Aki Moilanen

Tietoturvallisuuden mittaaminen julkishallinnon organisaatiossa

Opinnäytetyö
Syksy 2018
SeAMK Tekniikka
Teknologiaosaamisen johtaminen YAMK

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: Tekniikka

Tutkinto-ohjelma: Teknologiaosaamisen johtaminen YAMK

Tekijä: Aki Moilanen

Työn nimi: Tietoturvallisuuden mittaaminen julkishallinnon organisaatiossa

Ohjaaja: Alpo Anttonen

Vuosi: 2018 Sivumäärä: 106 Liitteiden lukumäärä: 2

Tämän tutkimuksen tarkoituksena oli kehittää Suomen metsäkeskuksen tietoturvallisuuden mittaamista osana tietoturvallisuuden hallintajärjestelmää. Tavoitteena oli kartoittaa, mitä tietoa tarvitaan tietoturvallisuuden hallinnan ja päätöksenteon tueksi, jotta voidaan suunnitella ja kohdentaa tarvittavia toimenpiteitä kohdeorganisaation tietoturvallisuuden varmistamiseksi. Tietotarpeiden kartoitus on vahvasti sidoksissa mittausnäkökulmiin ja menestystekijöihin sekä julkishallinnon organisaatiota ohjaavaan lainsäädäntöön. Näiden kautta oli tavoitteena tuottaa keskeinen tietoturvamittaristo.

Tutkimuksen alun teoriaosassa ja käsiteanalyyttisen tutkimusotteen avulla lähestyttiin tutkimuksen ongelmakenttää sekä tutkimuskysymyksiä ja tavoitetta, minkä kautta muodostettiin viitekehys empiriaosuudelle. Viitekehyksen muodostamisessa huomioitiin ensi sijassa normiperustaisuus, joka rakentui tietoturva-asetuksen perustason vaatimusten ja niitä tukevien Vahti-ohjeiden mukaan. Lisäksi viitekehyksen muodostamisen keskiössä oli alan kirjallisuus ja standardit, kuten tasapainotetun tuloskortin periaate ja ISO/IEC 27004:2016 -standardi, joiden mukaan määriteltiin tietoturvamittariston suunnitteluprosessi ja käyttöperiaatteet.

Tutkimuksen empiirisessä osassa käytettiin toiminta-analyyttistä tutkimusotetta, jossa kartoitettiin kohdeorganisaation keskeisiä tietotarpeita menestystekijöiden, riskiperusteisuuden ja tietoturvallisuuden perustason vaatimusten kannalta. Tietotarpeiden arvioinnin jälkeen määriteltiin mittauskohteet sekä tietoturvamittarit ja niiden käyttöperiaatteet. Tutkimuksen empiiriseen osioon kuului myös ydinjärjestelmien BIA-vaikutusanalyysien tekeminen. Siihen osallistui kohdeorganisaatiosta järjestelmien omistajat ja vastuuhenkilöt sekä edustaja tietoturvaorganisaatiosta. BIA-vaikutusanalyyseistä saadun tärkeysindeksin perusteella ydinjärjestelmät luokiteltiin kriittisyysluokkiin ja tuloksia käytetään tietoturvamittareiden ja resurssien kohdistamisessa priorisoiduille tietojärjestelmille.

Tutkimuksen tärkeimmät tulokset olivat tietoturvamittaristo ja niiden käyttöperiaatteet sekä mittariston suunnitteluprosessi. Nämä yhdessä muodostavat tietoturvallisuuden hallintajärjestelmän ylläpitoa ja päätöksentekoa tukevan mittausprosessin.

Avainsanat: tietoturvallisuus, mittaaminen, tietoturvariski, menestystekijä.

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: School of Technology

Degree programme: Master's Degree Programme in Technology Competence Management

Author: Aki Moilanen

Title of thesis: Information security measuring in a public administration organization

Supervisor: Alpo Anttonen

Year: 2018 Number of pages: 106 Number of appendices: 2

The purpose of this study was to develop the information security measuring of the Finnish Forest Centre as a part of the information security management system. The aim was to identify what kind of information is needed to support information security management and decision-making in order to be able to plan and target the measures necessary for ensuring the information security of the target organization. The mapping of information needs is strongly linked with measuring perspectives and success factors as well as the legislation governing the public administration organization, through which the aim was to produce a central security measuring system.

In the theoretical part of the study, a conceptual research method was used to approach the problem area of the research, as well as the research questions and the objective, through which a reference frame was created for the empirical part. In addition, the core of the reference framework was collected from literature and standards, such as the principles of the balanced scorecard and the ISO / IEC 27004: 2016 standard, according to which the design and operating principles of the security measuring system were defined.

In the empirical part of the study, an action-oriented research approach was used to map the most important information needs of the target organization in terms of success factors, risk inheritance and the basic level of information security. After evaluating the information needs, the measurement targets, together with the security measuring systems and their operating principles, were defined. The empirical part of the study also included making a business impact analysis (BIA) of the core systems, involving the system owners, the responsible persons from the target organization and the representative of the security organization.

The main results of the study were the security measuring system and its operating principles as well as the planning process of the measuring system, forming together a measuring process, which supports the maintenance and decision-making concerning the information security management system.

Keywords: information security, measuring, security risk, success factor.

SISÄLTÖ

Kuva- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

BIA	Toiminnan vaikutusanalyysillä (Business Impact Analysis) pyritään selvittämään ja kuvaamaan erilaisten haitallisten tekijöiden vaikutuksia tarkastelun kohteena olevaan toimintaprosessiin tai järjestelmään.
CAF	CAF (Common Assessment Framework) on EU-jäsenmaiden yhteistyönä kehitetty julkisen sektorin organisaatioiden laadunarviointimalli.
CERT	Tietoturvapoikkeamaryhmä (Computer Emergency Response Team). CERT-toiminnan päämääränä on tietojärjestelmien tietoihin kohdistuvien tietoturvaloukkauksien ja uhkien toteutumisen ennaltaehkäisy ja torjunta mahdollisimman objektiivisesti ja tehokkaasti.
EFQM	EFQM-mallin peruslähtökohta on toiminnan arviointi saavutettujen tulosten perusteella. Mallin avulla paikannetaan organisaation vahvuudet ja kehityskohteet sekä mitataan kehittymistä.
GDPR	General Data Protection Regulation (yleinen tietosuoja-asetus). Lakia on sovellettu EU-maissa 25.5.2018 alkaen.
HIP	Inhimillinen päätöksentekoprosessi (Human Information Processing) on lähestymistapa päätöksenteon tutkimukseen.
ISF	Tietoturvan kansainvälinen tutkimustalo (Information Security Forum).
ISMS	Tietoturvallisuuden hallintajärjestelmä, ISMS (Information Security Management System) on systemaattinen menetelmä ja prosessi, jolla hallitaan ja ylläpidetään organisaation tietoturvaa sekä suojataan niitä tietoja, joiden on katsottu tarvitsevan suojausta.

ISO/IEC 27000	ISO/IEC 27000 -sarja on joukko tietoturvallisuuden hallinnan parhaita käytäntöjä kuvaavia standardeja.
JulkICT	Julkisen hallinnon ICT-osasto toimii julkisen hallinnon digitalisaation edellytysten luojana ja suunnannäyttäjänä.
PDCA-malli	PDCA-malli (Plan, Do, Check, Act) on ongelman ratkaisumalli ja kehittämismenetelmä, joka on keskeisiä työkaluja jatkuvassa parantamisessa, laatujohtamisessa ja prosessinkehittämisessä.
RTO	Recovery Time Objective (RTO) tarkoittaa tavoitellun toipumisajan määrittelyä. Toipumisaika määrittelee sen ajan, sekunteina, tunteina tai päivinä, jonka kuluessa kyseessä oleva asia tai toiminto tulee saada palautettua takaisin toimintaan häiriötilanteessa.
RPO	Recovery Point Objective (RPO) tarkoittaa tavoitellun toipumispisteen määrittelyä. Toipumispiste määrittelee sen tilan, johon toiminta, tiedot tai järjestelmät tulee saada palautettua häiriön jälkeen.
SLA	Palvelutasosopimus eli SLA (Service Level Agreement) on asiakkaan ja palveluntarjoajan välinen sopimus, jossa määritellään palvelulle tietyt vaatimustasot. Sitä mitataan erityyppisillä mittareilla ja palvelutason alittamisesta seuraa yhteisesti sovittu sanktio.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä. Valtiovarainministeriön asettama ja johtama hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elin.
Valtori	Valtion tieto- ja viestintätekniikkakeskus.
VM	Valtiovarainministeriö.

1 JOHDANTO

Käytettävissä olevan tiedon määrä sekä sen merkitys organisaatioille on lisääntynyt räjähdysmäisesti. Viime vuosiin saakka ollaan toimittu tilanteessa, jossa tiedon hankinta on nähty niukkuutena ja vaivalloisena hankkia sekä päätökset ja ratkaisut on tehty suhteellisen vähäisen tiedon perusteella. Tiedon automaattisen keräämisen kautta tietomäärä on kasvanut ja niukkuus on muuttunut ylitarjonnaksi. Digitalisaation kasvaessa organisaatioilla on yhä suurempia haasteita tiedon hyödyntämisessä sekä sen tehokkaassa valjastamisessa tuotannontekijöiden ja suorituskyvyn parantamiseksi.

Julkishallinnon organisaatioiden toiminta perustuu vahvasti tietoon ja sen hyödyntämiseen. Tietojärjestelmät ja niiden sisältämät tiedot ovat keskeinen osa hallinnon toimintaa, ja hallinnon palveluita on sähköistetty ja automatisoitu laajasti. Tietoa välitetään organisaatioiden välillä yhä enemmän sähköisessä muodossa ja automatisoidut prosessit avaavat uudenlaisia näkymiä tiedon hyväksikäytölle ja kehittämiselle.

Organisaatioiden kasvanut tietopääoma ja siihen liittyvät prosessit kiinnostavat myös verkkorikollisia. Organisaatioita rasitetaan jatkuvilla tietoturvauhkilla, joiden realisoitumista pyritään poistamaan ja vähentämään ensisijaisesti proaktiivisilla, mutta viime kädessä myös reaktiivisilla keinoilla. Organisaation tietoturvallisuuden arvioinnilla ja riskienhallinnalla on merkittävä asema uhkien torjumisessa. Keskeisenä tavoitteena on tuottaa ymmärrys ja keinovalikoima riskien hallitsemiseksi. Priorisoiduilla toimenpiteillä pyritään parempaan tietoturvallisuuden hallinnan parantamiseen ja edelleen palveluiden ja tuotannontekijöiden häiriöttömään toimintaan.

1.1 Työn taustaa

Ensisijaisesti organisaation tietoturvatyön ja siihen osoitettujen resurssien tavoitteena on vähentää ja poistaa toimintaan kohdistuvia häiriöitä ja uhkatekijöitä. Toisaalta julkisen hallinnon organisaatioilla on velvollisuus huolehtia tietoturvallisuu-

destaan lainsäädännön asettamien vaatimusten mukaan, minkä osoittamiseksi organisaation tulee mm. huolehtia säännönmukaisesta tietoturvallisuuden arvioinnista. Tietoturvallisuuden strategisena kehittämistavoitteena on riskienhallintaa palvelevan tietoturvallisuuden johtamis- ja hallintajärjestelmän luominen sekä sen arvioiminen tarkoituksenomaisella tavalla.

Laki julkisen hallinnon tietohallinnon ohjauksesta (10.6.2011/634) antaa valtiovarainministeriölle ja muille ministeriöille toimivallan ohjata julkisen hallinnon tietohallintoa. Tietohallintolain tarkoituksena on tehostaa julkisen hallinnon toimintaa sekä parantaa julkisia palveluja ja niiden saatavuutta. Julkisen hallinnon yhteisestä ohjauksesta vastaa valtiovarainministeriössä toimiva JulkICT-osasto. Lisäksi julkisen hallinnon tieto- ja viestintäteknologiaa ohjaavat lait, asetukset, strategiat, linjaukset, ohjeet ja suositukset. (Tietohallinnon ohjaus 2011.)

Organisaatiot lunastavat oikeuden toimia yhteisöissä ja valtiossa lainsäädännöllisten ja yhteiskunnallisten prosessien avulla. Kansallinen ja kansainvälinen lainsäädäntö asettaa standardit organisaatioiden menettelytavoille, mutta huomionarvoista on se, että monet organisaatiot pyrkivät ylittämään lainsäädännön vähimmäisvaatimukset, jotta niiden maine säilyy ja paranee yhteiskunnallisena toimijana. (Kaplan & Norton 2004, 68.)

Valtionhallinnon tietoturvallisuuden kokonaisuutta ohjaa Valtioneuvoston periaatepäätös, jossa päätetään tietoturvallisuuden kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat tietoturvatyölle (Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009, 7-8). Kehittämisen painopisteisiin kuuluvat mm. riskienhallinnan, tietoturvallisuuden hallintajärjestelmän, mittareiden ja seurannan sekä palvelu- ja hankintaketjujen tietoturvallisuuden sekä varautumisen kokonaisvaltainen kehittäminen (Tietoturvallisuuden arviointiohje 2014, 14).

Viime vuosina julkishallinnossa on panostettu merkittävästi tietoturvatyöhön tietoturvallisuusasetuksen (2010) voimaantulon jälkeen. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) edellyttää tietoturvallisuuden perustason saavuttamista kaikilta valtionhallinnon virastoilta ja laitoksilta. Lisäksi tietoturvallisuusasetuksen tueksi annettiin VAHTI 2/2010 -ohje, jossa kuvataan tieto-

turvatasojen vaatimukset. Organisaatioiden tulee huolehtia, että käytössä on Valtiovarainministeriön VAHTI-ohjeisiin, tietoturvatasomäärityksiin ja varautumistoiminnan vaatimuksiin perustuvat suunnitelmat, ohjeet ja menettelyt, joita arvioidaan keskitetysti. (Tietoturvallisuuden arviointiohje 2014, 14.)

Tässä työssä kehitetään toimeksiantajan, Suomen metsäkeskuksen tietoturvallisuuden mittaamista. Suomen metsäkeskus on metsätaloutta palveleva ja edistävä asiantuntijatalo sekä osa julkishallintoa. Metsäkeskus tuo yhteiskunnalle ja asiakkaille lisäarvoa digitaalisin keinoin, mikä avaa yhä uusia mahdollisuuksia toimintojen automatisoinnille ja toimintamallien uudistamiselle.

Työn tavoitteena on suunnitella mittausprosessi ja mittaristo, joilla tuotetaan tietoa palvelujen taustajärjestelmistä, infrastruktuurista, käyttöympäristöstä ja toiminnasta, jota voidaan hyödyntää tietoturvallisuuden hallintajärjestelmän kehittämisessä ja tietoturvatoimintaa ohjaavassa päätöksenteossa. Työn kohdeorganisaatio esitellään tarpeellisin osin luvussa 5.

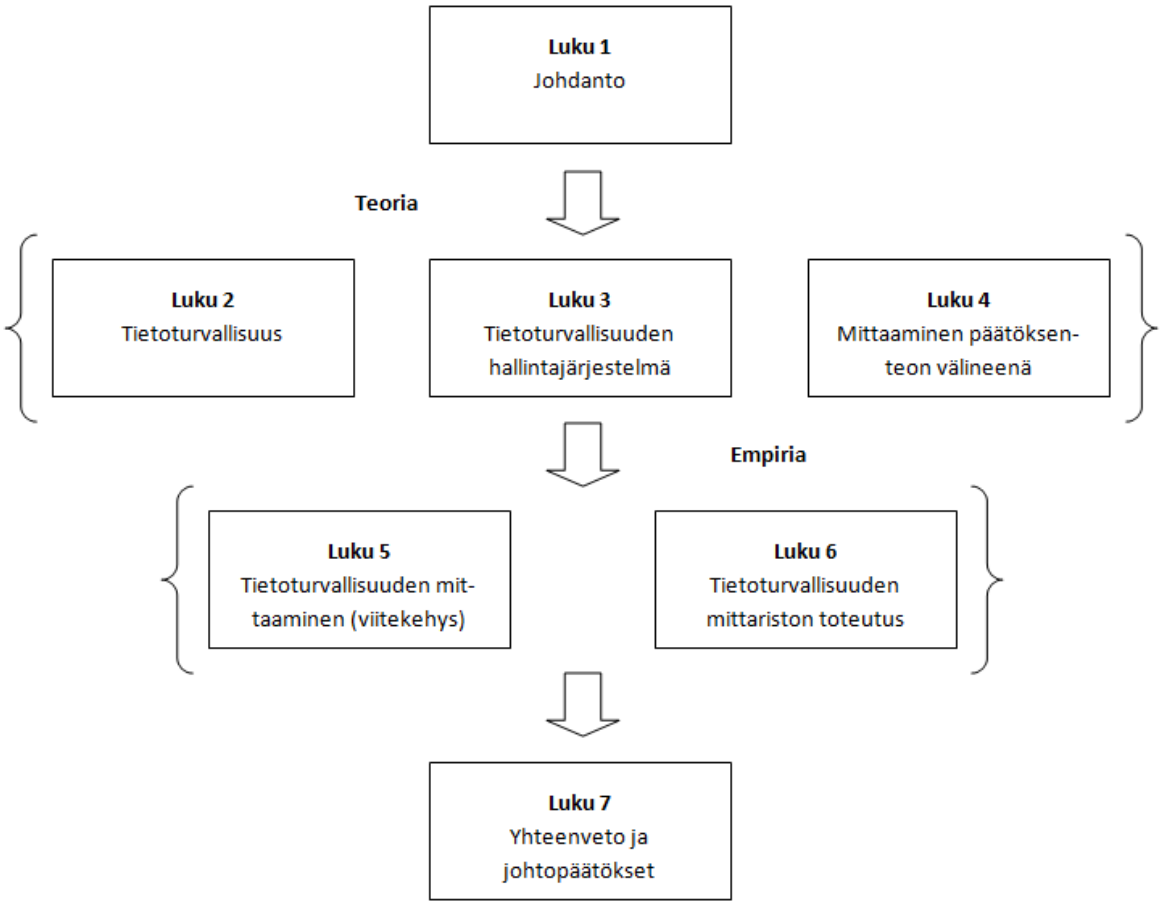
1.2 Työn rakenne

Tässä työssä noudatetaan soveltaen suunnittelutieteellisen tutkimuksen periaatteita ja rakenteita. Johdannossa (luku 1) avataan aihealuetta ja kuvaillaan työn lähtökohtaa, taustaa ja ongelmakenttää. Johdannossa esitetään myös tutkimusongelmat ja rajaukset sekä työn lähestymistapa ja metodologia. Luvuissa 2 - 3 käsitellään tietoturvallisuuteen liittyvää teoriaa, jonka lähtökohtana on tiedon ja tietoturvallisuuden hallinta sekä sen kuvaamisen prosessi, tietoturvallisuuden hallintajärjestelmä. Sen käsittely ja selittäminen on oleellista, jotta työssä saadaan riittävä ymmärrys tietoturvallisuuden mittaamisen ja ongelmanselvityksen taustoista.

Luvussa 4 käsitellään mittaamisen teoriaa ja periaatteita sekä tietoturvallisuuden mittaamisen käsitteitä ja luokittelua. Lisäksi luvussa esitetään tietoturvallisuuden mittaamiseen liittyviä haasteita ja perusteita sekä selvitetään, miksi tietoturvallisuutta mitataan.

Luvussa 5 esitetään tietoturvallisuuden mittaamisen viitekehys ja luvussa 6 työn empiirinen osuus, jossa käydään läpi tietoturvallisuuden mittariston toteuttamisen

kokonaisuus sekä BIA-vaikutusanalyysit ja niihin liittyviä keskeisiä tunnuslukuja kohdeorganisaation ydinjärjestelmistä. BIA-vaikutusanalyysien tunnuslukuja hyödynnetään tietojärjestelmien tärkeysluokittelussa ja mittariston kohdentamisessa priorisoiduille järjestelmille kriittisyyden mukaan. Empiirisen osuuden tuloksia tarkastellaan suhteessa kerättyyn teoriatietoon sekä osana diagnosointia ja kontekstin kuvaamista. Määrällisen, kvantitatiivisen aineiston avulla (esim. BIA-vaikutusanalyysit) kartoitetaan siten kohteita, joita tutkitaan laadullisen tutkimuksen keinoin yksityiskohtaisemmin. Työn viimeisenä osiona, luvussa 7, esitetään tutkimuksessa saavutetut tulokset ja johtopäätökset sekä tarkastellaan työn onnistumista suhteessa tutkimuskysymyksiin. Lopuksi pohditaan työhön liittyviä jatkotutkimusaiheita, jotka muodostavat jatkumon tietoturvamittareiden implementoinnissa tuotantokäyttöön. Kuvassa 1 on esitetty tutkimuksen rakenne.



Kuva 1. Tutkimuksen rakenne.

1.3 Viitekehys, tavoitteet ja tutkimusongelma

Julkishallinnon organisaatioiden tulee huolehtia yhteiskunnallisista velvoitteistaan, joihin kuuluu oleellisena osana tietoturvallisuudesta ja tietosuojasta sekä tietoturvallisuuden hallinnan osoitusvelvollisuudesta huolehtiminen. Tutkimuksen keskeinen teoreettinen viitekehys koostuu velvoitteista, joita julkishallinnon organisaatiolle kohdennetaan lainsäädännön ja edelleen Valtionhallinnon organisaatiolle osoitettujen Vahti-ohjeiden kautta. Pääsääntöisesti tietoturvavelvoitteet on implementoitu organisaatioiden strategiaan, politiikkaan ja tietoturvallisuuden hallintajärjestelmään, jonka arviointiin ja mittaamiseen liittyvä tarve muodostaa toisen työn toteuttamiseen liittyvän näkökulman viitekehyksen muodostamisessa. Lisäksi viitekehys rakentuu tutkimuksen alkuosan mittaamisen teorioista, joiden avulla tarkastellaan tietoturvallisuuden mittaamista päätöksenteon kannalta merkityksellisten mittareiden kehittämisessä.

Tässä työssä ensisijaisena lähtökohtana ja tavoitteena on määrittää tietoturvallisuuden mittarit sekä mittaamisen prosessi ja menettelytapa kohdeorganisaatiolle, ottaen huomioon vallitseva lainsäädäntö sekä valtionhallinnon ohjaus mm. VAHTI-ohjeistuksen kautta. Lisäksi työssä on tarve tunnistaa mitattavuuteen perustuvia työkaluja ja menettelytapoja helpottamaan tietoturvallisuuden hallintajärjestelmään kohdistuvaa ylläpitoa, päätöksentekoa ja raportointia.

