallinta turvallisuuskontekstissa

Kuten edellä kappaleessa 2.1 todettiin, käsitteet ja niiden käyttö eivät aina ole yksiselitteisiä. Tämä pätee myös käsitteeseen turvattava kohde. Esimerkiksi valtionhallinnon tietoturvallisuuden uudemmassa VAHTI-ohjeistuksessa käyttöön on valikoitunut termi turvattava kohde. ISO/IEC 27000 -sarjan standardeissa käytetään samassa tarkoituksessa käsitettä suojattava kohde. Valtiokonttoriin organisoidussa Valtion IT-palvelukeskuksessa ja sen tietoturvapalveluissa käytetään sekä suojattavan että turvattavan kohteen käsitettä (esim. Kinnunen 2010; Romppanen ja Rousku 2010; Viljanen 2010). Valtionhallinnon tietoturvasanastoon (2008, 121) on puolestaan valittu termiksi turvattava kohde, eikä suojattavan kohteen käsitettä mainita lainkaan. Muissa lähteissä vastaava käsite voi olla esitetty myös asiayhteytensä vuoksi hieman rajatummassa muodossa, kuten IT-resurssit (esim. COBIT 2007, 12).

Järvisten (2004, 5 - 6) mukaan kirjallisuuskatsaus tehdään käsitteiden ympärille. Käsitteet johdetaan tutkimusongelmasta. Onnistunut käsitteiden tunnistaminen tarjoaa hyvät mahdollisuudet myös harkittuun kirjallisuuden kartoittamiseen. Avainkäsitteiden avulla voidaan paikantaa aiheesta esitetyt näkemykset ja tuoda esille aihepiirin taustan ja liittymien hallinta. Katsauksen runko voidaan esittää taulukkomuodossa, jolloin riveillä ja sarakkeilla esitetään lähteet ja käsitteet sekä niiden kohtaaminen.

Tässä työssä tietoturvallisuuden hallinta mielletään systemaattiseksi toiminnaksi, jolloin siitä muodostuu vahva linkki käsitteeseen tietoturvallisuuden hallintajärjestelmä. Alustavasti tietoturvallisuuden hallintajärjestelmän käsite voidaan määritellä ISO/IEC 27001 -stanardin mukaisesti (2005, 12):

> **Tietoturvallisuuden hallintajärjestelmällä** tarkoitetaan sitä osaa yleisestä toimintajärjestelmästä, joka liiketoimintariskien arviointiin perustuen luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus.

Taulukkoon 1 on koottu tietoturvallisuuden hallintaan liittyviä avainlähteitä ja näkemys avainkäsitteiden käytöstä. Taulukon perusteella voidaan todeta, että tietoturvallisuuden hallintajärjestelmän ja turvattavan kohteen käsitteitä käytetään päälähteissä, mutta käsitteet on usein jätetty määrittelemättä. Turvattavan kohteen hallinnan käsitteen osalta tilanne on vielä vajavaisempi – käsitettä ei päälähteissä ole määritelty lainkaan, vaikka sitä niissä käytetään.

Lähde	Tietoturvallisuuden hallintajärjestelmä *(information security management system)*	Turvattava/ suojattava kohde *(asset)*	Turvattavan/ suojattavan kohteen hallinta *(asset management)*
ISO/IEC 27001 (tietoturvallisuuden hallintajärjestelmästandardi)	X	X	(x)
ISO/IEC 27002 (tietoturvallisuuden hallinnan menettelyohje)	(x)	(x)	(x)
ISO/IEC 27003 (tietoturvallisuuden hallinta-järjestelmän toteutusohje)	(x)	(x)	
ISO/IEC 27005 ja liite B (tietoturvallisuuden riskien-hallintastandardi)	(x)	X	
BSI-Standard 100-1 (tietoturvallisuuden hallintajärjestelmästandardi)	X	(x)	(x)
BSI-Standard 100-2 (tietoturvallisuuden hallinnan menettelyohje)		(x)	(x)
BSI-Standard 100-3 (tietoturvallisuuden riskien-hallintastandardi)		(x)	(x)
Standard of Good Practice (tietoturvallisuuden hallinnan menettelyohje)		(x)	(x)
KATAKRI, tietoturvallisuuden osa-alue (turvallisuusauditointi-kriteeristö)	(x)	X	(x)
VAHTI 8/2008 (tietoturvasanasto)	X	X	
VAHTI 3/2007 (tietoturvallisuuden hallinnan menettelyohje)	X	(x)	(x)
VAHTI 2/2010, tietoturvatasot (tietoturvallisuuden hallinnan menettelyohje)	(x)	(x)	(x)
VAHTI 7/2003 (tietoturvallisuuden riskien-hallintaohje)	(x)	(x)	

X = käsite on määritelty, käsitteen käyttö on johdonmukaista
(x) = käsitettä ei ole määritelty, mutta sitä (tai muuta lähikäsitettä) käytetään, lukijan on tulkittava merkitys asiayhteyden, esimerkkien tai käytettyjen lähdeviitteiden mukaan
(tyhjä) = käsitettä ei käytetä

Taulukko 1: Tutkimuksen tietoturvanäkökulmaan kytkeytyvät avainlähteet sekä ammatillisten käsitteiden määrittely ja käyttö

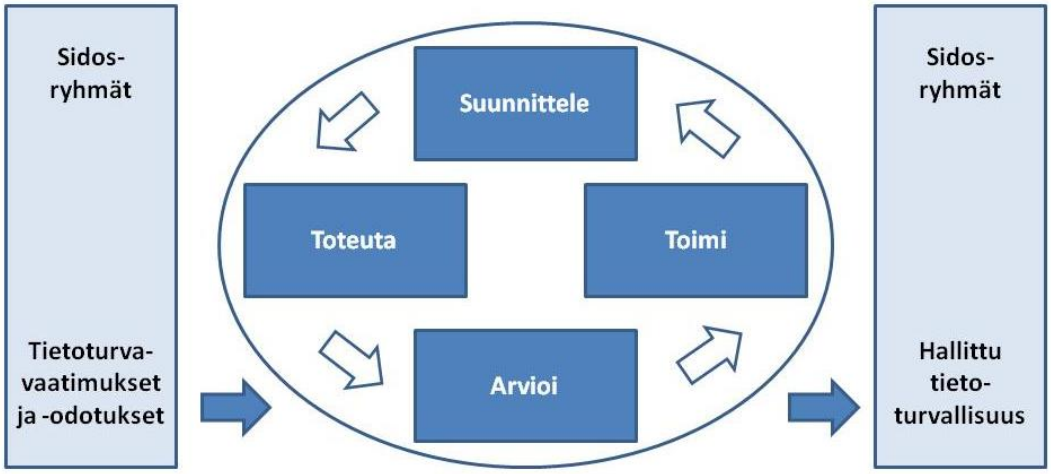
2.2.1 ISO/IEC/SFS-standardit

Standardisoinilla tarkoitetaan yhteisten toimintatapojen laatimista pyrkimyksenä helpottaa viranomaisten, elinkeinoelämän ja kuluttajien elämää (Suomen Standardisoimisliitto SFS 2011). Standardisoinnilla lisätään tuotteiden ja toimintamallien yhteensopivuutta ja turvallisuutta, suojellaan kuluttajaa ja ympäristöä sekä helpotetaan kotimaista ja kansainväistä kauppaa. Standardit laaditaan yhteistyönä työryhmissä ja komiteoissa, joihin voi osallistua viranomaisten, teollisuuden, kaupan, käyttäjien, kuluttajien sekä korkeakoulujen, tutkimuslaitosten ja järjestöjen edustajia. Standardien valmistelussa pyritään ottamaan huomioon kaikkien osapuolten näkökannat ja pääsemään sisältökysymyksissä yhteisymmärrykseen.

Laaja-alaisin standardisoimisjärjestö on ISO (International Organization for Standardization). Sähköalalla kansainvälisestä standardisointityöstä vastaa IEC (International Electrotechnical Commission) ja telealalla ITU (International Telecommunication Union). ISOn, IEC:n ja ITUn rinnalla toimivat eurooppalaiset standardisoimisjärjestöt CEN (European Committee for Standardization), sähköalan CENELEC (European Committee for Electrotechnical Standardization) ja telealan ETSI (European Telecommunications Standards Institute). Suomea edustaa ISOssa ja CENissä SFS, IEC:ssä ja CENELECissä sähkö- ja elektroniikka-alan kansallinen standardointijärjestö SESKO sekä ITUssa ja ETSIssä Viestintävirasto. (Suomen Standardisoimisliitto SFS.)

Standardointityön tulokset julkaistaan asiakirjoina, joita kuka tahansa voi hankkia ja käyttää. Standardien käyttö ja hyödyntäminen on maksutonta, mutta hankinta on maksullista. Standardit voivat olla voimassa pelkästään yhdessäkin maassa, mutta yhä useammin pyritään eurooppalaisiin ja kansainvälisiin standardeihin. Luonteeltaan standardit ovat suosituksia. Laaja-alaisuudestaan johtuen tässä työssä on kansainvälisillä standardeilla lähteinä suuri painoarvo.

ISO/IEC 27001 (2005, 10 - 11) on kansainvälinen standardi, joka määrittelee ne vaatimukset, jotka koskevat dokumentoidun tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, käyttämistä, valvontaa, katselmointia, ylläpitoa ja parantamista. Se ottaa huomioon organisaation liiketoimintariskit ja määrittelee vaatimukset turvamekanismien toteuttamista varten organisaation tai sen osien tarpeiden mukaisesti. ISO/IEC 27001 -standardissa hyödynnetään ”suunnittele - toteuta - arvioi - toimi” -mallia (PDCA-malli), joka jäsentää kaikki standardin hallintaprosessit (kuvio 2). Standardi toimii myös sertifioinnin perustana.



Kuvio 2: Tietoturvallisuuden hallinnan PDCA-sykli (ISO/IEC 27001:2005, 8 - 9)

Standardin mukaan tietoturvallisuuden hallintajärjestelmä luodaan takaamaan riittävien ja asianmukaisesti mitoitettujen turvamekanismien valinta. Turvamekanismien tehtävänä puolestaan on suojata suojattavia kohteita ja luoda luottamusta sidosryhmille. Käsitteellisesti suojattava kohde määritellään tarkoittamaan mitä tahansa, mikä on arvokasta organisaatiolle. Tämä käsite on standardissa määritelty ensimmäisenä kaikkiaan 16 käsitteen joukossa.

ISO/IEC 27001 -standardin vaatimusosan kolmeen ensimmäiseen konkreettiseen toimenpideryhmään sisältyy suojattavien kohteiden huomioon ottaminen (2005, 14 - 17). Kohteet on tunnistettava, kohteille on nimettävä omistajat ja kohteisiin liittyvät uhat on tunnistettava. Tästä toimenpiteet etenevät riskien arviointiin ja hallintaan. ISO/IEC 27001 -vaatimusstandardissa suojattavat kohteet asettuvat keskiöön, jonka ympärille tietoturvallisuuden ja riskien hallinnointi rakentuu.

ISO/IEC 27002 -standardi on tietoturvallisuuden hallintaa koskeva menettelyohje. Standardissa (2005, 14 - 15) tietoa pidetään erittäin tärkeänä suojattavana kohteena muiden tärkeiden liiketoiminnallisten kohteiden tavoin, minkä vuoksi tietoa on suojattava asianmukaisesti. Systemaattisessa ja toistuvassa turvallisuusriskien arvioinnissa on standardin mukaan otettava huomioon erilaiset muutokset, kuten muutokset suojattavissa kohteissa (ISO/IEC 27002:2005, 26 - 27).

Suojattavien kohteiden ohjeistus painottuu ISO/IEC 27002 -standardissa (2005, 50 - 57) kohteiden tunnistamiseen, luettelointiin, vastuuttamiseen, luokitteluun ja suojaamiseen. Kohteiden luetteloinnin avulla voidaan varmistaa kohteiden suojauksen tehokkuus. Suojattavien kohteiden luetteloa standardi pitää myös tärkeänä edellytyksenä riskien hallinalle. Suojatta-

van kohteen tärkeyden, liiketoiminnallisen arvon ja turvaluokituksen perusteella voidaan tunnistaa tarvittava suojaustaso. Suojattavien kohteiden luettelon tulee standardin mukaan sisältää kaikki tiedot, joita tarvitaan katastrofista toipumiseen, mukaan lukien kohteen tyyppi, tallennusmuoto, sijainti, varmuuskopiotiedot, lisenssitiedot ja arvo liiketoiminnalle.

Suojattavien kohteiden ryhmittelyesimerkkeinä ISO/IEC 27002 -standardissa mainitaan tiedot, ohjelmistot, fyysiset kohteet, palvelut, ihmiset ja heidän osaamisensa sekä maine. Omistajuuden eli vastuutuksen kautta näkökulma muuttuu hieman, sillä omistettavan kohteen esimerkkeinä tuodaan esille liiketoimintaprosessit, määritellyt joukot toimintoja, sovellukset ja määritellyt joukot aineistoa. Monimutkaisten kohteiden osalta voi olla tarkoituksenmukaista nimetä joukko suojattavia kohteita, jotka toimivat yhdessä tuottaen tiettyä toimintoa palveluna. Tällöin palvelun omistaja on vastuussa palvelun toimittamisesta, mihin sisältyy sitä tuottavien suojattavien kohteiden toiminta. Lisäksi todetaan tarve määritellä suojattavien kohteiden hyväksyttävä käyttö.

ISO/IEC 27003 -standardissa paneudutaan tietoturvallisuuden hallintajärjestelmän rakentamiseen. Standardin tarkoituksena on tuoda esille niitä seikkoja, jotka auttavat järjestelmän suunnittelussa ja toimeenpanemisessa. Osana tarvittavan vaatimustason määrittelyä standardissa otetaan esille suojattavien kohteiden tunnistamis- ja luokittelutarve (2010, 20 - 23). Tehtäväohjeistuksessa neuvotaan keräämään seuraavaa tietoa: prosessien yksilöidyt nimet, prosessien kuvaukset, prosessien kriittisyys organisaatiolle, prosessien omistajat, input- ja output-liityntäprosessit, prosesseja tukevat tietojärjestelmät ja tietoaineistot turvallisuustarpeiden mukaisesti luokiteltuina. Nämä tiedot ovat syötteenä rakentamisen seuraavalle vaiheelle, jossa arvioidaan riskit.

ISO/IEC 27005 on tietoturvallisuuden hallintajärjestelmäkontekstiin sovellettu riskienhallintastandardi. Standardi 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 (2008, 8 - 9). Standardissa suojattava kohde määritellään kaikeksi, jolla on arvoa, ja jota siten vaatii suojaamista. Samalla siinä muistutetaan, että kohteiden tunnistaminen on tehtävä soveltuvalla yksityiskohtaisuuden tasolla riskien arvioimiseksi. Syvyystason valinta vaikuttaa kuitenkin suoraan käsiteltävään tietomäärään ja samalla työmäärään. Edelleen pidetään tärkeänä tunnistaa jokaiselle kohteelle omistaja vastuun ja tilivelvollisuuden toteamiseksi. Omistajalla on usein myös paras näkemys kohteen arvosta ja vaikutuksista.

27005-standardin liiteaineistossa tarkastellaan kohteita yksityiskohtaisemmin asettamalla kohteet kahteen pääkategoriaan (2008, 30 - 31). Ensimmäisen tärkeysluokan kohteita tietoturvanäkökulmasta ovat 1) liiketoimintaprosessit, aliprosessit ja toiminnot ja 2) tietovaran-

not. Toissijaisia tukikohteita edellisille ovat mm. laitteet, ohjelmistot, verkot, henkilöstö, toimitilat ja organisaatio. Yleinen, ei turvallisuuteen sidottu, riskienhallintastandardi ISO 31000 puolestaan ei sisällytä omaan viitekehykseensä kohteita muuten kuin viittaamalla tarpeeseen soveltaa menettelyjä haluamaansa asiayhteyteen (2009, 10, 15 - 16).

2.2.2 BSI-standardit

Saksan tietoturvavirasto Bundesamt für Sicherheit in der Informationstechnik (BSI) on julkaissut tietoturvallisuuden hallintaa liittyviä standardeja paitsi kansalliseen julkishallinnon käyttöön, myös laajemmin hyödynnettäväksi. Standardit ovat pääosin ISO/IEC 27000 -sarjan standardeista johdettuja. BSI-Standard 100-1 kuvaa, miten tietoturvallisuuden hallintajärjestelmä määritellään ja suunnitellaan. Standardia käytetään myös sertifioinnin vaatimuslähteenä. Aineistossa mainitaan turvattavista kohteista epäsuorasti ja niukkasanaisesti, että tietoon ja liiketoimintaan kohdistuvat uhat on tunnistettava (2008, 29).

BSI-Standard 100-2:ssa neuvotaan ensimmäisen osan mukaisen hallintajärjestelmän rakentaminen. Esitetyssä mallissa lähtötilanteen kartoituksessa ja rakenneanalyysiä tarvitaan tiedot organisaatiosta, infrastruktuurista, tietojärjestelmistä, sovelluksista ja työntekijöistä (2008, 34 - 47). Mallissa varoitetaan liian syvällisen tarkkuustason johtamisesta hallitsemattomaan tieto- ja työmäärään. Vastaavasti mallissa annetaan neuvoja kohteiden tarkoituksenmukaiseen ryhmittelyyn, mikäli kohteet ovat esimerkiksi samantyyppisiä, konfiguroitu samalla tavalla, liitetty verkkoon samalla tavalla sekä samojen vaatimusten ja turvallisuustarpeiden alaisia. Kuvattu yhteneväisyys ei ole pelkkä työmäärä- ja hallittavuuskysymys, vaan tärkeä pyrkimys sisäiseen standardointiin parantaen turvallisuutta ja vähentäen kustannuksia. BSI-Standard 100-3 opastaa kohteiden riskienhallinnassa, mutta viittaa kohteiden kartoittamisen osalta 100-2 -standardiin.

Turvattavaa omaisuutta ja sen hallintaa käsitellään tarkemmin standardeja tukevassa IT-Grundschutz-käsikirjassa. Nimensä mukaisesti käsikirjassa painotutaan tietotekniikkaan ja kohteilla viitataan infrastruktuuriin, organsointiin, henkilöstöön ja teknisiin komponentteihin, jotka tukevat tietotekniikan avulla hoidettavia tehtäviä (2005, 22). Mallin mukaisesti kaikki tunnistetut kohteet linkitetään lähes 3000-sivuisen käsikirjan sisältämiin massiivisiin luetteloihin, katalogeihin, joissa on yksityiskohtaisesti käsitelty kohteisiin mahdollisesti liittyvät uhat ja turvamekanismivaihtoehdot.

2.2.3 SoGP-standardi

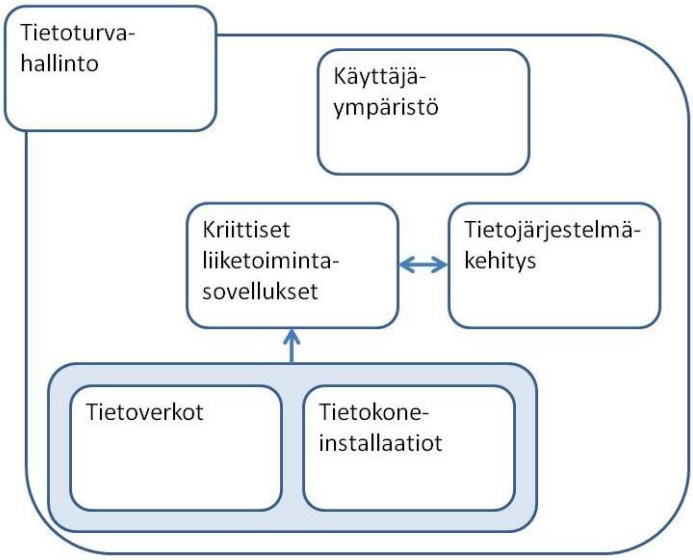
The Standard of Good Practice (SoGP) for Information Security (2007, 1 - 10) on kansainvälisen Information Security Forum (ISF) -järjestön tuottama yhtenäinen kuvaus tietoturvallisuu-

teen liittyvistä hyvistä käytännöistä. Tässä yhteydessä standardi tarkoittaa järjestön itse määrittämää suositusta jäsenilleen ja myös järjestön ulkopuolisille.

ISF on noin 300 organisaation muodostama yhteistyöfoorumi tietoturvallisuuden ja tietoriskien hallinnan kehittämiseen ja keskinäiseen tiedon jakamiseen. Poikkeuksellisesti edellä mainittu kuvaus on kuitenkin vapaassa jakelussa tarkoituksenaan levittää ja yhteen sovittaa foorumissa hyviksi tulkittuja käytäntöjä yleisemmäksi käytännöksi. Kuvauksen tarkoituksena on esittää tietoturvajärjestelyihin liittyvät menettelytavat liiketoimintalähtöisesti.

SoGP-mallin tietosisältö pohjautuu foorumin puitteissa tehtyyn tutkimukseen, jäsenistöltä selvitettyyn käytännön kokemukseen sekä aiheeseen liittyvien keskeisten standardien, viitekehysten ja mallien analysointiin ja integrointiin. Huomioon otetuista lähteistä nimeltä on mainittu ISO/IEC 27002, COBIT 4.1, Sarbanes-Oxley Act 2002, Payment Card Industry (PCI) Data Security Standard, Basel II 1998 ja EU:n tietosuojadirektiivi. Hyvien käytäntöjen kuvauksen kohderyhmäksi mainitaan tietoturvavastaavien ohella mm. liiketoimintavastaavat.

SoGP (2007, 3) on jäsennelty kuuteen näkökulmaan ja toimintaympäristöön. Nämä osa-alueet ovat tietoturvahallinto, käyttäjäympäristö, kriittiset liiketoimintasovellukset, tietojärjestelmäkehitys), tietoverkot ja tietokoneinstallaatiot. Jäsentelytavasta ja sisällöstä voidaan todeta, että mallissa on tulkittu tietoturvallisuutta käsitteellisesti lähinnä tietoteknisenä kysymyksenä. Vastaavasti mallin liiketoimintakytkentä on perusteltu toiminnassa tarvittavien tietoteknisten sovellusten kautta. Mallin johdantoteksti ja keskeinen kaaviokuva (kuvio 3) tukevat tätä käsitystä.



Kuvio 3: SoGP-mallin jäsentely (Standard of Good Practice for Information Security 2007, 3)

Kriittiset liiketoimintasovellukset ja niihin liittyvä turvallisuus toimivat SoGP-mallin (2007, 3) mallin suunnitteluytimenä. Suojattavien kohteiden hallinta rajautuu mallissa omaisuuden hallinnaksi. Tämä näkyy mallissa esitetyistä periaatteista: 1) käytetään testattuja, luotettavia ja hyväksyttyjä laitteita ja ohjelmistoja, jotka täyttävät turvallisuusvaatimukset ja on kirjattu omaisuusluetteloon (SoGP 2007, SM4.3) ja 2) tarvittavat tiedot laitteista ja ohjelmistoista lisensseineen tallennetaan omaisuusluetteloon (SoGP 2007, CI1.3). Kokonaisuutena tästä voidaan tehdä johtopäätös, että tässä mallissa keskeisimmät suojattavat kohteet ovat kriittiset liiketoimintasovellukset ja niiden tarvitsemat laitteet.

2.2.4 KATAKRI-kriteeristö

Kansallinen turvallisuuauditointikriteeristö KATAKRI (2009, 1 - 4) on viranomaisille ja yrityksille luotu yhtenäinen kriteeristö yhteisöturvallisuusmenettelyyn sekä omavalvontaa että auditointia varten. Kriteeristö jakautuu neljään pääosioon: hallinnollinen turvallisuus (turvallisuusjohtaminen), henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Auditoinnissa huomioidaan kaikkien neljän osion vaatimukset, joten osa-alueita ei pidä tästä näkökulmasta tarkastella itsenäisinä kokonaisuuksina. Suojattavia kohteita kriteeristössä käsitellään kuitenkin vain tietoturvallisuusosiossa. Suojattavalla kohteella tarkoitetaan kriteeristössä tietoa sekä sen käsittely-ympäristöä. Esimerkkeinä suojattavista kohteista mainitaan yksittäinen tietojärjestelmä, verkon osa ja yksittäinen työhuone.

Hallinnollisen tietoturvallisuuden erityisosa-alueella KATAKRIn (2009, 59 - 60) yhtenä pääkysymyksenä on toiminnalle tärkeiden suojattavien kohteiden tunnistaminen. Tässä yhteydessä mahdollisiksi kohteiksi esitetään toiminnot, tiedot ja järjestelmät. Täsmentävissä vaatimuksissa otetaan esille suojattavien kohteiden tunnistamisen lisäksi suojattaviin kohteisiin liittyvien uhkien tunnistaminen, kohteille nimetyt vastuuhenkilöt tai omistajat sekä kohteiden suojausmenetelmien suhteuttaminen kohteisiin ja niiden riskeihin.

KATAKRI tarjoaa myös tukea suojattavien kohteiden tunnistamiseen esimerkinomaisella todennuslomakkeella (2009, 101). Lomakemalli ohjaa käsittelemään tietojärjestelmiä, järjestelmissä olevia tietotyyppejä, niiden sijaintia ja luokittelua neliportaisella merkitysvaihtelulla (fataali merkitys, erittäin iso merkitys, merkittävä, vähäinen merkitys) neljällä tietoturvallisuuden tavoitealueella (luottamuksellisuus, käytettävyys, eheys, kiistämättömyys).

2.2.5 VAHTI-ohjeisto

Valtionhallinnon tietoturvasanasto VAHTI 8/2008 on valtiovarainministeriön alaisuudessa toimivan Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) tuottama sanasto, jonka tarkoituksena on yhtenäistää valtionhallinnon tietoturvaterminologia. Sanastossa on yli 1250 tietoturvakäsitteen määritelmää. Sanastoon sisällytetyistä termeistä on esitetty myös niiden englanninkieliset vastineet.

VAHTI-sanastossa (2008, 121, 147) on päädytty termiin turvattava kohde, eikä käsitettä suojattava kohde tunneta lainkaan. Turvattavalla kohteella tarkoitetaan sanaston mukaan kohdetta, joka on organisaatiolle arvokas, kuten ihmiset, resurssit, toiminta ja palvelut. Määritelmää täsmennetään tiedon käsittelyn osalta, jolloin turvattavia kohteita sanaston mukaan voivat olla esimerkiksi tiedot eri muodoissaan, inhimilliset resurssit, tietojärjestelmät, käyttöympäristö, fyysinen ympäristö, ulkoiset palvelut, hankinnat sekä edellä mainittuja palvelevat prosessit.

Tietoturvallisuudella tuloksia, VAHTI 3/2007, on valtionhallinnon yleisohje tietoturvallisuuden johtamiseen ja hallintaan strategioista käytännön toiminnaksi saattamiseen (kuvio 4).

Kuvio 4: Turvallisuus strategioista käytännön toimintaan (Tietoturvallisuudella tuloksia 2007, 44)

Tietoturvallisuudella tuloksia -ohjeessa tarkastellaan asiaa myös hyvän tiedonhallintatavan osana. Tällöin lähtökohtana on, että viranomaisella on kuvaukset tehtävistään, tiedoistaan ja asiakirjoistaan. Yleisohjeessa turvallisuusnäkökohdat sovitetaan prosesseihin ja toimintaan. Ohjeessa (2007, 13 - 16) todetaan tietoturvallisuudella tarkoitettavan tietojen ja palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi. Edelleen ohjeessa todetaan, että valtionhallinnon tiedot, tietojärjestelmät ja palvelut ovat yhteiskunnalle välttämättömiä, taloudellisesti korvaamattomia ja valtakunnan turvallisuuden ja toimintojen kannalta elintärkeitä.

Valtionhallinnon tietoturvastandardisointi kiteytyy VAHTI 2/2010 -soveltamisohjeeseen, jossa tietojen ja asiakirjojen salassa pidettävyyttä koskevan luokittelun ohella määritellään hallinnolliset ja tietotekniset tietoturvatasot sekä niihin liitetyt kriteerit. Vaikka jäsentelytapana on käytetty Common Assessment Framework (CAF) -mallia, on sisällössä runsaasti yhteisiä piirteitä mm. ISO/IEC 27001 -standardin kanssa. Tietoturvallisuuden hallintajärjestelmän ohella ohjeessa ja kriteeristössä asetetaan vaatimuksia mm. omaisuuden hallinnalle (2010, 114).