Työn keskeisiä tutkimuskysymyksiä on, millä prosesseilla, menetelmillä ja välineillä kerätään ja saadaan tuotettua informaatiota ja mittausdataa tietoturvallisuuden hallintajärjestelmästä. Lisäksi tutkimusongelmana on saada esille keskeiset mittarit tukemaan päätöksentekoa yhä muuttuvassa tietoturvakentässä.

Työn keskeiset tutkimuskysymykset ovat seuraavat:

- Miten tietoturvallisuuden mittaaminen parantaa tietoturvallisuuden hallintajärjestelmän toimivuutta ja ylläpitoa sekä ymmärrystä koskien tietoturvajärjestelmiä, tietoprosesseja ja tietoturvallisuuden tilaa?
- Miksi tietoturvadataa ja -informaatiota kerätään ja mitä ovat keskeiset tietoturvamittarit ja mistä mittausprosessi muodostuu?

- Mitä tietoa mittausprosessista tuotetaan ja miten kerättyä dataa ja informaatiota organisoidaan edelleen tietämykseksi ja käytännön soveltamiseksi?

Vastauksia tutkimuskysymyksiin etsitään ensin aihetta käsittelevästä kirjallisuudesta sekä Internetdokumentaatiosta. Teoriatiedon perusteella muodostetaan syvällisempi käsitys työhön liittyvästä aihepiiristä sekä viitekehyksestä, minkä perusteella mittausprosessi ja mittarit voidaan määrittää. Ensivaiheessa mittareita tarkastellaan mahdollisimman kattavasti, jonka jälkeen valitaan keskeiset mittarit, ottaen huomioon toimintaa ohjaava lainsäädäntö, kohdeorganisaation tietoturvallisuuden hallintajärjestelmä, infrastruktuuri sekä raportointi.

1.4 Tutkimusote ja metodologia

Tutkimusote on ”kattokäsite” ja sen kautta muodostuu metodologia, jonka alapuolella ovat tutkimusmenetelmät (metodit). Tutkimusote voidaan luokitella monella tavalla. Yksinkertaisimmillaan tutkimusote eli lähestymistapa voidaan jakaa laadulliseen (kvalitatiiviseen) ja määrälliseen (kvantitatiiviseen) tapaan. Usein määrällisistä tutkimusotteesta käytetään nimitystä positivistinen tai nomoteettinen lähestymistapa. (Kananen 2017, 13.)

Hermeneuttiseen tieteenkäsitykseen perustuvien tutkimusten havainnot ovat pääasiassa laadullisia ja niiden käsittely perustuu tutkijan tulkintaan. Tiedonhankinnan piiriin kuuluu mm. vaikeasti mitattavia asiayhteyksiä, ilmiöiden syitä ja tapahtumien prosesseja. Hermeneutiikkaan perustuvia tutkimusotteita kutsutaan eri tieteenaloilla erilaisilla nimityksillä, kuten tapaustutkimus (case-tutkimus), toimintatutkimus, toiminta-analyyttinen tutkimus ja kliininen tutkimus. (Olkkonen 1993 53, 67.)

Laadulliset tutkimukset rakentuvat aiemmista tutkittavan aiheen mukaisista tutkimuksista ja muotoilluista teorioista, empiirisistä aineistoista sekä tutkijan omasta ajattelusta ja päättelystä. Määrälliset tutkimukset perustuvat teorioiden lisäksi kerätyn aineiston pohjalta saatuihin mittaustuloksiin ja tutkijan ajattelutoimintaan. Laadullinen ja määrällinen tutkimus eroavat siinä, että niiden tutkimusasetelmat ovat erilaisia, mutta tutkimusotteilla voi olla myös yhteistä pinta-alaa tutkimusken-

tällä. Esimerkiksi tapaus- ja toimintatutkimuksessa voidaan käyttää molempia tutkimusotteita ja myös monenlaisia aineistonkeruumenetelmiä. (Saaranen-Kauppinen & Puusniekka 2012, 6.)

Laadullinen tutkimus tulee esille mm. silloin, kun ilmiötä ei tunneta eli ei ole teorioita, jotka selittäisivät tutkimuksen kohteena olevaa ilmiötä. Tutkimusotteen ja siihen liittyvän menetelmän täytyy tavoittaa tutkimuskohde, mikä ohjaa tutkimusotteen valintaa ongelmalähtöiseksi. Laadullinen tutkimus nähdään toisinaan esitutkimuksen roolissa ja määrällisen tutkimuksen katsotaan olevan varsinaista tutkimusta (Kananen 2014a, 16-19.)

Nykytutkimuksessa on yleistynyt moniparadigmallisuus tai triangulaatio, joissa tutkimusotteita käytetään rinnakkain ja jonkin tutkimusotteen tai -menetelmän käyttäminen ei siten sulje pois toista (Saaranen-Kauppinen & Puusniekka 2012, 6). Tässä tutkimuksessa käytetään pääosin laadullista tutkimusotetta ja tutkimuksessa hyödynnetään aiheesta aiemmin tehtyjä aineistoja, teorioita ja viitekehyksiä. Näitä täydennetään ja kehitetään edelleen tutkijan omalla päättelyllä ja havainnoinnilla, huomioiden kohdeorganisaation toimintaympäristö osana julkishallintoa. Tutkimuksessa on myös määrällisiä elementtejä ja niiden tarkastelu ja analysointi yhdistetään siten, että määrällisen aineiston avulla kartoitetaan kohteita, joita tutkitaan yksityiskohtaisemmin laadullisen tutkimuksen keinoin.

Tämän työn tavoitteena on lisätä tietoa tietoturvallisuuden mittaamisesta ja se on lähtenyt liikkeelle käytännön työssä havaitusta tarpeesta kehittää tietoturvallisuuden hallinnan mittareita ja hallintajärjestelmän mitattavuutta. Toisaalta, työn tavoitteena on myös kartoittaa julkishallinnon organisaatiolle kohdistuvia lainsäädännön velvoitteita erityisesti tietoturva-asetuksen ja asetusta ohjaavan Vahti-ohjeistuksen kautta.

Työtä lähestytään ja tutkimuskysymyksiin kerätään aineistoa sekä laadullisen että määrällisen menetelmän kautta. Tutkimuskysymysten kautta tarkennetaan teoreettista käsittelyä ja aineiston analyysiä, tavoitteena on suhteuttaa teoreettinen ja empiirinen osio tutkimusongelmaan. Tutkimuksen empiriaosuudessa hyödynnetään teoriaosuuden tietoa käytännön ympäristössä ja kohdeorganisaation tietoturvamittariston suunnittelussa.

Määrällisen ja laadullisen tutkimusotteen keskinäistä suhdetta määritettäessä on huomioitava niiden keskinäinen riippuvuus. Numeerista tietoa ei voi täysin välttää, kun tutkitaan asioiden merkityksiä ja merkityssisältöjä ei voi kokonaan välttää, kun tahdotaan tietoa aineiston määrällisistä suhteista. Kummatkin täydentävät toisiaan ja aineistoa koottaessa kysymykset kohdistuvat enemmän tai vähemmän määrälliseen tai laadulliseen puoleen ja painotuksista riippuen siten myös käytettävät aineiston analyysimenetelmät. (Anttila 2014.)

Perinteiset tutkimukset eivät pyri muutokseen, vaan kuvaamaan, selittämään ja ymmärtämään ilmiöitä. Osa tutkimuksista pyrkii muutokseen ja poistamaan ongelmia, joihin tarvitaan toimenpiteitä. Muutokseen pyrkivistä tutkimuksista käytetään nimitystä interventionistiset tutkimukset, jotka voidaan nähdä eräänlaisena yläkäsitteenä kaikille niille tutkimusmuodoille, jotka pyrkivät muutokseen. Muutokseen pyrkiviä tutkimuksia ovat toimintatutkimus, kehittämistutkimus ja konstruktiivinen tutkimus. (Kananen 2017, 10.)

Työhön liittyvää tutkimusongelmaa ja tutkimusstrategiaa pohdittaessa nousi esille, miten laadullista ja määrällistä osiota lähestytään ja mikä osa työstä toteutetaan empiirisesti sekä millä välineillä tuotetaan tietoa. Työn alkuosa on luonteeltaan käsiteanalyyttinen, jonka teoriakehikon muodostamisessa perehdytään aikaisempiin ongelmaa sivuaviin käsitteistöihin sekä ongelmaa koskeviin teorioihin.

Käsitteiden analyysiä, erittelyä ja määrittelyä tarvitaan kaikenlaisissa tutkimuksissa ja käsiteanalyysi voi toimia pohjana empiiriselle tutkimukselle. Ei-empiirisenä tutkimusotteena se on hyödyllinen tutkimuslähestymistapa, jota kunkin tieteenalan käsitteistön ja teorian kehittämisen vuoksi on välttämätöntä tehdä. (Puusa 2008, 36.)

Tutkimuksen alun käsiteanalyyttisten piirteiden lisäksi rajattiin työtä taustatyön ja kirjallisuuden perusteella interventionistisiin tutkimusmenetelmiin sekä case- eli tapaustutkimuksen menetelmään. Tässä tutkimuksessa on piirteitä jollain muotoa kaikista mainituista interventionistisista tutkimusmenetelmistä. Näistä lähempään tarkasteluun otettiin toimintatutkimus ja toiminta-analyyttinen tutkimusote.

Seuraavana esitellään Case-tutkimuksen ja interventionististen tutkimusten periaatteet, joiden käsittelytavat johdattavat työssä valittavan menetelmän, toiminta-analyyttisen tutkimuksen käyttöön.

Tapaustutkimus (case-tutkimus). Case- eli tapaustutkimus määritellään sellaiseksi empiiriseksi tutkimukseksi, jossa monipuolista ja monilla eri tavoilla hankittua tietoa käyttäen, tutkitaan tiettyä nykyistä tapahtumaa tai toimintaa tietyssä rajatussa ympäristössä. (Anttila 2014).

Tapaustutkimus on paljon käytetty menetelmä liiketaloustieteen, hallintotieteen sekä teknisen tieteen piirissä, joiden tutkimuskohteena on usein hallinnollisia, itsenäisiä kokonaisuuksia kuten yrityksiä ja muita hallinnollisia organisaatioita. Esimerkiksi julkishallinnolliset organisaatiot ovat tapaustutkimuksen luonteva kohde. (Aaltio 2014.)

Tapaustutkimuksessa on tarkoituksena tutkia intensiivisesti esimerkiksi yksilöitä, ryhmiä, laitoksia ja yhteisöjä. Tutkimuskohteena voi olla niiden taustatekijät, ajankohtainen asema ja tilanne, ympäristötekijät ja sisäiset tai ulkoiset vaikuttavat tekijät. Yleensä kysymys on hyvin monista yhdessä vaikuttavista seikoista, joten pyrkimyksenä on saada niistä mahdollisimman kokonaisvaltainen, seikkaperäinen ja tarkka kuvaus. Case-tutkimus on hyödyllinen, kun halutaan hyvää taustainformaatiota. Intensiivisenä menetelmänä sen avulla saadaan esiin oleellisia tekijöitä, prosesseja ja vuorovaikutussuhteita, joihin muilla menetelmillä voidaan kohdistaa lisähuomiota. Case-tutkimuksia käytetään usein valmisteltaessa myöhemmin samasta aiheesta jatkotutkimuksia. (Anttila 2014.)

Tyypillisesti laadullinen tutkimus on tapaustutkimusta ja ilmiötä pyritään kuvaamaan tiiviisti. Tapaustutkimuksessa aineisto rajataan yhteen tai muutamaan tapaukseen, eikä aineistoa yhdistellä monista eri tapauksista. Tapaus voi olla esimerkiksi yhteisötason tai organisaatiotason kertakokonaisuus. Ongelmaksi tavanomaisessa laadullisessa menetelmässä muodostuu vertailut ja selitykset, joita ei saada esiin kuten määrällisissä menetelmissä. Määrällisiä menetelmiä taas vaivaa se, ettei niissä saada esiin luonnollisen kielen avulla yksilö-, yhteisö- ja organisaatiotasolla tapahtuvaa keskustelua. (Anttila 2014.)

Tapaustutkimuksesta ja toimintatutkimuksesta löytyy samoja piirteitä, mikä aiheutuu siitä, että molemmissa tutkimuksissa kohteena on yksi tapaus, joka voi olla yhteisö, yritys, osasto, henkilö tai tapahtuma. Perusero liittyy tutkijan rooliin, joka on tapaustutkimuksessa ulkopuolinen havainnoija, joka ei osallistu itse tutkittavan ilmiön toimintaan. Lisäksi tapaustutkimus ei pyri muutokseen, vaan ilmiön ymmärtämiseen ja selittämiseen. Toimenpidesuosituksia ei myöskään testata käytännössä. (Kananen 2014b, 28.)

Kehittämistutkimus. Kehittämistyöllä tai kehittämistutkimuksella tarkoitetaan tutkimuksen tuloksena ja/tai käytännön kokemuksen kautta saadun tiedon käyttämistä uusien aineiden, tuotteiden, tuotantoprosessien, menetelmien ja järjestelmien aikaansaamiseen tai olemassa olevien olennaiseen parantamiseen. Tämäntapaista tutkimusta on esimerkiksi projekteissa tapahtuva tutkimus- ja kehittämistoiminta. (Anttila 2014.)

Kehittämistutkimuksella pyritään muutokseen, se ei ole oma tutkimusotteensa, vaan se on yhdistelmä laadullista ja määrällistä tutkimusta tai pelkästään laadullista tutkimusta. Kehittämistutkimuksessa muutoksen aikaansaamiseksi kehitetään tuotetta, menetelmää, organisaatiota tms. joskin kaikki muutosten aikaansaaminen ei ole kehittämistutkimusta. (Kananen 2015, 76.)

Usein kehittämistutkimusta, kuten myös tapaustutkimusta rinnastetaan toimintatutkimukseen. Kehittämistutkimuksessa tutkijan osallistumista muutoksen läpiviemiseen ei vaadita, toisin kuin toimintatutkimuksessa, jossa tutkija on mukana muutoksessa ja osallistuu itse interventioon. (Kananen 2014b, 27-29.)

Konstruktiivinen tutkimus. Konstruktiivinen tutkimus on innovatiivisia konstruktioita tuottava metodologia, jolla pyritään ratkaisemaan reaalimaailman ongelmia ja edelleen pyritään tuottamaan kontribuutiota sille tieteenalalle, jossa sitä sovelletaan. Tutkimusotteen ydinkäsite on (uusi) konstruktio, jolla on loputon määrä mahdollisia toteutumia. Kaikki ihmisen luomat artefaktit, kuten mallit, diagrammit, suunnitelmat, organisaatiorakenteet, kaupalliset tuotteet ja tietojärjestelmämallit, ovat konstruktioita. Niille on tunnusomaista se, että ne eivät ole löydettyjä, vaan ne keksitään ja kehitetään. Kehittämällä konstruktion, joka poikkeaa kaikesta jo ole-

massa olevasta, luodaan uudenlaisia konstruktioita, jotka itsessään kehittävät uutta todellisuutta. (Lukka 2014.)

Mikä tahansa konstruktio ei täytä tieteellisen tutkimuksen vaatimuksia. Sen on kytkeydyttävä aikaisempaan teoriaan, kirjallisuuteen ja tutkimukseen aiheesta sekä ratkaisun pitää perustua uutuuteen ja sen toimivuus on osoitettava. Lisäksi teoriaan perustuvan ratkaisun toimivuus todetaan käytännössä. Konstruktivismi alkaa siitä, mihin perinteinen tutkimus loppuu. Tutkijan täytyy miettiä, millä keinoilla (interventio) ongelma saadaan poistettua. Tämän lisäksi interventio täytyy toteuttaa ja arvioida sen jälkeen onnistuminen. (Kananen 2017, 14 - 15.)

Toimintatutkimus. Toimintatutkimuksen strategiassa lähtökohtana on tieteellisyyden ja käytännöllisyyden yhdistäminen ja vaikuttaminen tapahtuu tutkijan osallistumisella tutkimuskohteen toimintaan. Vaikuttamisen ja kehittämisen perustana on tutkimus, jota tutkija tekee tutkimuskohteen ympäristössä. Tutkimusstrategiana toimintatutkimus sisältää runsaasti erilaisia näkökulmia ja sitä voidaan toteuttaa erilaisten analyysimenetelmien kautta. (Koppa 2015.)

Toimintatutkimuksella on samanlaisia lähtökohtia kuin kehittämistutkimuksella, koska siinäkin yhdistetään kehittämistyö ja tutkimus. Molemmat tutkimusotteet auttavat ihmisiä tutkimaan todellisuutta, jotta sitä voitaisiin muuttaa, ja vastaavasti auttavat muuttamaan todellisuutta, jotta sitä voitaisiin tutkia. (Johnson 2015.)

Toimintatutkimus on lähellä kehittämistutkimusta ja konstruktiivista tutkimusta. Eroavaisuudet liittyvät mm. tutkijan rooliin, joka on toimintatutkimuksessa itse mukana muutosprosessissa, mutta kehittämistutkimuksessa ei välttämättä ja konstruktiivisessa tutkimuksessa ei. (Kananen 2017, 13).

Toimintatutkimuksen tavoitteena on muutos kuten konstruktiivisessa tutkimuksessa, mutta muutoksen kohteena on usein ihmisten toiminta. Lisäksi tutkija on itse mukana toiminnassa toteuttaakseen muutosprosessia. Toiminta-, kehittämis- ja konstruktiivisten tutkimusten väliset erot ovat hyvin pieniä ja ero on lähinnä siinä, onko tutkija itse mukana muutosprosessin toteuttamisessa vai ei ja mikä suhde ratkaisulla on aihealueen teoriapohjaan. Lisäksi toimintatutkimus ei ole oma tutkimusotteensa, vaan se hyödyntää muiden tutkimusotteiden aineistonkeruu- ja analyysimenetelmiä. (Kananen 2017, 17.)

Tutkija on toimintatutkimuksessa osa tutkittavan ilmiön toimintaa ja tutkittavan yhteisön jäsen. Toinen merkittävä piirre liittyy ongelman ratkaisuun ja sen kautta tapahtuvaan muutokseen. Toimintatutkimuksen toteuttaja toimii eräänlaisena organisaation muutosagenttina ja toimenpidesuositukset testataan myös käytännössä, eli tutkimuksessa tapahtuu interventio, jota ei tapahdu tapaustutkimuksessa. Yleistäen voidaan todeta, että toimintatutkimus menee tapaustutkimusta pidemmälle ja että tapaustutkimus on osa toimintatutkimusta. (Kananen 2014b, 28.)

Toiminta-analyyttinen tutkimus. Toiminta-analyyttisessa tutkimuksessa keskeistä on tutkijan ymmärrykseen perustuvat tulkinnat sekä kohteen ja tutkijan välinen liityntä kaikissa tutkimuksen vaiheissa, tavoitteena on pyrkiä ymmärtämään kohteena olevaa ongelmaa. Yleensä toiminta-analyyttiset tutkimukset käsittelevät organisaation toimintaa, johtamista, ongelmanratkaisua, päätöksentekoprosesseja sekä kehitys- ja muutosprosesseja. (Olkkonen 1993, 72-73.)

Toiminta-analyyttisessä tutkimuksessa on tutkimuskohteina usein ilmiöitä, joista pyritään saamaan syvällistä tietoa, vaikkei ole mahdollista pelkistää tutkimusasetelmaa sellaiseksi, että saadaan suuresta tapauksien joukosta edustavaa ja mitattavin suurein ilmaistavaa aineistoa objektiivisen käsittelyn kohteeksi. Tyypillistä on myös, ettei kohteesta ole saatavissa ainakaan yksinomaan ulkoisia, neutraaleja havaintoja, joita tutkija voisi tarkastella kuin mitattavia luonnonilmiöitä. Lisäksi kohdetapauksia on vähän, eikä niiden muodostamaan aineistoon voi sen vuoksi soveltaa tilastomatemaattisia menetelmiä. Toiminta-analyyttisellä otteella saadut tulokset ovat usein uusia hypoteeseja tai teorioita, muutos- tai kehitysprosessien selityksiä tai normatiivisia ohjeita. Tuloksina voidaan myös esittää kohdeorganisaatiossa aikaansaatuja muutoksia tai niihin tähtääviä tavoitteita. (Olkkonen 1993, 52, 73.)

Toiminta-analyyttisellä tutkimusotteella saatuihin tuloksiin liittyy yleistettävyyden ongelma ja tarkasteltavaksi jää, missä määrin esiin saadut tulokset voidaan yleistää koskemaan laajempaa joukkoa. Tarkastelu voidaan tehdä esimerkiksi päättelemällä ja analysoimalla piirteitä tutkituissa tapauksissa ja laajemmassa joukossa. Toiminta-analyyttisen tutkimuksen tuloksia ei testata käytännössä, kuten esimerkiksi interventionistisissa tutkimuksissa. Usein verifiointi jää tällä tutkimusotteella

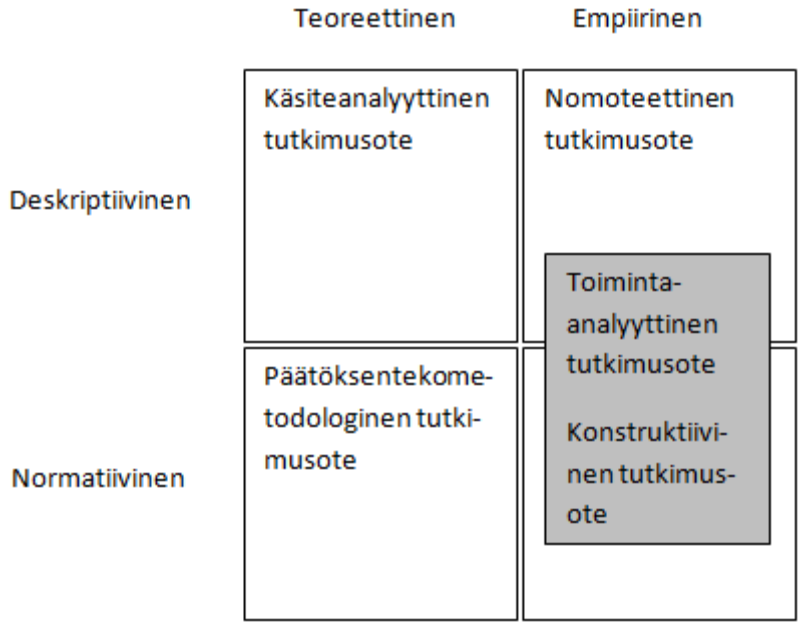
ratkaisematta ja testaus voidaan jättää myöhempien tutkimusten tehtäväksi. (Olkkonen 1993, 74.)