Tietoturvatasokriteeristössä todetaan tavoitteena, että organisaation vastuulla olevat laitteet, ohjelmistot ja rekisterit sekä niistä koostuvat tietojärjestelmät tunnistetaan, jotta niiden turvallisuudesta voidaan huolehtia. Varsinaisissa arviointikriteereissä tarkastellaan säädöstenmukaisten rekisteriselosteiden ja tietojärjestelmäkuvausten olemassaoloa, omaisuuden luettelointia, omistajuutta, luokittelua ja edellisiin liittyviä katselmointikäytäntöjä. Lisäksi kriteeristössä viitataan mm. ydintoimintojen, ydinprosessien ja toimintaympäristöjen tunnistamiseen ennen riskien arviointia. (2010, 96, 101.)

Valtionhallinnon tietoturvallisuuden riskienarviointiohjeessa VAHTI 7/2003 riskien hallinta kytketään tietoturvallisuuden hallintajärjestelmään (2003, 22). Samalla todetaan, että riskianalyysillä tunnistetaan suojattaviin kohteisiin kohdistuvat uhat, mutta hallintajärjestelmän ja kohteiden käsitteitä ei määritellä. Ohjeessa esitetyn tietoriskikartan (2003, 28) ja uhkien tunnistamiseen liittyvien tarkistuslistojen (2003, 29 - 40) kautta on nähtävissä, minkä kohteiden uhkia on tunnistettava sekä välillisesti tulkittavissa, että niihin liittyy suojausintressi.

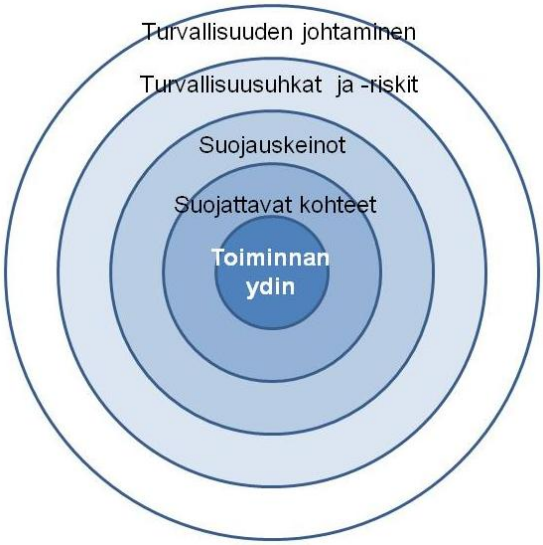
2.2.6 Muu ammattikirjallisuus

Kotimaisessa tietoturva-alan kirjallisuudessa suojattavan kohteen käsitteen lanseerasi -90-luvun lopulla Juha E. Miettinen. Hän tarkasteli tietoturvallisuutta organisaation toimintaprosessien ja hallussa olevien omaisuuserien kautta (1999, 70 - 94). Miettinen totesi, että organisaation hallitsemien omaisuuserien ja toimintaprosessien tunnistaminen on yksi ensimmäisistä

tehtävistä, kun ryhdytään ammattimaisesti kehittämään organisaation tietoturvallisuutta. Suojaamista ei voida toteuttaa tehokkaasti ilman kohteiden asianmukaista tunnistamista ja suojaaminen voi vahingossa kohdistua vääriin asioihin, väärässä laajuudessa ja väärällä tavalla.

Miettinen nosti tärkeimmiksi suojattaviksi kohteiksi organisaation prosessit, koska ne ovat toiminnan perusta. Lisäksi hän korosti sitä, että suojattavissa prosesseissa on kiinnitettävä erityistä huomiota prosessien tietojen suojaamiseen. Miettinen käsitteli aihetta prosessien tietoturvatarpeiden, luokittelun ja suojauksen sekä prosessien suojattavien kohteiden kautta ja esitteli näiden työstämiseen liittyviä menetelmiä.

Miettinen (2002, 12 - 13) palasi kohteiden suojaamiseen käsitellessään laajemmin organisaatioiden turvallisuutta ja sen johtamista. Miettisen mukaan suojattava kohde (myös suojauskohde) tarkoittaa tässä laajemmassa turvallisuuskontekstissa esimerkiksi asiaa, esinettä, toimintoa, tietoa, ihmistä tai prosessia, joka halutaan suojata siihen kohdistuvien uhkien torjumiseksi tai uhkien poistamiseksi kokonaan. Suojattavia kohteita ovat siten kaikki ne kohteet, jotka organisaatiossa on katsottu aiheelliseksi suojata. Tätä hän havainnollistaa turvallisuuskentän jäsentelyllä sisäkkäisiin kehiin (kuvio 5).

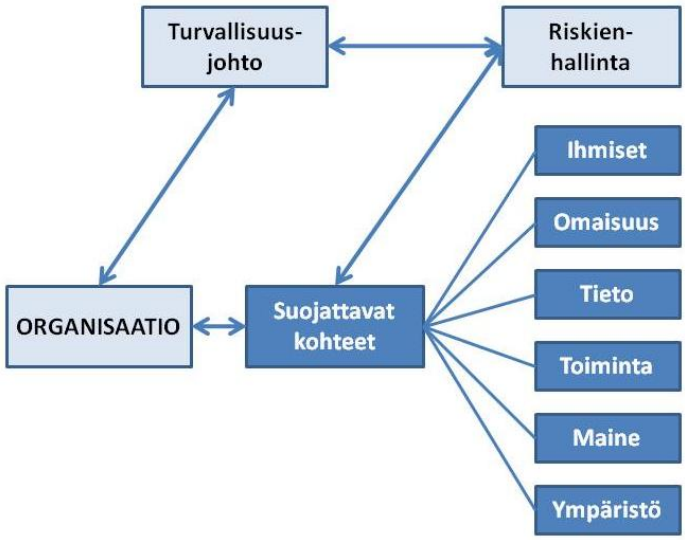


Kuvio 5: Yritysturvallisuuden kehät (mukaillen Miettinen 2002, 12)

Miettinen (2002, 55 - 56) yhdisti yritysturvallisuuden myös prosessien johtamiseen. Kun päivittäinen, operatiivinen, johtaminen tapahtuu organisaation toimintaprosessien kautta, on siinä otettava huomioon kaikki päivittäiseen johtamiseen tarvittavat asiat. Tähän kuuluu myös

vastuuhenkilö, prosessin omistaja, joka vastaa prosessin ylläpidosta ja kehittämisestä. Miettinen toteaa, että tähän vastuuseen lukeutuu myös vastuu turvallisuudesta.

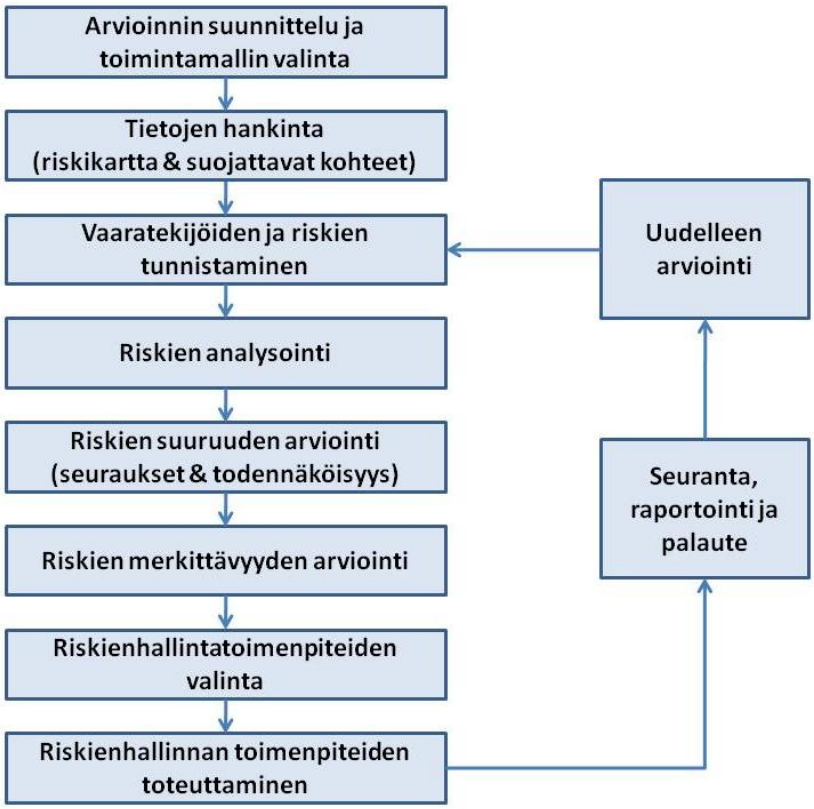
Myös Leppänen (2006, 61 - 78) lähtee yritysturvallisuudessa siitä, että organisaatiossa on määriteltävä ja arvioitava ne asiat, jotka ovat elintärkeitä sen toiminnan tavoitteiden saavuttamiseksi. Tällaiset kohteet ovat samalla myös niitä suojattavia kohteita, joiden vahingoittumattomuuden varmistamiseen turvallisuus- ja riskienhallintatoimenpiteet kohdistetaan. Kun suojattavat kohteet ja prosessit määritellään huolellisesti, turvallisuus- ja riskienhallintatoimenpiteet voidaan kohdistaa oikein ja samalla varmistaa prosessin toimintaa. Samalla hän tekee merkille pantavan huomion: ellei turvallisuustoimintaa ja riskienhallintaa kohdisteta prosesseihin, eivät ne myöskään tue prosessia. Leppänen tarkasteleekin turvallisuusjohtamista portfoliona, johon kuuluvat mm. organisaatio, suojattavat kohteet ja riskienhallinta (kuvio 6).



Kuvio 6: Suojattavat kohteet osana organisaation turvallisuusjohtamista (Leppänen 2006, 62 - 63)

Leppäsen mukaan suojattavat kohteet on määriteltävä sekä organisatorisesta että riskinäkökulmasta. Keskeisiksi suojattavien kohteiden ryhmiksi Leppänen nostaa ensin tärkeimpänä ihmiset, ja sitten omaisuuden, tiedon, toiminnan, maineen ja ympäristön. Leppänen avaa kaikkia kohteiden pääryhmiä ja tuo esille niiden monipuolisen ja runsaan sisällön, mutta muistuttaa aiheellisesti myös siitä, ettei kaikki mahdollinen tarkoita tärkeää suojattavaa kohdetta. Ryhmittely on esitetty käytännön turvallisuustyön jäsentelemiseksi, joten ryhmien mahdollisesta osittaisesta päällekkäisyydestä (esimerkiksi tieto voi olla myös omaisuutta) ei pidä tehdä ongelmaa.

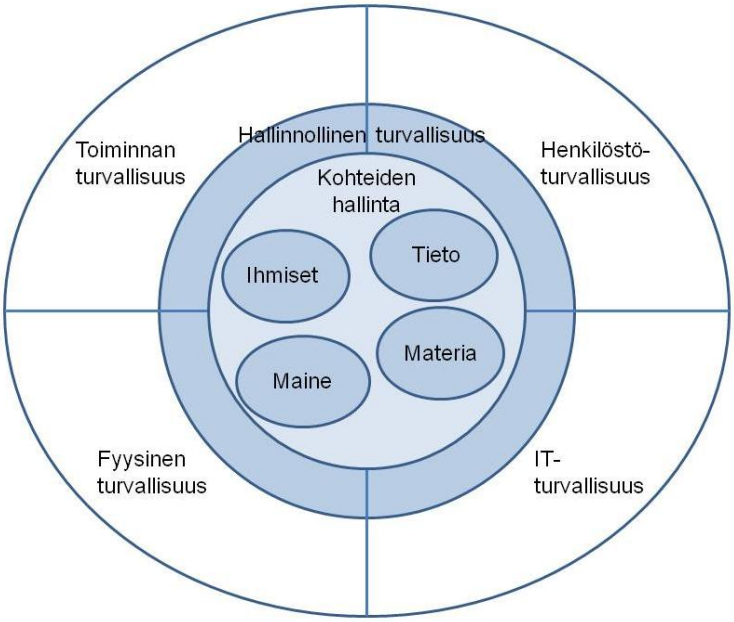
Valinnat suojattaviksi kohteiksi tehdään organisaatiokaavion, prosessimallien, omaisuusluettelon ja muiden tavoitteisiin liittyvien toimintojen mukaisesti, jotta saavutetaan riittävä yhtenäisyys ja yhteensopivuus organisaation muuhun toimintaan. Leppänen perustelee näkemystään ja suojattavien kohteiden yksilöimisen tärkeyttä myös sillä, ettei useinkaan ole selvää kuvaa siitä, mitä kohteita organisaatiossa on ja kenen vastuulla ne ovat. Yksilöintivaiheen jälkeen kohteen vastuuhenkilön tehtävänä on yhdessä turvallisuuden- ja riskienhallinnan asiantuntijoiden kanssa arvioida kohteisiin liittyviä riskejä. Leppänen sitoo siten suojattavien kohteiden tunnistamisen osaksi riskien arviointi- ja hallintaprosessia (kuvio 7).



Kuvio 7: Suojattavat kohteet riskienhallinnan osana (Leppänen 2006, 124)

Kyrölä (2001) puolestaan on pohtinut organisaation tietojen merkitystä ja arvoa sekä tietoriskien hallintaa erityisesti esimiesten näkökulmasta. Riskien hallinnan osana hän käyttää käsitteitä suojeltava tieto, suojattava tieto sekä tieto-omaisuus ja tietopääoma. Näitä täydentävinä suojeltavina kohteina Kyrölä mainitsee myös tietojen käsittelyyn liittyvät tilat ja tietojärjestelmät.

Virtanen (2002, 40 - 42) on kehittänyt nelisektorisen turvallisuusmallin, jossa turvattavina kohdealueina esitetään ihmiset, tieto, materia ja maine (kuvio 8). Mäkinen (2005, 166) täydentää kaaviota ottamalla kohteeksi myös ympäristön. Virtanen avaa turvallisuusmallissaan myös turvattavan kohteen hallinnan käsitettä. Hänen mallissaan kohteen hallinnalla tarkoitetaan kohteiden tunnistamista, merkityksen arviointia ja suojaamista.



Kuvio 8: Neljän sektorin turvallisuusmalli (Virtanen 2002, 41)

COBIT (2007) on laajasti sovellettu kansainvälinen tietotekniikan ohjaus- ja valvontamalli, jossa otetaan huomioon myös tietoturvallisuus. Ylätason hallintamallissa kuvataan suunnittelua ja organisointia, rakentamista ja toteuttamista, tuotantoa ja ylläpitoa sekä seurantaa ja arviointia. Näistä tehtäväalueista määritellään tarvittavat prosessit, tavoitteet, vastuu- ja tehtäväjako, mittarit sekä kypsyystasokriteerit. Turvattavien kohteiden käsitettä mallissa vastaa IT-resurssit, joka käsitteenä jäsentyy tietoon, sovelluksiin, infrastruktuuriin ja ihmisiin (2007, 12). Näkökulmiksi mallissa otetaan tehokkuus, vaikuttavuus, luottamuksellisuus, eheys, saatavuus, vaatimustenmukaisuus ja luotettavuus. Malli sisältää yhteensä 34 tietohallintoon, -järjestelmiin, ja -tekniikkaan liittyvää keskeistä tehtäväaluetta tai prosessia, mutta niiden joukossa ei ole erikseen omaisuuden hallintaa.

COBIT-mallin seuraavaan versioon integroitava The Business Model for Information Security, BMIS (2010) pyrkii kuvaamaan kokonaisvaltaisen lähestymistavan tietoturvallisuuden suunnitteluun, toteuttamiseen ja hallintaan menemättä turvamekanismeihin. Mallissa korostetaan

tietopääoman merkitystä organisaatioiden toiminnassa. BMIS koostuu neljästä peruselementistä ja kuudesta elementtejä toisiinsa liittävästä tekijästä. Keskeisinä elementteinä, jotka myös voidaan tulkita turvattaviksi kohteiksi, mallissa nimetään organisaatio, ihmiset, prosessit ja teknologia.

Generally Accepted Information Security Principles (GAISP) (2004, 13) määrittää 14 periaatetta tietoturvatoimintaan. Yksi niistä on tieto-omaisuuden hallinta. Jotta kohteita voidaan mallin mukaan hallinta, on ne ensin tunnistettava. Lisäksi jokaisesta kohteesta tulee kerätä ja dokumentoita seuraavat tiedot: tunnistetiedot, omistaja, sisältö, elinkaaren pituus ja vaihe, liittyminen (ja riippuvuus) muuhun ympäristöön, arvo (rahallinen tai muu), sensitiivisyys (luottamuksellisuus) ja kriittisyys (saatavuus, eheys). Lisäksi näitä tulee arvioida säännöllisesti uudelleen.

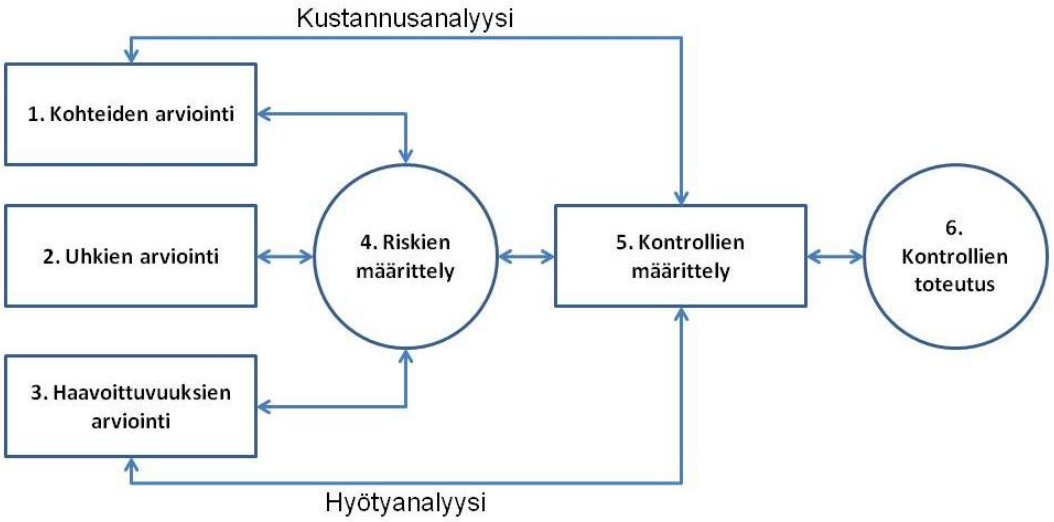
Roperin (1999, 13) määritelmä turvattavaksi kohteeksi on seuraava: henkilö, toimipaikka, laitteisto, materiaali, tieto tai toiminto, jolla on positiivista arvoa omistajalleen. Kohteella voi Roperin mukaan olla tiettyä arvoa myös ”vihollisen” näkökulmasta, mutta tämä arvo voi poiketa omistajan kokemasta arvosta suurestikin. Roper näkee turvattavien kohteiden tunnistamisen ja arvioinnin olevan lähtölaukauksena riskien arviointiin ja hallintaan (kuvio 9).

Curtis ja McBride (2005, 44) eivät määrittele turvattavien kohteiden käsitettä, mutta luettelevat niiden joukkoon kuuluvan mm. rahan, laitteet, työntekijät, tiedon, maineen ja fyysisen infrastruktuurin. Asset Protection and Security Management Handbook (2003, 2 - 3) ei myöskään sisällä suojattavien kohteiden tai niiden hallinnan käsitemäärittelyä, vaan tyytyy tarjoamaan esimerkkejä suojattavista kohteista: raha, saatavat, fyysinen ja älyllinen omaisuus, sisäiset tiedot, toimintaoikeudet ja -velvollisuudet sekä työntekijät. Kummassakaan lähteessä ei käsitellä kohteiden tunnistamista eikä hallintaa, mutta selvitetään uhkien ja riskien arviointia ja osa-aluekohtaisia turvallisuusratkaisuja.

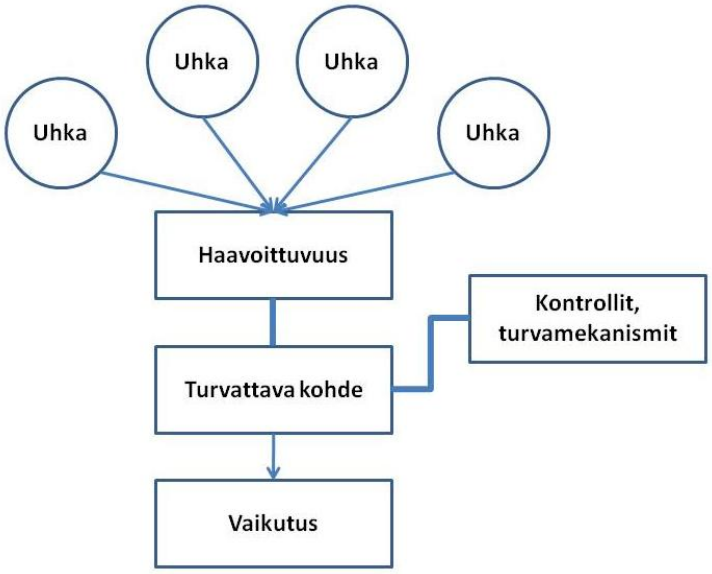
Brotby käsittelee teoksessaan tietoturvallisuuden johtamisen ja hallinnan kehittämistä sekä hallintajärjestelmän toteutusta viime vuosikymmenellä yleistyneen governance-termin alla. Suojattavaksi kohteeksi hän toteaa yksioikoisesti tiedot. Hallintanäkökulmasta tehtävänä on Brotbyn (2009, 37 - 39) mukaan tietojen omistajan nimeäminen sekä tietojen luokittelu luottamuksellisuus- ja käytettävyysvaatimusten osalta.

Burns-Howell, Cordier ja Eriksson (2003) ovat tarkastelleet turvallisuusriskien ja -kontrollien käsittelyä käytännön toteutusprojektien kautta. He toteavat lähtökohtanaan, että riskien ja turvallisuuden hallinnan työkalut epäonnistuvat käytössä, mikäli ne ovat liian monimutkaisia, vaikeaselkoisia, byrokraattisia ja puutteellisesti fokusoituja (2003, 11, 19 - 25). He asettavat riskien arviointi- ja hallintamallissaan kohteiden tunnistamisen ja arvioinnin ensimmäiseksi

toimenpiteeksi (kuvio 9). Kohteet ovat näkyvässä roolissa myös heidän riskien arvioinnin elementistössään (kuvio 10).



Kuvio 9: Yksinkertaistettu riskien arviointi- ja hallintamalli (Roper 1999, 6; Burns-Howell ym. 2003, 19)



Kuvio 10: Riskienarvioinnin elementtien kytkeytyminen toisiinsa (Burns-Howell ym. 2003, 37)

Burns-Howell ym. (2003, 11) esittävät käsitemäärittelynään, että turvattava kohde on mikä tahansa, jolla on arvoa ja joka tarvitsee suojausta. Esimerkkeinä tällaisista kohteista he ottavat esille ihmiset, toimipaikat, rakennukset, laitteet, materiaalit, toiminnot, valmistetut tuotteet, tiedot, tietojärjestelmät sekä maine ja imago. Kohteiden tunnistamistyössä he ovat havainneet hyödylliseksi käyttää jäsenneltyä potentiaalisten kohteiden tarkistuslistaa, joka helpottaa vastuutahon edustajia tunnistamaan omat kriittiset kohteet.

Osaksi kohteiden arviointia Burns-Howell ym. sisällyttävät kohteiden menettämis- ja vahingoittumiskustannusten arvioinnin ja priorisoivat kohteet tämän perusteella. Lisäksi he painottavat, että toimenpiteet tulee ensisijaisesti kohdistaa kriittisiksi luokiteltuihin kohteisiin. Käytännön työssä Burns-Howell ym. ovat todenneet, että vastuutahon näkemykset kohteista ja niiden arvoista ovat usein hyvin subjektiivisia. Objektiivisuuden lisäämiseksi he ovat pyytäneet vastuutahoa täsmentämään joitain seuraavista asioista: toiminnan jatkuvuuden edellytykset ilman kohdetta, kohteiden ja niiden toiminnalle tuottama arvo, kohteen korvaamis- ja viivekustannukset, vahingoittumisen tai epävakaaksi tulemisen kustannukset, kilpailuetuvaikutukset tai strateginen arvo.

Vellani (2007, 11 - 22) ottaa koko turvallisuustoiminnan lähtökohdaksi turvattavat kohteet. Esimerkiksi Vellanin riskienarviointiprosessin ensimmäisenä vaiheena on turvattavien kohteiden tunnistaminen (kuvio 11). Hän määrittelee turvattaviksi kohteiksi kaikki, joilla on arvoa organisaatiolle. Yleisellä tasolla hän näkee turvattavien kohteiden koostuvan ihmisistä, omaisuudesta ja tiedosta. Vellani painottaa kohteilla olevan erilaisia merkittävyyksiä. Hän nimittää kriittisiksi kohteiksi niitä, joita organisaatiossa tarvitaan suorittamaan sen päätarkoitusta ja -toimintoja. Lisäksi Vellani pohtii turvattavien kohteiden omistajuutta, luokitteluja, arvon määrittämistä ja inventointia (2007, 135 - 136).

Kuvio 11: Riskienarviointiprosessi (Vellani 2007, 11)

Fone ja Young ovat pohtineet riskien hallintaan liittyvää johtamista ja esimiesten tehtäväkenttää. He totesivat, ettei organisaatioiden perinteinen keskitetty riskienhallintatoiminto riskienhallintapäälliköineen ja -sihteereineen ole optimaalinen järjestely. Sen sijaan he suosittelevat, että organisaatiossa olisi riskienhallinnasta vastaava johtaja, jonka tehtäviin kuuluisi riskien hallintaan liittyvä viestintä, koordinointi, motivointi, yhteistyön organisointi ja

prosessin kehittäminen. Vastaavasti suurin osa varsinaisista riskienhallintatoimenpiteistä tulisi levittää varsinaiseen toimintaorganisaatioon osastoille, yksiköihin, toimintoihin ja prosesseihin. (2001, 45, 279.) Fone ja Young (2001, 299 - 302) päätyivät käytäntöön vietynä seitsemään yleiseen johtamistehtävään, joihin riskien ja myös turvallisuuden hallinnan näkökulmat ovat hyvin yhteensovitettavissa: 1) suunnittelu, 2) budjetointi, 3) organisointi, 4) resursointi, 5) ohjaus, 6) yhteistyö ja 7) raportointi.

Fonen ja Youngin (2001, 284 - 285) tekemän tutkimuksen perusteella keskeiset haasteet riskienhallinnalle ja sen viestimiselle ovat varsinaisen vastuuorganisaation puutteellinen tietämys riskien hallinnan periaatteista ja menettelytavoista, subjektiiviset näkemykset riskeistä ja tähän liittyvä huono vertailtavuus sekä riskienhallinnan merkityksen aliarviointi. Viestintään liittyy myös riskitiedon hallinta. Tiedonhallinnassa käytetään hyvin eritasoisia välineitä lähtien yksinkertaisista taulukoista päätyen erikoistuneisiin riskienhallinnan tietojärjestelmiin.

Välineestä riippumatta Fone ja Young näkevät kussakin organisaatiossa tarpeen kyetä vastaamaan seuraaviin tiedonhallinnallisiin kysymyksiin: Mitä tietoa riskeistä tarvitaan? Mistä tämä tieto saadaan tai haetaan? Mitkä ovat ajoitukseen liittyvät tarpeet? Milloin tietoa tarvitaan? Mikä on tuottavin ja tehokkain tapa siirtää tietoa? Mitä tiedolla tehdään? Kuka tai ketkä tarvitsevat tietoa, milloin ja missä muodossa? Mitkä ovat tiedonkulun esteet? Mitä vaikutuksia tiedonkulun parantumisella on?

Myös Kovacich ja Halibozek (2003, 167 - 182) ovat analysoineet turvattavien kohteiden hallintaan saamisen edellytyksiä. He toteavat, että vastuun kohteiden turvallisuudesta on oltava kohteiden omistajilla, eikä turvallisuusasiantuntijoiden pidä omia vastuuta itselleen. Kun organisaation varsinaisesta toiminnasta vastaavat esimiehet saadaan sitoutumaan oman vastuualueensa riskeistä ja turvallisuudesta huolehtimiseen, päästään parempiin lopputuloksiin. Tämän saavuttamiseksi Kovacich ym. luettelevat tarpeellisina keinoina turvattavat kohteet huomioivat turvallisuuspolitiikat ja -periaatteet sekä näitä tukevat menettelytapakuvaukset, vastuumääritykset, vastuullisten allekirjoittamat lausunnot kohteidensa hyväksyttävästä riski- ja turvallisuustasosta sekä suunnitelmat ja kuvaukset tarvittavista riskienhallinta- ja turvallisuustoimenpiteistä.

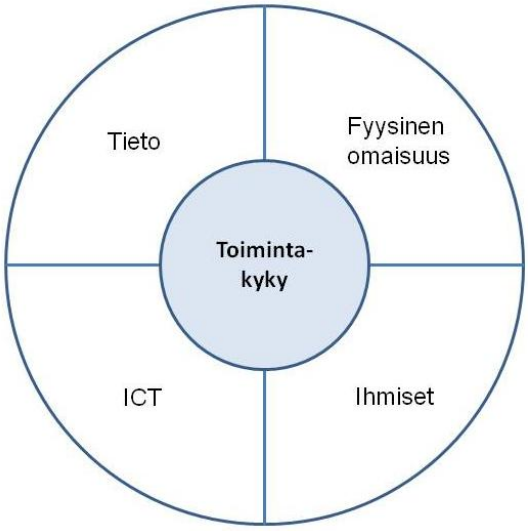
Turvallisuusorganisaation tehtävänä on Kovacichin ym. mukaan valmistella menettelytavat ja työkalut, tukea vastuutahoja menettelyjen toteuttamisessa sekä seurata ja valvoa edistymistä. He näkevät tämän vastuunjakonäkemyksen tuomina hyötyinä, että turvallisuusajattelu kuuluu selvästi jokaisen velvollisuuksiin, valta ja vastuu ovat toimintaorganisaatiolla, toimintaorganisaatiot kykenevät ottamaan huomioon omat erityistarpeensa ja turvallisuusorganisaatio välttyy jäämästä pullonkaulaksi yksikkötason turvallisuustilanteen kehittämisessä.

Fay (2002, 43 - 44) on samoilla linjoilla todetessaan, että linjaorganisaation turvallisuusvelvoitteita korostava politiikka on ehdoton etu kohteiden turvaamiseksi. Hän antaa esimerkin turvallisuuspolitiikkaan kirjattavasta velvoittavasta, mutta samalla motivointiin pyrkivästä kappaleesta:

> Johtajilla ja esimiehillä organisaation kaikilla tasoilla on velvollisuus huolehtia vastuu- ja tehtäväalueellensa kuuluvien resurssien, omaisuuden yms. kohteiden turvallisuudesta. Heidän tulee varmistaa, että sama vastuuvelvoite välittyy läpi organisaatiohierarkian. Edelleen heidän tulee varmistaa tarvittavien turvallisuusstandardien-, määräysten- ja -ohjeidenmukaisuus turvallisen työ- ja toimintaympäristön luomiseksi ja ylläpitämiseksi henkilöstölle, vieraille ja asiakkaille. Vastuualueen kohteiden turvallisuustilanteen arviointi on osa johtajien ja esimiesten vuosittaista tuloksellisuuden arviointia ja se voi vaikuttaa ansiokehitykseen ja harkinnanvaraisiin palkkioihin.

Turvattavien kohteiden luettelo on Fayn (2002, 101 - 102) näkemyksen mukaan laaja. Hän luettelee esimerkkeinä mm. työntekijät, sopimuskumppanit, asiakkaat, toimitilat, laitteet, tuotevaraston, rahat ja tiedot. Erikseen hän tuo vielä esille prosessit, jotka tarvitsevat resurssinsa ja aikaansaavat tuotokset esimerkiksi tuotteina tai palveluina.

Talbot ja Jakeman (2009, 261 - 263) määrittävät turvattavaksi kohteeksi esineen, asian tai prosessin, jota yksilö, yhteisö tai hallinto arvottaa ja arvostaa, ja joka on tärkeä odotettujen tulosten ja päämäärien saavuttamisen kannalta. He toteavat aluksi käsitteen perinteisesti kattavan ihmiset, tiedot, kiinteistöt, taloudelliset voimavarat ja maineen. Talbot ja Jakeman näkevät perinteisen määritelmän kuitenkin ongelmalliseksi kansainvälistyvässä toimintaympäristössä ja mainitsevat esimerkkinä kulttuurit, joissa rahalla tai ihmishengellä on totutusta poikkeava arvo. He haluavat nostaa myös tietotekniikan roolin paremmin esiin ja muotoilevat turvattavan kohteen käsitteen uudelleen: ihmiset, informaatio, (fyysinen) omaisuus sekä tieto- ja viestintäteknologia, joilla on arvoa tai joiden varassa toimintakykyisyys rakentuu ja säilyy (kuvio 12).



Kuvio 12: Toimintakykyä turvaavat kohteet (Talbot & Jakeman 2009, 264)

2.3 Kohteiden ja omaisuuden hallinta turvallisuuskontekstin ulkopuolella

2.3.1 PAS 55 -standardi

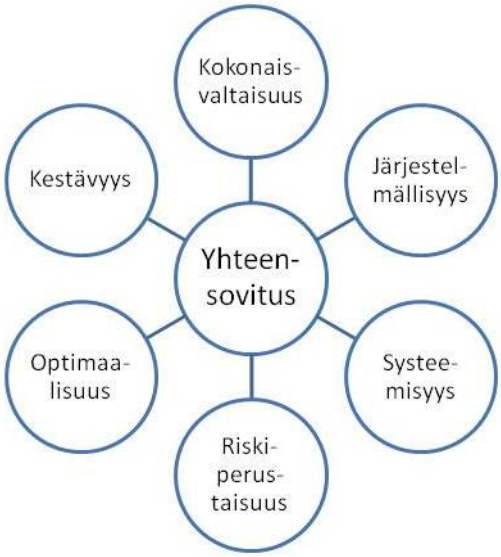
British Standards Institution (BSi) on julkaissut fyysisen omaisuuden hallintaa koskevan PAS 55-1:2008 -standardin (publicly available spesification). Se on samalla ainoa *asset management* -teeman kansainvälinen standardi. Yhteistyötahona määrityksen valmistelussa on toiminut omaisuudenhallinnan käytäntöihin keskittynyt järjestö The Institute of Asset Management (IAM). Standardissa määritellään kokonainen omaisuudenhallintajärjestelmä ja sen vaatimukset myös sertifiointitarpeita ajatellen. Standardin valmistelussa on otettu huomioon harmonisointitarpeet mm. ISO 14001- ja OHSAS 18001 -standardien kanssa.

PAS 55-1 -standardissa (2008, 2) määritellään omaisuuden hallinta seuraavasti (identtinen IAM:n määritelmän kanssa):

> **Omaisuuden hallinnalla** tarkoitetaan järjestelmällisiä ja koordinoituja toimenpiteitä ja käytäntöjä, joiden avulla organisaatio optimaalisesti ja kestävästi hallitsee omaisuutensa ja omaisuusjärjestelmänsä, niihin liittyvän suorituskyvyn, riskit ja kustannukset koko niiden elinkaarella organisaation strategisten tavoitteiden saavuttamiseksi.

Merkille pantavaa edellisessä määrityksessä on se, että hallinta kattaa omaisuuden koko elinkaaren. Määritelmän mukaisen omaisuudenhallinnan hyödyiksi standardissa mainitaan mm. parempi työturvallisuustaso, parempi kustannus/hyöty-suhde, parempi suunniteltavuus ja

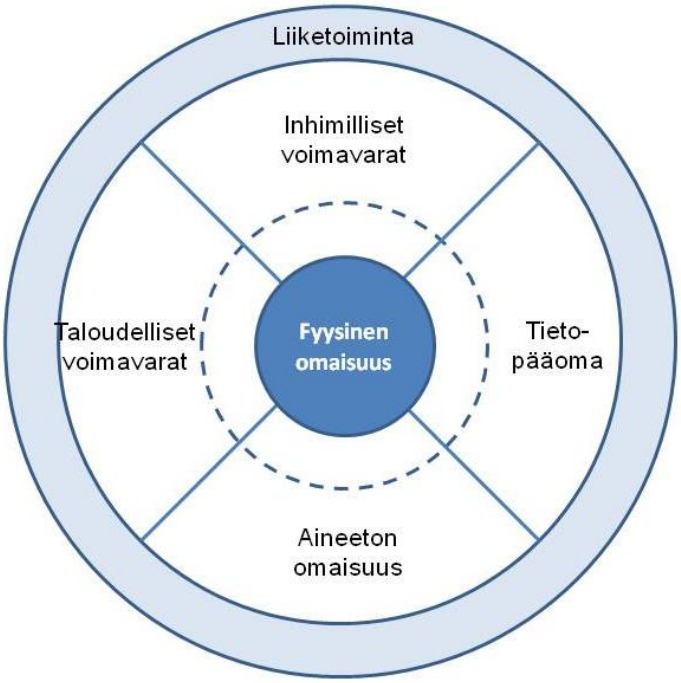
luottamus, näyttö vaatimusten täyttämisestä, parempi riskien hallinta ja valvonta sekä näyttö kestävän kehityksen tarpeiden huomioon ottamisesta (2008, v). Standardi määrittelee myös omaisuudenhallinnan pääperiaatteet ja osatekijät (kuvio 13).



Kuvio 13: Omaisuuden hallinnan pääperiaatteet (PAS 55-1:2008, v)

Pääperiaatteissa mainittu systeemisyys viittaa systeemiajatteluun. Sillä tarkoitetaan ymmärtämisen apuvälinettä, jolla voidaan kuvata monimutkaisien järjestelmien vaikuttavia osia ja näiden toiminnan yhteistulosta. Toisin kuin perinteinen analyysi, se ei pyri jakamaan tutkittavaa kohdetta osiin, vaan pyrkii ymmärtämään, miten eri osaset vaikuttavat kokonaisuuteen. (Mielonen 2011.) Yhteensovitettavina periaatteina systeemisyyden ohella ovat riskiperustaisuus, optimaalisuus, kestävyys, kokonaisvaltaisuus ja yleinen järjestelmällisyys. Näiden toimeenpano edellyttää standardin mukaan johtamista, tietoisuutta, sitoutumista ja koordinaatiota (2008, v).

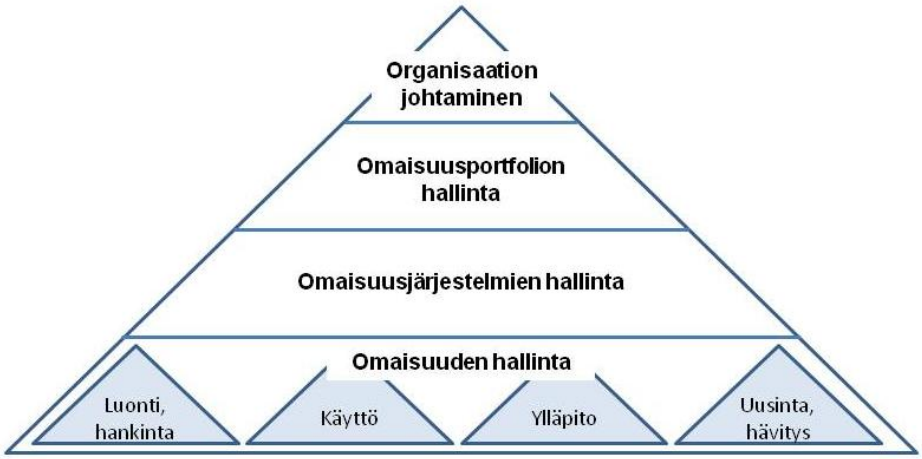
PAS 55-1 -standardissa todetaan, että fyysinen omaisuus edustaa yhtä omaisuustyyppien viidestä kategoriasta. Muut kategoriat ovat inhimilliset voimavarat, taloudelliset voimavarat, tietopääoma sekä muu immateriaalinen, aineeton omaisuus. Standardissa esitetään viitekehys, jossa näkyy fyysisen omaisuuden suhde muuhun omaisuuteen ja pääomaan sekä liiketoimintaan (kuvio 14).



Kuvio 14: Omaisuustyyppien viitekehys (PAS 55-1:2008, vi)

Katkoviivalla erotettu raja esittää PAS 55-1 -standardin painopistealuetta (2008, vi). Tietopääoman suuntaan rajapinnan keskeisiä teemoja ovat vaatimukset, suorituskyky, toimenpiteet, kustannukset ja mahdollisuudet. Aineettoman omaisuuden rajapinnassa ovat maine, imago, moraali, rajoitukset ja sosiaalinen näkökulma. Taloudellisen omaisuuden kanssa rajapinnassa esiintyvät elinkaarikustannukset, pääoman investointikriteerit, käyttökustannukset ja suorituskykyarvot. Inhimillisten voimavarojen rajapintaan kuuluvat motivaatio, viestintä, roolit ja velvollisuudet, osaaminen, kokemus, johtajuus ja yhteistyö. Asiayhteys liiketoimintaan tulee liiketoimintatavoitteiden, toimintaperiaatteiden, ohjesääntöjen, suorituskykyvaatimusten ja riskien hallinnan kautta. Näillä rajapinnoilla todetaan olevan vaikutusta siihen, miten fyysisen omaisuuden hallinnassa onnistutaan.

Standardissa pohditaan myös omaisuudenhallinnan haasteita. Niistä tuodaan esille mm. ajoittain ristiriitaiset odotukset lyhyen ja pitkän tähtäimen hyötyjen tavoittelussa. Omat haasteensa liittyvät myös erilaisiin tasoihin, joilla omaisuutta ja voimavaroja pitää tunnistaa ja hallita. Tämän vuoksi on nähty tarve jakaa omaisuuden hallinta eri tasoihin (kuvio 15).



Kuvio 15: Omaisuuden hallinnan tasot (PAS 55-1:2008, vii)

Omaisuudenhallintastandardissa noudatetaan PDCA-mallia: suunnittele - toteuta - arvioi - ylläpidä ja kehitä. Tämä näkyy myös standardin jäsentelyssä ja sisällössä. Standardin laajassa käsitteistössä huomio kiinnittyy omaisuudenhallintajärjestelmään (vrt. esim. laatujärjestelmä, tietoturvallisuuden hallintajärjestelmä). Käsite määritellään seuraavasti (PAS 55-1:2008, 2) (identtinen IAM:n määritelmän kanssa):

> **Omaisuudenhallintajärjestelmällä** tarkoitetaan organisaation omaisuuden hallinnan periaatteita, strategiaa, tavoitteita ja suunnitelmia sekä toimenpiteitä, prosesseja ja organisatorisia rakenteita niiden kehittämiseksi, toteuttamiseksi ja toimeenpanemiseksi sekä jatkuvasti parantamiseksi.

Omaisuudenhallintajärjestelmälle asetetaan PAS 55-1 -standardissa useita vaatimusalueita. Niistä keskeisiä päätason vaatimuksia ovat (2008, 6 - 19):

- Omaisuuden hallinnan politiikka (periaatteet)
- Omaisuuden hallinnan strategia, tavoitteet ja suunnitelmat (ml. jatkuvuus)
- Organisointi, vastuut, valtuudet ja velvollisuudet
- Koulutus, tietoisuus ja osaaminen
- Viestintä
- Dokumentointi
- Tiedon hallinta
- Riskien hallinta
- Vaatimusten ja vaatimustenmukaisuuden hallinta
- Muutosten hallinta
- Omaisuuden elinkaarihallinta

- Suorituskyvyn ja tilan seuranta
- Vahinkojen, virheiden, poikkeamien ja muiden erityistilanteiden hallinta
- Arviointi ja auditointi
- Korjaavat ja ehkäisevät toimenpiteet
- Jatkuva parantaminen
- Tallenteet
- Johdon katselmus

IAM:n Asset Management Competence Requirements Framework (2008, 9) kuvaa omaisuuden hallinnan erilaisia rooleja ja niihin liittyviä osaamisalueita. Nämä määrittävät osaltaan omaisuuden hallinnan olemusta. Keskeisinä osaamisalueina mainitaan 1) politiikan laatiminen, 2) strategian laatiminen, 3) omaisuuden hallinnan suunnittelu, 4) suunnitelmien toimeenpano, 5) tietoisuuden ja osaamisen levittäminen, 6) riskien hallinta ja suorituskyvyn parantaminen sekä 7) omaisuuden hallintaan liittyvä tiedonhallinta.

2.3.2 Muu ammattikirjallisuus

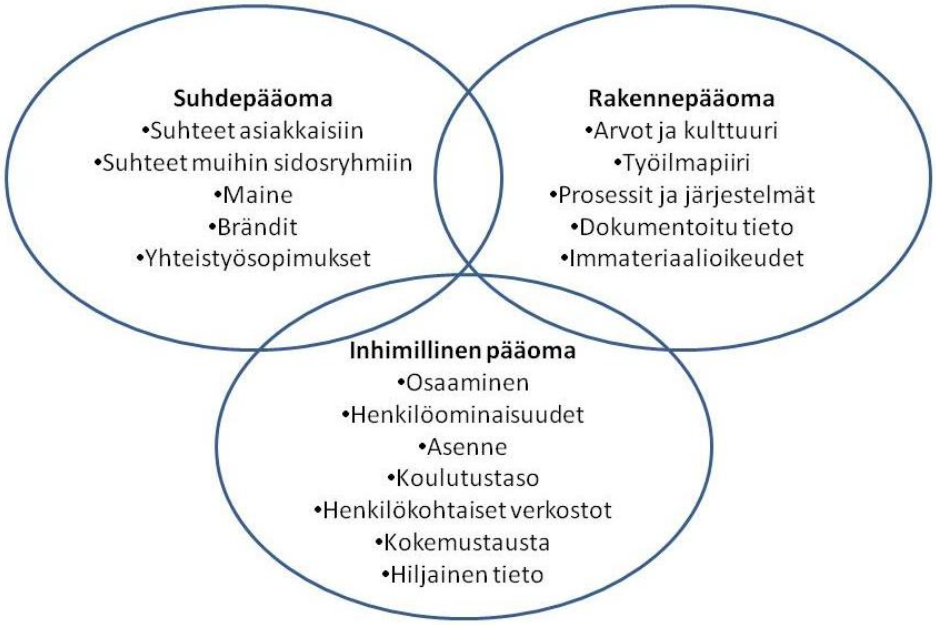
Kujansivu, Lönnqvist, Jääskeläinen ja Sillanpää (2007) ovat pohtineet laajasti liiketoiminnan aineettomia menestystekijöitä sekä niiden mittaamista, kehittämistä ja johtamista. Samalla he ovat tehneet rajanvetoa aineettoman ja fyysisen pääomalajin välille (taulukko 2). Myös näiden pääomalajien osa-alueet eroavat toisistaan, samoin niiden johtaminen, hallinta ja valvonta.

Fyysinen omaisuus/pääoma	**Aineeton omaisuus/pääoma**
Esim. tehtaan tuotantolaitteet	Esim. organisaation imago, asiakassuhteet
Konkreettisia asioita	Abstraktia, näkymätöntä
Selvät omistajasuhteet	Omistajuussuhteet vaikeita määrittää
Mahdollista ostaa ja myydä	Myyminen ja ostaminen usein mahdotonta
Sidottuna kerrallaan yhteen käyttötarkoitukseen	Voidaan hyödyntää samanaikaisesti eri käyttötarkoituksissa
Kuluu käytettäessä	Ei vähene käytettäessä
Investointiin liittyvät riskit ja mahdollisuudet paremmin hallinnassa	Investointiin liittyviä riskejä ja mahdollisuuksia vaikea arvioida etukäteen

Taulukko 2: Fyysisen ja aineettoman omaisuuden ja pääoman eroja (Kujansivu ym. 2007, 31)

Fyysinen pääoma on konkreettista ja selkeästi määritettävissä olevaa. Aineettomilla menestystekijöillä Kujansivu ym. tarkoittavat sekä organisaation strategisesti tärkeitä aineettomia resursseja että toimintoja, joilla parannetaan olemassa olevia resursseja ja tehostetaan niiden käyttöä sekä hankitaan uusia resursseja (2007, 27). Yritysten menestyminen pohjautuu heidän tutkimustensa mukaan entistä voimakkaammin aineettomiin menestystekijöihin.

Aineettoman omaisuuden tunnistamisessa Kujansivu ym. käyttävät myös aineettoman pääoman käsitettä (kuvio 16). Tällöin se merkitsee mm. älyllistä pääomaa, tietopääomaa, osaamispääomaa, aineetonta varallisuutta tai näkymättömiä voimavaroja. Vastaavissa yhteyksissä englanninkielisessä kirjallisuudessa esiintyy usein termi *intangible assets*.



Kuvio 16: Organisaation aineettoman pääoman osa-alueet (Kujansivu ym. 2007, 29)

Kujansivu ym. (2007, 30 - 31, 42) korostavat, että erilaisten aineettomien resurssien tulee yhdistyä toisiaan täydentävästi. Aineettoman pääoman luoma arvo syntyy vasta eri osa-alueiden yhdistyessä. Aineeton pääoma ei heidän mukaansa kuitenkaan itsessään tuota lisäarvoa. Vasta kun aineetonta pääomaa hyödynnetään, voidaan aikaansaada tuloksia.

Aineeton pääoma on myös dynaamista - muuttuvaa ja kehittyvää. Siihen liittyy riskejä, siihen voidaan myös vaikuttaa ja sitä voidaan johtaa ja hallita. Johtamisen ja hallinnan ensimmäisiin vaiheisiin kuuluu Kujansivun ym. (2007, 47 - 51) aineettoman pääoman tunnistaminen ja tähän he ehdottavat myös työkalua (taulukko 3). Taulukko itsessään antaa viitteitä PDCA-mallin

kaltaiseen kehittämiseen: suunnittelu, toteutus, seuranta ja arviointi sekä kehittäminen arviointi- ja mittaustulosten pohjalta.

Aineettomat resurssit	Resurssin toivetila	Resurssin tila nyt	Resurssin kehittämistoimet	Resurssin arviointi, mittaaminen
Osaaminen				
Henkilöominaisuudet				
Asenne				
Tieto				
Koulutustaso				
…				

Taulukko 3: Apuväline aineettoman pääoman kartoitukseen (ote: Kujansivu ym. 2007, 47)

2.4 Kytkentä organisaation johtamiseen

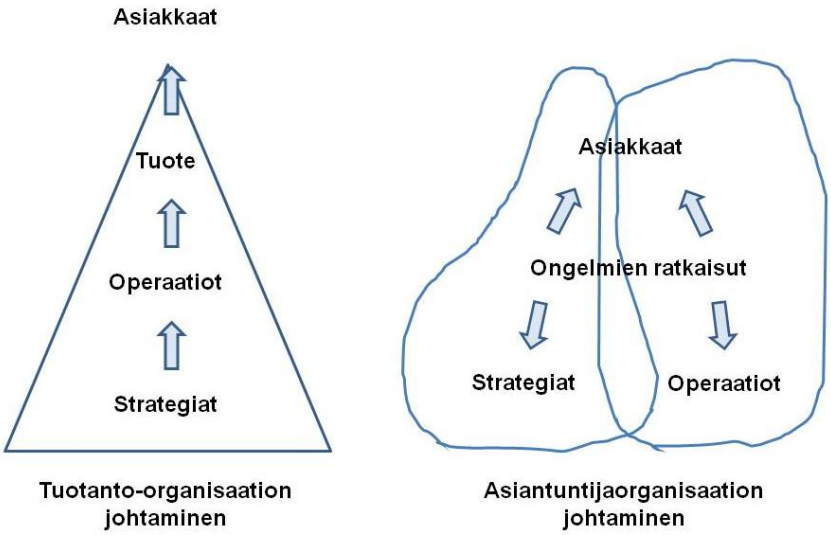
2.4.1 Johtamisen kokonaisuus ja tasot

Johtamisen perustehtävä on tukea organisaation toimintaa ja luoda mahdollisimman hyvät edellytykset laadukkaan ja tuottavan työn tekemiselle. Johtaminen ei kohdistu vain organisaation nykytilaan, vaan sillä pyritään vaikuttamaan myös siihen, minkälaiseksi organisaation tulevaisuus muodostuu. Johtamisen kautta toiminnalle määritellään haluttu suunta ja keinot, jotka otetaan harkitusti käyttöön. Johtamisen tarkoituksena on saada henkilöstö ymmärtämään ja hyväksymään mitä ja miten on tehtävä, jotta toiminta organisaation tavoitteiden saavuttamiseksi mahdollistuisi. Johtaminen on aina vuorovaikutteista. Johtaminen voidaan työpaikalla jakaa sen kohteen mukaan asiajohtamiseen ja ihmisten johtamiseen. (Johtaminen 2011.) Työterveyslaitos määrittelee johtamisen peruskäsitteistöä seuraavasti:

> **Johtamisella** tarkoitetaan kaikkea sitä ohjaavaa tai arvioivaa toimintaa, jota organisaatiossa tehdään sen päämäärien ja tavoitteiden täsmentämiseksi, toimintaedellytysten luomiseksi ja varsinaisen toiminnan ohjaamiseksi tavoitteiden mukaan (Johtaminen 2011).
>
> **Asioiden johtamisella** tarkoitetaan organisaation toiminnan ja toimintaprosessien hallintaa, suunnittelua, organisointia, kontrollointia sekä niihin liittyvää päätöksentekoa (Johtaminen 2011).
>
> **Ihmisten johtamisella** tarkoitetaan toisten ihmisten käyttäytymiseen vaikuttamista (Johtaminen 2011).

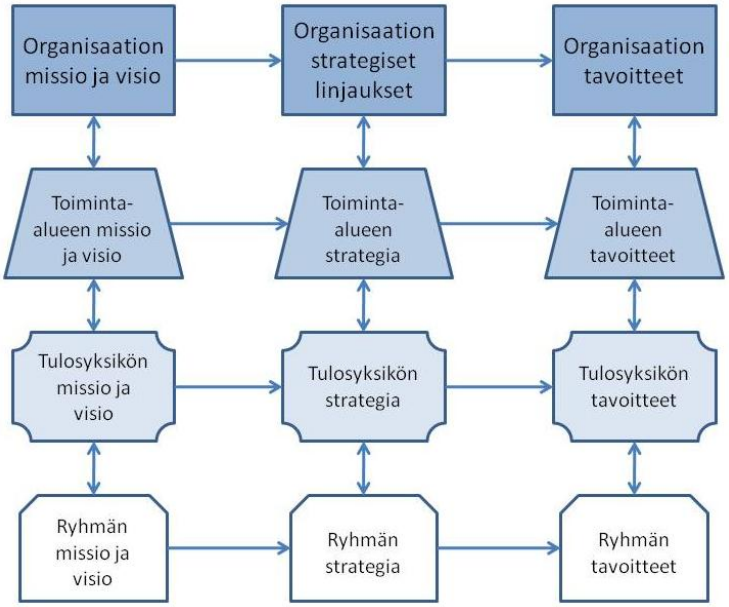
Johtaminen voidaan jakaa eri tasoihin. Strateginen taso viittaa organisaation pitkän aikavälin suunnitteluun ja niin sanottuihin suuriin linjoihin, ja siitä vastaa organisaation ylin johto. Käytännössä vähemmän käytetty termi taktinen taso viittaa keskipitkän aikavälin suunnitelmiin, ja siitä vastaa organisaation linjajohto. Operatiivisella tasolla puolestaan viitataan organisaation päivittäisen toiminnan johtamiseen, josta vastaavat suorittavan portaan esimiehet.

Myös organisaatioiden toiminnan luonne aiheuttaa Maunulan (1997, 9 - 12) mukaan eroja johtamiseen (kuvio 17). Vaikka erot ovat kärjistettyjä, niitä on hänen mukaansa mm. johtamishierarkiassa, ulkoisessa ja sisäisessä asiakasyhteistyössä ja kontaktipinnoissa. Erot eivät kuitenkaan ole laadullisia vaan nimenomaan toiminnan luonteesta johtuvia.



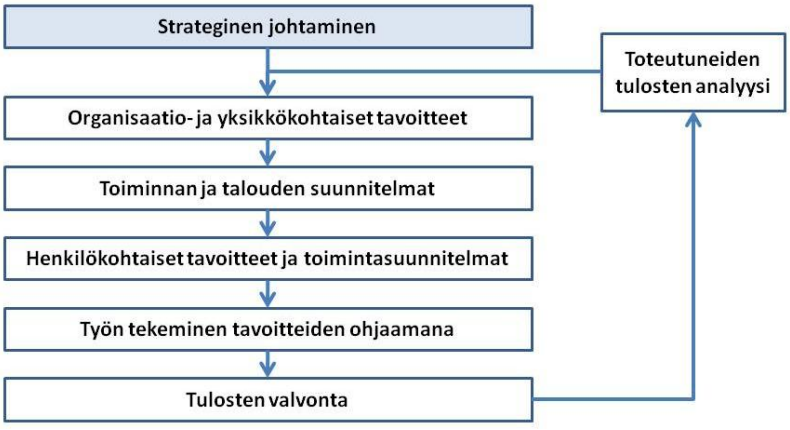
Kuvio 17: Tuotanto- ja asiantuntijaorganisaation periaate-eroja (Maunula 1997, 10)

Organisaation päätason strategia luo Viitalan ja Jylhän (2009, 268 - 269) mukaan kehykset kaikille organisaation eri prosesseissa, tehtäväalueilla ja yksiköissä luotaville strategioille. Näillä alastrategioilla päästrategia puretaan yksityiskohtaisempiin osiin, joista kukin antaa suuntaviivat yksittäisille vastuualueille (kuvio 18). Parhaimmillaan strategiset suunnitelmat muodostavat toisiaan tukevan kokonaisuuden.