Neilimo ja Näsi (1980, 67) ovat kuvanneet toiminta-analyyttisen tutkimusotteen ominaispiireet seuraavasti:

- Tarkoituksena ymmärtäminen; toisinaan muuttuvia tavoitteita
- Taustana usein tarkoitusperäinen, päämäärähakuinen (teleologinen) selittäminen
- Tieteellinen toimintatiede, ihmistiede
- Empiria mukana tavallisesti harvojen kohdeyksiköiden kautta
- Ei vakiintunutta metodologista säännöstöä
- Tuloksena syntyy usein eri tasojen käsitejärjestelmiä.

Tässä työssä on piirteitä tapaustutkimuksesta sekä interventionistisistä tutkimuksista (kehittämis- ja toimintatutkimus sekä konstruktiivinen tutkimus). Tutkimuksessa ei kehitetä varsinaista uutta teoreettista mallia tai menetelmää ja tutkimusongelman ratkaisussa sovelletaan teoreettisen viitekehyksen tuottamaa tietoa.

Työssä aikaisemmin esitetty konstruktiivinen tutkimusote muistuttaa toiminta-analyyttistä tutkimusta, sillä molemmilla on kytkentää käytäntöön ja niissä on myös tapaustutkimuksen piirteitä. Toiminta-analyyttisen tutkimuksen ensisijaisena tavoitteena on ongelman ymmärrys ja mahdollisen teorian kehittäminen ja konstruktiivisessa tutkimusotteessa lähdetään puolestaan ratkaistavasta ongelmasta, jonka ratkaisuun tai ratkaisumenetelmän kehittämiseen otteessa pyritään. Konstruktiivisessa tutkimuksessa osoitetaan tulosten hyödyllisyys ja otteen käyttöön liittyy siten myös tuloksen todentaminen käytännön sovellutuksin. (Olkkonen 1993, 76.) Kuvassa 2 havainnollistetaan tutkimusotteiden keskinäistä suhdetta.



Kuva 2. Liiketaloustieteen tutkimusotteiden keskinäiset suhteet (mukailtu lähteestä Kasanen et al. 1991, 317).

Työssä on tavoitteena tuottaa mittausprosessi sekä keskeiset tietoturvamittarit kohdeorganisaation tietoturvallisuuden hallintajärjestelmän arviointiin. Mittareiden käyttöönotto ja testaaminen jäävät työn ulkopuolelle, joten osa-alue tältä osin ei ole riittävän kattavaa, jotta voidaan puhua toimintatutkimuksesta (Kananen 2014b, 28) tai konstruktiivisesta tutkimusotteesta, jossa Kanasen (2017, 16) mukaan muutossykli sisältää konstruktion toteuttamisyrityksen, jolla testataan käytäntöön soveltuvuutta (pilotti). Työn tavoitteena on kuitenkin kehittää kohdeorganisaation tietoturvallisuuden hallintajärjestelmän toimintaa, mikä tuo tutkimusotteelle selvästi konstruktiivisia piirteitä.

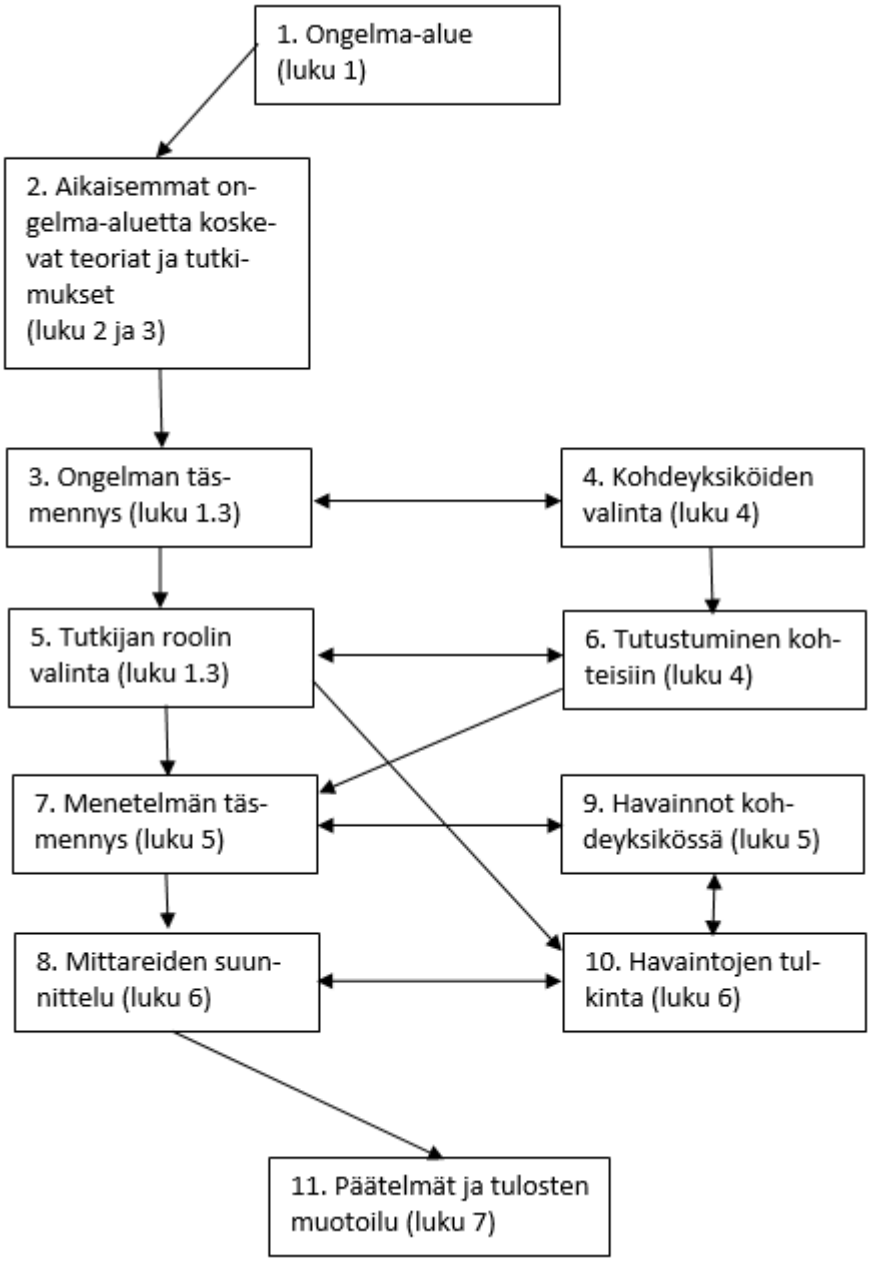
Tutkimusmenetelmäksi valittiin toiminta-analyyttinen tutkimus, sillä tutkimuksessa tutkitaan aihetta, jossa tavoitteena on muuttaa kohdeorganisaation tietoturvakäytäntöjä ja siten myös pyritään toiminnan muutokseen. Lisäksi tutkija on mukana muutoksessa ”muutosagenttina” toteuttamassa muutosprosessia, tässä tutkimuksessa osana kohdeorganisaation tietoturvallisuuden hallinnan ja hallintajärjestelmän keskeisiä rooleja. Erovaisuus toimintatutkimukseen ja konstruktiiviseen tutkimukseen liittyy mm. tutkijan rooliin ja tulosten verifiointiin, jota toiminta-analyyttisessä tutkimuksessa ei välttämättä tehdä. Ratkaisun toimivuuden testaus eli konstruktion oikeellisuuden osoittaminen jätetään siten myöhempien tutkimusten tehtäväksi ja tämän työn kohdeorganisaation osalta valittujen mittareiden ja

mittausprosessin toimivuus testataan tutkimuksen ulkopuolella osana organisaation tietoturvallisuuden hallinnan kehittämistä.

1.5 Työn etenemisen vaiheet

Työn keskeiset teemat ovat tietoturvallisuus, tietoturvallisuuden mittaaminen sekä tietoturvallisuuden hallintajärjestelmä ja sen tilasta raportointi. Mittausprosessin ja mittaamisen kohteen syvällisempi ymmärtäminen vaatii tietoturvallisuuden ja tietoturvallisuuden hallintajärjestelmän läpikäymisen sekä teorian, että kohdeorganisaation toiminnan osalta. Tietoturvallisuuden mittaaminen rajoitetaan tietoturvallisuuden hallintajärjestelmään kohdistuville keskeisille ja priorisoiduille mittareille, joiden valintaa ohjaa tietoturvallisuutta koskevan päätöksenteon tietotarpeet sekä julkishallinnon organisaatiota koskeva lainsäädäntö ja muut velvoitteet.

Tavoitteena on, että mittausprosessia voidaan jatkossa täydentää uusilla mittareilla mm. tietoteknisen infrastruktuurin kehittämisen kautta. Työssä tuotetaan ratkaisukonstruktio (mittausprosessi ja keskeinen mittaristo sekä käyttöönoton suunnittelu), mutta käyttöönotto, mahdollinen tekninen kehittäminen ja seuraavat vaiheet jäävät tutkimuksen jälkeiseen toteutukseen. Kuvassa 3 on esitetty toiminta-analyyttisen tutkimusotteen periaatteellinen rakenne ja työn etenemisen vaiheet, joissa on sekä konstruktiivisen että toiminta-analyyttisen tutkimusotteen piirteitä. Kuvassa on myös esitetty työvaiheiden luvut.



Kuva 3. Toiminta-analyyttisen tutkimusotteen periaatteellinen rakenne ja työn etenemisen vaiheet (mukailtu lähteestä Olkkonen 1993, 72).

2 TIETOTURVALLISUUS

2.1 Tiedon olemus ja tiedon turvaamisen taustaa

Organisaatioiden käsittelemällä ja ylläpitämällä tiedolla ja informaatiolla on arvoa ja merkitystä tavoitteiden toteutumisen kannalta. Toiminnan kannalta erityisen tärkeät tiedot ja asiat tulee aina määritellä huolellisesti sekä varmistaa niiden vahingoittumattomuus riskienhallintatoimenpiteillä. (Leppänen 2006, 61.)

Tieto kuuluu aina jollekin, sillä on aina kohde ja se koskee aina jotakin asiaa. Tieto voi esimerkiksi olla sähköinen informaatio tietokannassa tai se voi myös olla ajatus, joka on muodostunut työntekijän tietoisuuteen hänen työajallaan keräämän informaation pohjalta. (Leppänen 2006, 66-67.) Organisaation tiedon turvaamisessa on olennaista tiedostaa ja määritellä suojattava tieto kokonaistietomassasta.

Käsitteenä tietoturvallisuus on laaja kokonaisuus, josta on esitetty runsaasti määrittelyjä, riippuen mitä turvallisuuden osa-aluetta tarkastellaan. Tietoturvallisuuskäsitteeseen kuuluu teknisten ratkaisujen, kuten laitteiden ja ohjelmien lisäksi keskeisesti myös ihmisten toimintaan ja turvatoiminnan yleisiin järjestelyihin liittyvät turvallisuustekijät. Siten tietoturvallisuuden vaikutukset ulottuvat koko organisaatioon, kuten tuottavuuteen, taloudellisuuteen ja palvelujen laatuun. (Tietoturvallisuus ja tulosohjaus 2004, 15.)

Tietoturvallisuudella tarkoitetaan Vahdin dokumentin Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan (2007, 13) mukaan tietojen ja palvelujen sekä järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi normaali- ja poikkeusoloissa hallinnollisilla, teknisillä ja muilla toimenpiteillä. Tietoturvallisuusasetus 681/2017, 3 § 2 mom. määrittelee tietoturvallisuudella tarkoitettavan tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä.

2.2 Tietoturvapolitiikka ja tietoturvallisuuden hallintapolitiikka

Tietoturvapolitiikassa organisaation johto sitoutuu tietoturvallisuuteen ja sen toteuttamiseen. Tietoturvapolitiikassa ilmaistaan johdon tahtotila tietoturvallisuuden toteuttamiseksi ja kehittämiseksi sekä vastuut henkilöstö- ja esimiestasolla. (Johdon tietoturvaopas 2011, 18.)

Tietoturvapolitiikka toimii organisaatiota koskevien tietoturvasuunnitelmien ja ohjeiden pohjana. Sen luomista ja sisällönmuodostusta ohjaavat organisaation toiminnan tarkoitus ja strategia, riskianalyysi sekä lait ja määräykset. Standardien noudattamisessa sekä valmistautumisessa standardin mukaiseen sertifiointiin organisaation tietoturvapolitiikan on täytettävä näiden standardien vaatimukset. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 25.)

Tietoturvapolitiikka muodostaa selkärangan organisaation tietoturvallisuuden formaalille kehittämiselle. Laaksosen ym. (2006, 147) mukaan tietoturvapolitiikka ottaa yleensä kantaa seuraaviin asioihin:

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

Kansainvälisten standardisointiorganisaatioiden laatimassa ISO/IEC 27001 -standardissa (2005) tietoturvallisuuden hallintapolitiikka katsotaan tietoturvapolitiikan yläkäsitteeksi, jolloin molemmat politiikat voidaan kuvata samassa asiakirjassa. Organisaatioiden tulee standardin mukaan määrittää tietoturvallisuuden hallintapolitiikka ottaen huomioon liiketoiminnan ominaispiirteet, organisaatio, sijainti, suojattavat kohteet ja teknologia. (Andreasson & Koivisto 2013, 36.)

ISO/IEC 27001 –standardin (2005) mukaan tietoturvallisuuden hallintapolitiikan tulee:

- Sisältää puitteet tietoturvallisuuden tavoitteiden asettamiselle ja luoda yleinen suunta ja periaatteet tietoturvatoimenpiteille
- Ottaa huomioon liiketoiminnalliset sekä lakisääteiset että hallinnolliset vaatimukset ja sopimuksiin sisältyvät tietoturvavelvoitteet
- Olla yhdenmukainen niiden organisaation riskienhallinnan strategisen johtamisen puitteiden kanssa, joissa tietoturvallisuuden hallintajärjestelmä toteutetaan
- Luoda kriteerit, joita vastaan riskit arvioidaan
- Olla johdon hyväksymä.

ISO/IEC 27001 -standardin (2005) mukaan organisaation tietoturvapolitiikassa johto osoittaa sitoutumisensa tietoturvallisuuden hallintajärjestelmän luomiseen, käyttöönottoon, käyttöön, valvontaan, katselmointiin, ylläpitoon ja parantamiseen. Johdon edellytetään standardin mukaan myös sitoutuvan viestimään organisaatiolle tietoturvatavoitteiden ja tietoturvapolitiikan noudattamisen, niihin liittyvien lakisääteisten velvoitteiden noudattamisen sekä jatkuvan parantamisen tärkeydestä.

2.3 Tietoturvallisuuden osa-alueet ja hallintakeinot

Perinteisesti tietoturvallisuudella ymmärretään tiedon perusominaisuuksien, luottamuksellisuuden, eheyden ja käytettävyyden turvaamista (Laaksonen ym. 2006, 17). Tietoturvallisuus-käsitettä voidaan myös tarkastella ISO/IEC 27001 -standardin (2005) kautta, jonka mukaan edellisiin perusominaisuuksiin voi sisältyä myös muita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus. Lisäksi tietojen käytön yhteydessä puhutaan jäljitettävyydestä, tarkastettavuudesta ja tilivelvollisuudesta, joilla tarkoitetaan kaikkien tietojärjestelmissä tapahtuvien toimien kirjaamista sekä järjestelmien tietojen käytön seurantaa ja valvontaa (Tammisalo 2005, 8).

Tietoturvallisuuden johtaminen ja hallinta on luokiteltu osa-alueisiin seuraavasti:

- Hallinnollinen turvallisuus
- Tietoturvallisuuden organisointi
- Tietoaineistoturvallisuus

- Henkilöstöturvallisuus
- Fyysinen turvallisuus
- Tietoliikennepalveluiden turvallisuus
- Laitteistoturvallisuus
- Käyttöturvallisuus
- Ohjelmisto- ja ohjelmistokehityksen turvallisuus
- Jatkuvuuden ja erityistilanteiden hallinta.
  (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 23 - 78.)

Tietoturvallisuuden osa-alueet vaihtelevat sen mukaan, mitä standardia tai viitekehystä käytetään. Yleisesti sovellettavia kansainvälisiä standardeja ovat ISO27001 ja ISO27002-standardit, joiden lisäksi on esimerkiksi Internetistä saatavilla ISF:n sivustolta kansainvälisen Information Security Forumin ”Hyvien tietoturvakäytäntöjen standardi” (Information Security Forum 2016). ISO/IEC 27001 on ns. vaatimusstandardi, jonka mukaan organisaatio voi sertifioida oman toimintansa. ISO/IEC 27002 on ns. soveltamisstandardi, joka kuvaa miten ISO/IEC 27001 -standardin vaatimuksiin voidaan päästä.

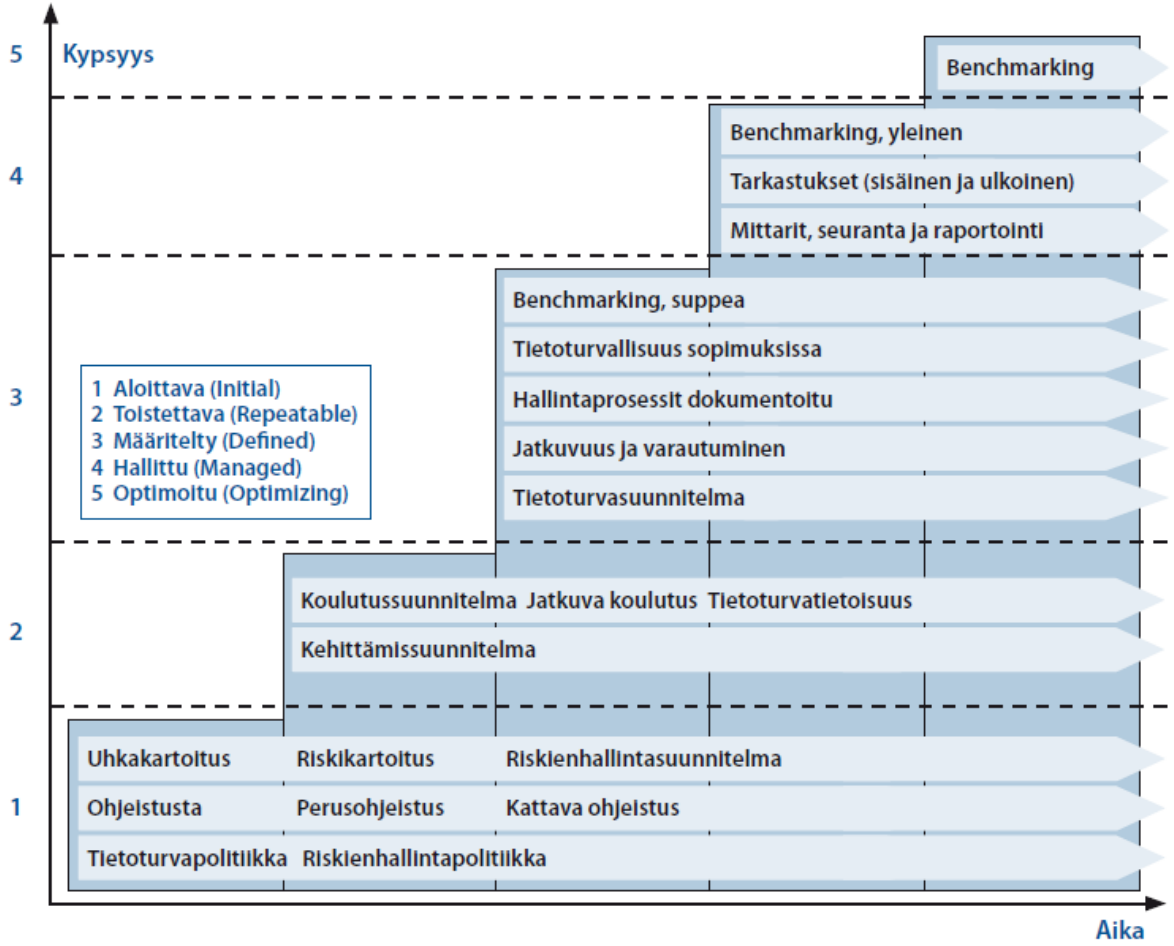
Tietoturvallisuuden osa-alueita tarkastellaan suhteessa edellä mainittuihin perusominaisuuksiin (luottamuksellisuus, eheys, käytettävyys), joilla pyritään hallitsemaan paremmin tietoturvallisuuden kokonaisuutta ja miten tietoturvallisuustoimet sijoittuvat osa-alueisiin**.** Esimerkiksi tietoturvallisuuden riskienarvioinnissa voidaan tietoturvallisuuden perusominaisuuksien avulla arvioida ja kategorisoida mitä tietoturvauhkia kohdistuu eri osa-alueisiin ja kohdistaa tarvittavia kehittämistoimenpiteitä riskien madaltamiseksi tai poistamiseksi.

2.4 Tietoturvallisuuden organisointi

Jotta tietoturvallisuus toteutuu käytännön toiminnassa, se tulee sisällyttää osaksi organisaation toimintaprosesseja. Tämä vaatii hyvää yhteistyötä tietoturvajohdolta, tietoturvallisuudesta vastaavalta operatiiviselta henkilöstöltä, palvelun omistajilta ja sen tuottajilta. Turvallisuusvaatimusten toteutumiseksi turvallisuutta lisäävät toi-

menpiteet on syytä huomioida mahdollisimman varhaisessa vaiheessa, jo prosesseja suunniteltaessa. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 37.)

Tietoturvallisuuden organisoinnissa on myös huomioitava tietoturvallisuuden kypsyystaso, joka asettaa reunaehdot turvallisten prosessien ylläpitoon ja kehittämiseen. Kypsyysmallin avulla määritetään organisaation tietoturvatoiminnan nykytila ja asetetaan sen kehittämiselle tavoitetaso, joka toteuttaa organisaation tietoturvallisuudelle linjatut vaatimukset. Kuvassa 4 on esimerkki tietoturvallisuuden kypsyysmallista, jota voidaan soveltaa tietoturvallisuuden hallintajärjestelmän kehittämisessä. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 42-43.)