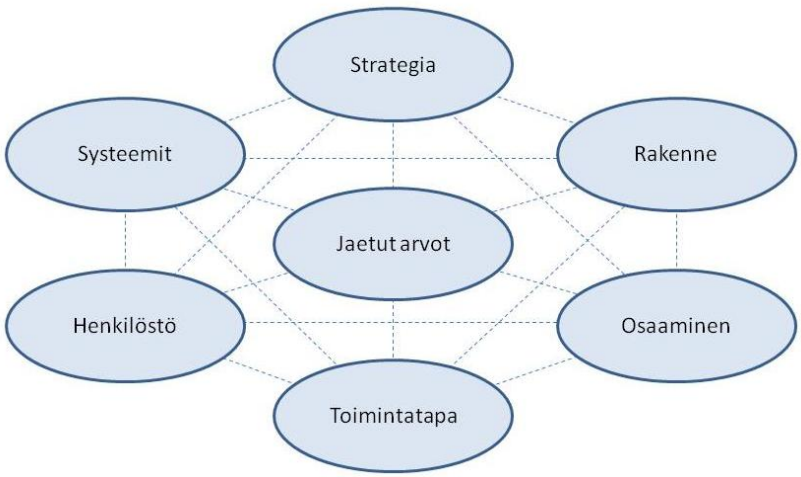
Kuvio 18: Strategisen suunnittelun hierarkia (Viitala & Jylhä 2009, 269)

Organisaatio osallistuu operaatioilla strategioiden toteuttamiseen. Peruskytkentä strategioista operatiiviseen johtamiseen on tehtävä Kamenskyn (2002, 278 - 280) mukaan hyvällä vuosisuunnittelulla. Hän viittaa tällä tavoitejohtamismalliin (kuvio 19), jonka avulla strategiat puretaan osastojen ja yksiköiden ja tarvittaessa myös alayksiköiden ja henkilötason vuositavoitteiksi ja toimintasuunnitelmiksi. Operatiivisella tasolla tulosten valvonta keskittyy tavoitteisiin ja on siten tiheämpää ja tarkempaa kuin strategisen tason valvonta.



Kuvio 19: Operatiivisen johtamisen malli (Kamensky 2002, 279)

Strategioiden toiminnallistaminen edellyttää Viitalan ja Jylhän (2009, 272 - 273) mukaan sitä, että organisaation toiminnan kokonaisuus muokataan strategiaa tasapainoisesti tukevaksi. Tähän he soveltavat ns. seitsemän S:n mallia *(strategy, shared value, structure, systems, style, staff, skills)*. Mallissa strategisten valintojen jälkeen kehitetään arvot, järjestelmät, henkilöstö, osaaminen, toiminnan rakenteet ja toimintatavat strategiaa tukevaan suuntaan (kuvio 20).



Kuvio 20: Seitsemän S:n malli (Viitala & Jylhä 2009, 273)

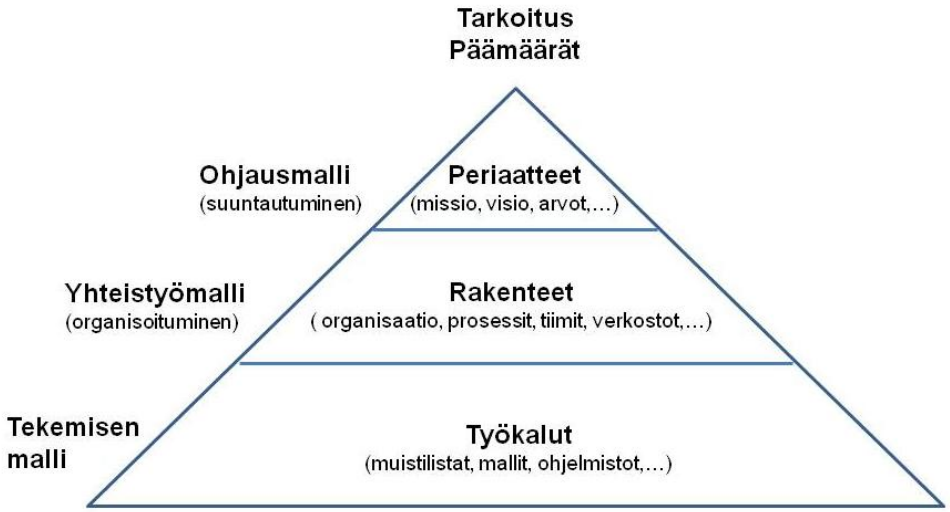
Edellä todettuun perustuen voidaan operatiivinen johtaminen määritellä seuraavasti:

> **Operatiivisella johtamisella** tarkoitetaan päivittäistä johtamista osasto-, yksikkö-, prosessi-, toiminto- ja henkilötasoilla.

2.4.2 Johtamis- ja toimintajärjestelmä

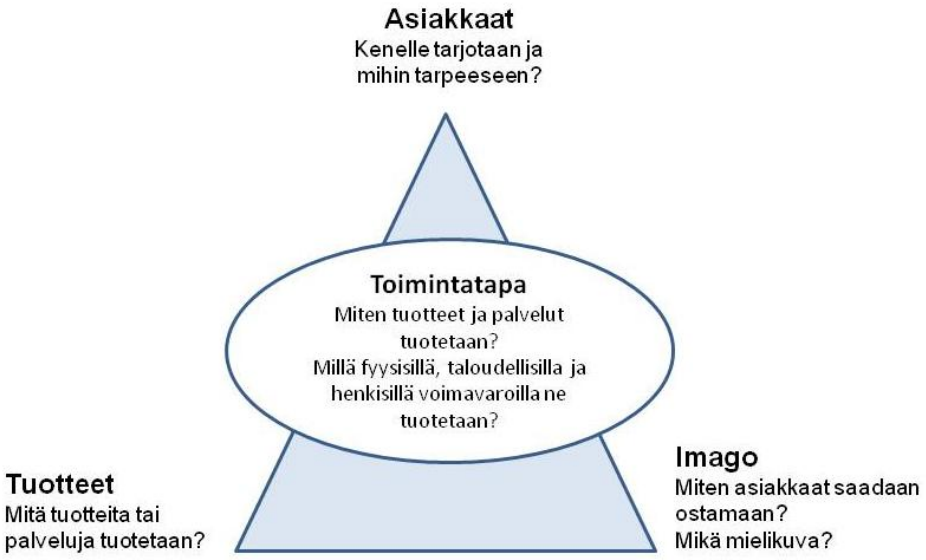
Johtamisjärjestelmät ovat keskeisiä johtamisen työvälineitä. Johtamisjärjestelmiä tarvitaan organisaation tavoitteiden asettamiseen, toiminnan suuntaamiseen, toimeenpanemiseen, tehostamiseen sekä seurantaan ja valvontaan. Johtamisjärjestelmät voidaan jakaa esimerkiksi strategisiin ja operatiivisiin johtamisjärjestelmiin.

Organisaatiota voidaan Laamasen (2002, 36) sekä Viitalan ja Jylhän (2008, 25 - 26) mukaan ajatella myös toimintakokonaisuutena ja toimintajärjestelmänä (kuvio 21). Malli on käyttökelpoinen useissa yhteyksissä ja soveltuu myös toiminnan loogisten tasojen tarkasteluun. Toimintajärjestelmän tehtävänä on mahdollistaa tavoitteiden ja päämäärien saavuttaminen.



Kuvio 21: Organisaation toimintajärjestelmä (Laamanen 2002, 36; Viitala & Jylhä 2009, 26)

Klassiseen liikeidean käsitteeseen kuuluu kolme peruskysymystä: kenelle, mitä ja miten (Viitala & Jylhä 2009, 51 - 52). Neljänneksi kulmakiveksi on myöhemmin lisätty imago eli millä asiakkaat saadaan ostamaan, mikä on olennaista kilpailussa menestymiselle. Kun nämä lähtökohdat yhdistetään liikeideaksi, voidaan samalla ryhtyä ratkaisemaan organisaation toimintatapaa eli miten sen tulee toimia (kuvio 22).

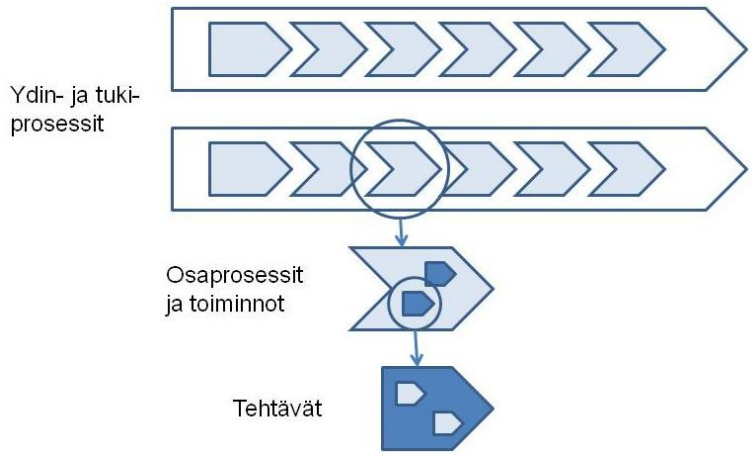


Kuvio 22: Liikeidea (Viitala & Jylhä 2009, 52)

Kujansivu ym. (2007, 143 - 156) toteavat, että organisaation menestystekijöitä johdetaan ja kehitetään monenlaisten järjestelmien avulla eri organisaatiotasoilla riippumatta siitä, ovatko menestystekijät aineellisia tai aineettomia. Monilla organisaatioilla on heidän mukaansa käytössä johtamisjärjestelmä, jolla ohjataan organisaation toimintaa, mihin sisältyy aineellisia ja aineettomia asioita. Tällöin on tarkoituksenmukaista kehittää olemassa olevaa johtamisjärjestelmää siten, että se ottaa mahdollisimman hyvin huomioon myös aineellisen ja aineettoman pääoman ja siten myös turvattavat kohteet.

2.4.3 Prosessimainen toimintatapa

Koska strategiat toteutetaan lopulta käytännön toiminnan tuloksena, on organisaatioissa Viitalan ja Jylhän (2009, 206 - 207) mukaan jakaa työ tarkoituksenmukaisiin rakenteisiin. Tällaiseen rakenteeseen voi sisältyä ydinprosesseja, tukiprosesseja, edellisistä tarkennettuja osaprosesseja, yksittäisiä toimintoja sekä käytännön tason työtehtäviä (kuvio 23). Lähtökohtaisesti kaikille tehtäville tarvitaan vastuuhenkilö ja tekijä.



Kuvio 23: Toiminnan hierarkkinen rakenne (Viitala & Jylhä 2009, 206)

Liiketoimintaprosessi on Laamasen (2002, 19 - 20) määritelmän mukaan joukko toisiinsa liittyviä toistuvia toimintoja ja niiden toteuttamiseen tarvittavat resurssit, joiden avulla syötteet muunnetaan tuotteiksi. Hän määrittelee myös, että toimintaprosessi on joukko loogisesti toisiinsa liittyviä toimintoja ja niiden toteuttamiseen tarvittavia resursseja, joiden avulla saadaan aikaan toiminnan tulokset. Prosessin käsite koostuu Laamasen määritelmien mukaan syötteistä, toiminnasta, resurssista, tuotoksesta ja suorituskyvystä.

Operatiivisen johtamisen ja prosessien kannalta mielenkiintoisia rooleja ovat johto, prosessin omistaja sekä yksikön vetäjä ja esimies. Laamasen (2002, 122) mukaan rooli tarkoittaa toimenkuvaa, joka kytkee ihmisen johonkin, esimerkiksi prosessiin ja selvittää, mikä hänen tehtävänsä prosessissa on. Laamasen näkemys mainituista rooleista sisältää prosessin ymmärtämisen, vakiinnuttamisen ja parantamisen (taulukko 4).

	Johto (johtoryhmän jäsen)	**Prosessin omistaja**	**Yksikön vetäjä, esimies**
Ymmärtäminen	• Prosessien tunnistaminen ja prosessikartan hyväksyminen • Prosessin omistajan ja esimiesten nimeäminen • Organisaation toimintaperiaatteiden luominen • Varmistuminen prosessin yhteensopivuudesta organisaation toimintaperiaatteisiin • Prosessikuvausten ja resurssitarpeiden hyväksyminen	• Rajapinnoista sopiminen • Prosessin kuvaaminen • Varmistuminen prosessin yhteensopivuudesta organisaation toimintaperiaatteisiin • Prosessin osaamisten, työkalujen ja ohjeiden tunnistaminen • Prosessin osallisten tietoisuuden varmistaminen	• Prosessin analysointi ja palautteen antaminen omistajalle • Vastuualueella tarvittavan osaamisen tunnistaminen • Oman roolin tunnistaminen
Vakiinnuttaminen	• Tasapainoisen strategian luominen, prosessien tavoitteista ja yksikön resursseista sopiminen • Strategian mukaisten resurssien varaaminen prosessien käyttöön • Prosessin omistajien ja esimiesten valtuuksista sopiminen • Prosessien suorituskyvyn katselmointi ja kehitystoimenpiteiden käynnistäminen	• Resurssien kiinnittäminen • Esimiesten ja johdon tietoisuuden varmistaminen prosessin tarpeista • Kriittisten työkalujen ja ohjeiden olemassaolon ja kunnon varmistaminen • Valvonta • Muutoksiin ja poikkeamiin reagointi	• Oma toiminta prosessin mukaan • Alaisten toiminnan prosessinmukaisuuden varmistaminen • Tarvittavien resurssien ja osaamisen hankkiminen
Parantaminen	• Kehittämistavoitteista sopiminen • Organisaationlaajuisten muutosten käsittely	• Kehittämistavoitteista sopiminen • Suorituskyvyn arviointi suhteessa tavoitteisiin • Hyvien ja parhaiden käytäntöjen tunnistaminen (myös prosessin ulkopuolelta) • Kehittämishankkeiden käynnistäminen • Prosessin systemaattinen arviointi	• Kehitystarpeiden tunnistaminen ja välittäminen omistajalle

Taulukko 4: Johdon, prosessin omistajan sekä yksikön vetäjän ja esimiehen prosessiroolit (mukaillen Laamanen 2002, 123 - 128)

Hyvään prosessikuvauksen tulee Laamasen (2002, 76) mukaan 1) sisältää prosessin kannalta kriittiset asiat, 2) esittää asioiden välisiä riippuvuuksia, 3) auttaa ymmärtämään sekä kokonaisuutta että omaa roolia, 4) edistää prosesseissa toimivien ihmisten yhteistyötä ja 5) antaa mahdollisuus toimia joustavasti tilanteen vaatimusten mukaan.

Tietohallinnon prosessien käsittelyn yhteydessä COBIT-mallissa (2007, 13 - 14) on vastaavasti odotusarvona ns. prosessikontrollien kuvaaminen. Mallin mukaiset prosessikontrollit ovat 1) prosessin tarkoitus ja tavoitteet, 2) prosessin omistajuus, 3) prosessin toistettavuus (mm. vuokaavio ja sanallinen kuvaus), 4) prosessin roolit ja velvollisuudet, 5) prosessin viiteasiakirjat ja 6) prosessin suorituskyvyn parantaminen.

Miettinen (1999, 28 - 31) yhdisti tietoturvallisuuden liiketoiminnalliseen näkökulmaan ja prosessitason näkökulmaan. Hänen mukaansa ilman toimintaprosessien ja tarvittavien omaisuuserien tunnistamista suojauksia on hankala kohdistaa oikeisiin kohteisiin ja oikeassa mittakaavassa, oikeassa muodossa ja oikea-aikaisesti. Vaarana on tällöin sekä yli- että alisuojaaminen.

Liiketoiminnallisesti tärkein kysymys Miettisen mukaan on: Miksi tietoturvallisuus on tärkeä asia liiketoiminnalle? Hän tarjoaa tämän selvittämiseen useita apukysymyksiä: Mitä tietoja organisaatio tarvitsee toiminnassaan? Mitä tiedoista ovat kaikkein tärkeimmät? Kuinka pitkään toiminta voi jatkuva ilman tärkeitä tietoja? Mitä tapahtuu, jos tärkeät tiedot joutuvat ulkopuolisen haltuun, katoavat, varastetaan tai niitä muutetaan luvatta? Mitä tapahtuu, jos tärkeät tiedot tuhoutuvat?

Miettinen (1999, 31 - 33) toteaa tietoturvallisuuden kehittämisen ja ylläpitämisen tarkoituksena olevan varsinaisen toiminnan tukeminen. Kun jokaisella organisaatiolla kuitenkin on omat toimintamallinsa ja työrutiininsa, on tietoturvatoiminnan integroiduttava niihin. Organisaation toiminta muodostuu Miettisen mukaan toimintaprosesseista (jäsentyneinä tai jäsentymättöminä) ja erilaisista omaisuuseristä, eli fyysisistä ja ei-fyysisistä suojauskohteista. Prosessitason tarkastelu tietoturvanäkökulmasta alkaa tällöin Miettisen mukaan suojattavien kohteiden ja suojausta vaativan toiminnan selvittämisellä.

Prosessitason selvittämiseen Miettisen ehdottamia apukysymyksiä ovat: Mistä toimintaprosesseista organisaation toiminta muodostuu? Mitkä toimintaprosessit ovat organisaatiolle tärkeimpiä? Mitkä ovat prosessien heikkouden ja vahvuudet? Mitä fyysisiä ja ei-fyysisiä suojauskohteita toimintaan liittyy? Mitkä suojausta vaativista kohteista ovat tärkeimpiä toiminnalle? Mikä on suojattavien kohteiden tärkeysjärjestys? Mitkä ovat suojattavien kohteiden heikkoudet ja vahvuudet?

2.5 Yhteenveto

Turvattavista kohteista on turvallisuus- ja tietoturvakontekstissa esiteltyjen lähteiden perusteella varsin yhtenäinen perusnäkemys, mutta varsinaiset käsitemäärittelyt eroavat toisistaan. Hallintaulottuvuus turvattaviin kohteisiin jää alueeksi, jota tunnutaan pitävän niin itsestään selvyytenä, ettei hallinnan käsitemäärittelyä lähteistä löytynyt. Asia jää lähteiden lukijoiden muodostaman mielikuvan varaan. Turvattavien kohteiden hallinnan (*asset management*) otsikoiden alla annettavat ohjeistukset pahentavat asiaa, sillä niissä painotetaan vain kohteiden tunnistamista, vastuuttamista, arvottamista ja luokittelua turvallisuustoiminnan lähtökohtana. Kohteiden varsinaista hallintaa tämän jälkeen ei käsitellä, vaan ”vastuu” siirtyy riskien hallinnalle.

Hakeutuminen turvallisuuskontekstin ulkopuolelle tarjoaa laajempaa näkökulmaa. Fyysisen omaisuuden hallinnan käsite on myös määritelty selvästi. Erityisesti omaisuuden hallinnan standardissa esitetty elinkaariajatus tuo ratkaisevan näkemyseron kattavuuteen. Lisäksi standardi avaa kokonaista omaisuudenhallintajärjestelmää ja omaisuuden elinkaarella huomioon otettavia näkökohtia ja hallintatoimenpiteitä.

Johtamista käsittelevä osuus tuo varmuutta siihen, että tietoturvallisuus, tietoturvallisuuden hallinta, turvattavat kohteet ja turvattavien kohteiden hallinta ovat sovitettavissa organisaatioiden johtamis- ja toimintajärjestelmiin ja prosesseihin tarvitsematta luoda uusia rakenteita. Liityntäpinnat ovat konkreettisia.

3 Tutkimus- ja kehittämismenetelmät

Perustavaa laatua oleva ero tutkimuksella ja tutkimuksellisella kehittämisellä suhteessa arkiajatteluun on siinä, että tutkimustyössä käytetään systemaattisia menetelmiä (Ghauri & Grønhaug 2005, 12). Tutkimukseen pohjautuva tieteellinen tieto eroaa Aaltolan (2010, 13 - 20) mukaan arkitiedosta siinä, että tiedolle voidaan asettaa täsmällisempiä vaatimuksia esimerkiksi tarkkuuden, selkeyden, johdonmukaisuuden ja varmuuden osalta. Tieteen tehtävänä on myös kyetä korjaamaan omia tuloksiaan, mikäli aiempi tieto osoittautuu epäpäteväksi. Tieteen hyödyllisyyden kannalta on lisäksi keskeistä, että tiede kohdistuu todellisuuteen.

Aaltola (2010, 13 - 20) näkee tieteen erityispiirteiden sijaitsevan sekä tutkimuksen tuloksissa että tutkimustoiminnan prosessissa. Hän selventää näkemystään esitellessään neljää erilasta tapaa omaksua käsityksiä: 1) itsepäisyyden menetelmä - pitäminen kiinni omista alkuperäisistä uskomuksistaan, 2) auktoriteetin menetelmä - tukeutuminen erehtymättömänä pitämäänsä auktoriteettiin, 3) apriorinen menetelmä - luottaminen omaan olettamaansa kykyyn muodostaa tietoa pelkästään järjen, oivalluksen tai älyllisen intuition avulla, ja 4) tieteellinen menetelmä - tutkimuksellisten menetelmien käyttäminen kulmakivinään objektiivisuus ja julkisuus. Keskeisenä haasteena tieteessä Aaltola näkee kyvyn ymmärtää todellisuuden erilaisia ilmiöitä ja niiden välisiä yhteyksiä.

Tämä tutkimus- ja kehittämistyö toteutettiin soveltavana tutkimushankkeena suunnittelutieteeseen kuuluvaa konstruktiivista tutkimusmetodia käyttämällä. Tässä luvussa perustellaan tehdyt valinnat sekä kuvataan käytetyt menetelmät ja niiden soveltaminen. Tarkoituksena on samalla auttaa muodostamaan käsitys myöhemmin esitettävien tulosten luotettavuudesta.

3.1 Menetelmällinen perusta

Tutkimustyöllä tuotetaan uutta tietoa, jolla on käyttöä joko tieteen edistämisessä tai käytännössä, tai molemmissa. Tutkimus jaetaan tavallisesti perus- ja soveltavaan tutkimukseen (Järvinen & Järvinen 2004, 103). Erilaisia tutkimusmetodeja on runsaasti ja tutkijan tehtävänä on valita niistä se tai ne, jotka parhaiten ohjaavat ja auttavat tutkimusongelman ratkaisemisessa – ongelma määrää käytettävän metodin.

Tässä työssä tutkimusstrategisena perusvalintana oli ongelmanratkaisuun ja toimintasuosituksiin tähtäävä soveltava tutkimus. Soveltavalle tutkimukselle (vs. teoreettinen perustutkimus) on kuvaavaa, että siihen kuuluu esimerkiksi ongelmien ratkaisua, vaikutusten ennustamista, kehittämistä, testaamista, kenttätyötä ulkopuolisten organisaatioiden kanssa, metodien yhdistelyä ja aikataulullisesti rajattua työtä (Hirsjärvi, Remes & Sajavaara 2002, 121).

Järvisten (2004, 8 - 9, 12, 15) näkemyksen mukaan tutkimuksen perimmäisenä tarkoituksena mainitut kuvaaminen, selittäminen, ennustaminen tai kontrolli, eivät kata kaikkia tutkimuksia. Esimerkkinä he mainitsevat tietojärjestelmän konstruoinnin, jossa tarkoituksena on pikemminkin tutkia, voidaanko ja millä tavalla saada aikaan tietty uusi konstruktio. Edelleen tarkoitus voi konstruoinnin lisäksi olla myös systeemin ymmärtäminen, sen uudelleensovitus tai arviointi. Konstruktiivisen tutkimuksen piiriin voidaan sijoittaa myös kaikki hyödyllisyyttä painottavat tekniset, sosiaaliset ja tiedolliset innovaatiot. Konstruointi voi olla uusi innovaatio tai entisen parantaminen.

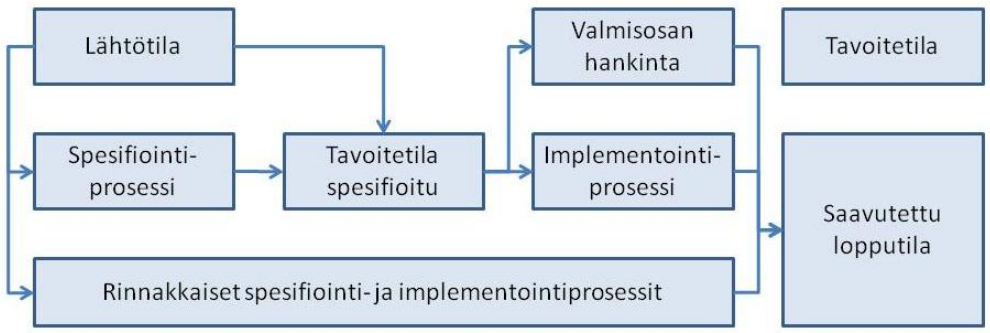
Mikäli tutkimuskysymys sisältää esimerkiksi rakentamisen, parantamisen, korjaamisen, sovittamisen tai laatimisen kaltaisia verbejä, se viittaa suunnittelutieteeseen (Järvinen & Järvinen 2004, 103). Valitussa tutkimusaiheessa tarkoituksena on parantaa ja yhdenmukaistaa turvattavien kohteiden hallintaa sekä kehittää malli ja työkalu turvattavien kohteiden haltuunottoon tietoturvanäkökulmasta. Suunnittelutieteellisesti tarkasteltuna tarkoituksena on tällöin luoda tietämystä suunnittelua ja toteutusta eli konstruktio-ongelmien ratkaisemista varten ja arvioida konstruoidun ratkaisun, innovaation, käyttökelpoisuutta ja hyödyllisyyttä. Näin ollen tutkimus on luontevaa toteuttaa soveltavana tutkimushankkeena suunnittelutieteeseen kuuluvaa konstruktiivista tutkimusmetodia käyttämällä.

Järvisten (2004, 103) näkemyksen mukaan konstruoinnin tulokset voivat olla konstrukteja, malleja, metodeja tai toteutuksia. Konstruoinnin lähestymistapa puolestaan voi olla joko rakentamista tai arviointia. Joka tapauksessa uudenkin innovaation hyödyllisyys on jossain vaiheessa arvioitava. Järviset (2004, 104) tiivistävät suunnittelutietämyksen kolme pääaluetta seuraavasti: 1) kohteen suunnittelu - lopputuloksen suunnittelua ja määrittelyä, 2) prosessin suunnittelu - suunnittelua, miten eri resursseja käyttäen lopputulos saadaan aikaan, ja 3) toteutuksen suunnittelu - käytännön toimenpiteiden suunnittelua pääsemiseksi alkutilasta haluttuun lopputilaan.

Suunnittelutieteessä tyypillinen tutkimustulos on esimerkiksi teknologinen sääntö, joka voidaan Järvisten (2004, 104 - 105) mukaan määritellä yleisen tietämyksen tihentymäksi. Se liittää innovaation haluttuun tulokseen tai suorituskykyyn tietyllä alueella sovellettaessa. Olennaista tällaisten sääntöjen osalta on niiden systemaattinen testaaminen. Sääntö on testattu, kun sen toimivuus tarkoitetussa asiayhteydessä on systemaattisesti osoitettu. Tutkijan itse suorittamaa säännön testausta voidaan kutsua α-testaukseksi ja riippumattomien kolmansien osapuolten testausta ß-testaukseksi. Konstruktin valmiiksi rakentaminen viittaa suunnitteluongelman ratkeamiseen. Rakentamisen tulosta arvioidaan siitä käyttäjäyhteisölle koituvan arvon ja hyödyn perusteella.

Järviset (2004, 106) nostavat innovaation toteuttamisen yhdeksi keskeiseksi tavaksi myös kokeilemisen. Siinä teknologisia sääntöjä kehitellään ja testataan yhteistyössä käyttäjien kanssa todellisessa sovellusympäristössä. Yhteistyötilanteiden jälkeen pohditaan, mitä tietämystä kyseisestä tapauksesta voidaan siirtää seuraaviin vastaavanlaisiin tapauksiin ottaen huomioon tapausten yhtäläisyydet ja erot. Tätä kokeiluprosessia voidaan soveltaa niin α- kuin ß-testaukseenkin.

Innovaation toteuttamisen perusprosessi on Järvisten (2004, 107) kuvaamana hyvin yksinkertainen: lähtötila - toteuttaminen - tavoitetila. Tavoitetilanteeseen voidaan pyrkiä eri tavoilla (kuvio 25). Tavoista riippumatta niihin sisältyy spesifiointia eli määrittelyä ja implementointia eli toteuttamista. Sekä spesifiointiprosessi että implementointiprosessi voidaan tarvittaessa jakaa useampaan vaiheeseen.



Kuvio 24: Konstruktion vaihtoehtoisia toteutustapoja (Järvinen & Järvinen 2004, 108)

Järvisten mallissa erityisesti merkille pantavaa on valmisosan käyttöön liittyvä vaihtoehto. Osa implementoinnista voidaan hoitaa hankkimalla yksi tai useampi valmisosa. Valmisosan ideana Järvisten (2004, 111) mukaan on, että ”pyörää ei kannata keksiä uudelleen”. Mahdollisen valmisosan hankinnassa paneudutaan potentiaalisten vaihtoehtojen selvittämiseen, vertailemiseen sekä tarvittaessa mahdollisen hankinnan toteuttamiseen.

Tavoitetila heijastaa Järvisten (2004, 108 - 109) mukaan tutkijoiden, suunnittelijoiden tai päättäjien arvoja. Tavoitetila esittää, miten asioiden pitäisi olla. Spesifiointiprosessin tarkoituksena on tuottaa kuvaus tavoitetilanteesta. Jos tutkija yksin määrittää uutta innovaatiota, hänen ei tarvitse sovittaa sitä useamman intressiryhmän erilaisiin tavoitteisiin, vaan voi painottaa uuden innovaation määrittelyä. Kirjallisuustutkimuksen avulla voidaan varmistua innovatiivisuudesta, mutta myös pieni parannus voi olla hyväksyttävää.

Käytännön innovaatioissa Järviset (2004, 109) näkevät usein olevan kyseen tilanteesta, jossa on useita osapuolia ja intressiryhmiä, ja joilla on omia toiveita, jopa vastakkaisia pyrkimyksiä tutkijan hahmotteleman innovaation ja tavoitetilan suhteen. Käytännössä tavoitetilaa ei aina saavuteta. Tavoite voi jäädä kokonaan saavuttamatta tai tavoitteesta voidaan hieman jäädä, mutta siitä voidaan mennä ylikin.

Implementointiprosessissa pääkysymys on Järvisten (2004, 109 - 110) mukaan muodossa: miten. Ratkaisua voidaan lähestyä esimerkiksi ongelmanreduktion heuristiikalla, jolloin pääongelma jaetaan ensiksi ratkaistaviin pienempiin osa-ongelmiin. Tila-siirtymä-heuristiikkaa käytettäessä edettäisiin lähtötilasta kohti tavoitetilaa peräkkäisten tilanmuutosten kautta, esimerkiksi siirtymällä vaiheittain yleisemmästä yksityiskohtaisempaan kuvaamiseen ja rakentamiseen.

Eteneminen voi olla myös hyvin evolutionääristä, jolloin tavoitetilan määrittelyä ja sen toteuttamista hoidetaan rinnakkain esimerkiksi tuottamalla prototyyppejä ja vertaamalla niitä ajateltuun tavoitetilaan. Eräs keskeinen syy rinnakkaisen spesifiointi- ja implementointiprosessin käyttämiseen on Järvisten (2004, 111 - 113) mukaan vaikeudessa kuvitella sellaista, mitkä ei aiemmin ole ollut olemassa. Esimerkiksi ohjelmistokehityksessä on käytetty metodia, jossa uusi versio tai sen luonnos annetaan koekäyttöön, sitä ylläpidetään ja suuremman muutostarpeen ilmaantuessa tuotetaan uusi versio. Asteittaisessakin kehittämisessä kehittämistutkimus on kyettävä päättämään, mitä vaikeuttaa jatkuvasti syntyvät uudet parantamisideat.

Suunnittelutieteen rakentamisen tuloksista Järviset (2004, 113 - 114) nostavat esille käsitteistön, mallin, metodin ja realisoinnin. Uutta käsitteistöä voidaan luoda, mutta koko käsitteistöä ei yleensä ole syytä uusia, sillä innovaation omaksuminen ja käyttö hankaloituu ilman kiinnekohtia käyttäjille tuttuun käsitekarttaan. Uusi malli kuvaa mahdollista realisaatiota ja se voi esittää tavoitetilaa prosessin alussa tai sen aikana. Mitä yksityiskohtaisemmaksi tavoitetilan kuvaus saadaan, sitä paremmin sen toteutettavuus, hyödyt ja sivuvaikutukset ovat arvioitavissa. Metodi käsittää tarvittavat askeleet, esimerkiksi ohjeiston muodossa, joita käytetään tehtävän suorittamiseen. Askeleet voivat koostua teknisistä, sosiaalisista ja tiedollisista resursseista uudella tavalla. Metodin onnistuneisuuden mittarina voi olla sen arviointi jollain tavalla parempi aiempiin metodeihin verrattuna.

Tieteellistä arviointia varten Järviset (2004, 115) tähdentävät, että rakentamisprosessi on kuvattava yksityiskohtaisesti perustellen valinnat ja päätökset. Samalla on osoitettava ratkaisun alkuperäisyys ja paremmuus aiempiin verrattuna. Soveltuva raportointimalli voi koostua Järvisten mukaan esimerkiksi seuraavista osista: 1) johdanto, 2) keskeisen idean tai konseptin esittely ja vertailu muihin vaihtoehtoihin, 3) rajoitukset, 4) merkittävin suunnitteluongelma, sen parhaat ratkaisuvaihtoehdot ja vaihtoehdon valinta perusteluineen, 5) muut alemman

tason suunnitteluongelmat, 6) toteutuksen (lopputilanteen) kuvaus tai konstruoinnin yksityiskohtainen suunnitelma, 7) uuden innovaation alustava arviointi ja 8) pohdinta tulosten merkityksestä, rajoituksista, suosituksista ja jatkotutkimuskohteista.

Innovaation arvioinnissa voidaan käyttää mittausta, joka edellyttää mittarin määrittelyä ja suorituksen mittaamista kyseisellä mittarilla. Järviset (2004, 118 - 124) ovat tutkineet arviointitutkimuksessa käytettyjä mittareita ja kehittäneet myös omia. Järviset itse painottavat helppokäyttöisyyttä, hyödynnettävyyttä, todellisuudenmukaisuutta sekä johdonmukaisuutta. Vastaavasti he suhtautuvat kriittisesti mallin täydellisyyteen ja yksityiskohtaisuuteen innovaation arviointikriteereinä, sillä malli on abstraktio realisaatiosta. Yksityiskohtaisen mallin kuvaus olisi tavattoman laaja, mikä yksityiskohtineen peittäisi alleen realisaation oleelliset asiat. Taulukkoon 5 on koottu tiivistetty näkemys käyttökelpoisista arviointikriteereistä ja -näkökulmista. Olennaista on aina arvioida, missä määrin asetetut tavoitteet saavutettiin.

Tutkimustulos	**Mahdolliset arviointikriteerit ja -näkökulmat**
Käsitteistö	• Ymmärrettävyys • Helppokäyttöisyys • Rajakäsitteiden yhtenäisyys • Hyödynnettävyys
Malli, tavoitetila	• Mallin ja todellisuuden vastaavuus • Lujuus, sisäinen johdonmukaisuus • Kuvien esitysmuodon ja sisällön suhde, tuki ymmärrettävyydelle • Mediavalinnan tarkoituksenmukaisuus
Metodi	• Operationaalisuus - metodin kyky suorittaa tehtävä, ihmisten kyky tehokkaasti käyttää metodia • Tehokkuus • Yleisyys • Helppokäyttöisyys • Sovellusalueen huomiointi - tarvittavat tekniset, inhimilliset tai tiedolliset resurssit
Realisaatio	• Innovaation tehokkuus ja vaikuttavuus • Innovaation vaikutukset ympäristöön ja käyttäjiin • Innovaation odottamattomat positiiviset ja negatiiviset vaikutukset • Taloudelliset, tekniset ja fyysiset vaikutukset • Sosiaaliset ja poliittiset vaikutukset • Investointien arviointi - kustannus-/hyötyanalyysi, laajuus-, arvostus-, mittaus-, jaksotus- ja kohdistusongelmien arviointi • Korjaavan, sopeuttavan, parantavan ja ehkäisevän huollon tarpeen ja kustannusten arviointi • Asetettujen tavoitteiden saavuttamisen aste

Taulukko 5: Konstruktiivisen tutkimuksen tulosten käyttökelpoisia arviointikriteerejä (lähtökohtana Järvinen & Järvinen 2004, 123)

3.2 Lähtötila

Tutkimus- ja kehittämisympäristönä toimi valtionhallinnon organisaatio, joka jakautui rakenteellisesti osastoihin ja yksiköihin. Prosessiajattelu organisaatiossa oli voimistumassa ja tietoa mallintava arkkitehtuurityö aloitettu. Organisaatiossa oli keskitetty tietoturvatoiminto, joka tehtävänä oli rakentaa ja ottaa käyttöön systemaattinen tietoturvallisuuden johtamis- ja hallintajärjestelmä. Samalla tuli ottaa huomioon valtionhallinnon tietoturva-asetuksen (681/2010) ja tietoturvatasojen (VAHTI 2/2010) – tai niistä aiemmin saatavilla olleiden luonnosten – implementointi.

Kehittämistä ja toimeenpanoa ohjattiin projektina, jonka ohjausryhmässä olivat edustettuina ylin johto, yleishallinnon johto, talousjohto, tietohallintojohto sekä substanssi- ja turvallisuustoiminta. Tällä kokoonpanolla pyrittiin osaltaan vaikuttamaan siihen, että ratkaisuissa tulisi huomioitua kattavasti toteuttamiskelpoisuus, organisaation toimintaympäristö johtamisjärjestelmineen ja käytännön realiteetteineen, ja että johto sitoutuisi menettelyjen ja työkalujen käyttöönottoon ja taustatukeen käytäntöjen levittämisessä laajemmin organisaatioon.

Projektin erityisenä tavoite- ja tehtäväalueena tietoturvallisuuden johtamis- ja hallintajärjestelmän kehittämisen ohella oli tämän työn kannalta osastojen ja yksiköiden tietoturvatilanteen kehittäminen ja vakiinnuttaminen, turvattavien kohteiden hallinta sekä asiakokonaisuuteen liittyvän tiedon hallinta. Spesifiointi- ja implementointivaiheen kuvauksissa keskitytään näistä kenttätyöhön ja tiedonhallintaan, mutta taustatekijöitä tuodaan myös esille, koska kehittämistoimenpiteet tuli liitää osaksi samassa projektissa kehitettävää laajempaa järjestelmää.

Kohdeorganisaatiossa kehitettävää konstruktiota voitiin pitää uutena innovaationa, sillä aiempia, korvattavia yhtenäisiä toimintamalleja ei ollut. Myöskään valmista muista organisaatioista kopioitavaa mallia ei ollut tiedossa. Koska tarkoituksena oli parantaa ja yhdenmukaistaa turvattavien kohteiden hallintaa sekä kehittää malli ja työkalu, todettiin suunnittelutieteellinen konstruktiivinen tutkimusmetodi tarkoitukseen sopivimmaksi.

3.3 Spesifiointiprosessi

Spesifiointivaihe käynnistyi esitutkimuksella, johon sisältyi tarpeiden alustava määrittely, kirjallisuusselvitys sekä ulkoisen työkalu- ja tuotetarjonnan selvittäminen. Kirjallisuusselvityksessä pyrittiin tunnistamaan aihepiirin keskeiset kansalliset ja kansainväliset vaatimuslähteet kuten säädökset, määräykset, standardit, suositukset, ohjeet sekä harkitusti niitä täydentävää muuta kirjallisuutta. Lisäksi tarkasteltiin tietoturvallisuuskontekstin ulkopuolisia, mutta

lähestymistavaltaan tai aihepiiriltään lähellä olevia muita aineistoja. Kirjallisuusselvityksen tarkoituksena oli selvittää käsitteet ja aiheesta jo valmiiksi tuotetut toimintamallit tai niiden osat. Selvityksen laajuus ja keskeiset tulokset on esitelty tämän tutkimuksen luvussa 2.

Edes jossain määrin tarpeita vastaavia tietojärjestelmiä löydettiin vain yksi. Se osoittautui kuitenkin niin kalliiksi, ettei sen hankintaan nähty aihetta – ainakaan ennen tarkempaa tarpeiden ja vaatimusten selvittämistä ja organisaation sopivien menettelytapojen määrittelyä ja kuvaamista. Muut vaihtoehdot edellyttivät joko voimakasta räätälöintiä tai täysin oman tietojärjestelmän rakentamista. Näin ollen kehittelyvaiheen työkaluksi päätettiin rakentaa yksinkertainen ja edullinen Excel-pohjainen kirjaustyökalu, jolla turvattavien kohteiden hallintaan saamista voitaisiin puutteistaan huolimatta kokeilla ja tukea, ja josta saatavia kokemuksia voitaisiin myöhemmin hyödyntää tarpeiden täsmentämiseksi ja varsinaisen tietojärjestelmän kehittämiseksi tai hankkimiseksi.

Spesifiointivaihe jatkui organisaation toimintaan tutustumisella mm. organisaatiota itseään koskevan lainsäädännön, velvoittavien määräysten, toimintastrategian, työjärjestysten sekä toiminnan ja talouden johtamis-, suunnittelu-, toimeenpano- ja seurantamenettelykuvausten kautta. Tarkoituksena oli saada riittävä ymmärrys organisaatiosta, johon uudet konstruoitavat menettelytavat ja työkalut tuli sovittaa.

Selvitystyö palveli myös rinnakkain tehtyä tietoturvastrategiatyötä, johon sisältyi nykytilanteen ja toimintaympäristön kartoitus, tavoitetilanteen määrittely, tarvittavien kehittämistoimenpiteiden suunnittelu tavoitetilanteeseen pääsemiseksi sekä edistymisen ohjaamista ja seurantaa helpottavien mittareiden määrittely. Osastojen ja yksiköiden osalta tavoitteet painottuivat turvattavien kohteiden ja riskien hallintaan sekä henkilöstön tietoturvatietoisuuteen ja -osaamiseen. Osana tietoturvallisuuden johtamis- ja hallintajärjestelmän rakentamista uusittiin myös organisaation tietoturvapolitiikka.

3.4 Spesifioitu tavoitetila

Spesifiointiprosessin lopputuloksena valmistui tavoitetilanteen kuvaus. Osastojen ja yksiköiden turvattavien kohteiden, tietoturvallisuuden ja riskien hallinta todettiin tehtäväksi, joka järjestelmällisesti läpikäytynä on tietointensiivistä työtä. Koska projektin yhtenä tehtäväalueena oli jo alun pitäen tietoturvatiedon hallinta, valittiin kenttätyön lähtökohdaksi tarve määrämuotoiselle toimintamallille ja työkalulle.

Tavoitetilan kuvaus konkretisoitui turvattavien kohteiden hallintamenettelyn vaatimusmäärittelyyn. Määrittelyssä kuvattiin selvitetyt liiketoimintavaatimukset, toiminnalliset vaatimukset, arkkitehtuurivaatimukset, käytettävyysvaatimukset ja laatuvaatimukset (taulukko 6).

Tunnus	Yksilöllinen tunnus jokaiselle vaatimukselle
Kuvaus	Mahdollisimman yksiselitteinen, täsmällinen ja mitattava, mutta samalla myös tiivis ja selkeä kuvaus vaatimuksesta • Liiketoimintavaatimukset: ylimmän tason vaatimukset • Toiminnalliset vaatimukset: tuotokselta vaadittavat perusominaisuudet, mitä sillä pitää pystyä tekemään • Arkkitehtuurivaatimukset: tietoturva-arkkitehtuuriin (tietoturvallisuuden johtamis- ja hallintajärjestelmään) liittyvät vaatimukset ja rajoitukset • Käytettävyysvaatimukset: tuotoksen käyttämiseen ja hyödyntämiseen liittyvät vaatimukset • Laatuvaatimukset: tuotoksen käyttäjien ja kehittäjien kannalta tärkeät ominaisuudet (esim. saatavuus, tehokkuus, joustavuus, skaalautuvuus, yhteensopivuus, luotettavuus, vertailtavuus, testattavuus, ylläpidettävyys)
Lähde	Keneltä tai mistä vaatimus on peräisin (merkintä helpottaa mahdollisten kilpailevien vaatimusten priorisointia)
Prioriteetti	1 = välttämätön, 2 = tarpeellinen, 3 = toivottava, 4 = poistettu

Taulukko 6: Kehittämistehtävässä käytetty vaatimusmäärittelymalli

Tässä esitettävät vaatimusmäärittelyt (taulukko 7) edustavat niiden ensimmäistä versiota. Alustavia vaatimusmäärittelyjä työstettiin eteenpäin erityisesti hallinnollisen ja teknisen projektipäällikön keskinäisessä vuoropuhelussa. Vaatimusmäärittelyjä kehitettiin projektin edetessä, pilotoitaessa ja ohjaus- ja käyttäjäkokemusten karttuessa. Spesifiointi- ja implementointiprosessit olivat tältä osin rinnakkaisia.

Tunnus	Kuvaus	Lähde	Prior.
	Liiketoimintavaatimukset		
BR001	Organisaation tulee tunnistaa tietoturvallisuuden hallintajärjestelmään kuuluvat turvattavat kohteet ja niiden omistajat	ISO 27001 BSI	1
BR002	Kohteen vaikuttavuus on arvioitava (esim. kohteen käytön laajuus, henkilömäärä, eri organisaatio-osat, kriittisyys toiminnoille,…)		2
BR003	Toimintamallin sovittaminen organisaation toimintajärjestelmään (mm. tulosohjaus, talouden ja toiminnan suunnittelu, vuosikello)		1
	Toiminnalliset vaatimukset		
FR001	Turvaamista tarvitsevat kohteet tunnistetaan, saadaan hallintaan ja saadaan pidettyä hallinnassa		1
FR002	Kaikki turvattavat kohteet tulee yksilöidä selkeästi, kaikki merkittävät kohteet tulee luetteloida ja luetteloiden ylläpidosta huolehtia	ISO 27002	1

Tunnus	Kuvaus	Lähde	Prior.
FR003	Informaatioresurssit (=suojattavat kohteet) sopivalla tasolla eriteltyinä, esim. • Tietokokonaisuus A • Sovellus B • Verkko C • Tietokoneinstallaatio D • Henkilöt, tilat • Kriittiset toiminnot, prosessit		2
FR004	Turvattavista kohteista kirjataan ominaisuudet: • Tunnistetiedot • Omistaja • Sisältö • Elinkaaren pituus ja vaihe • Liittyminen (ja riippuvuus) muuhun ympäristöön • Arvo (rahallinen tai muu) • Sensitiivisyys (luottamuksellisuus), luokittelu • Kriittisyys (saatavuus, eheys), luokittelu • Nykykontrollit	GAISP	1
FR005	Tiedon ja tietojenkäsittelypalveluihin liittyvien turvattavien kohteiden hyväksyttävän käytön säännöt tulee yksilöidä, dokumentoida ja toteuttaa	ISO 27002	3
FR006	Pilkkominen tarkemmin turvattaviin alakohteisiin: data, sovellukset, tekniikka, tilat, henkilöt, palvelut/prosessit • Suojattavat (ala)kohteet • Vastuuhenkilöt/"omistajat" ja muut roolit • Tavoitteet, tietoturva(kontrolli)tavoitteet • Prosessikuva, tehtäväketju • Kohteen dokumentaatio (ohjaava ja kuvaava) • Käytössä olevat tietoturvamekanismit/-kontrollit • Mittarit	COBIT	1
	Arkkitehtuurivaatimukset		
AR001	Suojattavien kohteiden tunnistaminen on riskien arvioinnin lähtökohta.	ISO 27001	1
AR002	Menettelyjen ja työkalujen soveltuminen osaksi tietoturvallisuuden johtamis- ja hallintajärjestelmää		1
	Käytettävyysvaatimukset		
UR001	Suojattavista kohteista tietoineen muodostetaan ja ylläpidetään ”konfiguraatiotietokanta”, vrt. CMDB		2
UR002	Menettelyjen ja työkalujen selkeys, ymmärrettävyys ja helppokäyttöisyys ”kentällä”, ei saa viedä kohtuuttomasti aikaa		1
UR003	Kerättäviä tietoja voidaan yhdistellä, linkittää ja yhteiskäyttää		3
	Laatuvaatimukset		
QR001	Luotettavuus ja vertailtavuus eri yksiköiden, prosessien ja toimintojen osalta - yhteismitalliset menettelyt		2

Taulukko 7: Alustavat turvattavien kohteiden hallinnan vaatimusmäärittelyt

Tietoturvastrategiassa asetetuista yleistavoitteista tässä työssä huomioon otettavia tavoitteita olivat 1) varsinaisen toiminnan tavoitteiden saavuttamisen tukeminen, 2) uusien tehokkaampien toimintatapojen mahdollistaminen, 3) tietoturvallisuudesta huolehtiminen osana normaalia toiminnan kehittämistä, riskienhallintaa ja tulosohjausta, 4) tietoturvatason säädösten ja määräysten mukaisuus, 5) toimialan erityisvaatimusten täyttäminen, 6) resurssien suuntaaminen keskeisiin kohteisiin, 7) menettelyjen hyvien käytäntöjen mukaisuus sekä 8) menettelyjen tuleminen dokumentoiduksi.

Projektisuunnitelmaa täydennettiin tehtäväaluekohtaisilla työsuunnitelmilla. Siten myös kenttätyön ja tiedonhallinnan osalta laadittiin erilliset, mutta yhteen sovitetut työsuunnitelmat. Työsuunnitelmiin kirjattiin työn kuvaus, tavoitteet, henkilöresursointi, vaiheistus, tehtävät vastuuhenkilöineen, aikataulut, edistymisraportointi, suunnitelman toteuttamisen riskien arviointi ja hallinta sekä viestintä.

Kohdeyksiköiden ja -toimintojen riskienhallinnan osalta tehtiin linjaus, että tietoturvallisuuden osalta ei valmistella omaa toimintamallia, joten tämä osio määriteltiin ns. valmisosaksi. Tarkoitus oli myöhemmin sovittautua organisaation erikseen kehitettävään kokonaisvaltaiseen riskienhallintamalliin. Kohdekohtaisissa työpajoissa riskien arviointi sovittiin toteutettavaksi kunkin työpajan vetäjän sopivaksi katsomalla tavalla, mutta arvioinnista kirjattavien tulosten tuli olla määrämuotoisia. Projekti- ja työsuunnitelmissa varattiin tilaa menettelyjen ja työkalujen pilotoinnille ja jatkokehittämiselle ennen lopullista ratkaisua ja sen toimeenpanoa.

Käsitteistön osalta tavoitteeksi asetettiin sekä käytettävän termistön ja käsitteistön kuvaaminen (ns. deskriptiivinen sanastotyö) että termistön käytön selkeyttäminen ja yhdenmukaistaminen (ns. normatiivinen sanastotyö).

3.5 Implementointiprosessi

Projekti toteutettiin siten, että tekninen projektipäällikkö toimi ensisijaisen mallin ja työkalurungon rakentajana vaatimusmäärittelyjen ja kirjallisuusselvityksen pohjalta. Työkalu toteutettiin Excel-taulukkolaskentasovelluksella sijoittamalla kukin osakokonaisuus omalle välilehdelleen. Välilehtirakenteeseen päädyttiin siksi, että työpajoissa osakokonaisuudet olisi helpompi pitää toisistaan erillään ja pohdinnoissa olisi helpompi keskittyä juuri haluttuun dataprojektorin näytöllä kulloinkin näkyvään asiaan. Tehtyä kehitysvälinevalintaa tuki se, että riittävän käyttökelpoinen työkalu saataisiin rakennettua nopeasti ja edullisesti kokemusten kartuttamiseksi. Välineen käyttö olisi myös entuudestaan riittävän tuttua niin kehittäjille kuin tuleville käyttäjillekin. Tämän jälkeen projektipäälliköt yhdessä toisiaan haastaen koeponnistivat mallia ja työkalua ja tekivät siihen ensivaiheen parannukset.

Seuraavaksi malli ja työkalu siirtyivät projektiryhmän arvioitavaksi. Muutosten jälkeen projektipäälliköt toteuttivat valmistelluilla välineillä kolme pilottityöpajaa eri yksiköissä. Näissä työpajoissa mallin ja työkalun kehittäjät vetivät itse turvattavien kohteiden työpajat, joten vaihetta voidaan kutsua myös α-testaukseksi. Saatujen kokemusten jälkeen tehtiin vielä pienimuotoisia täsmennyksiä. Ohjausryhmä pidettiin tietoisena mallista ja työkalusta kehitysvaiheineen varmistaen, että lupa jatkokehitykselle ja koekäytölle on olemassa. Ohjausryhmä toi erityisesti esille huolen siitä, etteivät menettelyt saa olla liian raskaita tullakseen hyväksytyksi varsinaisessa toiminnassa.

Seuraavassa vaiheessa välineistö käytiin uudelleen läpi projektiryhmässä ja projektiryhmäläiset aloittivat varsinaisen kenttätyön osastoilla ja yksiköissä tietoisena, että malli ja työkalu eivät välttämättä ole vielä stabiileja. Välineistö siirtyi siten eri käyttäjien kautta ß-testausvaiheeseen. Kun 12 kohdetta oli käyty läpi, käsiteltiin saadut kokemukset jälleen yhdessä. Kokemusten ja ideoiden läpikäynnistä kehittyi projektiryhmän kokouksissa myös säännöllisesti toistuva aihe. Ohjausryhmässä päätettiin tässä vaiheessa, että riskianalyysi sijoitetaan sopivassa muodossa samaan menettelyyn ja työkaluun.

Käsitteistöä tarkasteltiin kriittisesti hyödyntäen Sanastokeskuksen (2010) ohjeistuksia sanastotyöstä. Käsiteanalyysissä selvitettiin sekä käsitteiden sisältö että eri käsitteiden väliset suhteet. Tarkastelun tuloksena jouduttiin muokkaamaan myös arvovaltaisten lähteiden esittämiä määritelmiä, mutta varottiin ohjeistuksen mukaisesti muuttamasta käsitteen alaa.

3.6 Saavutettu lopputila

Menettelytapakuvaus laadittiin siten, että se täyttää prosessikuvauksen perusvaatimukset ja se ottaa kantaa kaikkiin COBIT-mallin esittämiin prosessikontrolleihin. Turvattavien kohteiden hallinnan käsitteistö määriteltiin ja toimintamalli kiinnitettiin sekä tietoturvallisuuden että organisaation johtamisen järjestelmiin myös kuvauksen muodossa. Kehitetyssä mallissa toteutuvat kaikki alustavan vaatimusmäärittelyn ensimmäisen ja toisen prioriteetin vaatimukset. Käsitteet ja kuvaukset hyväksyttiin projektin ohjausryhmässä. Kun mallia ja työkalua verrattiin esitutkimuksessa ja spesifiointivaiheessa tehtyihin selvityksiin ja projektihenkilöstön kokemuksiin ja tietoihin muista organisaatioista, voitiin todeta, että askeleet tietoturvatoiminnan jalkauttamiseksi ovat olleet merkittäviä.

Osastoihin ja yksiköihin kohdistuvasta ohjatusta tietoturvatoiminnasta käytettiin projektissa nimitystä kohdespesifinen tietoturvatyö. Ensivaiheessa kyse oli kunkin kohteen vastuuhenkilöiden ja henkilöstön tietoturvakoulutuksesta sekä arvokkaiden, turvattavien kohteiden tunnistamisesta ja hallintaan ottamisesta. Tähän hallintaan sisällytettiin mm. vastuuhenkilöiden

nimeäminen, kohteeseen liittyvien vaatimusten ja tarpeiden tunnistaminen, tarvittavien resurssien ja riippuvuuksien tunnistaminen, vaikuttavuuden arviointi, uhkien, riskien ja suojauskeinojen tunnistaminen sekä tarvittavien tietoturvatoimenpiteiden määrittely.

Välineistö paketoitiin ja hyväksyttiin viralliseksi versioksi 1.0. Välineistöllä käytiin läpi yli 40 yksikköä tai toimintoa (toimeenpano jatkuu), joilta myös kerättiin systemaattisesti palautetta. Palautteen johdosta ja työpajojen vetämisestä kertyneen lisäkokemuksen kautta itse malli ja väline on toistaiseksi pidetty ennallaan, mutta käytännön työpajatoimintaa on ajallisesti tiivistetty lähes puoleen alkuperäisestä. Joidenkin yksiköiden kohdalla on ehditty pitää jo asiaan liittyvä vuosikatselmointi ja tarkoituksena on, että vähitellen mallin ja työkalun käyttö jää täysin yksiköiden itsenäiseksi toiminnaksi. Tämän onnistumiseksi tarjolle on asetettu keskitetyt tukipalvelut sekä seuranta ja yksiköitä koskevat raportointivelvoitteet normaalin tulosvastuun raportointimenettelyjen mukana. Vastaavasti organisaation johto osoitti tukensa menettelylle mm. mahdollistamalla sen, että toistaiseksi yksiköiden tulosohjauksen tavoitteisiin voidaan tuoda tietoturvatavoitteita (jotka ovat täytettävissä uutta toimintamallia ja työkalua käyttämällä).