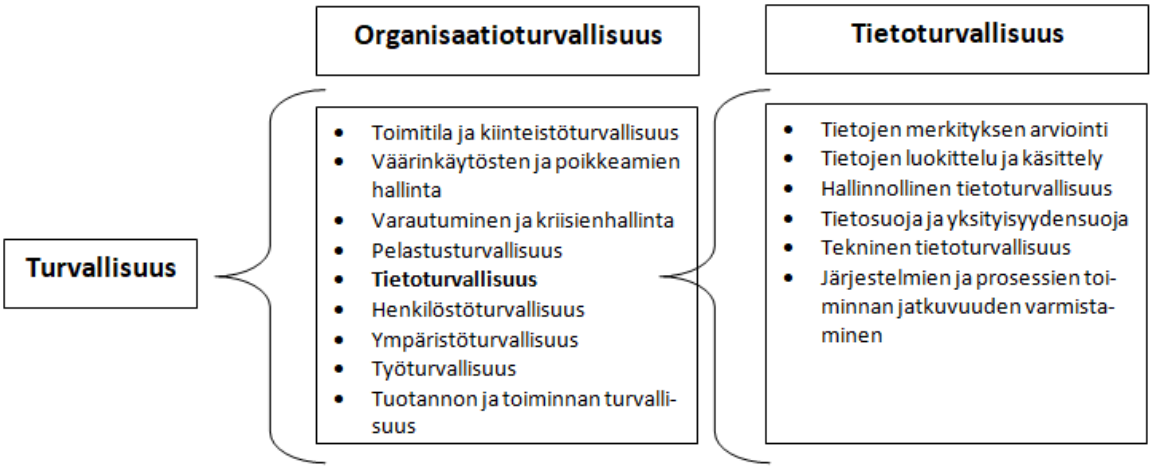


Kuva 4. Tietoturvallisuuden kypsyysmallin soveltaminen tietoturvallisuuden hallintajärjestelmän kehittämisessä. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 38).

2.5 Tietoturvallisuus osana organisaatioturvallisuutta

Turvallisuusjohtaminen sisältää kaikki osa-alueet ja toiminnot, joiden avulla varmistetaan organisaation tavoitteiden saavuttaminen ja suojattavien kohteiden vahingoittumattomuus. Perinteisiä turvallisuusjohtamisen osa-alueita ovat henkilöturvallisuus, työturvallisuus, palo- ja pelastustoiminta, tietoturvallisuus, valmiustoiminta, ympäristöturvallisuus, tuotannon ja toiminnan turvallisuus, toimitilaturvallisuus, ulkomaantoimintojen turvallisuus sekä vakuuttaminen. (Leppänen 2006, 57.)

Organisaatioturvallisuuden kokonaisuus on aina määriteltävä tapauskohtaisesti, mutta lähtökohtana voidaan pitää yleisesti tunnettuja kokonaisuuksia (Leppänen 2006, 59). Kerkon (2001, 225) mukaan tietoturvallisuuden osa-alueessa on järkevää toteuttaa yhtenäistä ja suunnitelmallista hallintajärjestelmää yksittäisten ja hajanaisten sekä usein kalliiden investointiluontoisten turvallisuusjärjestelyjen asemasta. Kuvassa 5 havainnollistetaan organisaatioturvallisuuden ja tietoturvallisuuden välistä suhdetta.



Kuva 5. Tietoturvallisuus osana organisaatioturvallisuutta (mukailtu lähteestä Elinkeinoelämän yritysturvallisuusmalli 2016, 3).

2.6 Tietoturvallisuuden johtaminen

Tietoturvallisuuden johtaminen on osa kaikkea johtamistoimintaa. Se perustuu Laaksosen ym. (2006, 117) mukaan määrätietoiseen ja organisoituun toimintaan ja johtamistapa on samanlaista kuin muissakin toiminnoissa:

- Asetetaan tavoitteet
- Määritellään vastuut
- Osoitetaan riittävät resurssit.

Johdon lisäksi jokaisen organisaatiossa työskentelevän kuuluu huolehtia tietoturvallisuudesta joko yleiseen tai erityiseen toimintavastuuseen liittyen. Organisaation tietoturvapolitiikalla johto sitouttaa organisaation toimimaan halutulla tavalla ja siinä määritellään mm. henkilöstön tietoturvavastuut, joilla varmistetaan laadukas tietojen ja tietoturvallisuuden hallinta kaikissa prosesseissa ja palveluissa.

Johto tarvitsee päätöksentekoa ja ohjaamistoimintaa varten kokonaisnäkemyksen organisaation eri tasojen toiminnasta, prosesseista, henkilöstön osaamisesta sekä toimintaan liittyvistä keskeisistä riskeistä. Tietoturvallisuuden johtaminen on järjestettävä siten, että asetetut tavoitteet ovat oikeassa suhteessa organisaation kokonaisturvallisuuteen. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 27.)

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

Tietoturvallisuuden johtamiseen on laadittu alan parhaiksi käytännöiksi kutsuttuja viitekehyksiä, malleja ja standardeja, joiden lisäksi on runsaasti dokumentteja ja muistilistoja, jotka auttavat hallitsemaan tietoturvallisuuden osa-alueiden hallinnassa. Mallien tavoitteena on tuoda määrämuotoisuutta tietoturvallisuuden hallintaan liittyviin käytäntöihin, joskin nämä apuvälineet ovat tehottomia, mikäli tietoturvallisuutta johdetaan irrallisena toimintona muusta johtamisesta. (Laaksonen ym. 2006, 115.)

2.7 Tietoriskien hallinta

Riskienhallinnan tavoitteena on mahdollistaa organisaation menestyminen, toiminnan jatkuvuus ja tavoitteiden saavuttaminen. Riskienhallinta on luonteeltaan järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan organisaation päätöksentekoa, johtamista ja kehittymistä. Vaikka riski-sanaa käytetään usein uhkan synonyyminä, se voi olla myös positiivinen asia, johon voi liittyä mahdollisuus saada hyötyä jollakin toimenpiteellä. (Ohje riskienhallintaan 2017, 11.)

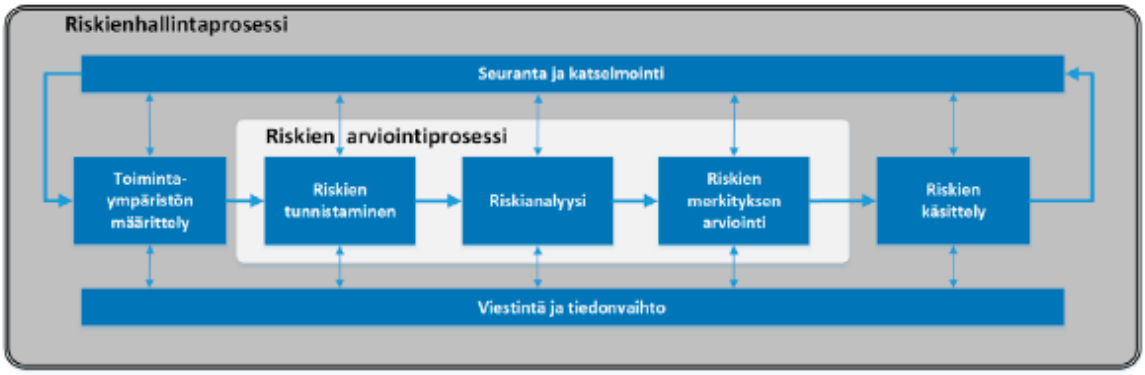
Riskienhallinta on osa organisaation johtamisen ja toiminnan prosesseja, suunnittelua ja seurantaa. Johtamista ja päätöksentekoa varten tarvitaan ajantasainen, oikea ja riittävän kattava käsitys riskeistä sekä organisoitu riskienhallinnan vastuut ja seurantajärjestelmä. Kuvassa 6 havainnollistetaan riskienhallinnan kokonaisuus ja viitekehys. Huomioitavaa on, että johtamisen ohella riskienhallinta koskee organisaation koko henkilöstöä esimerkiksi poikkeavien havaintojen ilmoittamismenettelynä. (Ohje riskienhallintaan 2017, 11.)

Kuva 6. Riskien hallinnan kokonaisuus ja viitekehys (Ohje riskienhallintaan 2017, 12).

Riskienhallinnan perustan muodostaa riskianalyysi, jonka perusteella pyritään selvittämään mahdollisimman kattavasti ne toimet, joilla uhkia ja mahdollisuuksia hallitaan. Pääsääntöisesti riskienhallintaan liittyy epävarmuuden huomioon ottaminen, mikä on usein uhka tai vaara, josta voi seurata jotakin negatiivista tai toiminnan

kannalta epäedullista. Toisaalta se voi myös tarkoittaa positiivista mahdollisuutta ja onnistumisen kautta tulevaa hyötyä tai etua, mikäli saadaan minimoitua tai vältätettyä epävarmuustekijät. (Ohje riskienhallintaan 2017, 11 - 12.)

Riskien hallintaprosessi on keskeinen osa organisaation tietoturvallisuuden hallintajärjestelmää. Kuvassa 7 esitetään riskien arviointi- ja hallintaprosessi, joka havainnollistaa riskien hallintajärjestelmää sekä organisaation tietoriskien arviointi- ja hallintatoimia.



Kuva 7. Riskienhallintaprosessi (Ohje riskienhallintaan 2017, 18).

Riskienhallinnalla pyritään pääsääntöisesti hallitsemaan epävarmuuksien vaikutuksia organisaation toimintaan. On tunnistettu, että täydellinen hallinta on mahdotonta, minkä vuoksi organisaation tai toiminnon on määriteltävä joko tietoisesti tai tiedostamattaan oma riskienhallinnan taso ja siihen tarvittavat resurssit**.** Hallintatoimenpiteiden toteuttamisen kustannuksien ja vaikutuksien tulee olla mitattavissa, jotta voidaan tuottaa havaittavissa olevaa lisäarvoa organisaation toiminnalle. (Ohje riskienhallintaan 2017, 14.)

2.8 Toiminnan vaikutusanalyysi (BIA)

Toiminnan vaikutusanalyysillä (Business Impact Analysis) pyritään selvittämään ja kuvaamaan erilaisten haitallisten tekijöiden vaikutuksia tarkastelun kohteena olevaan toimintaprosessiin tai järjestelmään. Vaikutusanalyysiä voi käyttää työkaluna ja pohjana mm. toiminnan jatkuvuutta uhkaavien riskien arvioinnille sekä toimintojen väliselle priorisoinnille ja niiden välisten riippuvuuksien tunnistamiselle. (Toiminnan jatkuvuuden hallinta 2016, 24.) Esimerkiksi Valtiovarainministeriön tuotta-

malla vaikutusanalyysi -työkalulla voidaan selvittää ja arvioida tietoturvan merkitystä ja erilaisten häiriöiden, kuten käyttökatkosten, tietojen menetyksen tai päivittymättömyyden vaikutuksia tarkasteltavana olevaan kohteeseen (Vaikutusanalyysi (BIA, Business Impact Analysis) käyttäjän ohje 2016, 3).

Toimenpiteenä BIA-vaikutusanalyysissä kerätään tietoa toimintaympäristöstä haastattelemalla toiminnasta tai järjestelmästä vastaavia henkilöitä ja käymällä läpi dokumentaatiota. Keskeistä on kyseisen toiminnan tai järjestelmän tuntemus, jolloin vaikutusanalyysiin ja arviointiin saadaan mahdollisimman yksityiskohtaista tietoa tarkasteltavasta kohteesta. Näin saadaan kartoitettua erilaisten riskien toteutumisen vaikutuksia ja voidaan valita oikeat ja riittävät jatkotoimenpiteet. (Toiminnan jatkuvuuden hallinta 2016, 44.) Lisäksi analyysin avulla voidaan luokitella tarkasteltavat kohteet tärkeysindeksin mukaan. Indeksilukua voidaan käyttää esimerkiksi eri järjestelmien keskinäisen tärkeyden vertaamiseen ja tehdä priorisointia järjestelmien välillä. (Vaikutusanalyysi (BIA, Business Impact Analysis) käyttäjän ohje 2016, 16-17).

Vaikutusanalyysiin sisältyvien tekijöiden vertaaminen keskenään on haasteellista, joten analyysiä helpottamaan ja kriittisyysluokan arviointia edesauttamaan on kehitetty erilaisia työkaluja ja malleja. Valtionhallinnon vaikutusanalyysien tekemiseen on laadittu mm. BIA-vaikutusanalyysityökalu, joka on kehitetty ja toteutettu Valtion tieto- ja viestintätekniikkakeskuksen Valtorin toimesta valtionhallinnon korotetun tietoturvatason ja varautumisen yhteishankkeen (KoTVa) aikana. Työkalu on tarkoitettu järjestelmään tai palveluun kohdistuvien häiriöiden vaikutusten arviointiin.

Tässä työssä on käytetty BIA-vaikutusanalyysityökalua kohdeorganisaation ydinjärjestelmien arvioimiseen ja tärkeysluokitteluun. Vaikutusanalyysin raportin yhteenveto-osuudessa saadaan tuloksena mm. ydinjärjestelmien tärkeysindeksit, joiden mukaan järjestelmät voidaan tärkeysluokitella sekä suunnitella ja resursoida tietoturvallisuuden mittaaminen tärkeysluokan mukaan. Jäljempänä työtä (luku 6.5) esitetään BIA-vaikutusanalyysin prosessi, osallistujat sekä tulokset ja johtopäätökset. BIA-vaikutusanalyysityökalun rinnalla käytetään samassa yhteydessä tuotettua täyttöohjetta, joka on jäsennelty BIA-työkalun mukaisesti kuuteen pääkohtaan. Liitteessä 2 on BIA-vaikutusanalyysityökalun täyttöpohja.

2.9 Lainsäädäntö ja normiohjaus

Tietoturvallisuuden tarkoituksena on luoda hallinnon asiakkaisiin luottamus hallinnon toimivuuteen ja sillä on sidos kaikkiin viranomaisten tietojenkäsittelyä koskeviin säädöksiin. Tietoturvallisuus on yksi niistä elementeistä, joilla mahdollistetaan viranomaisen lainmukainen toiminta tietojenkäsittelyn yhteydessä. Lisäksi se voidaan nähdä oleellisena osana palvelujen ja toiminnan piirteitä ja ominaisuuksia, joilla täytetään asetetut ja odotetut tarpeet. Voidaan todeta, että tietoturvallisuus on siten keskeinen viranomaistoimintojen laatuvaatimus. (Voutilainen, 2012, 125.)

Tietoturvallisuus on valtionhallinnossa voimakkaassa muutostilassa. Pääosin muutos johtuu yhteiskunnan keskeisten toimintojen ja tarjottavien palvelujen sähköistymisestä sekä kasvavasta tietoteknisestä riippuvuudesta. Lisäksi organisaatiot joutuvat varautumaan yhä runsastuviin ja moninaisimpiin turvallisuusuhkiin, jotka kohdentuvat tietoverkkoihin, tietojärjestelmiin, organisaatioiden arkaluontoisiin tietoihin sekä avainhenkilöihin ja asiakkaisiin. (Johdon tietoturvaopas 2011, 15.)

Valtionhallinnossa toteutetaan pääosin normiperustaista tietoturvallisuuden ohjausta, jossa organisaatiot ottavat huomioon lainsäädännön velvoitteet ja tietoturvatoiminnan perusteet. Keskeisiä hallinnan toteuttamisen välineitä ovat standardit, hallintamallit ja suositukset. Niiden avulla valtionhallinto pyrkii saamaan organisaatiot toimimaan tietyllä tavalla tai vaihtoehtoisesti estämään ei-haluttua toimintaa. Lisäksi on huomioitava ohjeet sekä organisaatiota sitovat sopimusvelvoitteet. Entistä tärkeämpiä ovat myös organisaation ydintoiminnan asettamat toiminnan jatkuvuuteen ja tiedon turvaamiseen liittyvät vaatimukset, joiden merkitys korostuu yhteiskunnan palveluiden sähköistyessä. Kuvassa 8 havainnollistetaan lainsäädännön ja normiohjauksen sekä ohjeiden ja velvoitteiden keskinäisiä suhteita organisaation tietoturvallisuuden hallinnassa. (Teknisen ICT-ympäristön tietoturvataso-ohje, 2012, 12.)

Kuva 8. Lainsäädäntö ja normiohjaus tietoturvallisuuden hallinnassa. (Teknisen ICT-ympäristön tietoturvataso-ohje 2012, 12).

Organisaation tulee varmistaa, että on tunnistettu sitä koskeva tietoturvallisuuden lainsäädäntö sekä sille asetetut tietoturvavelvoitteet, joista keskeisiä ovat tietotur-va-asetuksen ja sen perusteella annetut tietoturvatasojen vaatimukset (Johdon tietoturvaopas 2011, 15).

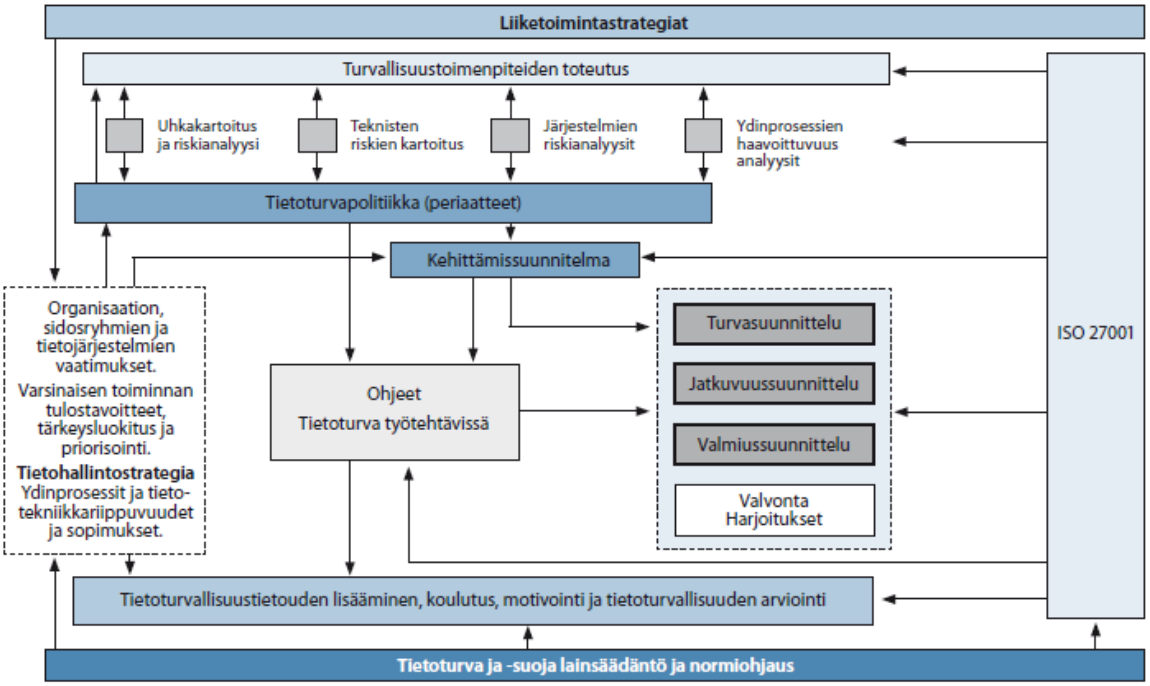
3 TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

3.1 Hallintajärjestelmän tavoitteet

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

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

Ajan tasalla oleva tietoturvapolitiikka ja siihen liittyvät asiakirjat sekä säännöllinen tietoriskien hallinta ovat tietoturvallisuuden hallintajärjestelmän olennaisimmat osat. Tietoturvastrategia ja -suunnitelmat laaditaan näiden pohjalta, mikä edelleen mahdollistaa tietoturvavaatimusten mukaiset tietoturvaratkaisut. Tietoturvallisuuden hallintajärjestelmä sisältää tietoturvatoiminnan säännöllisen mittaamisen, jolla arvioidaan mm. tietoturvatoiminnan tehokkuutta ja tarkoituksenmukaisuutta. Kuvassa 9 esitetään tietoturvallisuuden hallintajärjestelmän malli. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 42.)



Kuva 9. Tietoturvallisuuden hallintajärjestelmän malli. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 41).

3.2 Tietoturvallisuuden hallintaprosessi

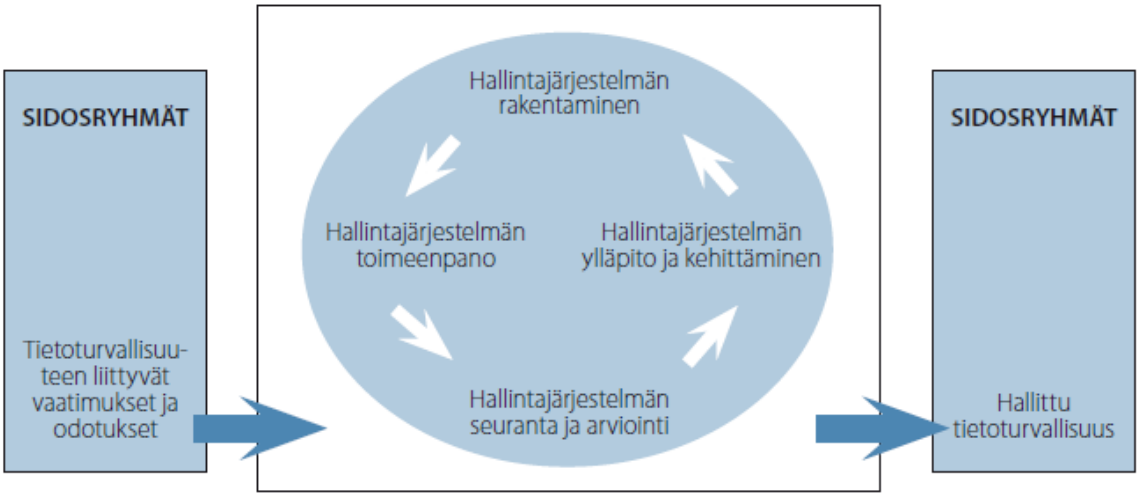
Tietoturvallisuuden hallinnan kehittämisessä voidaan käyttää apuna erilaisia kypsyysmalleja, joiden avulla voidaan määrittää tietoturvatoiminnan nykytila sekä asettaa kehittämiselle tavoitetaso (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 38, 42). Organisaatio voi myös sitoutua noudattamaan tietoturvallisuuden kehittämisessä tietoturvastandardien kuvaamia prosessimalleja.