Varsinaiset tiedonhallinnan ongelmat ja vaatimusmäärittelyjen kolmannen prioriteetin vaatimukset on tarkoitus ratkaista myöhemmin joko valmisohjelmistolla tai rakentamalla uusi tietojärjestelmä ottaen samalla huomioon työkalun mahdolliset muut laajemmat käyttötarpeet. Nämä tarpeet liittyvät lähinnä kerätyn tiedon kokoamiseen yhteen ja sitä kautta hallittuun yhteiskäyttöön sekä laajentamiseen koko turvallisuustoimintaan. Haasteeksi nousevat erityisesti pääsyn hallinta ja sensitiivisen tiedon suojaaminen. Järjestelmä itsessään muodostuisi merkittäväksi turvattavaksi kohteeksi.

Konstruktion raportointi on jaettu useaan osaan tätä tutkimustyötä:

1) Johdanto, ks. luvut 1, 3.1 ja 3.2
2) Keskeisen idean tai konseptin esittely ja vertailu muihin vaihtoehtoihin, ks. luvut 3.2, 3.3, 3.4, 4 ja 5
3) Rajoitukset, ks. luvut 1.3, 3.2, 3.3 ja 5
4) Merkittävin suunnitteluongelma, sen parhaat ratkaisuvaihtoehdot ja vaihtoehdon valinta perusteluineen, ks. luvut 1.1, 2, ja 3
5) Muut alemman tason suunnitteluongelmat, ks. luvut 1.1, 2 ja 3
6) Toteutuksen (lopputilanteen) kuvaus tai konstruoinnin yksityiskohtainen suunnitelma, ks. luvut 3.4, 3.6 ja 4
7) Uuden innovaation alustava arviointi, ks. luvut 3.6 ja 5
8) Pohdinta tulosten merkityksestä, rajoituksista, suosituksista ja jatkotutkimuskohteista, ks. luku 5

4 Tutkimustulokset

Valitussa tutkimustehtävässä lähtökohtana oli tietoturvallisuuden hallinnan kannalta tarkasteltuna se, ettei turvattavista kohteista ja niiden hallinnasta käsitteellisesti ollut löydettävissä vakiintunutta määritelmää ja toimintamallia. Tietoturvattavien kohteiden hallinnasta ei myöskään ollut löydettävissä käytännöllistä kuvausta eikä hallintaan soveltuvaa työkalua. Tutkimuksen edetessä tämä käsitys vahvistui entisestään pysyttäessä tietoturva-alan omassa lähdeaineistossa. Turvallisuusalan ulkopuolinen tarkastelu avasi uusia tarkastelukulmia, joita hyödynnettiin myös ratkaisun kokoamisessa. Näiden johdosta myös alan peruskäsitteet otettiin kriittiseen tarkasteluun.

Tutkimuksen pääkysymyksenä oli: Miten tietoturvallisuuden kannalta keskeisiä kohteita hallitaan? Pääkysymyksen ratkaisemiseksi tarvittavia apukysymyksiä tutkimuksessa olivat: Mitä tietoturvattavat kohteet ovat? Mitä tietoturvattavien kohteiden hallinta on? Työn tarkoituksena oli tuottaa malli, jota käyttämällä voidaan parantaa ja yhdenmukaistaa tietoturvattavien kohteiden hallintakäytäntöjä osana normaalin toiminnan ja samalla tietoturvallisuuden johtamista ja hallintaa.

Tässä luvussa esitetään tulokset, joihin todellisessa kehittämistyössä päädyttiin. Keskeiset esitettävät tulokset ovat uusi tietoturvattavien kohteiden hallinnan viitekehys ja käsitteistö, kohteiden hallinnan kytkentä normaaliin johtamis- ja toimintajärjestelmään sekä tietoturvallisuuden johtamis- ja hallintajärjestelmään, tietoturvattavien kohteiden hallinnan menettelytapakuvaus sekä tietoturvattavien kohteiden hallintaan käytettävän työkalun kuvaus. Viitekehyksen jälkeinen teksti on myös kohdevirastolle laadittu tulos.

4.1 Uusi viitekehys

Tutkimustyön tuloksena kehitetyssä uudistetussa viitekehyksessä on kyse eri teorioiden yhdistämisestä ja yhteensovittamisesta siten, että käytäntöön vietävä lopputulos palvelee samalla organisaation ydintoimintaa, prosessin johtamista, riskien hallintaa, omaisuuden hallintaa sekä tietoturvallisuutta. Tämän seurauksena päädyttiin täsmentämään ja täydentämään lähtötilanteen viitekehyksessä (luku 2) esitettyjä käsitteitä. Myös eräät tietoturvallisuuden peruskäsitteet on määritelty uudelleen, vaikka siihen sisältyy omat vaaransa. Uudet esitettävät määritelmät eivät kuitenkaan radikaalisti poikkea niiden tavanomaisesta tietoturva-alan tulkinnasta, eivätkä ne vaikuta käsitteiden puhekieliseen käyttöön. Kriittisen tarkastelun kautta on sen sijaan pyritty lähestymään valittujen käsitteiden syvällisempää ja täsmällisempää olemusta perustellen tehdyt valinnat.

Tietoturvallisuus-käsitteen perusmääritelmät lähtevät lähes poikkeuksetta luottamuksellisuuden, eheyden ja käytettävyyden tavoitteista viitaten niihin liittyvään tekemiseen (ISO/IEC 27001) ja järjestelyihin (VAHTI 8/2008). Näkökulma on verkottuneessa toimintaympäristössä tarpeettoman suppea ja kaipaa täydennyksenä viitteen osapuolten tunnistamiseen ja tapahtumien kiistattomuuteen. Lisäksi, mikäli tietoturvallisuus määritellään tekemisen ja järjestelyjen kautta, ei tällaista määritelmää voida käyttää itse käsitteen tilalla järkevästi.

Esimerkiksi lauseen ”tavoitteena on hyväksyttävä tietoturvallisuus” tilalle ei voida kirjoittaa samaa tarkoittaen tai järkevästi, että ”tavoitteena on hyväksyttävä tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttäminen”, tai että ”tavoitteena ovat hyväksyttävät järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus”. Varsinaisena tavoitteena ei voi olla tekeminen, eikä ainakaan pelkkä säilyttäminen, tai mikään järjestely. Pikemminkin kyse on olotilasta.

Olotilaan pohjautuva määritelmä on toimiva myös yhdyssanoissa, kuten tietoturvallisuus-, tai lyhyemmin, tietoturvapoikkeama ja tietoturva-auditointi. Sama koskee myös roolia tietoturvapäällikkö, joskin hieman virheellisesti käännettynä englanninkielisestä ilmaisusta *information security manager*, joka varsinaisesti tarkoittaa päällikkyyden sijaan tietoturvallisuuden ”manageroijaa” eli hallintatehtäviä suorittavaa henkilöä. Useilla suomalaisilla tietoturvapäälliköillä ei olekaan alaisia, vaan kyse on roolinimikkeestä. Englanninkielellä on ryhdytty käyttämään myös roolia *chief information security manager*, johon jo selvästi liittyy asiaan liittyvää päällikkyyttä tai jopa johtajuutta. Tietoturvallisuus-käsitettä on yhdyssanoissa luontevaa käyttää myös lyhyemmässä tietoturva-muodossa. Käytettävä määritys on:

> **Tietoturvallisuudella** tarkoitetaan tiedon luottamuksellisuuden, eheyden, käytettävyyden, todennettavuuden ja kiistämättömyyden tilaa.

Tietoturvallisuuden hallinnan käsitettä ei yleisesti ole määritelty. Käsitteen tilalla on usein esitetty tietoturvallisuuden hallintajärjestelmä, mutta se viittaa tiettyyn järjestelmään, systeemiin, kun taas ”pelkkä” hallinta on tekemistä ja luonteeltaan jossain määrin vapaamuotoisempaa. Tarpeet ja hyväksyttävyyden rajat voivat vaihdella toimintaympäristöstä riippuen suuresti. Käsitteellistä eroa, mutta myös sidonnaisuutta, kuvastaa se, että tietoturvallisuuden hallintaa voi kehittyneemmässä toimintaympäristössä toteuttaa esimerkiksi tietoturvallisuuden hallintajärjestelmää käyttämällä.

ISO/IEC 27001 -standardin määritelmä tietoturvallisuuden hallintajärjestelmästä on melko kattava, muttei ongelmaton. Määritelmään sisältyvä liiketoiminta-termin käyttö aiheuttaa usein hämmennystä julkishallintoyhteydessä. Lisäksi järjestelmän rakentaminen pelkästään riskien arvioinnin varaan on ilmeisen suppea lähestymistapa ja tarvitsee lisäkseen toiminnasta

lähtevät tarpeet ja toimintaan liittyvät vaatimukset. Pelkkään riskien arviointiin perustuvan asianmukaisen hallintajärjestelmän rakentaminen olisi myös äärettömän raskas tehtävä.

Järjestelmään liitettynä tavoitteena hyvä tietoturvallisuus on suunnaltaan varsin oikea, mutta käytetty laatumääre on toisaalta myös ongelmallinen. Jollakin tarve voi olla myös erinomaiseen tai vaikkapa korkean tason tietoturvallisuuteen. Jollekin toiselle voi taas riittää toimialan keskiarvo tai perustaso.

Käsitteen kautta voidaan myös pohtia, onko tietoturvallisuus hallinnassa. Tällöin on tarkoituksenmukaista kytkeä käsitteeseen jonkinlainen odotusarvo tai tasovaatimus. Hyväksyttävä taso on sopivampi ilmaus, sillä se pitää määritelmän käyttökelpoisena eri tilanteissa. Lisäksi hyväksyttävä taso on määriteltävissä erikseen. Esimerkiksi standardinmukaisessa hallintajärjestelmässä organisaation johdon tehtävänä on asettaa hyväksyttävä taso. Käytettävät määritykset ovat:

> **Tietoturvallisuuden hallinnalla** tarkoitetaan toimenpiteitä ja käytäntöjä tietoturvallisuudesta huolehtimiseksi tavoitteena hyväksyttävä tietoturvallisuus.
>
> **Tietoturvallisuuden hallintajärjestelmällä** tarkoitetaan sitä osaa yleisestä toimintajärjestelmästä, joka odotuksiin, tarpeisiin, vaatimuksiin ja riskien arviointiin perustuen luodaan ja toteutetaan, ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyväksyttävä tietoturvallisuus.

Turvattavien ja suojattavien kohteiden määritelmissä viitataan yleisesti, mm. ISO/IEC 27001 ja VAHTI 8/2008, mihin tahansa, mikä on arvokas organisaatiolle ja jatkamalla sitten määritelmiä esimerkeillä ao. kohteista. Esimerkkien käyttötarve itse määritelmässä viittaa siihen, ettei käsitettä ole onnistuttu määrittelemään riittävän täsmällisesti. Täsmällisempää on tunnistaa vaihtoehtojen pääryhmät ja mainita ne, jolloin kaikki esimerkit määritelmässä käyvät tarpeettomiksi.

Turvattavilla ja suojattavilla kohteilla tarkoitetaan määritelmissä samaa asiaa. Vivahde-erona on kuitenkin se, että suojaamisen voi mieltää kohteen ympärille rakennettavana ”kuorena” ulkopuolisten uhkien varalta (vrt. sadesuoja, murtosuoja), kun taas turvaamista voidaan pitää kokonaisvaltaisempana ulkoisten, sisäisten ja kohteeseen itseensä sisältyvien uhkien huomioon ottavana toimintana. Mikäli käsitettä käytetään erityisesti tietoturvakontekstissa, eikä tietoturvayhteys selvästi käy asiayhteydestä esille, on sen syytä näkyä sekä käsitteessä että sen määritelmässä. Mikäli asiayhteys on selvä, voidaan käyttää lyhyempää muotoa. Uudet määritykset ovat:

Turvattavalla kohteella tarkoitetaan asiaa, toimintaa, omaisuutta tai ihmistä, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi turvallisuusnäkökulmasta.

Tietoturvattavalla kohteella tarkoitetaan asiaa, toimintaa, omaisuutta tai ihmistä, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi tietoturvallisuusnäkökulmasta.

Turvattavien ja tietoturvattavien kohteiden hallinnan käsitettä ei yleisesti ole määritelty. Englanninkielisissä tietoturva-aiheisissa lähteissä, kuten ISO/IEC 27000 -sarja, käytetään tosin *asset management* -termiä, sitä kuitenkaan määrittelemättä. Sisällöllisesti asiayhteydessä käsitellään yleensä tunnistamista, omistajuutta ja luokittelua. Ne eivät kuitenkaan vielä merkitse kohteen hallintaa, vaan pikemminkin luovat hallinnan elinkaarella tarvittavia ensi askeleita, joita tarvitaan kohteen saamiseksi ja pitämiseksi hallinnassa. Uudet määritykset ovat:

Turvattavan kohteen hallinnalla tarkoitetaan toimenpiteitä ja käytäntöjä turvattavan kohteen turvallisuudesta huolehtimiseksi kohteen koko elinkaarella tavoitteena kohteen hyväksyttävä turvallisuus.

Tietoturvattavan kohteen hallinnalla tarkoitetaan toimenpiteitä ja käytäntöjä tietoturvattavan kohteen tietoturvallisuudesta huolehtimiseksi kohteen koko elinkaarella tavoitteena kohteen hyväksyttävä tietoturvallisuus.

Määriteltyjen käsiteiden eheyttä ja keskinäistä yhteensopivuutta voidaan tarkastella lauseilla, jotka sisältävät useampia mainituista käsitteistä. Esimerkkeinä käytetään lauseita: ”Tietoturvattavan kohteen vastuuhenkilö vastaa tietoturvattavan kohteen tietoturvallisuuden hallinnasta” (taulukko 8) ja ”Tietoturvapäällikkö järjestää tietoturvallisuuden hallintajärjestelmän mukaisen turvattavan kohteen tietoturva-auditoinnin” (taulukko 9).

Ydinlause	Käsitemääritelmiä käyttämällä avattu lause
Tietoturvattavan kohteen	Asian, toiminnan, omaisuuden tai ihmisen, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi tietoturvallisuusnäkökulmasta,
vastuuhenkilö vastaa	vastuuhenkilö vastaa
tietoturvattavan kohteen	asian, toiminnan, omaisuuden tai ihmisen, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi tietoturvallisuusnäkökulmasta,
tietoturvallisuuden	tiedon luottamuksellisuuden, eheyden, käytettävyyden, todennettavuuden ja kiistämättömyyden tilan
hallinnasta.	toimenpiteistä ja käytännöistä tietoturvallisuudesta huolehtimiseksi tavoitteena hyväksyttävä tietoturvallisuus.

Taulukko 8: Käsitetesti 1

Ydinlause	Käsitemääritelmiä käyttämällä avattu lause
Tietoturvapäällikkö	Tiedon luottamuksellisuuden, eheyden, käytettävyyden, todennettavuuden ja kiistämättömyyden tilan hallintatehtäviä suorittava henkilö
järjestää	järjestää
tietoturvallisuuden hallintajärjestelmän	sen yleisen toimintajärjestelmän osan, joka odotuksiin, tarpeisiin, vaatimuksiin ja riskien arviointiin perustuen luodaan ja toteutetaan, ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyväksyttävä tietoturvallisuus
mukaisen	mukaisen
turvattavan kohteen	asian, toiminnan, omaisuuden tai ihmisen, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi turvallisuusnäkökulmasta
tietoturva-auditoinnin.	tiedon luottamuksellisuuden, eheyden, käytettävyyden, todennettavuuden ja kiistämättömyyden tilaa koskevan auditoinnin.

Taulukko 9: Käsitetesti 2

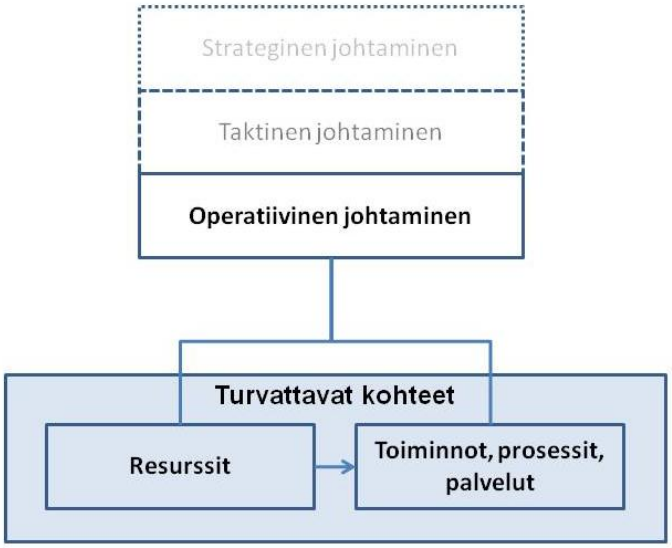
Käsitetestien tuloksena voidaan todeta, että esitettyjen määritelmien logiikka kestää niiden sijoittelun lauseisiin (vaikka lauserakenteista luonnollisesti tulee kömpelöitä).

4.2 Kytkentä johtamis- ja toimintajärjestelmään sekä tietoturvallisuuden johtamis- ja hallintajärjestelmään

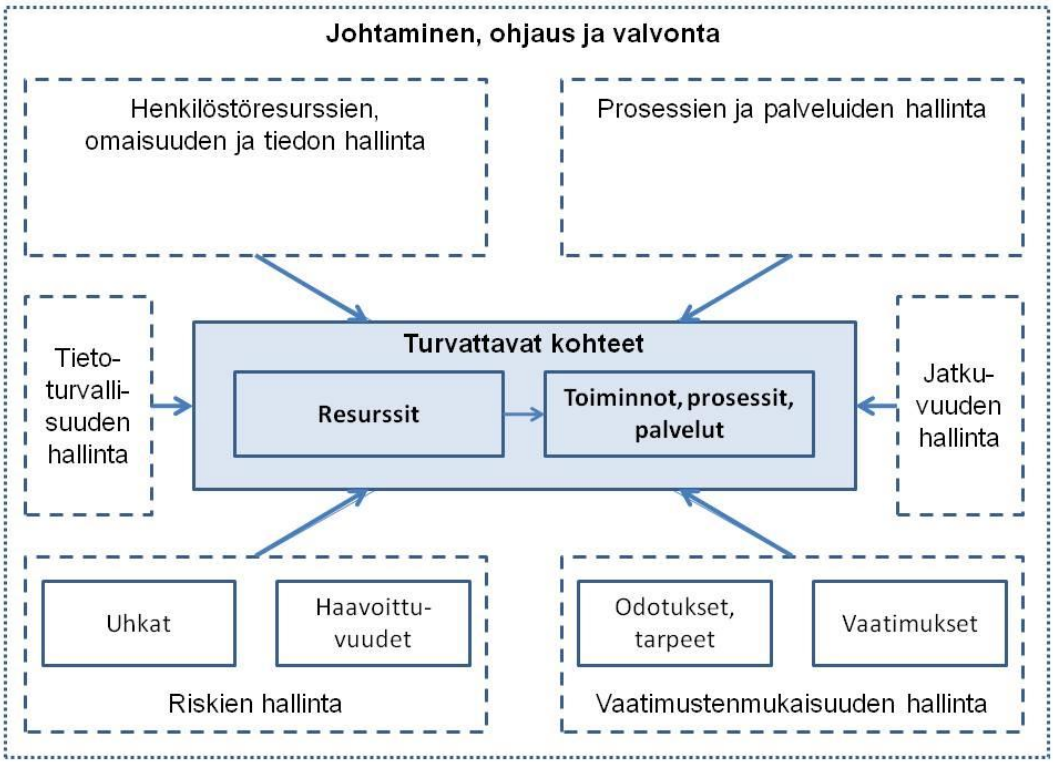
Tietoturvattavat kohteet liittyvät väistämättä organisaation normaaliin toimintaan, koska kohteita ovat mm. prosessit, toiminnot, palvelut, ihmiset, tietojärjestelmät ja tietoaineistot. Kun toiminnan ei haluta olevan sattumanvaraista, kaikkia mainittuja kohteita johdetaan ja hallitaan organisaation johtamis- ja toimintajärjestelmän mukaisesti. Konkreettisimmillaan kyse on operatiivisesta tasosta (kuvio 25).

Johtamiseen, ohjaukseen ja valvontaan liittyy monia ulottuvuuksia, joilla on liityntäpinta myös tietoturvattaviin kohteisiin. Tällaisia näkökulmia ja osa-alueita ovat mm. henkilöstöhallinto, taloushallinto ja (käyttö)omaisuuden hallinta, tietohallinto, prosessien hallinta, palveluiden hallinta, vaatimustenmukaisuuden hallinta sekä riskien, turvallisuuden ja jatkuvuuden hallinta (kuvio 26). Kaikilla näillä osa-alueilla on tärkeää tunnistaa, mihin niiden työ kohdistuu ja mitä resursseja työssä tarvitaan. Kun kohteisiin on intressejä useasta suunnasta, on pohdittava myös turvattavan kohteen vastuu- ja tehtävänäkökulmat tarkoituksenmukaisesti. Osasta

huolehditaan yksikössä, toiminnossa, prosessissa tms. itse, mutta osasta huolehtivat organisaation muut yhteisiä palveluja tarjoavat rakenteet omine asiantuntijoineen.



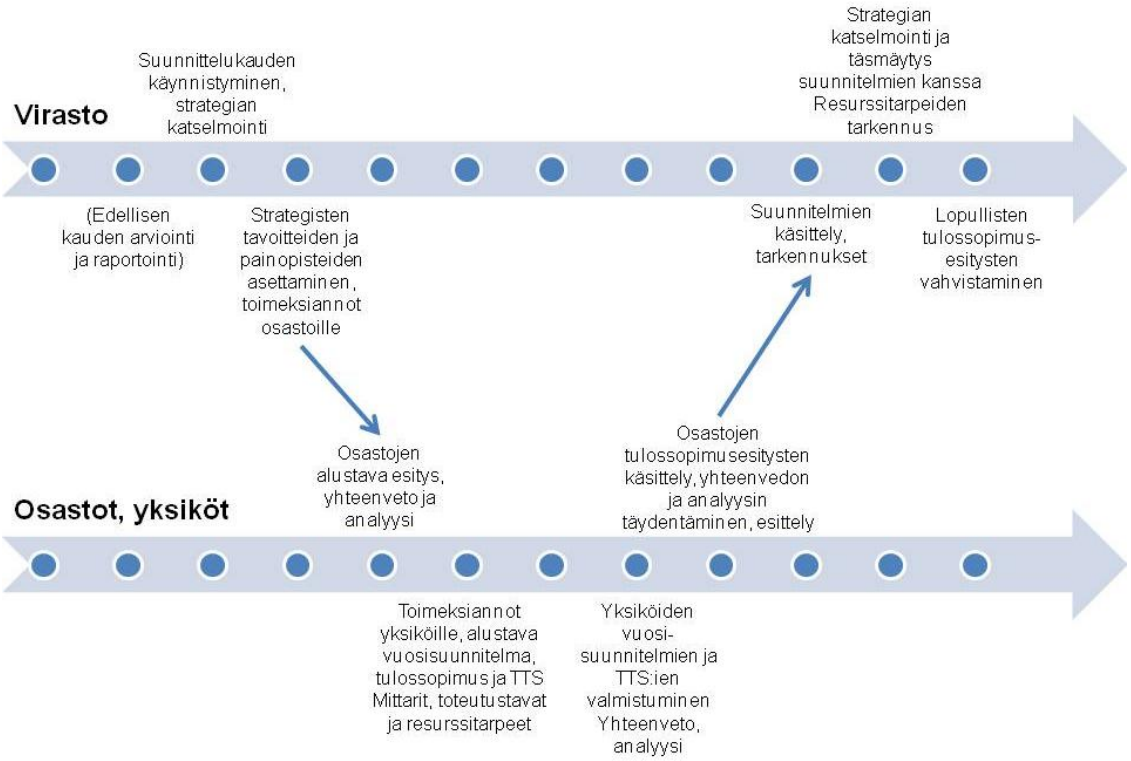
Kuvio 25: Operatiivinen johtaminen ja turvattavat kohteet



Kuvio 26: Turvattavien kohteiden johtamis- ja hallintaulottuvuuksia

Tarkastellun viraston tärkeimmät tietoturvatoiminnalla turvattavat kohteet ovat tiedot ja varsinaiseen toimintaan liittyvät prosessit ja toiminnot sekä näitä tukevat resurssit ja infrastruktuuri. Tietoturvajärjestelyillä huolehditaan viraston omien ja sen hallussa olevien tietojen ja niiden käsittelyn hallinnollisesta, teknisestä ja fyysisestä tietoturvallisuudesta tietojen olomuodosta ja sijainnista riippumatta. Tietoturvatoiminta kattaa koko viraston toiminnan, kaikki osastot ja yksiköt. Tietoturvallisuuden kehittäminen sovitetaan yhteen palveluprosessien, toimintatapojen, henkilöstön koulutuksen ja teknisten ratkaisujen kehittämisen kanssa.

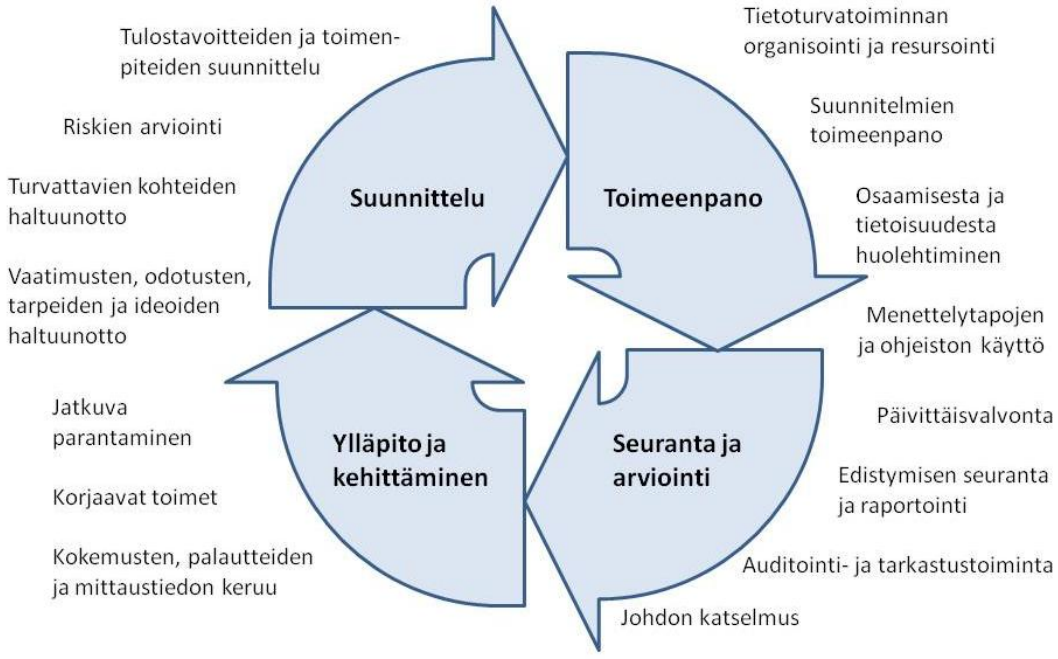
Tietoturvallisuuden johtamisjärjestelmä on malli tietoturvatoiminnan kiinnittymisestä viraston ohjaus- ja johtamisjärjestelmään sekä sisäiseen valvontaan. Tietoturvallisuuden johtamisjärjestelmä on osa viraston johtamisjärjestelmää ja siten yhteensopivaa muun johtamisen kanssa. Toiminnan tietoturvallisuus liittyy myös kaikkiin sisäisen valvonnan tavoitteisiin: 1) toiminnalle ja taloudelle asetetut tavoitteet saavutetaan, 2) toiminnassa ja taloudessa noudatetaan lakia sekä viraston vastuulla oleva omaisuus ja varat ovat turvattu ja 3) toiminnasta ja taloudesta tuotetaan ulkoisia ja sisäisiä tarpeita varten oikeat ja riittävät tiedot. Tietoturvallisuudesta huolehtiminen on osa normaalia toiminnan kehittämistä, riskienhallintaa ja tulosohjausta (kuvio 27).



Kuvio 27: Toiminnan ja talouden suunnittelun (TTS) vuosikello

Työjärjestyksen mukaan viraston sisäinen valvonta toteutetaan ensisijaisesti sisäisen valvonnan tavoitteiden saavuttamisen turvaavilla toimintatavoilla ja työjärjestelyillä sekä toimintaketjuihin ja menettelyihin sisältyvinä johtamis-, ohjaus-, seuranta- ja raportointitoimenpiteillä kaikissa yksiköissä. Osastot ja yksiköt vastaavat toimenpiteistä omalla vastuualueellaan ja omissa tehtävissään. Osastot ja yksiköt vastaavat niille asetettujen tulostavoitteiden saavuttamisesta sekä tavoitteiden saavuttamista vaarantavien seikkojen tunnistamisesta ja hallinnasta omalla tehtäväalueellaan.

Tietoturvallisuuden hallintajärjestelmä on toimintamalli tietoturvallisuuden kehittämiseen, toteuttamiseen, valvontaan, katselmointiin, ylläpitämiseen ja parantamiseen. Tietoturvallisuuden hallintajärjestelmän 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 ja jatkuva parantaminen (kuvio 28). Viraston tietoturvallisuuden hallintajärjestelmässä sovelletaan ISO 27001:2005 -standardia.



Kuvio 28: Tietoturvallisuuden hallintajärjestelmä

Virastossa ylläpidetään johdon määrittelemää tietoturvapolitiikkaa, joka kuvaa suhtautumisen tietoturva-asioihin, tietoturvatoiminnan tavoitteet ja vastuujaon sekä keskeisiä toimintaperiaatteita. Viraston toimintastrategiaa tukeva tietoturvastrategiatyö lähtee toimintaympäristön analysoinnista ja nykytilanteen arvioinnista edeten tavoitetilanteen määrittelyyn ja siihen pääsemiseksi tarvittavien kehittämistoimenpiteiden suunnitteluun. Virastossa tunnistetaan ja vastuutetaan toiminnan ja tietoturvallisuuden kannalta tärkeät turvattavat kohteet. Turvattaviin kohteisiin ja toimintaan yleisestikin liitetään riskien tunnistaminen ja arviointi, joiden perusteella määritellään tavoitteena oleva hyväksyttävä riskitaso ja siihen pääsemiseksi tarvittavat toimenpiteet.

Tietoturvallisuuden hallintajärjestelmän keskeisistä menettelyistä ylläpidetään menettelytapakuvauksia ja tarvittaessa niihin liittyviä työohjeita ja varsinaisia tietoturvaohjeita. Voimassa olevat tietoturva-asiakirjat ja toiminnasta syntyvät tallenteet muodostavat hallitun kokonaisuuden. Tietoturvatoiminta organisoidaan ja resursoidaan siten, että suunniteltuihin ja päätettyihin tietoturvatehtäviin on riittävät ja pätevät resurssit. Valmistellut suunnitelmat toimeenpannaan. Organisaatiossa huolehditaan siitä, että jokaisella on riittävät tiedot ja taidot tietoturvavelvoitteisiinsa vastaamiseen. Annettujen menettelytapojen ja ohjeiden noudattaminen on normaaliin työhön sisällytettävä ominaisuus. Tietoturvallisuuteen liittyvien häiriöiden, ongelmien ja muiden poikkeamien käsittelyyn ja hallinnointiin on valmiiksi määritelty menettelytapa.

Valvonta on oleellinen osa tietoturvatoimintaa ja hallintajärjestelmää. Päivittäisvalvonta sisältää hallinnollista, fyysistä ja teknistä valvontaa, jonka henkilöstöä koskevat periaatteet käsitellään yhteistoimintamenettelyssä. Päätettyjen toimenpiteiden edistymistä seurataan ja siitä myös raportoidaan sovitusti. Tietoturvatoiminto järjestää suunnitelmiensa mukaisia auditointeja arvioidakseen hallintajärjestelmän ja tietoturvallisuuden todellisen tilan, vaatimustenmukaisuuden ja varsinaiselle toiminnalle tulevien hyötyjen saavuttamisen. Lisäksi sisäinen ja ulkoinen tarkastus arvioi tietoturvatoimintaa. Johdon katselmus -menettelyssä käsitellään säännönmukaisesti hallintajärjestelmän ja tietoturvan tila sekä merkittävimmät muutos- ja kehitystarpeet varmistaen johdon hallintaotetta asiakokonaisuudesta.

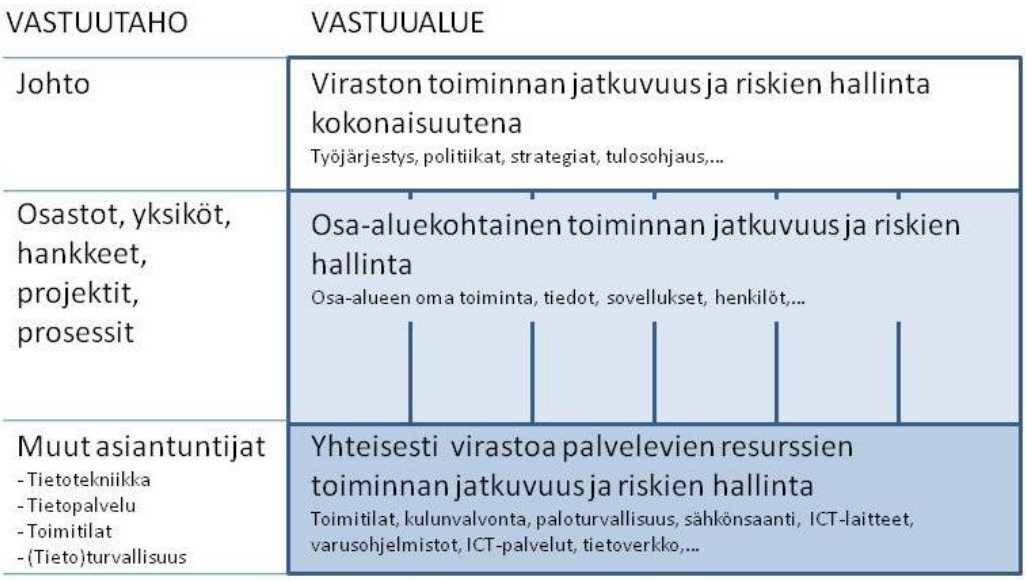
Kokemukset, palautteet ja mittaustiedot kerätään ja analysoidaan. Tarvittaessa ryhdytään korjaaviin tai ennaltaehkäiseviin ja parantaviin toimenpiteisiin. Yleisenä tavoitesuuntana on sekä hallintajärjestelmän että tietoturvallisuuden asteittainen, todennettavissa oleva paraneminen.

Tietoturvallisuuden hallintajärjestelmä merkitsee virastossa prosessimaista toimintamallia tietoturvallisuuden kehittämisessä, toteuttamisessa, valvomisessa, ylläpitämisessä ja parantamisessa. Tietyt toimenpiteet toistuvat säännöllisesti. Itse tietoturvatoiminta ja suunnitel-

mien toteuttaminen on jatkuvaa ja ympärivuotista. Esimerkiksi turvattavien kohteiden ja riskien hallinta on jatkuvaa toimintaa, ohjeita päivitetään muutostarpeiden ilmaantuessa, koulutuksia ja auditointeja järjestetään ympärivuotisesti. Tietoturvallisuuteen liittyvät keskeiset toimenpiteet merkitään näkyviin vastuualueen vuosikelloon tai kalenteriin.

Osastojen ja yksiköiden osalta keskeisiä yleisen tason tietoturvatoimenpiteitä ovat turvattavien kohteiden haltuunoton ja hallinnassa pitämisen tarkistus, tietoriskien arviointi ja tarvittavien toimenpiteiden suunnittelu. Dokumentoidusti tämä tapahtuu vastuualueen Tietoturvakortin laatimisella tai päivittämisellä. Lisäksi tehtävänä on henkilöstön ja esimiesten tietoturvakoulutustilanteen tarkistus.

Työmäärältään, kustannuksiltaan tai laajavaikutteisuudeltaan merkittävät toimenpiteet on lisäksi otettava huomioon TTS-valmistelussa. Muilta osin osastot ja yksiköt voivat ajoittaa tietoturvatoimenpiteensä oman vuosikellonsa mukaiseen tai muuten tarkoituksenmukaiseen ajankohtaan. Viraston tietoturvallisuuden vastuualueet jakautuvat yleisellä tasolla määritellyn vastuu- ja kontrolliarkkitehtuurin mukaisesti (kuvio 29).



Kuvio 29: Vastuu- ja kontrolliarkkitehtuuri

Viraston tietoturvatoiminnan organisointi, vastuut ja tehtävät -kuvauksessa tulkitaan ja avataan vallitsevia normeja ja käytäntöjä, eikä siinä ole tarkoitus olla työjärjestystä ohittavia vastuumäärityksiä. Mahdollisissa ristiriitatapauksissa työjärjestyksen sanamuoto on ratkaiseva. Tietoturvallisuudesta vastaavat kaikki virastossa työskentelevät, kukin oman tehtävä- ja

vastuualueensa osalta. Jokaisella osastolla, yksiköllä, henkilöllä, hankkeella, projektilla ja prosessilla on siten vastuu tietoturvallisuudesta oman tehtäväalueensa osalta.

Organisointikuvauksessa määritellään kaikki merkittävät viraston tietoturvallisuuteen vaikuttavat roolit ja toimijat. Yksittäinen henkilö voi toimia useammassa roolissa, kuten esimerkiksi henkilökuntaan kuuluvana, esimiehenä ja projektin ohjausryhmän jäsenenä. Kokonaisvastuu- ja -tehtäväalue muodostuu tällöin eri roolien yhdistelmistä. Tietoturvattavan kohteen kannalta keskeisiä toimijoita koskeva asiakirjaote esitetään taulukossa 10.

Rooli/toimija	Vastuualue	Tehtävät
Osastot, yksiköt, toiminnot, hankkeet, projektit ja prosessit (ao. vastuuhenkilöt)	• Oman vastuu- ja tehtäväalueen tietoturvallisuus	• Tietoturvavaatimusten ja -tarpeiden huomioon ottaminen omalla vastuu- ja tehtäväalueella - Osa-aluekohtaisten vaatimusten ja tarpeiden tunnistaminen - Turvattavien kohteiden tunnistaminen ja vastuuhenkilöiden nimeäminen - Uhkien tunnistaminen ja riskien arviointi sekä tarvittaviin toimenpiteisiin ryhtyminen - Huolehtiminen tarvittavien kontrollien määrittelystä, suunnittelusta, toteuttamisesta, toimeenpanosta, tuesta ja ylläpitämisestä - Seuranta ja valvonta • Työmäärältään, kustannuksiltaan tai laajavaikutteisuudeltaan merkittävien toimenpiteiden vieminen osaksi TTS-valmistelua
Turvattavan kohteen vastuuhenkilö	• Turvattava kohde	• Turvattavaan kohteeseen liittyvien vaatimusten ja tarpeiden tunnistaminen • Uhkien tunnistaminen ja riskien arviointi sekä tarvittaviin toimenpiteisiin ryhtyminen • Huolehtiminen tarvittavien kontrollien määrittelystä, suunnittelusta, toteuttamisesta, toimeenpanosta, tuesta ja ylläpitämisestä • Seuranta ja valvonta

Taulukko 10: Ote tietoturvatoiminnan organisoinnista, vastuista ja tehtävistä

4.3 Menettelytapakuvaus

4.3.1 Johdanto

Tässä asiakirjassa kuvataan viraston tietoturvallisuuden kannalta merkittävien turvattavien kohteiden hallintamenettely.

Tietoturvattavalla kohteella tarkoitetaan asiaa, toimintaa, omaisuutta tai ihmistä, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi tietoturvallisuusnäkökulmasta. Turvaamisintressi kohdistuu tiedon luottamuksellisuuden, eheyden, käytettävyyden, todennettavuuden ja kiistämättömyyden tilaan.

Lähtökohtaisesti tärkeimmät viraston tietoturvatoiminnalla turvattavat kohteet ovat 1) varsinainen toiminta ja toimintaan liittyvät prosessit ja toiminnot, 2) tietovarannot sekä 3) näitä tukevat resurssit ja infrastruktuuri (esim. tietojärjestelmät, tietotekniikka ja toimitilat).

Henkilöstö kokonaisuudessaan on turvattava kohde. Henkilöstöön liittyviä suojelu- ja turvallisuusnäkökohtia otetaan kuitenkin huomioon jo muissa, mm. henkilöstöhallintoon, esimiestoimintaan, työsuojeluun ja työturvallisuuteen liittyvissä menettelytavoissa ja suunnitelmissa, joten ne voidaan päällekkäisyyden välttämiseksi haluttaessa rajata tämän menettelytavan ulkopuolelle.

4.3.2 Menettelytavan päämäärät ja tulostavoitteet

Menettelytavan tarkoituksena on ylläpitää varmuutta siitä, että virastossa tunnistetaan tärkeät turvattavat kohteet ja että erityisesti näiden tekijöiden osalta tietoturvatarpeet tiedostetaan ja tietoturvallisuus on hyväksyttävällä tasolla.

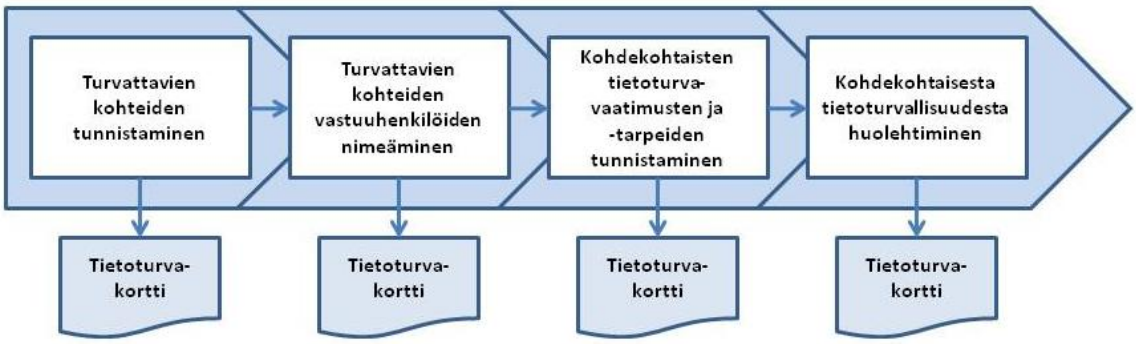
Menettelytavan tavoitteena on, että turvattavien kohteiden tietoturvallisuus on hallinnassa.

4.3.3 Menettelytavan omistajuus

Menettelytavan omistaja on viraston tietoturvapäällikkö.

Omistaja vastaa menettelytavasta ja sen kehittämisestä. Omistajan tehtäviin kuuluu huolehtia menettelytapaan liittyvästä suunnittelusta, yhteentoimivuudesta muiden menettelytapojen kanssa, ohjaavasta dokumentaatiosta ja tietoisuuden jakamisesta, suorituskyvyn mittaamisesta sekä kehittämismahdollisuuksien tunnistamisesta ja huomioon ottamisesta.

4.3.4 Toistettava tehtäväketju



Kuvio 30: Turvattavien kohteiden hallintamenettely

Virastossa tarkistetaan vähintään vuosittain, mitkä ovat tietoturvanäkökulmasta tärkeimmät turvattavat kohteet. Turvattavat kohteet tunnistetaan osastoilla ja yksiköissä sekä tarvittaessa myös muilla osa-alueilla, joilla on viraston tehtävien hoidon kannalta merkitystä tai jossa käsitellään kriittistä tietoa.

Kullekin turvattavalle kohteelle nimetään vastuuhenkilö, jonka tehtävänä on huolehtia kohteen peruskuvauksesta, tietoturvavaatimusten ja -tarpeiden tunnistamisesta, riskien arvioinnista ja tarvittavista tietoturvatoimenpiteistä tai niiden esittämisestä sekä osallistua tarpeiden ja toimenpiteiden yhteensovittamiseen. Turvattavan kohteen vastuuhenkilön velvollisuuksiin kuuluu myös huolehtia kontrollikuvausten ylläpitämisestä sekä kohteeseen liittyvien tietoturvatapahtumien ja -toimenpiteiden kirjaamisesta. Edellä mainittujen tietojen kirjaamistyökaluna toimii Tietoturvakortti (Excel-taulukko).

4.3.5 Avaintehtäviin liittyvät roolit ja vastuut

Avainvaiheet/-tehtävät	Tallenteet	Osaston, yksikön, palvelun, prosessin, toiminnon tms. vastuuhenkilö	Turvattavan kohteen vastuuhenkilö	Kontrolliomistaja	Tietoturvapäällikkö
Turvattavien kohteiden tunnistaminen	Tietoturvakortti	OT	K	I	I
Turvattavien kohteiden vastuuhenkilöiden nimeäminen	Tietoturvakortti	OT	K	I	I
Kohdekohtaisten tietoturvavaatimusten ja -tarpeiden tunnistaminen	Tietoturvakortti	K	OT	K	I
Kohdekohtaisesta tietoturvallisuudesta huolehtiminen	Tietoturvakortti	K	OT	K/T	I

T = Toteutusvastuullinen *(Responsible)*
O = Omistaja ja tilivelvollinen *(Accountable)*
K = Konsultaatio- ja yhteistyötaho *(Consulted)*
I = Informoinnin kohde *(Informed)*

Kontrolliomistaja = Henkilö tai taho, joka vastaa yksittäisestä, konkreettisesta kontrollista/suojamekanismista/turvajärjestelystä, jota turvattavassa kohteessa käytetään ja/tai tarvitaan. Yksittäinen kontrolli puolestaan voi palvella yhtä tai useampaa kohdetta tai jopa koko organisaatiota, joten kontrolliomistajan on yhteensovitettava mahdollisesti erilaisiakin tarpeita. Esimerkiksi toimitilaturvallisuuden, tietoteknisen turvallisuuden ja tietoturvaohjeiston osalta voi löytyä yksikön ulkopuolisia kontrolliomistajia. Tällöin otetaan yhteyttä suoraan ao. vastuuyksikköön ja epäselvissä tapauksissa tietoturvapäällikköön.

Taulukko 11: Avaintehtäviin liittyvät roolit ja vastuut

4.3.6 Ohjausasiakirjat

Asiakirja	Suojaustaso tai turvallisuusluokka	Sijainti
Tietoturvallisuuden johtamis- ja hallintajärjestelmän yleiskuvaus	Suojaustaso IV Käyttö rajoitettu	Asiakirjahallintajärjestelmä Intranet
Tietoturvatoiminnan organisointi, vastuut ja tehtävät	Suojaustaso IV Käyttö rajoitettu	Asiakirjahallintajärjestelmä Intranet
Turvattavien kohteiden hallintamenettely	Suojaustaso IV Käyttö rajoitettu	Asiakirjahallintajärjestelmä

Taulukko 12: Ohjausasiakirjat

4.3.7 Tallenteet

Tallenne	Muoto	Toteutus-vastuullinen	Sijainti	Suojaustaso tai turvallisuusluokka	Säilytysaika
Tietoturva-kortti	Hallinnollinen asiakirja (Excel-taulukko)	Osaston, yksikön, palvelun, prosessin, toiminnon tms. vastuuhenkilö Turvattavan kohteen vastuuhenkilö	Kohde (kopio - tietoturva-päällikköllä)	Suojaustaso IV Käyttö rajoitettu tai Suojaustaso III Luottamuksellinen	Voimassaolo + 1 v

Taulukko 13: Tallenteet

4.3.8 Menettelytavan mittarit

Menettelytavan tavoitteet	Mitattava asia	Mittaustapa	Mittaustulos-tavoitteet	Tulosvastuullinen
Menettelytavan tavoitteena on, että turvattavien kohteiden tietoturvallisuus on hallinnassa.	Viraston johdon, osastojen ja yksiköiden vastuuhenkilöiden tietoisuus menettelytavasta	Infotilaisuuksien osallistujatiedot		Tietoturvapäällikkö
	Tietoturvakorttien olemassaolo ja tietosisällön asianmukaisuus	Tietoturva-toiminnon tekemä vertailu työjärjestyksestä tunnistettavissa oleviin organisaation ja toiminnan osa-alueisiin		Osastojen ja yksiköiden vastuuhenkilöt Turvattavien kohteiden vastuuhenkilöt
		Tietoturvakortit ja niiden katselmointi		Tietoturvapäällikkö yhteistyössä osastojen ja yksiköiden vastuuhenkilöiden kanssa

Taulukko 14: Menettelytavan mittarit

4.4 Työkalun kuvaus

Turvattavien kohteiden kirjaamistyökaluna toimii Excel-pohjainen Tietoturvakortti. Työkalun välilehtitulosteet on esitetty liitteessä 1. Seuraavassa taulukossa esitetään työkalun välilehti-rakenne ja tietosisältö.

Välilehdet	Tietosisältö
Kuvailutiedot	• Laatija • Tarkastaja • Hyväksyjä • Versio n:o • Tiedoston nimi • Tallennuspaikka
Turvattavien kohteiden luettelo	• Korttityyppi (kokoava kortti / täsmäkortti) • Turvattavan kohteen nimitys • Muut yksilöivät tunnistetiedot • Käyttötarkoitus ja/tai tehtävän tarkoitus • Turvattavan kohteen vastuuhenkilö
Vaatimukset	• Ulkoiset vaatimuslähteet • Sopimukset • Sisäiset vaatimuslähteet
Tarpeet	• Virastolähtöiset tietoturvatarpeet
Resurssit ja riippuvuudet	• Syöte, input-liittymät • Resurssit • Tulos, output-liittymät
Merkitys	• Luottamuksellisuuden menetys • Eheyden menetys • Käytettävyyden menetys (alle tunti / puoli päivää / vuorokausi / 2-3 vuorokautta / viikko / kuukausi) • Tunnistettavuuden menetys • Kiistämättömyyden menetys
Riskianalyysi	• Tunniste • Vaihe, tilanne, osa-alue • Uhka • Uhkan vaikutusalue • Haavoittuvuus, altistava tekijä • Nykykontrollit • Todennäköisyys • Vakavuus • Riskitulo • Toimenpidetarpeet
Toimenpidesuunnitelma	• Ajoitus • Toimenpide • Hoidetaan paikallisesti / hoidetaan keskitetysti • Toteutusvastuuhenkilö tai -taho • Kiireellisyys (pieni / keskimääräinen / suuri) • Merkittävyys (pieni / keskimääräinen / suuri) • Työmääräarvio • Kustannusarvio • Status
Tapahtumapäiväkirja	• Pvm • Klo • Tietoturvatapahtumat ja toimenpiteet

Taulukko 15: Tietoturvakortin välilehdet ja tietosisältö

5 Arviointi

Valitussa tutkimustehtävässä tutkimusongelma rakentui siitä, ettei tietoturvallisuuden hallinnan kannalta merkittävistä turvattavista kohteista ja niiden hallinnasta ollut vakiintunutta käsitystä eikä turvattavien kohteiden hallinnasta ollut löydettävissä käytännöllistä kuvausta eikä työkalua. Tutkimuksen pääkysymyksenä oli: Miten tietoturvallisuuden kannalta keskeisiä kohteita hallitaan? Tutkimustuloksissa annetaan vastaus, joka koostuu toimintamallista, menettelytapakuvauksesta, sekä sitä tukevasta työkalusta. Pääkysymyksen ratkaisemiseksi tarvittavia apukysymyksiä tutkimuksessa olivat: Mitä tietoturvattavat kohteet ovat? Mitä tietoturvattavien kohteiden hallinta on? Tutkimustuloksissa annetaan vastaukset apukysymyksiin määrittelemällä tietoturvattavien kohteiden ja niiden hallinnan käsitteistö.

Työn tarkoituksena oli tuottaa malli, jota käyttämällä voidaan parantaa ja yhdenmukaistaa tietoturvattavien kohteiden hallintakäytäntöjä osana normaalin toiminnan ja samalla tietoturvallisuuden johtamista ja hallintaa. Tässä luvussa pohditaan, missä määrin asetetut tavoitteet saavutettiin, saatiinko vastaus tutkimusongelmaan ja -kysymyksiin ja oliko työn viitekehys onnistunut. Lisäksi tarkastellaan kehittämisprosessin luotettavuutta, siirrettävyyttä ja käyttökelpoisuutta.

Luotettavuus on Toikon ja Rantasen (2009, 121 - 122) mukaan tieteellisen tiedon keskeinen tunnusmerkki. Arvioitavana ovat tällöin tutkimusmenetelmät, tutkimusprosessi ja tutkimustulokset. Määrällisissä tutkimuksissa luotettavuutta arvioidaan usein reliabiliteetin ja validiteetin käsitteiden kautta. Kehittämistoiminnassa luotettavuuden kriteerit ovat tieteellisen luotettavuuden kriteerejä vain siltä osin kun kehittämistoimintaan liittyy selkeitä tutkimuksellisia asetelmia. Laadullisen tutkimuksen yhteydessä käytetään Toikon ja Rantasen mukaan mieluummin vakuuttavuuden käsitettä ja kehittämistoiminnassa erityisesti käyttökelpoisuutta. Näitä kaikkia luotettavuuden näkökulmia voidaan joka tapauksessa soveltaa myös kehittämistoimintaan. Tulosten arviointitapa puolestaan pohjautuu Järvisten (2004, 118 - 124) esittämään malliin, joka on tarkoitettu erityisesti konstruktiivisen tutkimuksen tulosten käyttökelpoisuutta koskevaan pohdintaan.

5.1 Tutkimus

5.1.1 Metodi

Tutkimus toteutettiin soveltavana tutkimushankkeena suunnittelutieteeseen kuuluvaa konstruktiivista tutkimusmetodia käyttämällä. Metodi on määritelty tutkimuskirjallisuudessa (mm. Järvinen & Järvinen 2004) sekä tässä työssä ja metodia on noudatettu kaikissa vaiheissa

tavoitteiden asettamisesta ja spesifioinnista aina implementointiin ja α- ja β-testauksiin sekä konstruktion arviointiin saakka. Metodi osoittautui tämän työn kannalta hyödylliseksi ja käyttökelpoiseksi. Vaikka testaukseen sisältyi kehittäjästä riippumaton β-vaihe, olisi vastaavaa arviointia kuitenkin vielä syytä laajentaa kattavammin käyttäjien itsenäiseen mallin ja työkalun käyttövaiheeseen ja siitä kerättävään palautteeseen. Sinällään kehittämistyössä käytetyt menetelmät ovat yleispäteviä ja niitä voidaan tarvittaessa hyödyntää sellaisenaan.

5.1.2 Validiteetti, reliabiliteetti ja vakuuttavuus

Validiteetti eli pätevyys viittaa Toikon ja Rantasen (2009, 122) mukaan siihen, että tutkimuksessa mitataan sitä, mitä oli tarkoitus mitata. Tässä tutkimuksessa validiteettia voidaan pohtia lähinnä vain käytettyjen käsitteiden ja tehtyjen valintojen johdonmukaisuuden kautta, koska esimerkiksi kyselylomakkeita ei ole käytetty eikä tilastollisia analyysejä tehty. Uuteen viitekehykseen uusine käsitemäärittelyineen johtava kehittämistyö sen sijaan pyrittiin tekemään perustellusti ja johdonmukaisesti käytettyyn aineistoon nojautuen. Keskeiset käsitteet määriteltiin ja käsitteiden toimivuus osoitettiin testaamalla käsitteitä ja määritelmiä käytännön lauserakenteissa. Työn lopputuloksissa huomioitiin turvallisuuskontekstin ja sen ulkopuolelta haetun lähdeaineiston viitoittama sisältö.

Reliabiliteetti eli luotettavuus liittyy Toikon ja Rantasen (2009, 122) mukaan mittarien ja tutkimusasetelmien toimivuuteen, saatujen vastausten korreloituvuuteen ja toistettavuuteen. Tässä tutkimuksessa, kuten kehittämistoiminnassa yleensäkin, reliabiliteetin pohtiminen on ongelmallista, sillä kehittäminen tehtiin juuri tietyssä yksittäisessä organisaatiossa ja siinä vallitsevissa olosuhteissa sekä toiminta- ja turvallisuuskulttuurissa. Kun kehittämisen lopputulokset kohdistettiin tiettyyn organisaatioon, jäi aineisto siltä osin väistämättä suppeaksi, mikä puolestaan voi heijastua toistettavuuteen. Tuloksia voidaan kuitenkin hyödyntää laajasti erilaisissa julkisissa ja yksityisissä organisaatioissa, mutta hyödyntäminen vaatii aina jonkin asteista soveltamista valittuun kohdeorganisaatioon. Soveltamistarve koskee lähtökohtaisesti kaikkia malleja.