ISO/IEC 27001 -tietoturvastandardin mukaisessa kehittämisen PDCA (Plan, Do, Check, Act) -prosessimallissa tehtävät voidaan jakaa neljään osaan:

1. Suunnittelu ja rakentaminen (Plan), jossa prosessi käynnistetään, tehdään liiketoimintavaikutus- ja riskianalyysit sekä muodostetaan niiden pohjalta jatkuvuusstrategia.
2. Toimeenpano ja noudattaminen (Do), jossa suunnitellut ratkaisut toteutetaan ja aloitetaan koulutus.
3. Seuranta ja arviointi (Check), jossa prosessin tilasta tuotetaan tietoa valvonnan, testauksen, katselmointien, auditointien ja raportoinnin avulla.

4. Ylläpito ja kehittäminen (Act), jossa ratkaisuja parannetaan kerättyjen tietojen perusteella.
   (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 38.)

Kuvassa 10 esitetään tietoturvallisuuden hallintaprosessi, joka kuvaa tietoturvallisuuden hallintajärjestelmän kehittämisen ja ylläpitämisen prosessin sekä olennaisin osin myös tietoturvallisuuden johtamisjärjestelmän. Tavoitteena on saavuttaa ja ylläpitää hallittu tietoturvakokonaisuus, joka mahdollistaa organisaation tavoitteiden toteutumisen sekä toiminnan luotettavuuden. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 39.)



Kuva 10. Tietoturvallisuuden hallintaprosessi. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 39).

Tietoturvallisuuden tavoitetason saavuttaminen tarkoittaa yleensä monivuotista kehityshanketta, jonka tavoitteet on kuvattu talous- ja toimintasuunnitelmissa, jaoteltuna useammalle vuodelle. Hanke on syytä osittaa niin, että vuositasolla kehitystoiminnalle voidaan asettaa mitattavat tavoitteet sekä osoittaa tarvittavat resurssit, jotta tavoitteet voidaan saavuttaa. (Tietoturvallisuudella tuloksia/yleisohje tietoturvallisuuden johtamiseen ja hallintaan 2007, 42.)

4 MITTAAMINEN PÄÄTÖKSENTEON VÄLINEENÄ

4.1 Mittaamisen perusteet

Mittari (engl. measure) tarkoittaa Lönnqvistin ja Mettäsen (2003, 31) mukaan täsmällisesti määriteltyä menetelmää, jonka avulla kuvataan tietyn menestystekijän suorituskykyä. Saaren (2006, 38) mukaan mittarilla tarkoitetaan niitä sääntöjä, joiden mukaisesti mittauksen kohteen jollekin ominaisuudelle määritetään sitä kuvaava mittaluku. Toisinaan mittarista voidaan käyttää termiä tunnusluku ja myös muita synonyymejä käytetään läpi mittausprosessin, kuten mittaamisen kohteella, mittaukseen valitulla mittarilla ja mittaustuloksella. Vakiintuneen käytännön mukaan tunnusluvulla voidaan liiketoiminnassa tarkoittaa sekä mittaria että sen tuottamaa mittalukua. (Saari 2006, 37.)

Perussuureiden mittaamiseen käytetään mittayksiköitä, jotka on sovittu kansainvälisessä SI-järjestelmässä. Termiä mitta käytetään myös toiminnan ohjauksessa, missä se tarkoittaa mittaamiseen valittua mittayksikköä tai sitä kaavamuotoilua, jota mittaamisessa käytetään. (Saari 2006, 38.) Kuvassa 11 esitetään yhteenveto mittauksessa käytetyistä synonyymeistä.

Kuva 11. Mittaustermien synonyymejä (Mukailtu lähteestä Saari 2006, 38).

Tieteellisesti pätevällä mittarilla on tietyt vaatimukset. Mittarin määrittäminen lähtee siitä, että ensin määritellään asia tai ilmiö, jota halutaan mitata. Tämä edellyttää ilmiön täsmällistä käsitteellistämistä. Seuraavaksi määritellään konkreettinen mittari. Tutkittava ilmiö on siis operationalisoitava, eli käsitteet määritellään sellaisiksi analyyttisiksi käsitteiksi, joita voidaan mitata. Mittari voidaan kehittää itse, mutta usein voidaan myös käyttää valmiita mittareita. Niiden käytössä on erityisen tärkeää selvittää, mitä se tarkkaan ottaen mittaa ja mikä on ollut alkuperäinen kohderyhmä. (KvantiMOTV menetelmätietovaranto 2003.)

Mittaristo (engl. measurement system) on laajempi kokonaisuus ja käsite, joka muodostuu mittauskohteen kannalta keskeisistä mittareista. Se voi esimerkiksi olla kokoelma mittareita, mikä on kehittynyt, kun siihen on lisätty uusia mittareita. Lisäksi mittaristo voi olla jonkin mittaristomallin tai -viitekehyksen mukaan systemaattisesti rakennettu. Hyvän mittariston tulee olla kattava kokonaisuus, joka on käyttökelpoinen johdon päätöksenteossa. (Lönnqvist & Mettänen 2003. 31.)

Tunnusluvut tuotetaan yleensä mittaamalla ja usein myös arvioimalla. Ohjaustarpeita varten toiminnan mittaaminen on paras tapa saada tietoa ohjattavasta kohteesta. Tunnuslukujen teoria on pitkälle mittaamisen teoriaa ja Saaren (2001, 40) mukaan mittaamisessa voidaan määritellä kolme vaihetta:

1. Mittarin määrittely eli sen merkityksen kertominen
2. Mittarin valinta tai kaavan muotoilu
3. Mittaaminen eli mittaustulosten tuottaminen.

Mittaamisella tähdätään asian tai tekijän kuvaamiseen tunnusluvulla tai laadullisella määreellä. Tekijöille voidaan määritellä siten objektiivisia tai subjektiivisia määrällisiä mittareita/tunnuslukuja tai laadullisia kuvauksia ja arvioita kohteesta. Mittaamista suunniteltaessa on hyvä esittää kysymykset miksi, ketä varten, mitä ja miten mitataan. Mittauksen tarkoitus on kuvata rajatutut piirteet näkymästä, jonka tavoitteena on mahdollisimman realistinen kuva kohteesta. Hyvien mittareiden tulisi luoda selittävyyttä ja läpinäkyvyyttä organisaation menestymiseen ja johtaa siten toimintaan ja päätöksentekoon. (Aineettoman pääoman johtaminen 2004, 33.)

Mittareita voidaan luokitella monella eri tavalla. Lönnqvist ja Mettänen (2003, 31-34) ovat määritelleet keskeiset tavat mittareiden luokittelussa seuraavasti:

- Taloudelliset/ei-taloudelliset mittarit
- Kovat/pehmeät mittarit
- Objektiiviset/subjektiiviset mittarit
- Suorat/epäsuorat (välilliset) mittarit.

Hyvän mittarin tulee Lönnqvistin ja Mettäsen (2003, 34) mukaan täyttää mahdollisimman hyvin seuraavia mittausteoreettisia ominaisuuksia:

- Validiteetti kuvaa mittarin kykyä mitata sitä menestystekijää, jota on tarkoitus mitata.
- Reliabiliteetti kuvaa mittarin arvon satunnaisvirhettä; reliaabelin mittarin tulokset eivät vaihtele satunnaisesti, vaan ne ovat johdonmukaisia.
- Relevanssi kuvaa sitä, onko mittari olennainen sen käyttäjän kannalta.
- Käytännöllisyys kuvaa mittarin kustannustehokkuutta eli hyöty-vaivasuhdetta.

Mittarin validiteetti ja reliabiliteetti ovat erityyppisiä ongelmia kuin relevanssi ja käytännöllisyys. Kaksi ensimmäistä ongelmaa voivat olla vaikeasti havaittavissa ja poistettavissa, kun taas kaksi jälkimmäistä suhteutetaan johdon kokemaan mittaustarpeeseen sekä mittarin hyötyihin ja haittoihin eli johto voi itse päättää sen tarkoituksiin sopivista mittareista. (Lönnqvist & Mettänen 2003, 36.)

Hyvä mittaaminen edellyttää hyvin perusteltua teoriaa, huolellista käsitteiden määrittelyä sekä niihin perustuvaa täsmällistä mallinnusta. Saari (2006, 30) esittää päättelyketjun oleelliset vaatimukset seuraavasti:

1. Ilmiön kuvaaminen
2. Käsitteellistäminen eli ilmiön kuvaaminen käsitteiden avulla
3. Ilmiön mallintaminen
4. Mittauksen toteuttaminen
5. Mittaustulosten analysointi ja vertailu
6. Johtopäätökset.

Mittausprosessista kertyvän tiedon kerääminen ja työn organisointi on huomioitava. Seurantajärjestelmän tulee kehittyä, kun kokemusta karttuu riittävästi mittareiden soveltuvuudesta kohteeseen. Toisaalta mittareita ei ole hyvä muuttaa jatkuvasti, sillä johdonmukaista tulosten aikasarjaa seuraten muutoksien kehittymistä voidaan selittää. Mittareita tulee siten sekä analysoida että testata säännöllisesti. (Aineettoman pääoman johtaminen 2004, 36-37.)

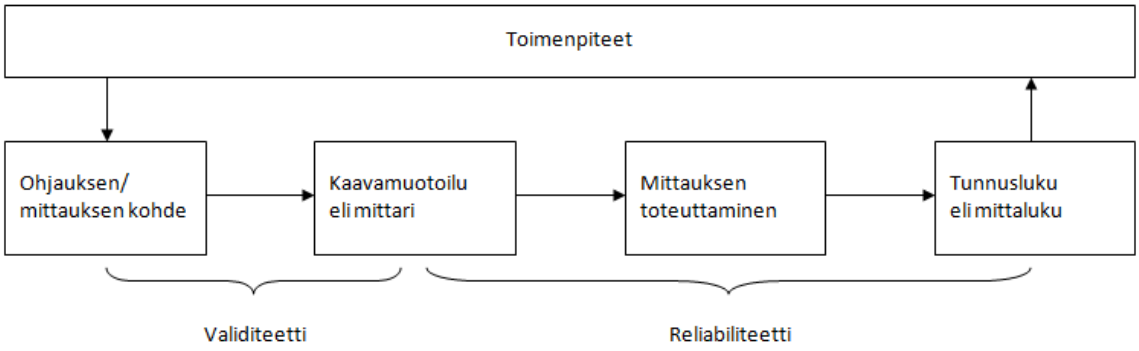
Seuraavassa on kuvattu mittareiden ja järjestelmän soveltuvuuden testaus ja kehittäminen:

- Mittaako mittari haluttua asiaa; tunnistetaanko mittarin avulla haluttua toimintaa, kehitystä tai tulosta.
- Voidaanko mittarin tuloksissa tapahtuneita muutoksia selittää; ovatko muutokset loogisia toimintaan nähden ja mikä niihin on vaikuttanut, voidaanko mittareiden välillä tunnistaa linkkejä ja vaikutusta toisiinsa.
- Voidaanko toimintaa suunnata tulosten mukaan ja tehdä päätöksiä; resurssien ja toimintavaihtoehtojen priorisointi, tavoitteiden asettaminen ja palkitseminen, aineettomien investointien ja kulujen erottaminen.
- Mitä seurantajärjestelmältä odotetaan; mitä tavoitellaan ja mihin pyritään seuraavaksi.
  (Aineettoman pääoman johtaminen 2004, 36-37.)

4.2 Mittaaminen osana johtamista ja päätöksentekoa

Mittaaminen on oleellinen keino ilmiöiden ymmärtämiseen ja selittämiseen. Mittaamisen avulla saadaan tietoa, joka johtaa ilmiön parempaan ymmärtämiseen ja sitä kautta myös ilmiön parempaan hallintaan tai sen huomioon ottamiseen päätöksenteossa. (Saari 2006, 33.)

Mittaaminen on tärkeä johtamisen väline, jonka ominaisuuksia voidaan parantaa ja kehittää, mikäli tarpeet on tunnistettu hyvin. (Saari 2006, 41). Kuva 12 havainnollistaa tunnuslukujen tuottamista ja niiden käyttöä ohjauksessa.



Kuva 12. Tunnuslukuohjauksen periaate (mukailtu lähteestä Saari 2006, 41).

Mittaamiseen perustuvia johtamisen ja päätöksenteon välineitä pidetään yleisesti tuloksekkaan johtamisen ehtona. Mittaaminen voi Saaren (2006, 35) mukaan tuottaa hyötyjä ja siten parantaa päätöksentekoa useilla osa-alueilla:

- Mittaaminen parantaa kommunikaatiota eri osapuolten välillä ja tekee mahdolliseksi yhteisen ymmärryksen kohdeasiasta.
- Mittaamisen avulla voidaan tunnistaa parannustarpeita.
- Mittaamisen avulla voidaan ymmärtää ongelmia paremmin.
- Mittaamisen avulla voidaan arvioida vaihtoehtoja.
- Mittaamisen avulla voidaan seurata etenemistä kohti tavoitetta.
- Mittaamisen avulla voidaan kvantifioida ja raportoida aikaansaadut tulokset ja muutokset.

Mittareille asetettavat vaatimukset perustuvat siihen, miten käyttökelpoisia ne ovat organisaation johdon päätöksenteolle. Päätöksenteko voidaan jakaa Laitisen (2003, 147) mukaan karkeasti kolmeen vaiheeseen:

1. Tietojen eli mittaustulosten tuottaminen ja niiden syöttäminen edelleen päätöksentekojärjestelmään.
2. Tietojen eli mittaustulosten painottaminen ja hyväksikäyttö päätöstä tehtäessä (inhimillinen päätöksentekojärjestelmä, Human Information Processing, HIP).
3. Päätös, josta seuraa tietyt tulemat (päätöksen arvo).

Seurannan tarkoitus määrittelee myös, mitä asioita organisaation tulee mitata. Johtamisen tavoitteiden ja tarkoituksen määrittämisen kautta organisaatio voi kohdentaa resursseja oikeisiin kohteisiin seuraavasti:

<u>Strateginen johtaminen ja päätöksenteko</u>

- Strategian toteuttamiseen tarvittavien resurssien varmistaminen ja kohdentaminen
- Strategian muuntaminen seurattaviksi toimenpiteiksi
- Tavoitteiden viestiminen ja strategian käytäntöön vieminen
- Strategian toteutuminen; tavoitteiden ja niiden saavuttamisen todentaminen, tulosten ja kehitystrendien tuottaminen. (Aineettoman pääoman johtaminen (2004, 34.)

Suoritusten seuranta

- Tuottavuuden ja tuloksellisuuden arviointi. (Aineettoman pääoman johtaminen (2004, 34.)

Prosessien ja toimintatapojen kehittäminen

- Toimintatapojen ja prosessien jatkuva parantaminen sekä organisointi
- Tieto organisaation toimintaperiaatteista ja vaikuttajista toiminnanohjaukseen ja päätöksentekoon. (Aineettoman pääoman johtaminen (2004, 34.)

Osaamisen kehittäminen

- Strategisen osaamisen vahvistaminen
- Osaamisten kehittymisen seuranta. (Aineettoman pääoman johtaminen (2004, 34.)

Sisäinen viestintä ja toimintatavat

- Kannusteiden kytkentä toiminnanseurantaan ja henkilöstön arviointiin
- Motivointi korostamalla mitattavaa asiaa, johon työntekijä näkee tehtävänsä kautta vaikuttavan; tiimien ja yksilötason tavoitteet. (Aineettoman pääoman johtaminen (2004, 34.)

Sidosryhmäviestintä

- Tuloksentekokyvyn, riskien ja arvonmuodostuksen kannalta kriittisten tekijöiden ja tulosten johdonmukainen raportointi sidosryhmille.
- Sidosryhmän tarpeiden ja odotusten täyttyminen; päätöksentekoon ja tyytyväisyyteen vaikuttavien tekijöiden ja toiminnan arviointi. (Aineettoman pääoman johtaminen (2004, 34.)

Muutostilanteiden hallinta; liiketoiminnan laajentaminen, yritysjärjestelyt

- Aineettoman pääoman varmistaminen ja arvottaminen muutostilanteessa. (Aineettoman pääoman johtaminen 2004, 34.)

Mittareiden muotoa määrittelee myös mittaamisen käyttötarkoitus. Tuleekin tiedostaa, valitaanko mittari esimerkiksi suoritusten seurannan vai toiminnan ohjauksen tarkoituksessa. Suoritusten seuranta mittaa toiminnan tehokkuutta ja suoritusky-

kyä tulosten määränä, laatuna ja aikana sekä resurssien hyödyntämistä arvioimalla niiden käyttöä ja tuloksia suhteessa panostuksiin. Toiminnan ohjaus mittaa toimintaa suhteessa tavoitteisiin ja ennakoi resurssien riittävyyttä niiden tasoa, sijaintia ja käyttöä arvioimalla. (Aineettoman pääoman johtaminen 2004, 34.)

Organisaation tulee myös määritellä keitä varten mittaamista tehdään, mikä vaikuttaa siihen, miten mittaaminen tulee suorittaa ja miten asioita kuvataan. Esimerkiksi ulkoisessa raportoinnissa, joissa tiedon käyttäjänä on organisaation ulkopuolinen taho, annettu tieto on pääsääntöisesti objektiivista. Objektiiviset mittarit perustuvat aina todennettaviin tapahtumiin, joita voidaan kuvata määränä, aikana tai rahana. Objektiivisten mittareiden etuna on niiden tarkkuus, luotettavuus ja edullisuus. Toisaalta luotettavuus voi heikoimmillaan kuvata pelkästään mittausteknistä validiteettia. (Aineettoman pääoman johtaminen 2004, 35.)

Sisäisessä toiminnanohjauksessa tiedon objektiivisuudesta voidaan joustaa, mikäli subjektiivinen tieto tuottaa laadullisesti parempaa tietoa johtamisen, toiminnanohjauksen ja päätöksenteon näkökulmista. Esimerkiksi laadullisten arviointien tai kyselyjen avulla voidaan useimmiten kuvata laajemmin mitattavan tekijän ominaisuuksia ja ulottuvuuksia sekä toiminnan laatua tuloksen taustavaikuttajana, jotta toimenpiteitä voidaan kohdentaa oikein. (Aineettoman pääoman johtaminen 2004, 35.)

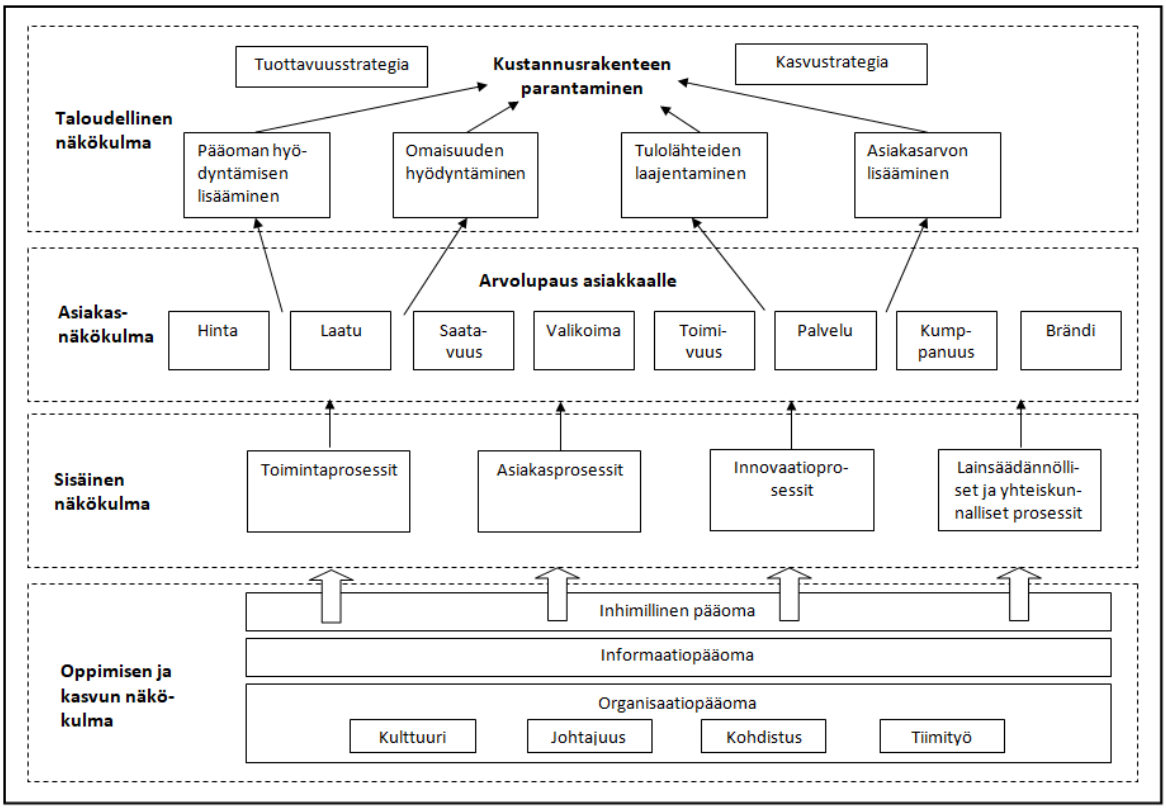
4.3 Suorituskyvyn mittaaminen

Suorituskyky-termistä (engl. performance) on esitetty useita eri määritelmiä. Lönnqvistin ja Mettäsen (2003, 20) mukaan suorituskyky määritellään mitattavan kohteen kyvyksi saavuttaa asetettuja tavoitteita. Suorituskyvyn rinnalla tai sen synonyyminä on käytetty termiä suoritus, joka kuvaa paremminkin jo tapahtunutta tulosta, kun taas suorituskyky viittaa parhaaseen mahdolliseen suoritukseen.

Organisaation suorituskykyä voidaan tarkastella useasta eri näkökulmasta. Tunnetuin lähestymistapa on Kaplanin ja Nortonin (1996, 44) esittämä tasapainotettu tuloskortti, Balanced Scorecard -malli, jossa suorituskykyä tarkastellaan neljästä näkökulmasta.

Kuvassa 13 esitetään tasapainotettu mittaristo, jossa havainnollistetaan eri näkökulmien suhteita toisiinsa:

- Taloudellinen näkökulma
- Asiakkaan näkökulma
- Sisäisten prosessien näkökulma
- Oppimisen ja kehittymisen näkökulma.



Kuva 13. Tasapainotettu tuloskortti (mukailtu lähteestä Kaplan & Norton 2004, 72).

Tasapainotetussa mittaristossa eri näkökulmat mahdollistavat tasapainon lyhyen ja pitkän aikavälin tavoitteiden välillä sekä kovien ja pehmeiden mittareiden välillä. Taloudellisessa näkökulmassa mittarit ovat tyypillisesti kovia ja kertovat menneestä, kun taas oppimisen ja kehittymisen näkökulmassa mittarit ovat usein pehmeitä ja mittaavat tulevaa. Onnistuttaessa hyvin saavutetaan tasapaino haluttujen tulosten ja niihin vaikuttavien tekijöiden kesken. (Lönnqvist & Mettänen 2003, 38.)

Lönnqvist ja Mettänen (2003, 39) ovat kuvanneet tasapainotetun tuloskortin näkökulmia sekä havainnollistanut kuhunkin näkökulmaan liittyvää mittaamista seuraavasti:

- Taloudellisen näkökulman mittareilla on kaksi erillistä tehtävää: Ne määrittelevät strategian taloudellisen suoritustason ja niiden perusteella määräytyvät muiden näkökulmien mittarit ja tavoitteet.
- Asiakasnäkökulman mittauskohteista tärkeimmät ovat markkinaosuudet, asiakasuskollisuus, asiakkaiden määrä, asiakastyytyväisyys ja asiakkaiden kannattavuus. Organisaatiossa on otettava huomioon sekä olemassa olevat että potentiaaliset, uudet asiakkaat.
- Sisäisten prosessien mittauksessa tulee keskittyä prosesseihin, joilla on suurin vaikutus asiakastyytyväisyyteen ja edelleen taloudellisiin tavoitteisiin. Erityisen tärkeää on tunnistaa kriittisimmät sekä eliminoida arvoa tuottamattomat sisäiset prosessit.
- Oppimisen ja kehittymisen näkökulma sisältää mittareita, jotka mittaavat organisaation kehittymistä ja oppimista. Tavoitteet johdetaan kolmen muun näkökulman tavoitteista.

Tasapainotettu mittaristo mahdollistaa organisaation näkemisen neljästä näkökulmasta ja tarjoaa vastauksen neljään peruskysymykseen, jotka Laitinen (2003, 377) on esittänyt seuraavasti:

- Millaisina omistajamme näkevät meidät (taloudellinen näkökulma)?
- Millaisina asiakkaamme näkevät meidät (asiakkaan näkökulma)?
- Missä asioissa meidän täytyy olla ylivoimaisia (sisäisten prosessien näkökulma)?
- Millä tavalla me voimme jatkuvasti parantaa suorituskykyämme ja arvon tuottamista (oppimisen ja kehittymisen näkökulma)?

4.4 Tietoturvallisuuden mittaamisen merkitys

On havaittu useita tekijöitä, jotka indikoivat tietoturvallisuuden yhä kasvavaa merkitystä organisaatioissa. Esimerkiksi digitalisaation kasvaessa julkishallinnolla on tarve lisätä verkkopalvelujaan, mikä aiheuttaa lisääntyvää tarvetta huolehtia yksityisyyden suojaan liittyvien suojaustoimenpiteiden varmistamisesta. Tietoturvallisuuden hallintaan liittyvien manuaalisten rutiinien poistaminen aiheuttaa järjestelmien kriittisyyden lisääntymistä, mikä voi hankaloittaa organisaation prosessien

toimintaa ongelmissa. Yksityisyyden suoja ja yleinen tietoturvatietoisuus ohjaa myös organisaatioita huolehtimaan, että tarjottavat palvelut ovat tietoturvallisia ja luotettavia käyttää. (Lundholm ym. 2011, 7.)

On tärkeää määritellä riittävä ja asianmukainen tietoturvallisuuden taso. Koska organisaation tietoturvallisuuden rakentaminen pelkästään teknisillä ratkaisuilla ei ole mahdollista, menestyksekkääseen tietoturvallisuuden hallintaan sisällytetään teknisen näkökulman lisäksi myös inhimillinen ja organisationaalinen näkökulma. Tietoturvallisuuden mittaamisessa ja mittareissa otetaan em. näkökulmat huomioon ja niitä on hyvä käyttää hyväksi myös organisaatioiden riskienhallinnassa. (Lundholm ym. 2011, 7.)

Laajasti siteeratun, Lordi Kelvinin toteamuksen mukaan, ”If you cannot measure it, you can not improve it” kehittäminen ja parantaminen vaatii avukseen mittaamista. Tämän voidaan todeta pätevän myös tietoturvallisuuden mittaamisessa, sillä luonnollisesti on helpompaa tehdä myös tietoturvallisuuden hallintaan ja kehittämiseen liittyviä päätöksiä, mikäli päätöksenteon ja johtamisen tukena on riittävää ja luotettavaa näyttöä. (Savola 2010, 230.)

Johtaminen ja päätöksenteko ilman mittaamista on vaikeaa tai lähes mahdotonta ja tietoturvallisuuden johtaminen ei tee tähän poikkeusta. Tehokas mittaaminen ja raportointi on oleellista toimittaessa lainsäädännön mukaisten määräysten ehdoilla, parannettaessa tehokkuutta ja valvonnan vaikuttavuutta sekä varmistettaessa strategian mukaisten toimien kohdentamista luotettavalla ja tarkoituksenmukaisella tavalla. Tietoturvallisuuden alan termeissä ilmenee jonkinasteista monitulkintaisuutta, kun puhutaan mittaamisesta tai tietoturvallisuuden mittaamisesta. Yleisesti ottaen termejä (tietoturva) mittari ja mittaaminen käytetään usein rinnakkain. Viime aikoina on ollut havaittavissa, että jälkimmäistä on alettu käyttää yleisemmin ja esimerkiksi standardeissa. (Barabanov ym. 2011, 4.)

Tietoturvallisuuden mittaaminen liittyy oleellisena osana tietoturvallisuuden päätöksentekoon. Puhutaan myös tietoturvallisuuden suorituskyvyn mittaamisesta, jossa tarkastellaan organisaation tietoturvallisuuden tehokkuutta ja vaikuttavuutta.

Tietoturvallisuuden mittaamisella saadaan Jansenin (2009, 1) mukaan määrällistä ja objektiivista tietoa tietoturvallisuuden eri osa-alueista:

- Strategian tukemiseen
- Laadun varmistamiseen
- Valvontatoimenpiteiden tehokkuuden arviointiin.

Tietoturvallisuuden mittaamisen järjestelmällinen tutkimus ja kehitystyö on suhteellisen nuorta, kokonaisvaltaisesti sekä laajasti hyväksytty lähestymistapa on puuttunut. Viime aikoina tietoturvallisuuden mittaaminen on kuitenkin saanut ansaitsemaansa huomiota ja siitä on tullut nopeasti kasvava tutkimuksen kohde. Tutkimuksessa onkin havaittu tarve määritellä tarkemmin ja laajemmin tietoturvallisuuden mittaamiseen liittyvää luokittelua ja sanastoa. (Savola 2010, 197.)

5 TIETOTURVALLISUUDEN MITTAAMINEN

5.1 Kohdeorganisaation tietoturvallisuuden mittaamisen kehittäminen

Tutkimuksen kohdeorganisaationa on metsäalan asiantuntijatalo, Suomen metsäkeskus, jonka perustan muodostaa Suomen metsäkeskuksesta annetun lain mukainen prosessiorganisaatio, jossa ylintä päätösvaltaa käyttää johtokunta. Metsäkeskus on osa julkishallintoa ja sen toimintaa ohjaa maa- ja metsätalousministeriö, jonka strategian mukaisesti tavoitteena on turvata uusiutuvien luonnonvarojen kestävää käyttöä sekä luoda edellytyksiä niihin perustuville elinkeinoille. Laki Suomen metsäkeskuksesta 418/2011 1 § 1 momentissa: ”Metsäkeskuksen tehtävänä on metsiin perustuvien elinkeinojen edistäminen, metsiä koskevan lainsäädännön toimeenpano ja metsätietoihin liittyvien tehtävien hoitaminen.”

Suomen metsäkeskuksella on pitkä historia. Ensimmäinen läänin metsälautakunta perustettiin 1917 ja 2010-luvulle tultaessa organisaatiosta on kasvanut Suomen metsäkeskus. Nykyisin Metsäkeskus profiloituu metsäalan asiantuntijatalona, joka kerää ja jakaa tietoa Suomen metsistä, valvoo metsälainsäädännön noudattamista sekä edistää kestävää metsätaloutta ja alan elinkeinoja. Tehtävänä on myös toteuttaa kansallista metsästrategiaa ja alueellisia metsäohjelmia sekä neuvoa metsänomistajia metsien hoidossa ja hyödyntämisessä. (Metsäkeskus 2018.)

Metsäkeskuksesta löytyy monipuolista metsä- ja luonto-osaamista sekä metsäalan elinkeinojen tuntemusta. Metsäkeskus kouluttaa vuosittain tuhansia metsänomistajia, satoja metsäalan ammattilaisia sekä tekee pitkäjänteistä työtä oppilaitoksissa lasten ja nuorten parissa. (Metsäkeskus 2018.)

Tämän työn kannalta tietoturvan mittaamisen kohdentamiseen ja kehittämiseen vaikuttaa mm. luvuissa 1.1 ja 1.14 määritellyt periaatteet, joiden mukaan tietoturvatyön tavoitteena on vähentää ja poistaa toimintaan kohdistuvia häiriöitä ja uhkatekijöitä sekä huomioida lainsäädäntö ja normatiivinen ohjaus. Lisäksi tietoturvallisuuden mittaamisella saadaan tuotettua tietoa tietoturvallisuuden säännöllistä arviointia ja johdon päätöksentekoa varten.

Työn tavoitteena on suunnitella mittareita, jotka tuottavat tietoa lainsäädännön vähimmäisvaatimusten mukaan (tietoturvallisuuden perustaso), mikä parantaa valmiuksia huolehtia tietoturvallisuuden arviointiin ja raportointiin liittyvistä velvollisuuksista sekä varmistaa osaltaan myös asianmukaisen tietoturvallisuuden hallintajärjestelmän toiminnan. Yhtä lailla tietoturvamittareiden suunnittelussa on huomionarviosta kohdeorganisaation maine yhteiskunnallisena toimijana, jolloin toiminnassa voidaan myös ylittää lainsäädännön vähimmäisvaatimukset. Lisäksi mittariston suunnitteluun vaikuttaa kohdeorganisaation toimintojen digitalisointi ja automatisointi, joilla tuodaan yhteiskunnalle ja asiakkaille lisäarvoa digitaalisin keinoin. Digitalisaatio ja uudet palvelut tuovat painoarvoa säännönmukaisella mittaamisella kerätylle tiedolle. Mittaamisesta muodostuu jatkuvaa toimintaa ja aikasarjoja, joiden perusteella voidaan kehittää palvelujen tietoturvaa sekä pyritään varmistamaan häiriötön toiminta ja toimimaan proaktiivisesti uhkatekijöitä vastaan.

Tietoturvamittarien suunnittelemisessa ja kehittämisessä kohdataan erilaisia haasteita, joskin ne ovat pääpiirteissään samanlaisia kuin muidenkin organisaatiossa tapahtuvien mittareiden suunnittelussa. Kohdeorganisaatiossa suunnittelun haasteet liittyvät mittareiden ja mittaamisen tavoitteiden määrittelyyn. Ne ovat sidoksissa mm. organisaation tietoturvallisuuden hallinnan kypsyystasoon sekä yhteiskunnallisiin ja lainsäädännöllisiin velvoitteisiin.

Julkishallinnossa tietoturvallisuuden arviointi ja mittaaminen kuuluvat keskeisesti tietoturvallisuuden tulosohjaukseen, jonka tarkoituksena on saada informaatiota kehittämis- ja ohjauspäätöksiä varten. Arvioinneilla luodaan tilannekuvaa suunnitelmien ja tavoitteiden laatimisen tueksi sekä riippumattoman näkemyksen saamiseksi tietoturvallisuuden tilasta. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 31-32.) Organisaation tietoturvatoiminnan seuraamisessa systemaattinen ja jatkuva mittaaminen mahdollistaa myös tietoturvallisuuden hallintajärjestelmän jatkuvan kehittämisen sekä hallintaprosessin toiminnan, kuten aiemmissa luvuissa 3.1 ja 3.2 on kerrottu.

Tietoturvallisuuden mittaus on prosessimuotoista ja se on osa johtamisen ja tietoturvallisuuden hallintaprosessia. Jatkuvasti kehittyvällä mittaamisella ja mittausprosessilla saavutetaan merkittävää hyötyä tietoturvallisuuden parantamisessa. Toiminnan ohjausta ja organisaation onnistumisen arviointia tehdään monella ta-

solla, joten tarvitaan mittareita eri ohjaustasojen ja tavoitteenasettelujen tarpeisiin. Ylemmällä tasolla käytetään strategisia mittareita, joita on myös lukumääräisesti vähemmän. Operatiivisella tasolla käytetään enemmän mittareita, jotka ovat myös tarkempia ja joiden tulee osaltaan tukea strategisten tavoitteiden toteutumisen seurantaa. Tavoitteena on, että mittaamisesta muodostuu jatkuvaa toimintaa ja aikaansaadaan aikasarjoja, joten käytettävän mittareiden on oltava riittävän selkeitä. Yleisohjeena on pidetty, että mittareita tulee olla mieluummin liian vähän ja kuvaavia ja ohjaavia, kuin paljon ja kaiken kattavia. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 34.)

Tietoturvallisuuden mittaamisen kohdentamisessa on huomioitava tulosohjauksen kannalta merkittävät tietoturvallisuuden arviointikohteet:

- Toteutuvatko toiminnan riskien hallintaan liittyvät tietoturvatavoitteet?
- Mikä on tietoturvallisuuden nykytaso suhteessa asetettuun tavoitetasoon ja mitä ovat edellytykset tietoturvatavoitteiden toteuttamiseen (osaaminen, resurssit)?
- Mikä on tietoturvallisuuden hallintajärjestelmän kehittyneisyys ja laatu?
- Mitä tietoturvariskejä on tunnistettu ja miten tunnistettuja riskejä hallitaan?
- Onko verkko- ja järjestelmätason tietoturvaratkaisujen (tietoturva-arkkitehtuuri) tavoitetila määritelty ja toteutettu?
- Miten eri aikaväleille asetetut tavoitteet ovat toteutuneet?
- Seurataanko tietoturvatoiminnan kustannuksia ja tehdäänkö ohjauspäätöksiä niiden perusteella?
- Onko säädösperustainen tietoturvataso toteutunut?
  (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 34.)

Lisäksi on tarpeellista ottaa arvioinnin ja mittaamisen kohteeksi myös kriittiset tietojärjestelmäkokonaisuudet.

5.2 Työssä käytettävä mittaristomalli

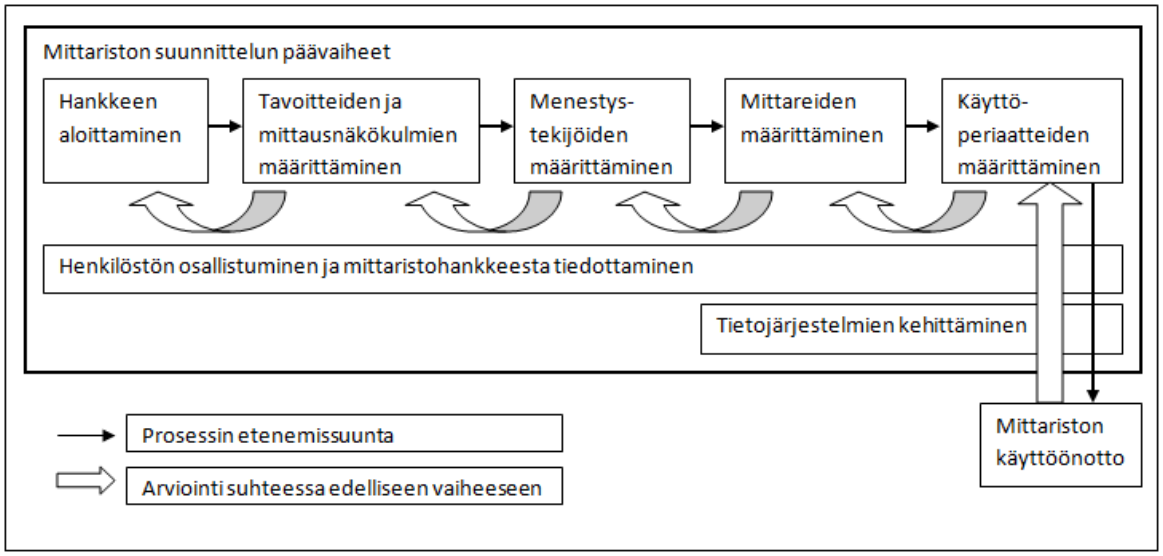
Mittariston suunnittelussa voidaan käyttää erilaisia mittaristomalleja, kuten Balanced Scorecard. Kirjallisuudesta löytyy useita erilaisia prosessimalleja mittariston

suunnittelua varten, joissa suunnittelu etenee hieman eri tavoin. Prosessimalleilla on tiettyjä yhteisiä piirteitä ja useat mallit etenevät samalla tavoin, strategisista tavoitteista kriittisten menestystekijöiden tunnistamisen kautta mittareiden määrittämiseen. Eri mallien vaiheiden määrä ja nimet, tehtäväkokonaisuudet ja työmenetelmät vaihtelevat vaikka mallit ovat melko samanlaisia. (Lönnqvist & Mettänen 2003, 83.)

Malleja ei kannata noudattaa orjallisesti ja Lönnqvist ja Mettänen (2003, 83) toteavat, että valittua mallia tulee muokata niin, että se sopii kyseisen organisaation tarpeisiin. Tässä työssä käytetään Lönnqvistin ja Mettäsen (2003, 84) esittämää asiantuntijaorganisaation suorituskykymittariston mallia.

Tietoturvallisuuden mittariston suunnitteluprosessi on esitelty kuvassa 14 ja siihen kuuluu viisi päävaihetta:

1. Hankkeen aloittaminen
2. Tavoitteiden ja mittausnäkökulmien määrittäminen
3. Menestystekijöiden määrittäminen
4. Mittareiden määrittäminen
5. Mittareiden käyttöperiaatteiden määrittäminen.
   (Lönnqvist & Mettänen 2003, 84.)



Kuva 14. Asiantuntijaorganisaation suorituskykymittariston malli (mukailtu lähteestä Lönnqvist & Mettänen 2003, 84).

Mittariston 5-vaiheinen suunnitteluprosessi soveltuu hyvin tämän työn toiminta-analyyttiseen tutkimusmenetelmään ja sen etenemismalliin. Se on esitetty luvussa 1.5 (kuva 3), jonka mukaan suunnitellaan mittausprosessi ja keskeinen mittaristo.

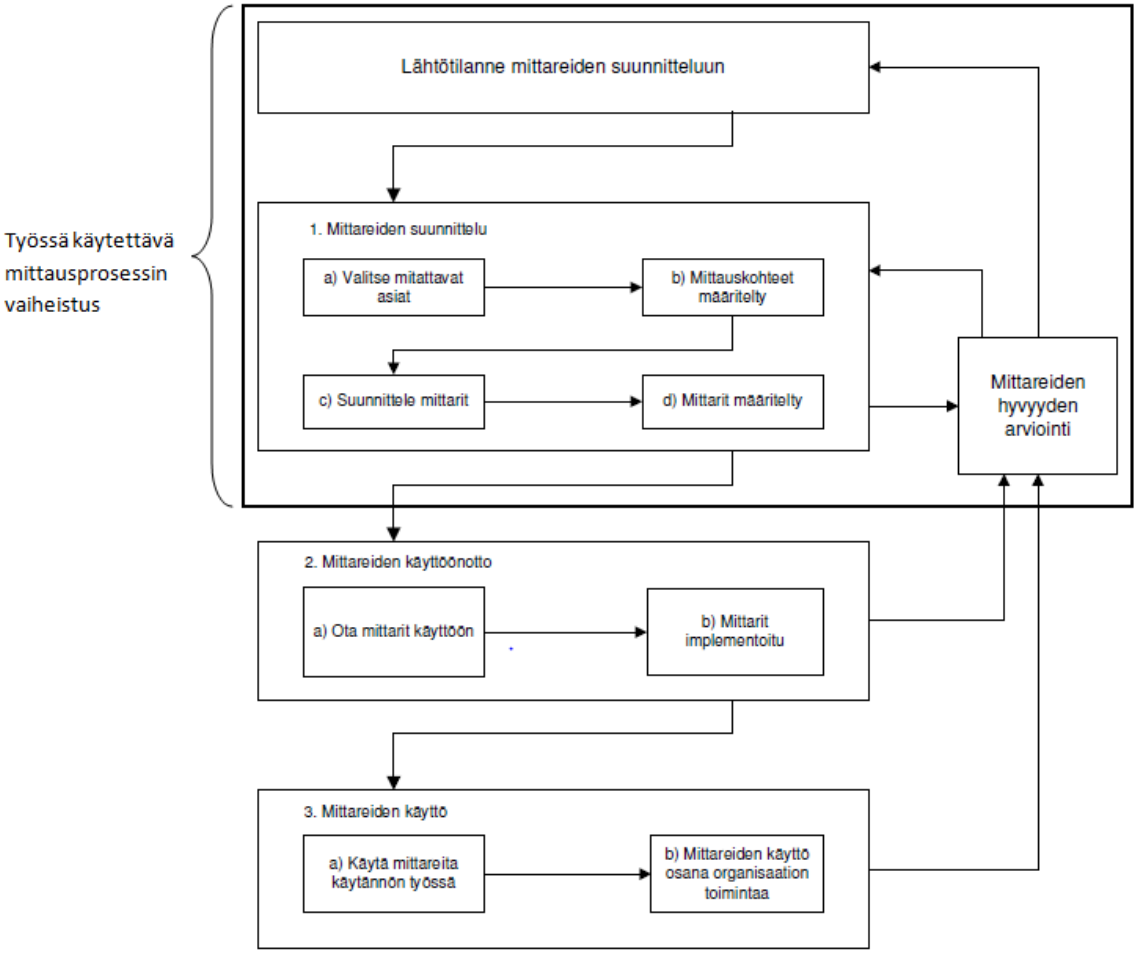
Mittariston suunnitteluprosessin vaiheista mittareiden määrittäminen voidaan edelleen sijoittaa Lönnqvistin (2004, 143) esittämän mittausprosessin 1 vaiheeseen kuvan 15 mukaan, jossa mittariston suunnittelu etenee seuraavasti:

a) Valitaan mitattavat asiat
b) Määritellään mittauskohteet
c) Suunnitellaan mittarit
d) Määritellään mittarit.