Laadullisessa tutkimuksessa reliabiliteettia ja validiteettia olennaisempaa on kuitenkin pohtia tutkimuksen vakuuttavuutta (Toikko & Rantanen 2009, 123). Tausta-aineistoon perehdyttiin standardien ja ammattikirjallisuuden osalta varsin laajasti. Tieteellistä tutkimusaineistoa lähteissä sen sijaan oli niukasti, mikä johtui siitä, että tutkimusaihetta ei samasta näkökulmasta oltu juurikaan tutkittu. Tutkimusta löytyi runsaasti mm. tietoturvallisuudesta, taloudellisen pääoman hallinnasta ja johtamisesta, mutta niissä esitetyt tulokset eivät olleet tämän työn kannalta relevantteja eikä niiden sisällyttäminen tähän tutkimukseen erilaisen näkökulmansa vuoksi siten ollut perusteltua. Tutkimuksessa tehdyt valinnat, tulkinnat ja kehittely pyrittiin omassa, uudessa viitekehyksessään tekemään ja esittämään perustellusti. Koh-

deorganisaatio ja sen kulttuuri otettiin kehittämisessä huomioon siten, että kehittäjä perehtyi organisaatioon toimimalla organisaation kanssa yhteistyössä runsaat kaksi vuotta ja tutustumalla mm. organisaation avainhenkilöstöön ja sisäiseen ohjeistukseen.

5.2 Tulokset

5.2.1 Käsitteistö

Tutkimuksen aiheena oli tietoturvattavien kohteiden hallinta operatiivisen johtamisen näkökulmasta. Tutkimuksessa määriteltiin seuraavat käsitteet: turvattava kohde, tietoturvattava kohde, turvattavan kohteen hallinta, tietoturvattavan kohteen hallinta ja operatiivinen johtaminen. Lisäksi rajakäsitteinä määriteltiin: tietoturvallisuus, tietoturvallisuuden hallinta, tietoturvallisuuden hallintajärjestelmä, omaisuuden hallinta, omaisuudenhallintajärjestelmä, johtaminen, asioiden johtaminen ja ihmisten johtaminen. Käsitemääritelmät on esitetty kootusti liitteessä 2. Määritelmien tarkoituksena oli muodostaa käsitteellisesti looginen ja esityksen kannalta yhtenäinen kokonaisuus tutkimusaiheesta. Osa arvovaltaisissakin lähteissä määritellyistä käsitteistä määriteltiin siihen sisältyvistä riskeistä huolimatta uudelleen, jotta käytettävästä käsitteistöstä olisi saatu tämän työn kannalta yhtenäinen ja toimiva kokonaisuus. Uusilla määritelmillä ei kuitenkaan muutettu käsitteiden yleistä puhekielistä merkitystä, vaan pikemminkin pyrkimyksenä oli osoittaa aiempiin määritelmiin liittyviä ongelmia ja vastaavasti täsmentää käsitteitä tutkimuksellista käyttöä ja jatkokehittämistä varten.

5.2.2 Malli ja työkalu

Kehitetty tietoturvattavan kohteen hallinnan lähestymistapa on merkittävästi laajempi kuin standardeissa esitetty malli. Kun standardeissa rajoitutaan kohteiden tunnistamiseen, vastuuttamiseen ja luokitteluun, ei niissä käytetystä hallintaterminologiasta huolimatta edetä varsinaiseen hallintavaiheeseen. Nyt kehitetyssä mallissa huomioitiin edellisten lisäksi mm. kohteen tietoturvavaatimukset ja -tarpeet, tarvittavat resurssit ja muut riippuvuudet, kohteen merkitys organisaatiolle, riskit, tarvittavat toimenpiteet sekä toimenpiteiden ja tapahtumien kirjaaminen.

Todelliseen käyttötarpeeseen ja -tilanteeseen kehitetyssä mallissa otettiin huomioon mm. organisaation johtamisjärjestelmä ja tietoturvallisuuden hallintajärjestelmä, joihin tietoturvattavien kohteiden hallintamalli ja -työkalu pyrittiin sovittamaan. Mallista tehdyn menettelytapakuvauksen, työkalun sekä niihin liittyvän koulutuksen, työpajatoiminnan ja tukipalveluiden kautta pyrittiin edistämään yhtenäistä toimintatapaa, jota käyttämällä voitaisiin parantaa ja yhdenmukaistaa tietoturvattavien kohteiden hallintakäytäntöjä osana normaalin toiminnan ja samalla tietoturvallisuuden johtamista ja hallintaa. Käyttäjille suunnattu doku-

mentti oli tarkoitus pitää tiiviinä, helppolukuisena ja ymmärrettävänä kuvauksena, joka on saatavilla sähköisessä muodossa organisaation intranetistä. Malli, työkalu ja niihin sisältyvä kieliasu pyrittiin muotoilemaan siten, ettei käyttäjä tarvitse esimerkiksi syvällistä tietoturva- tai tietoteknistä osaamista.

Kohdeorganisaation yksiköillä ja niiden vastuuhenkilöillä oli ja on tulosohjauksselliset tavoitteet ja velvoitteet huolehtia tietoturvallisuudesta. Mallia ja työkalua käyttämällä keskeiset tietoturvavelvoitteet ovat täytettävissä, joten käytölle on sisäänrakennettu kannuste ja johdon tuki. Toimintamalli myös osaltaan turvaa yksikön vastuuhenkilöä, sillä hänelle muodostuu mahdollisuus dokumentoidusti osoittaa, että vastuualueen tietoturvavelvoitteista on huolehdittu asianmukaisesti. Vastuuhenkilön vaihtuessa valmistellut näkökulmat ovat myös siirrettävissä seuraajan jatkohyödynnettäväksi. Työn tulokset on levitetty organisaation laajuiseen käyttöön ja ne ovat vähitellen muodostumassa vakiintuneeksi, normaaliksi tavaksi toimia. Mallin käytön jatkuvuutta tuetaan sitomalla siihen tulostavoitteita sekä vuosittainen toiminnan ja talouden suunnittelusykli vuosikellokiinnityksineen. Näin ollen voidaan todeta, että kehittämistyön päätavoite on onnistuttu saavuttamaan.

Konstruoitu malli ja työkalu ovat käyttöönoton myötä johtaneet siihen, että yksiköissä tietoisuus vastuullaan olevista tietoturva-asioista, -uhkista ja toimenpidetarpeista on parantunut. Tämä perustuu dokumentoitumiseen, yhteisten käsittelytilaisuuksiin ja vastuutukseen. Kehitetyn mallin myötä tietoturvatoimintaa on saatu jalkautettua varsinaiseen toimintaan huomattavasti syvällisemmin kuin pelkkiä määräyksiä ja ohjeita jakamalla. Lisäksi asiaan liittyvä koordinointi ja valvonta ovat tulleet käytännön tasolla mahdolliseksi, vaikka työkalun toteutustapa yksittäisinä tietoturvakorttitiedostoina vielä asettaakin rajoituksia. Toimintamalli ja työkalun käyttö itsessään eivät sido liikaa käyttäjäorganisaation resursseja, sillä asiaan liittyvä vuosittainen hallinnollinen työ ensimmäisen toteutuskierroksen jälkeen on noin 1-2 tuntia kunkin hallittavan kohteen osalta. Varsinaiset tietoturvatoimenpiteet ovat luonnollisesti asia erikseen ja niihin tarvittava työ ja muu panostus voi vaihdella kohteittain runsaastikin.

5.2.3 Siirrettävyys

Kehitetyt käsitteet, malli ja työkalu ovat luonteeltaan yleiskäyttöisiä. Tulokset ovat myös yhteensopivia standardinmukaisen tietoturvallisuuden hallintajärjestelmän, valtionhallinnon tietoturvatasomallin sekä kansallisen turvallisuusauditointikriteeristön tietoturvaosion kanssa. Käytännön soveltamistyötä tarvitaan kuitenkin uuden mallin kytkemisessä kohdeorganisaation johtamisjärjestelmään, menettelytavan kytkemisessä avainhenkilörooleihin, ohjausasiakirjojen yksilöinnissä, realististen mittareiden määrittelyssä sekä itse toimintamallin jalkauttamisessa. Malliin on sisällytetty joustavuutta ns. valmisosa-ajattelun myötä, jolloin esimerkiksi riskien arvioinnissa voidaan käyttää organisaatiossa jo mahdollisesti olemassa olevaa mallia ja

työkalua. Malli ja työkalu ovat myös jatkokehitettävissä ja mahdollisesti tuotteistettavissa myös kaupalliseen käyttöön niin työkalujen kuin asiantuntijapalveluidenkin muodossa vastaamaan paremmin kunkin kohdeorganisaation tarpeita. Malliin ja työkaluun voidaan tällöin sisällyttää myös uusia elementtejä ja vielä tiiviimpää kytkentää niihin standardeihin, määräyksiin tms., joita organisaatiossa on tarpeen soveltaa. Samalla on kuitenkin syytä varoa, ettei mallista tule liian raskasta käyttäjäorganisaation kannalta.

5.3 Johtopäätökset ja suositukset

Kokonaisarvioina voidaan todeta, että tutkimuksen pääkysymykseen ja apukysymyksiin tietoturvattavien kohteiden hallinnasta on esitetty vastaukset ja tarvittavat käsitteet aiheesta on määritelty. Tavoitteeksi asetettu tietoturvattavien kohteiden hallintamalli osana normaalin toiminnan ja tietoturvallisuuden johtamista ja hallintaa on kehitetty ja kuvattu. Kehittämismenetelmää ja tuloksia sekä niiden siirrettävyydestä ja tuotteistamismahdollisuutta on esitetty arviot.

Mikäli organisaatiolla on tietoturvallisuusnäkökulmasta tärkeitä turvattavia kohteita, on suositeltavaa määritellä niiden hallintaan yhtenäinen organisaation toimintatapoihin soveltuva malli. Tässä työssä esitetty malli tarjoaa työhön yhden perustellun lähtökohdan. Sitä kannattaa kuitenkin täsmentää organisaatiokohtaiset tarpeet huomioon ottaen.

Jatkokehittämisessä ja tuotteistamisessa niin mallin kuin työkalunkin osalta on suositeltavaa paneutua huolelliseen vaatimusmäärittelyyn. Tällöin voidaan huomioida esimerkiksi järjestelmän ja tietojen samanaikainen yhteiskäyttötarve, käyttöoikeudet ja -valtuudet sekä suojaustarpeet, koska järjestelmästä tietoineen muodostuu itsessään merkittävä turvattava kohde. Samalla jatkokehityksessä on suositeltavaa tarkastella kerättävien tietojen määrämuotoistamista, jolloin tietoja voidaan helpommin linkittää ja yhdistellä, etsiä riippuvuuksia ja hakea laajempia hyötyjä vaikkapa ajantasaisen tilannekuvan muodostamiseksi.

Lähteet

Menetelmät

Aaltola, J. & Valli, R. (toim.) 2007. Ikkunoita tutkimusmetodeihin I. Jyväskylä: PS-kustannus.

Aaltola, J. 2010. Filosofia, tiede, ymmärtäminen. Teoksessa Aaltola, J. (toim.) Ikkunoita tutkimusmetodeihin II. Jyväskylä: PS-kustannus, 12 - 27.

Ghauri, P. & Grønhaug, K. 2005. Research Methods in Business Studies. Harlow: Prentice Hall.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2002. Tutki ja kirjoita. Helsinki: Tammi.

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

Sanastotyö. 2010. Sanastokeskus TSK. Viitattu 24.10.2010. http://www.tsk.fi/

Toikko, T. & Rantanen, T. 2009. Tutkimuksellinen kehittämistoiminta. Tampere: Tampere University Press.

Tutkimusaihe

Asset Management Competence Requirements Framework. 2008. Bristol: Institute of Asset Management.

Asset Protection and Security Management Handbook. 2003. POA Publishing LLC. Boca Raton, FL: Auerbach.

Brotby, K. 2009. Information Security Governance. A Practical Development and Implementation Approach. Hoboken, NJ: John Wiley & Sons.

BSI-Standard 100-1. 2008. Information Security Management Systems (ISMS). Version 1.5. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

BSI-Standard 100-2. 2008. IIT-Grundschutz Methodology. Version 2.0. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

BSI-Standard 100-3. 2008. Risk analysis based on IT-Grundschutz. Version 2.5. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Burns-Howell, T., Cordier, P. & Eriksson, T. 2003. Security Risk Assessment and Control. Leicester: Perpetuity Press.

COBIT 4.1. 2007. (Control Objectives for Information and Related Technology). Rolling Meadows, IL: IT Governance Institute.

Curtis, G.E. & McBride, R.B. 2005. Proactive Security Administration. New Jersey, NJ: Pearson Prentice Hall.

Fay, J.J. 2002. Contemporary Security Management. Woburn, MA: Butterworth-Heinemann.

Fone, M. & Young, P.C. 2001. Public Sector Risk Management. Woburn, MA: Butterworth-Heinemann.

Generally Accepted Information Security Principles (GAISP). 2004. V 3.0. Portland, OR: Information Systems Security Association.

ISO 31000:2009. Risk management - Principles and guidelines. Geneva: International Organisation for Standardization.

ISO/IEC 27001:2005. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen Standardisoimisliitto SFS; Geneva: International Organisation for Standardization.

ISO/IEC 27002:2005. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki: Suomen Standardisoimisliitto SFS; Geneva: International Organisation for Standardization.

ISO/IEC 27003:2010. Information technology. Security techniques. Information security management system guidance. Geneva: International Organisation for Standardization.

ISO/IEC 27005:2008. Information technology. Security techniques. Information security risk management. Geneva: International Organisation for Standardization.

IT-Grundschutz Manual. 2005. Bonn: Bundesamt für Sicherheit in der Informationstechnik (BSI).

Johnson, B.R. 2005. Principles of Security Management. New Jersey, NJ: Pearson Prentice Hall.

Johtaminen. 2011. Työturvallisuuskeskus. Viitattu 3.1.2011. http://www.tyoturva.fi

Kamensky, M. 2002. Strateginen johtaminen. Helsinki: Kauppakaari.

Kansallinen turvallisuusauditointikriteeristö (KATAKRI). 2009. Helsinki: Puolustusministeriö.

Kinnunen, E. 2010. Kypsyysajattelu tietoturvallisuuden hallinnan apuna. Helsinki: Valtiokonttori. Viitattu 28.12.2010. http://www.valtiokonttori.fi/

Kovacich, G.L. & Halibozek, E.P. 2003. The Manager's Handbook for Corporate Security. Establishing and Managing a Successful Assets Protection Program. Burlington, MA: Butterworth-Heinemann.

Kujansivu, P., Lönnqvist, A., Jääskeläinen, A. & Sillanpää, V. 2007. Liiketoiminnan aineettomat menestystekijät. Mittaa, kehitä ja johda. Helsinki: Talentum.

Kyrölä, T. 2001. Esimies ja tietoriskien hallinta. Helsinki: WSOY.

Laamanen, K. 2002. Johda liiketoimintaa prosessien verkkona. Helsinki: Suomen Laatukeskus.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Turvallisuusjohtamisen portfolio: Helsinki: Talentum.

Maunula, R. 1997. Esimiehenä asiantuntijayhteisössä ja -tiimissä. Helsinki: Otava.

Mielonen, S. 2011. Systeemiajattelu. Aalto Yliopisto. Viitattu 13.4.2011. http://mlab.taik.fi/polut/Yhteiskunnalliset/tyokalu_systeemiajattelu.html

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

Miettinen, J.E. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Mäkinen, K. 2005. Strategic Security. A Constructivist Investigation of Critical Security and Strategic Organisational Learning Issues: Towards a Theory of Security Development. Helsinki: ACIE Publications.

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

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. 2010. VAHTI 2/2010. Helsinki: Valtiovarainministeriö.

PAS 55-1:2008. Asset Management. Specification for the optimized management of physical assets. London: British Standards Institution.

Romppanen, M. & Rousku, K. 2010. Suojattavat kohteet ja kohteiden luokittelu. Helsinki: Valtiokonttori. Viitattu 28.12.2010. http://www.valtiokonttori.fi/

Roper, C.A. 1999. Risk Management for Security Professionals. Woburn, MA: Butterworth-Heinemann.

Ruuhilehto, K. & Vilppola, K. 2000. Turvallisuuskulttuuri ja turvallisuuden edistäminen yrityksessä. TUKES-julkaisu 1/2000. Helsinki: Turvatekniikan keskus.

Suomen Stanardisoimisliitto SFS. 2010. Viitattu 22.11.2010. http://www.sfs.fi

Talbot, J. & Jakeman, M. 2009. Security Risk Management Body of Knowledge (SRMBOK). Hoboken, NJ: John Wiley & Sons.

The Business Model for Information Security. 2010. Rolling Meadows, IL: ISACA.

The Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2011. Viitattu 5.4.2011. http://www.coso.org/resources.htm

The Institute of Asset Management. 2011. Viitattu 2.1.2011. http://theiam.org/

The Oxford Advanced Learner's Dictionary. 2011. Oxford: Oxford University Press. Viitattu 2.1.2011. http://www.oxfordadvancedlearnersdictionary.com

The Standard of Good Practice for Information Security. 2007. London: Information Security Forum.

Tietoturvallisuudella tuloksia. 2007. Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. VAHTI 3/2007. Helsinki: Valtiovarainministeriö.

Tiivis tietoturvasanasto. 2004. TSK 31. Helsinki: Sanastokeskus TSK.

Valtionhallinnon tietoturvasanasto. 2008. VAHTI 8/2008. Helsinki: Valtiovarainministeriö.

Vellani, K.H. 2007. Strategic Security Management. Burlington, MA: Butterworth-Heinemann.

Viitala, R. & Jylhä, E. 2008. Liiketoimintaosaaminen. Helsinki: Edita Publishing.

Viljanen, L. 2010. Tietoturvan tasot ja palvelusopimukset käytännössä. VIP:n koulutusaineisto. Helsinki: Valtiokonttori. Viitattu 28.12.2010. http://www.valtiokonttori.fi/

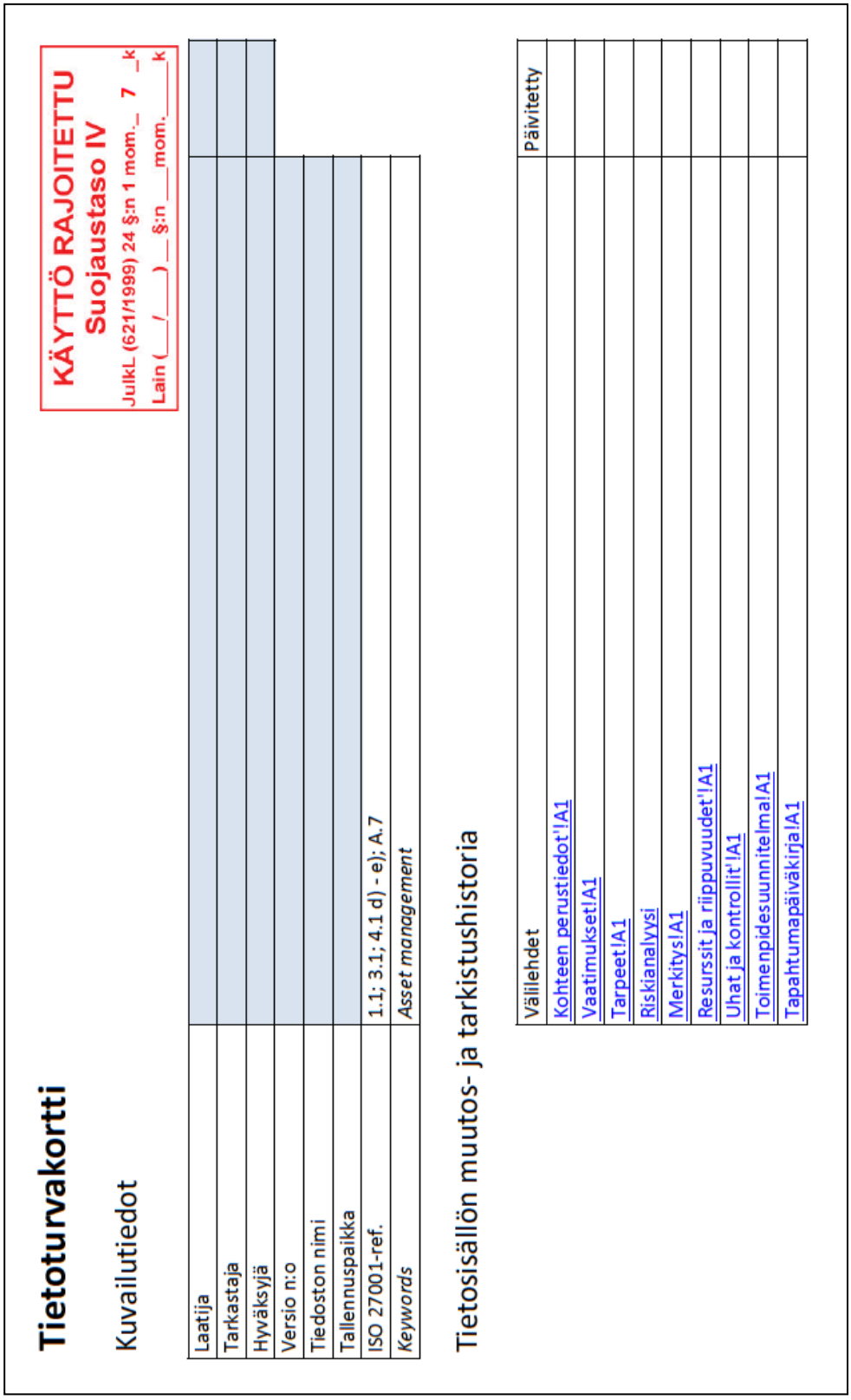
Virtanen, T. 2002. Four Views on Security. Espoo: Otamedia.

Kuviot

Taulukot

Liitteet

Liite 1: Työkalun näyttömallit



Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (__/___) __ §:n ___mom.____k

Kuvailutiedot

Laatija	
Tarkastaja	
Hyväksyjä	
Versio n:o	
Tiedoston nimi	
Tallennuspaikka	
ISO 27001-ref.	1.1; 3.1.; 4.1 d) - e); A.7
Keywords	*Asset management*

Tietosisällön muutos- ja tarkistushistoria

Välilehdet	Päivitetty
Kohteen perustiedot!A1	
Vaatimukset!A1	
Tarpeet!A1	
Riskianalyysi	
Merkitys!A1	
Resurssit ja riippuvuudet!A1	
Uhat ja kontrollit!A1	
Toimenpidesuunnitelma!A1	
Tapahtumapäiväkirja!A1	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Turvattavien kohteiden luettelo

Korttityyppi	<Klikkaa ja valitse korttityyppi>

Turvattavan kohteen nimitys	Muut yksilöivät tunnistetiedot	Käyttötarkoitus ja/tai tehtävän tarkoitus	Turvattavan kohteen vastuuhenkilö

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Vaatimukset

Ulkoiset vaatimuslähteet	
Sopimukset	
Sisäiset vaatimuslähteet	

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Tarpeet

Virastolähtöiset tietoturvatarpeet	

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Resurssit ja riippuvuudet

Mistä yksiköistä, prosesseista tai toiminnoista ollaan riippuvaisia tai mikä on se ulkopuolinen "syöte", josta tämä tehtäväketju käynnistyy	
ALOITA TÄSTÄ: Kirjaa ensin, mitä tietoaineistoja, sovelluksia, tekniikkaa, erityistiloja, avainhenkilörooleja, ulkopuolisia palveluita tms. tarvitaan, jotta toiminto/tehtävät voidaan hoitaa	
Mitkä ovat ne myöhemmät yksiköt, prosessit tai toiminnot, jotka ovat riippuvaisia tämän tehtäväketjun sujumisesta tai odottavat siltä tuloksia	

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Merkitys

VAHINKOTYYPPI	LUOKKA (A/B/C/D/E)	TÄYDENTÄVÄ VAHINKOKUVAUS
Luottamuksellisuuden menetys - paljastuminen sivullisille		
Eheyden menetys - virheellistyminen, korruptoituminen		
Käytettävyyden menetys - tuhoutuminen, katoaminen, toimimattomuus, poissaolo		
* Alle tunti		
* Puoli päivää		
* Vuorokausi		
* 2-3 vuorokautta		
* Viikko		
* Kuukausi		
Tunnistettavuuden menetys - ei voida osoittaa tekijää, toimijaa		
Kiistämättömyyden menetys - ei voida osoittaa tapahtuman olemassaoloa		

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Riskianalyysi

Tunniste	Vaihe, tilanne, osa-alue	Uhka	Uhkan vaikutusalue	Haavoittuvuus, altistava tekijä	Nykykontrollit	Toden-näköisyys	Vakavuus	Riskitulo	Toimenpidetarpeet

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Toimenpidesuunnitelma

*) 1 = suuri, 2 = keskimääräinen, 3 = pieni

Ajoitus	Toimenpide	P = Hoidetaan paikallisesti, K = Hoidetaan keskitetysti	Toteutusvastuuhenkilö tai -taho	Kiireellisyys (*) 1/2/3	Merkittävyys (*) 1/2/3	Työmääräarvio	Kustannusarvio	Status

Päivitetty	
Tekijä	

Tietoturvakortti

KÄYTTÖ RAJOITETTU
Suojaustaso IV
JulkL (621/1999) 24 §:n 1 mom._ 7 _k
Lain (___/____) __ §:n ___mom._____k

Tapahtumapäiväkirja

Pvm	Klo	Tietoturvatapahtumat ja toimenpiteet

Päivitetty	
Tekijä	

Liite 2: Keskeiset käsitteet

Asioiden johtamisella tarkoitetaan organisaation toiminnan ja toimintaprosessien hallintaa, suunnittelua, organisointia, kontrollointia sekä niihin liittyvää päätöksentekoa.

Ihmisten johtamisella tarkoitetaan toisten ihmisten käyttäytymiseen vaikuttamista.

Johtamisella tarkoitetaan kaikkea sitä ohjaavaa tai arvioivaa toimintaa, jota organisaatiossa tehdään sen päämäärien ja tavoitteiden täsmentämiseksi, toimintaedellytysten luomiseksi ja varsinaisen toiminnan ohjaamiseksi tavoitteiden mukaan.

Omaisuuden hallinnalla tarkoitetaan järjestelmällisiä ja koordinoituja toimenpiteitä ja käytäntöjä, joiden avulla organisaatio optimaalisesti ja kestävästi hallitsee omaisuutensa ja omaisuusjärjestelmänsä, niihin liittyvän suorituskyvyn, riskit ja kustannukset koko niiden elinkaarella organisaation strategisten tavoitteiden saavuttamiseksi.

Omaisuudenhallintajärjestelmällä tarkoitetaan organisaation omaisuuden hallinnan periaatteita, strategiaa, tavoitteita ja suunnitelmia sekä toimenpiteitä, prosesseja ja organisatorisia rakenteita niiden kehittämiseksi, toteuttamiseksi ja toimeenpanemiseksi sekä jatkuvasti parantamiseksi.

Operatiivisella johtamisella tarkoitetaan päivittäistä johtamista osasto-, yksikkö-, prosessi-, toiminto- ja henkilötasoilla.

Tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden, käytettävyyden, todennettavuuden ja kiistämättömyyden tilaa.

Tietoturvallisuuden hallinnalla tarkoitetaan toimenpiteitä ja käytäntöjä tietoturvallisuudesta huolehtimiseksi tavoitteena hyväksyttävä tietoturvallisuus.

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan sitä osaa yleisestä toimintajärjestelmästä, joka odotuksiin, tarpeisiin, vaatimuksiin ja riskien arviointiin perustuen luodaan ja toteutetaan, ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyväksyttävä tietoturvallisuus.

Tietoturvattavalla kohteella tarkoitetaan asiaa, toimintaa, omaisuutta tai ihmistä, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi tietoturvallisuusnäkökulmasta.

Tietoturvattavan kohteen hallinnalla tarkoitetaan toimenpiteitä ja käytäntöjä tietoturvattavan kohteen tietoturvallisuudesta huolehtimiseksi kohteen koko elinkaarella tavoitteena kohteen hyväksyttävä tietoturvallisuus.

Turvattavalla kohteella tarkoitetaan asiaa, toimintaa, omaisuutta tai ihmistä, joka on arvokas ja hyödyllinen, ja johon liittyy turvaamisintressi turvallisuusnäkökulmasta.

Turvattavan kohteen hallinnalla tarkoitetaan toimenpiteitä ja käytäntöjä turvattavan kohteen turvallisuudesta huolehtimiseksi kohteen koko elinkaarella tavoitteena kohteen hyväksyttävä turvallisuus.