Mittaristoon ja mittausprosessiin liittyy myös erilaisia ongelmia, jotka voivat vaikeuttaa koko mittariston tai yksitäisen mittarin käyttöönottoa. Esimerkiksi tietolähteiden tulee olla kunnossa, jotta käyttöönotto sujuu suunnitellusti ilman ongelmia. Mittareihin tarvittavaa informaatiota kerätään erilaisista tietolähteistä, kuten kyselyistä ja tietokannoista. Toisaalta joihinkin mittareihin tarvittava tieto on jo valmiina olemassa, mutta yleensä myös valmista informaatiota joudutaan muokkaamaan mittarin edellyttämään muotoon. Toisinaan mittaria varten tarvittavaa informaatiota on liian vaikea tai jopa mahdotonta saada. Datan kerääminen voi osoittautua myös liian kalliiksi ja työlääksi mittarin tuottamaan hyötyyn nähden. (Lönnqvist & Mettänen 2003, 103-104.)

Tässä työssä on ensisijaisesti tavoitteena ottaa käyttöön mittareita, joihin tarvittava tieto on valmiina olemassa ja jotka voidaan ottaa käyttöön ilman mittavaa työpanosta. Tavoitteena on ensivaiheessa ottaa käyttöön muutama keskeinen mittari, joiden implementoinnin jälkeen voidaan tehdä jatkosuunnitelmia mittariston edelleen kehittämiseksi ja laajentamiseksi. Näin toimien toteutetaan myös aikaisemmassa luvussa 5.1 mainittuja yleisiä suosituksia, joiden mukaan mittareita tulee olla mieluummin liian vähän ja kuvaavia ja ohjaavia, kuin paljon ja kaiken kattavia.

Kuvan 15 mukaan mittareiden suunnittelu etenee vaiheistetusti a → d. Ennen kuin mittarit voidaan ottaa käyttöön, niiden käytettävyys arvioidaan ja tarvittaessa mittari palautuu suunnitteluvaiheeseen. Näin mittausprosessista tulee iteratiivinen, jolloin prosessissa voidaan palata taaksepäin esimerkiksi tavoitteiden muuttuessa. Tässä työssä suunnitellaan mittaristo kuvan 14 suunnitteluprosessin ja kuvan 15 (lähtötilanne + a–d + hyvyyden arviointi) mittausprosessin mukaan. Työn ulkopuolelle jäävät siten mittausprosessin vaiheet 2 (mittareiden käyttöönotto) ja 3 (mittareiden käyttö), jotka jäävät tutkimuksen jälkeiseen toteutukseen. Tietoturvamittareiden käytettävyyden arviointia tehdään useassa vaiheessa suunnitteluprosessia ja lopullinen mittareiden arviointi tehdään mittareiden käyttöönoton, testaamisen ja tuotantokäytön yhteydessä.



Kuva 15. Mittausprosessin vaiheet (mukailtu lähteestä Lönnqvist 2004, 143).

5.3 Tietoturvallisuuden mittaamisen viitekehys

Työn keskeisenä viitekehyksenä toimii valtionhallinnon organisaatioita ohjaava lainsäädäntö sekä sitä tukeva Vahti-ohjeistus, jotka määrittävät tietoturvallisuuden minimi- ja tavoitetasoa sekä soveltuvia tapoja toteuttaa tietoturvaratkaisuja. Tietoturvatoiminnan johtamisen kautta toteutetaan lainsäädännön ja edelleen valtionhallinnon ohjausta asettamalla organisaatiolle kehittämistavoitteita ja turvallisuustasoon liittyviä tavoitteita sekä seuraamalla tuloksia määritellyillä mittareilla tulosohjauksen puitteissa. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 16.) Työn käsiteanalyyttiseen vaiheeseen liittyy viitekehyksen määritteleminen, minkä arvioimiseksi käydään seuraavaksi läpi tietoturvallisuuden mittaamiseen liittyvää Vahti-ohjeistusta, joka on keskeinen dokumentaatio valtionhallinnon ohjauksen toimeenpanossa.

5.3.1 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä

Valtionhallinnon tietoturvallisuuden kehittämistä koskeva periaatepäätös ohjaa valtionhallinnon tietoturvallisuuden kokonaisuutta. Siinä päätetään tietoturvallisuuden kehittämisen periaatteista ja painopisteistä sekä linjataan keskeiset suuntaviivat viranomaisten tietoturvatyölle. Kehittämisen painopisteisiin kuuluvat mm. riskienhallinnan, tietoturvallisuuden hallintajärjestelmän, mittareiden ja seurannan sekä palvelu- ja hankintaketjujen tietoturvallisuuden sekä varautumisen kokonaisvaltainen kehittäminen. Periaatepäätöksen mukaan tietoturvamittareiden kehittäminen ja käyttö johtamisessa kuuluu organisaation tietoturvallisuuden johtamisen kehittämiskohteisiin. (Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 2009, 10.)

Viranomaisilla tulee olla valtiovarainministeriön Vahti-ohjeisiin, tietoturvatasomäärityksiin sekä varautumistoiminnan vaatimuksiin perustuvat suunnitelmat, ohjeet ja menettelyt, joita arvioidaan keskitetysti (Tietoturvallisuuden arviointiohje 2014, 14).

5.3.2 Valtioneuvoston asetus tietoturvallisuudesta

Valtioneuvoston asetus tietoturvallisuudesta (681/2010) edellyttää tietoturvallisuuden perustason saavuttamista kaikilta valtionhallinnon virastoilta ja laitoksilta. Asetuksen 23§:n mukaan viranomaisen tietojenkäsittely on saatettava vastaamaan asetuksen 5§:ssä säädettyjä perustason tietoturvavaatimuksia. Sen tueksi annettiin Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (Vahti 2/2010), jossa kuvataan tietoturvatasojen konkreettiset toimenpiteet ja vaatimukset.

Tietoturvallisuuden arviointi ja mittaaminen on tietoturvallisuusasetuksessa yhtenä vaatimuskokonaisuutena ja sen merkitystä korostaa myös arviointitoiminnasta erikseen annettu lainsäädäntö. Viranomaisten tulee varmistaa oman organisaation, palveluiden ja tietoaineistojen turvallisuus, jonka toteuttamiseksi tulee arvioida säännöllisesti tietoturvallisuuden tilaa sekä toteutettujen tietoturvatoimenpiteiden asianmukaisuutta ja riittävyyttä. (Tietoturvallisuuden arviointiohje 2014, 11-13.)

Sisäisten ja ulkoisten arvioiden avulla organisaatiossa saadaan tietoa jatkuvan parantamisen toteuttamiseen, millä mahdollistetaan hyvä tietoturvallisuuden hallinnan kehittäminen aikaisemmin kappaleessa 3.2 mainitun tietoturvallisuuden hallintaprosessin mukaisesti (PDCA).

5.3.3 Tietoturvallisuuden tuloksellisuuden arviointi ja mittaus

Organisaation toimintaa tarkastellaan tulosohjauksessa kokonaisuutena ja tulostavoitteiden asettamisessa käytetään useita eri näkökulmia. Tietoturvallisuuden tulosohjauksessa voidaan hyödyntää sekä laadullisia että määrällisiä tarkasteluja ja tietoturvallisuuden mittaamisen osalta voidaan esittää kysymys, miten tietoturvallisuuden kehittämistoimenpiteiden vaikutuksia valvotaan ja arvioidaan ja onko organisaatiossa käytössä mittaristo. Kunkin organisaation tulee miettiä keskeiset tehtävänsä ja ryhtyä tarvittaviin toimenpiteisiin toimintojen jatkuvuuden turvaamiseksi. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 23.)

Organisaation tietoturvallisuuden tuloksellisuuden arviointi ja mittaus perustuu asetettujen tavoitteiden ja toiminnan tilan seurantaa palveleviin mittareihin. Tulosohjauksen ja tulostavoitteiden kannalta on tärkeää tiedostaa, että mikäli tavoitteena on kehittää tietoturvallisuuden hallintajärjestelmää, niin silloin tulee arvioida tietoturvallisuuden hallintajärjestelmän kehitysvaihetta. Sen lisäksi voidaan mitata kehitysvaiheen mukaisesti tietoturvatoiminnalle asetettuja tuloksellisuus- ja laatutavoitteita sekä kustannuksia. Näiden avulla voidaan asettaa uusia kehittymistavoitteita ja tuottaa myös tilannekuvaa valtionhallinnolle organisaatioiden tietoturvallisuuden tilasta sekä kehittämisinvestointien ja tietoturvatyön hyödyistä. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 33.)

Tietoturvallisuuden tulosohjaukseen kuuluu keskeisesti arviointi ja mittaaminen, minkä tarkoituksena on saada riittävästi tietoa kehittämis- ja muita ohjauspäätöksiä varten. Arvioinnit sopivat tilannekuvan luomiseen tavoitteiden laatimisen tueksi sekä riippumattoman näkemyksen saamiseksi tietoturvallisuuden tilasta. Systemaattinen, jatkuva mittaaminen sopii puolestaan hyvin jatkuvan tietoturvatoiminnan seuraamiseen. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 32.)

Tietoturvallisuudella tuloksia (2007, 10) mukaan tietoturvallisuuden tasoa tulee mitata tulosohjausprosessiin kytkettyjen mittareiden avulla, joilla varmistetaan tietoturvatavoitteiden saavuttaminen niin vuositasolla kuin pidemmällä aikajaksolla. Tietoturvallisuuden arviointiprosessi on osa organisaation johtamista ja tulosohjausta, johon liittyvät johdon vahvistamat tietoturvallisuuden mittarit (Tietoturvallisuudella tuloksia 2007, 15).

Tulosohjauksen näkökulmasta tärkeimmät tietoturvatavoitteiden seurantakohteet ovat:

- Asetettujen tavoitteiden toteutuminen
- Toiminnan laatu
- Kustannukset.

  (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 26.)

Seurannassa voidaan käyttää sekä arviointeja että kvantitatiivisia mittareita. Usein arviointi on ainoa keino tarkastella esimerkiksi kehittämistavoitteiden toteutumista ja toiminnan laatua. Toisaalta kustannuksia ja toteutunutta tietoturvatasoa voidaan seurata määrällisin perustein. Seurannalla ja mittaamisella haetaan tukea ohjauspäätöksille, jolloin arviointien ja mittausten tulee olla tarkoituksenmukaisia juuri tätä taustaa vasten. Seurannan ja arvioinnin kohteena ovat siten asetetut tavoitteet ja operatiiviseen tietoturvatoimintaan liittyvät tapahtumat. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 27.)

5.3.4 Tietoturvallisuuden hallintajärjestelmä

Valtiovarainministeriön Ohjeen tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (Vahti 2/2010) tavoitteena on tehostaa ja yhdenmukaistaa julkisuuslain (Laki viranomaisen toiminnan julkisuudesta 621/1999) ja tietoturvallisuusasetuksen (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 621/2010) täytäntöönpanoa. Ohjeen mukaisella toiminnalla organisaatio voi saavuttaa toiminnassaan ja yhteistyössään asetuksen mukaisen tietoturvatason, joka tasapainottaa riskienhallinnan ja kustannustehokkuuden. Tietoturvatason saavuttaminen ja edelleen kehittäminen edellyttää tietoturvallisuuden hallintajär-

jestelmää, joka rakentuu organisaatiolle asetettujen tehtävien toteuttamisen mahdollistamiseksi hyvää tiedonhallintatapaa noudattaen. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 6, 45.)

Tietoturvallisuuden hallintajärjestelmän olennaisimmat osat ovat ajantasainen tietoturvapolitiikka ja siihen liittyvät ohjeet, asiakirjat sekä säännöllinen riskienhallinta, joka koskee nykyistä toimintaa ja suunniteltuja muutoksia. Tietoturvallisuuden hallintajärjestelmä sisältää tietoturvatoiminnan tehokkuuden ja tarkoituksenmukaisuuden säännöllisen mittaamisen ja arvioinnin. (Tietoturvallisuudella tuloksia 2007, 40).

Tietoturvallisuuden hallintajärjestelmän vuositavoitteet voidaan jakaa kahteen osaan:

- Tietoturvallisuuden kehittäminen
- Tavoiteltava ja mitattavissa oleva tietoturvataso.
  (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 25.)

Operatiiviselle tietoturvatoiminnalle voidaan asettaa määrällisiä mittareilla mitattavissa olevia tuloksellisuus- ja laatutavoitteita, joita ovat esimerkiksi häiriöiden vähentyminen, koulutuksen toteutuminen ja tietoturvatoiminnan kustannuksiin liittyvät tavoitteet. Voidaan myös pisteyttää toimintaa laadullisen arvioinnin näkökulmasta ja arvioida esimerkiksi kypsyystasoa. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 26.)

5.3.5 Tietoturvallisuuden hallinnan arviointi

Tietoturvallisuuden hallintajärjestelmään ja sen toimintojen kehittämiseen kuuluu keskeisesti seuranta ja arviointi. Organisaation tietojenkäsittelyn riskit sekä tietoturvallisuuden tila ja johtaminen on arvioitava systemaattisesti. Arviointi voi olla sisäistä itsearviointia tai organisaatioiden keskinäistä vuorovaikutteista toimintaa esimerkiksi viranomaisten välillä tai ulkoistamiseen liittyvää sopimuspohjaista toimintaa, joita varten luodut menetelmät ja mittaristot antavat työkaluja jatkuvaluonteiseen arviointiin. (Tietoturvallisuus ja tulosohjaus 2004, 22.)

Arvioinnit ovat oleellinen osa tietoturvallisuuden hallintajärjestelmän toimintamallia ja ne muodostavat osaltaan toiminnalle laadullisia ja määrällisiä mittareita. Laadullisia ovat mm. tehdyt arviot ja raportoidut tapahtumat ja mittaamisessa arvioidaan toiminnan onnistumista, jolloin se sopii hyvin toiminnan tilan ja siinä tapahtuneen kehityksen arviointiin. Määrällinen mittaaminen perustuu systemaattiseen mittaamiseen ja siinä voidaan seurata esimerkiksi tulosten aikaansaamiseen käytettyä työaikaa, kustannuksia, työajan menetyksiä, tietoturvapoikkeamien lukumäärää tai tietoturvakoulutuksen määrää. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 32.)

Määrällinen mittaaminen soveltuu hyvin operatiivisen tietoturvatoiminnan mittaamiseen ja ajoittain tarvitaan myös tilannekohtaista mittaamista, joka on suunniteltava uusien tilanteiden ja toiminnallisten vaatimusten mukaan. Esimerkiksi teknisen tietoturvallisuuden mittaus antaa kokonaiskuvaa ICT-ympäristöstä ja auttaa arvioimaan siihen liittyviä uhkia. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 33.)

Tietoturvallisuuden hallintaa käsitellään Vahti 2/2010 ohjeessa CAF-laatumallista johdettujen osatoimintojen avulla seuraavasti:

- Johtajuus
- Strategiat ja toiminnan suunnittelu
- Henkilöstö
- Kumppanuudet ja resurssit
- Toiminnan prosessit
- Mittaaminen.
  (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 45.)

Osatoiminnoista tietoturvallisuuden mittaaminen eli arviointi tarkoittaa niitä toimenpiteitä, joiden avulla varmistutaan nykytilanteen toimintojen tasosta, joka sisältää toiminnan arvioinnin ja todentamisen (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 46).

Tietoturvallisuuden hallinnan arviointi muodostuu riittävän kattavasta seurantajärjestelmästä tietoturvallisuuden eri osa-alueiden tilanteen arvioimiseksi. Organisaa-

tion tulee laatia määräajoin seurantaraportti tietoturvallisuuden tilasta ja esitellä se ylimmälle johdolle johdon katselmuksessa. Seurantaraportti koostuu osatoimintojen sekä niiden alakohtien tuloksista, jossa kunkin käsiteltävän asian osalta nähdään asetettu tavoite ja arvio nykytilanteesta. (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta 2010, 47.)

5.3.6 Tietoturvatason arviointi ja mittaaminen

Tietoturvallisuuden johtaminen vaatii perustellun päätöksen tavoitellusta tietoturvallisuuden tasosta. Tietoturvatason toteutumista on pystyttävä mittaamaan ja analysoimaan säännöllisesti ratkaisuja valittaessa. Tietoturvan mitattavuus ja mittarit on valittava siten, että saatavien tietojen perusteella voidaan tehdä johtopäätöksiä tietoturvallisuuden tasosta ja tarvittaessa ryhtyä tietoturvallisuutta parantaviin toimenpiteisiin. Mittareiden avulla ohjataan tietoturvallisuuden kehittämiseen kokonaisuuden kannalta, ei pistemäisiin ratkaisuihin. Tietoturvallisuutta kehitettään iteratiivisesti käytössä olevien resurssien ja ympäristön muutosten ohjaamana, joten mittarit ovat oleellisia myös pidemmän aikavälin kehityksen seurannassa. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 31.)

Tietoturvatason mittaamiselle hyvän lähtökohdan antaa keskeisten tietojärjestelmien itsearviointi. Säännöllisillä, suunnitelluilla itsearvioinneilla voidaan seurata organisaation tietoturvallisuuden kehitystä ja tehtyjen tietoturvatoimenpiteiden vaikutusta. Valtionhallinnon organisaatioiden yhteistyö mahdollistaa vertaiskehittämisen ja oman tietoturvallisuuden mittaamisen muihin verrattuna. Lisäksi itsearviointia voidaan tehdä jatkuvaluonteisesti myös henkilötasolla. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 95.)

Säännöllinen ulkoinen arviointi antaa uutta näkökulmaa organisaation tietoturvatasoon, tilanteeseen ja kehittämiseen. Ulkoisen arvioinnin avulla voidaan löytää organisaation tietoturvallisuutta heikentäviä toimintatapoja ja ratkaisuja, joita ei esimerkiksi itsearvioinnissa ole havaittu valittujen mittareiden tai tahattoman tuloshakuisuuden kautta. Ulkoisissa arvioinneissa organisaation on itse selkeästi rajattava mitattava kokonaisuus ja määriteltävä mittauksen tavoitteet. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 95.)

Auditointi eli tarkastaminen eroaa arvioinnista siten, että auditoinnilla valvotaan annettujen ohjeiden ja sääntöjen toteutumista. Arvioinnilla halutaan puolestaan mitata kohteen tietoturvallisuuden tasoa ja etsitään mahdollisia parannuskohteita. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 96.)

5.3.7 Tietoturvallisuuden tilan ja kehityksen mittaaminen

Tietoturvallisuuden tilaa ja kehitystä mitattaessa haasteena on mittareiden ja mittaustapojen valinta. Arviointi on pääsääntöisesti subjektiivista, arvioijan kokemuksesta ja tiedosta riippuvaa. Tarkkaa seurantaa varten tarvitaan kuitenkin mittaamista, jonka on oltava jatkuvaa, toistettavaa, nopeaa, ennustettavien virhemarginaalien sisällä pysyvää ja tavoitteellista. Lisäksi tulosten on oltava analysoitavissa ja verrattavissa aiempiin mittaustuloksiin. Erilliset mittaustapahtumat eivät saa olla toisistaan riippuvaisia ja mittaustuloksesta on pystyttävä päättelemään tarvittavat toimenpiteet. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 96.)

Mittaustapahtuman kulkua voidaan havainnollistaa seuraavasti:

- Määritetään mittaamisen tavoitteet ja kohteet
- Määritetään mittarit
- Suoritetaan mittaus
- Arvioidaan mittaustulosten luotettavuus ja hyöty
- Tehdään johtopäätökset ja suoritetaan korjaavat toimenpiteet
- Tehdään uudelleenmittaus toimenpiteiden onnistumisen varmistamiseksi
- Vertaillaan mittaustuloksia ja haetaan trendejä.
  (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 96.)

Tietoturvallisuuden mitattavuus on huomioitava tietojärjestelmiä kehitettäessä tai hankittaessa, jonka yhteydessä on oleellista huomioida myös mittaustulosten raportointi. Samasta mittaustapahtumasta voidaan tarvita yksityiskohtaisten mittaustulosten lisäksi erilaisia näkymiä, kuten yhteenvetoja ja trendikuvauksia. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 96.)

Valvonta voidaan käsittää mittaamisen osa-alueena. Esimerkiksi teknisin keinoin voidaan valvoa organisaation toimintaa sovellus- ja verkkotasolla. Osana hallintajärjestelmien ja sovellusten toiminnan seurantaa liittyy keskeisesti hälytykset, joiden avulla voidaan tavoittaa mahdolliset väärinkäytökset ja ongelmatilanteet. (Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004, 97.)

5.3.8 Tietoturvatoiminnan mittarit

Tietoturvatason toteutumista voidaan seurata pysyväisluontoisilla mittareilla ja tyypillisiä seurantakohteita ovat tietoturvapoikkeamat ja tietoturvatoiminta sekä niissä tapahtuneet muutokset. Näille voidaan mitata absoluuttisia arvoja ja siten myös seurata tietoturvatason kehittymistä. Luotua mittaristoa voidaan täydentää toiminnan ja tietoturvallisuuteen vaikuttavien tekijöiden mittaamisessa tapahtuvan kehittymisen myötä. Esimerkiksi auditointitoiminnan kehittyessä voidaan seurantaan lisätä kohteittain tehdyt auditoinnit (tietojärjestelmät, verkot, operaattorin palvelut ym.). (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 36.) Seuraavaksi on lueteltu esimerkinomaisesti keskeisiä tietoturvamittareita, joita on käytetty julkishallinnon organisaatioissa ja joita voidaan hyödyntää tietoturvallisuuden mittaamisessa.

Tapahtuneet tietoturvapoikkeamat, joiden tavoitteena on seurata ja mitata toiminnalle aiheutuvaa haittaa ja hankkia tietoa tietoturvatoimenpiteiden suunnittelua varten:

- Ilmoitetut/tietoon tulleet toimenpiteitä vaatineiden tietoturvatapahtumien lukumäärä
- Vahinkojen määrä (esimerkiksi sähköposti- ja tietoliikennepalvelujen ja muiden toiminnalle kriittisten järjestelmien keskeytysten pituudet ja lukumäärä)
- Virus- ja muut haittaohjelmavahingot ja torjuntaprosentti
- Tietoverkon poikkeukselliset kuormitustilanteet
- Raportoitujen tietoturvarikkomusten luonne ja määrä
- Varkauksien lukumäärä.
  (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 34.)

Tietoturvapoikkeamien hallinta, minkä tavoitteena on seurata toteutettujen tietoturvatoimenpiteiden tehokkuutta:

- Havaitut virus- ja muut haittaohjelmat
- Havaitut (esimerkiksi palomuuriin pysähtyvät) tunkeutumisyritykset
- Havaitut palvelunestohyökkäykset
- Roskapostitilanne
- Toteutetut torjuntaohjelmien päivitykset
- Toteutetut tietoturvapäivitykset
- Tietoliikenneyhteyksien kapasiteetti ja käytettävyys
- Epäonnistuneiden tunkeutumisyritysten lukumäärä järjestelmiin. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 34.)

Tietoturvatoimintaa kuvaavia mittareita, joiden tavoitteena on arvioida tietoturvatoiminnan tehokkuutta seuraamalla suoritteita ja käytettyjä panoksia:

- Tietoturvatoiminnan kustannukset (kehittäminen, operatiivinen toiminta, investoinnit)
- Tietoturvallisuustyön työtunnit tai henkilötyöpäivät
- Tietoturvaryhmän kokousten lukumäärä
- Tietoturvakoulutuksen koulutuspäivien ja/tai opetustuntien määrä, osallistujalukumäärä
- Henkilöstölle suunnattujen tiedotteiden lukumäärä
- Tietoturvasopimusten lukumäärä ja luonne
- Tietoturvakatselmointien lukumäärä kohteittain
    - Tietojärjestelmien tietoturvasuunnitelmat (toipumissuunnitelmat)
    - Henkilöstöturvallisuus
    - Käyttöoikeudet
    - Tietoaineistot (suojaus, varmistukset, laatu)
    - Operaattorin palvelut
    - Toimitilat
    - Tietoliikenne ja verkot
    - Laitteet
    - Määriteltyjen prosessien mukainen toiminta

- Suunnitelmat ja ohjeet mukaan lukien jatkuvuus- ja valmiussuunnitelmat
- Vastuut, delegoinnit
- Tietoturvasopimukset
- Riskikartoituksen ajantasaisuus.
  (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 34.)

Tietoturvallisuuden mittaamista voidaan tehdä tulostavoitteita vasten, jolloin mitataan erikseen kehittämistavoitteiden toteutumista, tietoturvapoikkeamia ja toiminnan tehokkuutta. Lisäksi organisaation tulee arvioida vuosittain tietoturvallisuuden hallintajärjestelmänsä kypsyysaste ja kehityssuunnitelma, kunnes haluttu tietoturvallisuuden tavoitetaso on saavutettu. On ollut havaittavissa, että organisaation tietoturvallisuuden hallintajärjestelmän muodostamisvaiheessa mittareita ja arviointeja on suhteellisen runsaasti ja tietoturvatoiminnan kehittyessä ja vakiintuessa mittareiden määrä on vähentynyt. Saavutettua tietoturvatasoa ylläpidetään ja kehitetään edelleen, minkä vuoksi myös mittarit vaativat osaltaan jatkuvaa arviointia ja kehittämistä, jotta voidaan varmistua niiden hyödyllisyydestä ja tarkoituksenmukaisuudesta. Lisäksi muutokset tietoturvallisuuden toimintaympäristössä edellyttää mittareiden ja arviointimenetelmien jatkuvaa ajantasaistamista. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 36.)

5.3.9 ICT-varautumisen mittaaminen

Tietohallintolaissa (634/2011) velvoitetaan julkista hallintoa suunnittelemaan ja kuvaamaan kokonaisarkkitehtuurinsa julkishallinnon tietojärjestelmien yhteentoimivuuden mahdollistamiseksi ja varmistamiseksi. Lisäksi laki velvoittaa julkishallinnon organisaatioita noudattamaan yhteentoimivuuden kuvauksia ja määrityksiä sekä asettaa valtiovarainministeriölle ohjaus- ja koordinointivelvoitteen. Yhtenäiset vaatimukset edesauttavat julkishallinnon ja talouselämän toimintojen yhtenäistämistä sekä palvelujen jatkuvuuden varmistamista erilaisissa häiriötilanteissa. (ICT-varautumisen vaatimukset 2012, 17.)

Vahti 2/2012-ohjeessa asetetaan ICT-varautumisen vaatimuksia organisaation toiminnalle, palveluille sekä tieto- ja viestintäteknisten järjestelmien ja palveluiden toteuttamiselle. Viitekehyksenä vaatimusten muodostamiselle on hyödynnetty yleisesti käytettyjä EFQM ja CAF laadunarviointimalleja sekä vaatimuksissa ISO standardeja 27001 ja 22301. Vahti 2/2012-ohjeessa varautumisvaatimukset on ryhmitelty kuuteen osaan kuvan 16 mukaan. Varautumisvaatimukset ovat yleisvaatimuksia, jotka kuvaavat toteutettavan, varautumista tukevan toimenpiteen, joita täsmentää toteuttamista ohjaavat perustason, korotetun tason ja korkean tason vaatimukset. Osat 1–4 sisältävät organisaation toiminnan ja kypsyyteen liittyviä vaatimuksia ja osa 5 asettaa vaatimuksia teknisille järjestelmille, prosesseille ja ratkaisuille. Kuudennessa osassa on kuvattu mittaaminen, raportointi ja auditointi, joissa on esitetty vaatimuksia toiminnan sisäiselle ja ulkoiselle mittaamiselle. Ne tuottavat johtamiselle, strategioille ja toiminnan suunnittelulle tarvittavaa tietoa häiriötilanteita sietävän toiminnan kustannustehokkaalle kehittämiselle. (ICT-varautumisen vaatimukset 2012, 19, 41.)

Kuva 16. ICT-varautumisen vaatimukset (2012, 19).

Jatkuvuuden hallintaa, tiedon turvaamista sekä varautumisen toteutumista ja tuloksellisuutta on seurattava säännöllisesti arvioinneilla, joita voidaan tehdä itse tai antaa ulkopuolisen toteutettavaksi. Raportoinnilla huolehditaan välittömistä häiriö- ja poikkeamailmoituksista sekä vuosikelloon sidotusta, analysoidusta yhteenveto-

raportoinnista. (ICT-varautumisen vaatimukset 2012, 41.) Jäljempänä on kuvattu Vahti 2/2012 -ohjeen mukaiset mittaamista, raportointia ja auditointia koskevat ICT-varautumisen vaatimukset sekä esimerkkejä vaatimusten soveltamiseksi.

ICT-varautumisen vaatimukset (2012, 81) ohjeessa on kuvattu ICT-varautumisen mittaamisen vaatimuksia (toteutumisen ja tarkoituksenmukaisuuden seuraaminen ja arviointi) sekä esimerkkejä vaatimusten soveltamiseksi seuraavasti:

1. Perustaso

a) Jatkuvuuden, tiedon turvaamisen ja varautumisen tavoitetason saavuttamista seurataan toiminnan ja talouden suunnitteluprosessissa.
   i. Organisaatiossa on auditointisuunnitelma, jonka pohjalta auditoidaan esimerkiksi ensimmäisenä vuonna organisaatiossa hallintaprosessit, seuraavan vuonna kaikkien ulkoistus- ja palvelutasosopimusten tietoturvaan ja jatkuvuuteen liittyvät vaatimukset ja kolmantena kriittiset tietojärjestelmät. Organisaatio voi tehdä auditoinnit esimerkiksi vuosikellon mukaisesti

a) Palvelutuottajien tuottamien tietojenkäsittelypalveluiden tilaa ja kehittämistoimenpiteitä seurataan säännöllisesti.
   i. Asiakaskatselmointi suoritetaan sovittuna aikana ja siinä käsitellään sovittujen toimenpiteiden tilanne ja sovitaan uusista toimenpiteistä, joita jatkuvuudenhallinnan osalta olisi perusteltua ryhtyä tekemään. Asiakaskatselmoinnilla seurataan toimenpiteiden edistymistä.

a) Auditoinnit tai itsearvioinnit toteutetaan suunnitelmallisesti ja ne ovat johdon hyväksymiä.
   i. Organisaation johto on hyväksynyt periaatteet, joiden mukaisesti yksiköt arvioivat joka toinen vuosi oman toimintansa tietoturvallisuutta ja raportoivat tuloksista.
   (ICT-varautumisen vaatimukset 2012, 81.)

2. Korotettu taso

a) Sisäinen tarkastus toimintona (tarkastussuunnitelma) ja esimiehet suorittavat säännöllisesti tuotteiden, palvelujen, toimintojen, prosessien ja järjestelmien riskiarvioinnin sekä jatkuvuuden hallinnan tarkastuksia.

i. Mittaustulokset on analysoitava, eikä pelkästään seurattava lukumääriä. Auditoinneista mittareina voi olla negatiivisten löydösten määrä ja vakavuus. Mittaus prosessina on tärkeä jotta saadaan sisältöä kehittämistoimenpiteiksi. Mittari 1: kuinka suuri osa kehittämisehdotuksista muuttuu toimenpiteiksi. Mittari 2: kuinka suuri osa sovelluskehitystyöstä menee virheiden korjaamiseen. Mittaamiseen olisi hyvä saada yhteinen kehikko. Mittari: Montako korjauskierrosta toimitettu järjestelmä joutuu käymään ensimmäisen toimituksen jälkeen.

a) Palveluverkoston varautumisen ja tiedon turvaamisen toimenpiteiden katselmointeja ja auditointeja toteutetaan.
   i. Oman toiminnan osalta tehdään yhteistyössä sisäisen tarkastuksen kanssa päällekkäisen työn välttämiseksi. Tietoturvallisuuden resursointia erityistilanteita ja poikkeusoloja varten seurataan organisaation toiminta- ja taloussuunnittelun toteutumassa. Palveluntoimittajan kanssa sovitaan auditointirytmi ja kirjataan asia Toiminnan ja talouden suunnittelun koordinaation varmistamiseksi. Organisaation turvallisuusjohto koordinoi auditoinnit ja tarkastukset.

a) Poikkeamahavaintojen pohjalta toiminnon tai kohteen omistaja määrittelee ja vastuuttaa kehittämistoimenpiteet, joilla havaitut riskit saadaan hyväksyttävälle tasolle.
   i. Riskienhallinnan seurantaraporttiin kirjataan toimenpiteet ja niiden arvioitu vaikutus. Uudet turvakontrollit kirjataan ja niiden toimivuutta toimintaprosessissa seurataan. Korkean tason järjestelmät auditoi kansallinen tietoturvallisuusviranomainen.
   (ICT-varautumisen vaatimukset 2012, 81.)

3. Korkea taso

a) Varautumis- ja tietoturva-auditoinnit toteutetaan kansallisen tietoturvallisuusviranomaisen ohjeistuksen mukaisesti.
   i. Ulkopuolisia resursseja tarvitaan teknisen puolen ratkaisujen arviointiin, sillä hallinnossa on liian vähän eri teknisten osa-alueiden auditointikokemuksen omaavia asiantuntijoita.
   (ICT-varautumisen vaatimukset 2012, 81.)

Vaatimuksia on kuvattu perustason, korotetun tason ja korkean tason vaatimusten mukaan. Tässä työssä keskeinen merkitys on ICT-varautumisen mittaamiseen liittyvillä perustason vaatimuksilla, joka on myös tietoturvallisuusasetuksessa (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681) määritelty organisaation minimitaso, minkä mukaiseksi tietojenkäsittely on saatettava vastaamaan.

ICT-varautumiseen liittyvien varautumistarpeiden kokoamisesta, varautumisvaatimusten asettamisesta, ohjauksesta ja toteutuksen ohjauksesta vastaa valtiovarainministeriö. On linjattu, että julkishallinnossa käytettävien varautumisen vaatimusten tulee kattaa koko verkostoitunut toimintaprosessi hallinnonalojen rajat ylittäen ja lähtökohta on, että jokainen prosessiin kuuluva organisaatio on täyttänyt tietoturva-asetuksen mukaisen tietoturvallisuuden perustason. (ICT-varautumisen vaatimukset 2012, 25.)

ICT-varautumisen vaatimuksiin liittyvä tietoturvallisuuden mittaaminen on osa tämän työn viitekehystä ja jäljempänä tässä työssä tuodaan esille myös ISO/IEC standardi 27004:2016, jossa määritellään ISO/IEC 27001:2013 -standardiin pohjautuva tietoturvallisuuden mittaaminen.

5.3.10 Jatkuvuuden hallinnan mittaaminen

Jatkuvuuden hallintajärjestelmän muodostavat prosessit, toimenpiteet, työkalut ja suunnitelmat, joiden avulla varmistetaan organisaation toiminnan jatkuvuus. Hallintajärjestelmän toiminta perustuu jatkuvaan kehittämiseen sekä vaatimusten seuraamiseen ja päivittämiseen. Jatkuva kehittäminen ja toiminnan optimointi perustuvat suunnittelulle asetettuihin tavoitteisiin ja mittareihin, joita tarkastellaan säännöllisesti. (Toiminnan jatkuvuuden hallinta 2016, 29.)

Mittaamisella, raportoinnilla ja auditoinneilla tuotetaan johtamisessa sekä strategioiden ja toiminnan suunnittelussa tarvittavaa tietoa, jota voidaan käyttää häiriötilanteita sietävän toiminnan kustannustehokkaaseen kehittämiseen. Jatkuvuuden hallintaa, tiedon turvaamista ja varautumisen toteutumista ja tuloksellisuutta on seurattava ja arvioitava säännöllisesti. Organisaatio voi arvioida toimintaa itsenäi-

sesti tai antaa sen toteuttamisen ulkopuoliselle toimijalle. (Toiminnan jatkuvuuden hallinta 2016, 61.)

Jotta jatkuvuuden hallinnan prosessia voidaan mitata ja edelleen parantaa, organisaatiolla tulee olla keinot, kyvykkyydet ja työkalut mittaamiseen. Heti jatkuvuuden hallintaa käynnistettäessä on syytä miettiä, mitä, milloin ja millä työkaluilla mittausta tehdään ja miten saatuja tuloksia arvioidaan. Tulosten ja toimenpiteiden vaikuttavuuden luotettavan arvioinnin varmistamiseksi on historiatieto säilytettävä ja varmistettava tulosten yhteismitallisuus. Lisäksi pidemmän aikavälin seurannalla varmistetaan, että jatkuvuuden hallinnan toimenpiteet ja valitut mittarit vastaavat muuttuvaa toimintaympäristöä. Esimerkiksi ulkoistuksen lisääntyminen vaatii painopisteen siirtämistä palvelutuottajien jatkuvuus- ja toipumissuunnitteluun sekä myös mittareiden seurantaan. (Toiminnan jatkuvuuden hallinta 2016, 61.)

Jatkuvuuden hallinnan seuranta ja mittaaminen tehdään yleensä harjoitusten ja testien yhteydessä sekä arvioimalla jälkikäteen toteutuneita häiriötilanteita. Saadut tulokset analysoidaan, dokumentoidaan ja raportoidaan, johon tulee sisällyttää välittömät häiriö- poikkeamailmoitukset sekä vuosikelloon sidotut, analysoidut yhteenvetoraportit. (Toiminnan jatkuvuuden hallinta 2016, 61.)

Jatkuvuuden hallintaan valittujen mittareiden on hyvä liittyä organisaation ydintoimintoihin ja mitata asetettujen tavoitteiden täyttymistä. Mittaaminen ja seuranta sidotaan jatkuvuuden hallinnan vuosikelloon sekä merkittävät häiriötilanteet ja niistä toipuminen sisällytetään mittaamiseen. Kuitenkin on huomioitava, että seuranta ja mittaustulokset eivät saa perustua pelkästään toteutuneisiin häiriötilanteisiin vaan pääosa mittaustuloksista tulee perustua erilliseen mittaristoon. (Toiminnan jatkuvuuden hallinta 2016, 62.)

Seuraavassa luettelossa on esimerkkejä mitattavista kohteista:

- Toteutuneet palautusajat ja -pisteet vs. toipumisskenaarioissa arvioidut tavoitteet (RTO ja RPO)
- Riskianalyysin onnistuminen (BIA vs. toteutunut vahinko, SLA:n vastaavuus)
- Reagointi-, vaste- ja läpimenoajat (oma henkilöstö, palvelutarjoaja jne.) vs. luvatut

- Suunnittelemattomien käyttökatkojen pituus
- Jatkuvuus- ja toipumissuunnitelmien sisällön ajantasaisuus (vastaavatko suoritetut toipumistoimenpiteet suunniteltuja; vastaavatko toiminnan prosessit kuvattuja?)
- Viestinnän onnistuminen (saavatko oikeat tahot oikean tiedon oikeaan aikaan?)
- Tapahtuneet merkittävät virhe- ja häiriötilanteet vs. skenaariot joihin on varauduttu
- Hallintajärjestelmän vuosikellon mukaisten toimenpiteiden toteutuminen
- Dokumenttien ajantasaisuus
- Koulutusten järjestäminen ja kohdentaminen
- Hallintajärjestelmän auditoinnit ja standardinmukaisuus
- Omien seurantajärjestelmien havainnointikyky.
  (Toiminnan jatkuvuuden hallinta 2016, 62.)

6 TIETOTURVALLISUUDEN MITTAAMISEN TOTEUTUS

Tietoturvallisuuden mittariston toteuttamisessa otetaan huomioon Metsäkeskuksen rooli osana julkishallintoa, mikä asettaa toiminnalle normatiivisia velvoitteita mm. sisäisen toiminnan näkökulmasta. Strategialla on myös keskeinen merkitys tarkoituksenmukaisen ja onnistuneen mittariston määrittelyssä. Visiosta ja strategiasta johdetut menestystekijät ja mittausnäkökulmat liittyvät kiinteästi tavoitteiden saavuttamisen arviointiin ja siten myös tietoturvallisuuden tilan arviointiin ja mittaamiseen.

Mittauskohteiden valinnassa painotetaan menestystekijöitä, joilla on merkitystä kohdeorganisaation tietoturvallisuuden johtamisen ja hallinnan sekä strategian ja tulostavoitteiden onnistumisessa. Julkishallinnon organisaation tulee säännönmukaisesti huomioida toiminnassaan vallitseva lainsäädäntö, säännöt ja viranomaisen toimintaan kohdistuvat vaatimukset sekä niiden toteuttamiseen tähtäävä Vahti-ohjeistus, mikä ohjaa keskeisesti myös kohdeorganisaation mittauskohteiden valintaa. Tietoturvallisuusasetuksen voimaantulon ja siirtymäajan jälkeen Vahti-ohjeissa on säännönmukaisesti linjattu organisaatioiden tietoturvallisuuden vähimmäisvaatimukset (perustason vaatimukset) sekä myös korkeamman tason vaatimuksia (korotettu taso, korkea taso).

6.1 Mittariston tavoitteiden ja mittausnäkökulmien määrittäminen

Kohdeorganisaation tietoturvallisuuden mittareiden suunnittelussa keskeisenä normatiivisena viitekehyksenä on lainsäädännön velvoitteet sekä tietoturvaasetuksen perustason tietoturvavaatimukset ja niiden toteutusta tukeva Vahti-ohjeistus. Työn tavoitteena on kartoittaa mittareita, joilla voidaan arvioida vaatimusten toteutumista kohdeorganisaation tietoturvallisuuden hallintajärjestelmässä. Lisäksi mittareita kartoitetaan ja mittaamista kohdennetaan ISO/IEC 27004:2016 -standardin suositusten, riskienhallinnan sekä ydinjärjestelmien osalta BIA-vaikutusanalyysien kautta. Tässä työssä tuotetaan kohdeorganisaatiolle soveltuvat keskeiset mittarit, huomioiden ensi sijassa infrastruktuurin ja tietoprosessien tällä hetkellä tuottama aineisto. Kun mittaristo ja mittausprosessi on testattu ja otettu

käyttöön, tavoitteena on myöhemmässä vaiheessa edelleen kehittää mittaristoa osana tietoturvallisuuden hallintaprosessia.

Työn empiirisessä osiossa käytetään luvussa 4.2 kuvattua asiantuntijaorganisaation suorituskykymittariston mallia sekä mittausprosessia. Näiden lisäksi mittaamisen tueksi kartoitettiin sopivaa standardia, jonka avulla saadaan määriteltyä, millaisilla mittareilla kohdeorganisaatiossa voidaan mitata tietoturvallisuuden hallintajärjestelmää sekä tietoturvallisuuden toteutumisen tehokkuutta. Vahti-ohjeissa on usein viitattu ISO/IEC-standardiperheeseen, kuten Vahti 3/2007 -ohjeessa, jossa esitetään ISO/IEC 27001 Tietoturvallisuuden hallintajärjestelmää koskeva kansainvälinen standardi PDCA-mallin soveltamisessa ja ISO 27001 osana tietoturvallisuuden hallintajärjestelmän mallia. Vahti 2/2012 -ohjeessa on viitekehyksenä käytetty ICT-varautumisen vaatimuksissa ISO-standardeja 27001 ja 22301 sekä Vahti 2/2014 -ohjeessa on viitattu ISO 27001 -standardin vaatimuksiin, joita voidaan toteuttaa tietoturvallisuuden hallintajärjestelmän (ISMS, Information Security Management System) avulla.

Koska kohdeorganisaation tavoitteena on kehittää myös tietoturvallisuuden hallintajärjestelmää (ISMS), mittaamisen määrittelemisen tueksi valittiin standardi ISO/IEC 27004:2016. Se on tarkoitettu organisaatioille avuksi tietoturvan tason ja tietoturvallisuuden hallintajärjestelmän vaikuttavuuden arviointiin, kun halutaan täyttää standardin ISO/IEC 27001:2013 kohdassa 9.1 esitetyt vaatimukset:

a) Tietoturvallisuuden tason seuranta ja mittaaminen
b) Tietoturvallisuuden hallintajärjestelmän ja sen prosessien ja hallintakeinojen vaikuttavuuden seuranta ja mittaaminen
c) Seurannan ja mittausten tulosten analysointi ja arviointi.

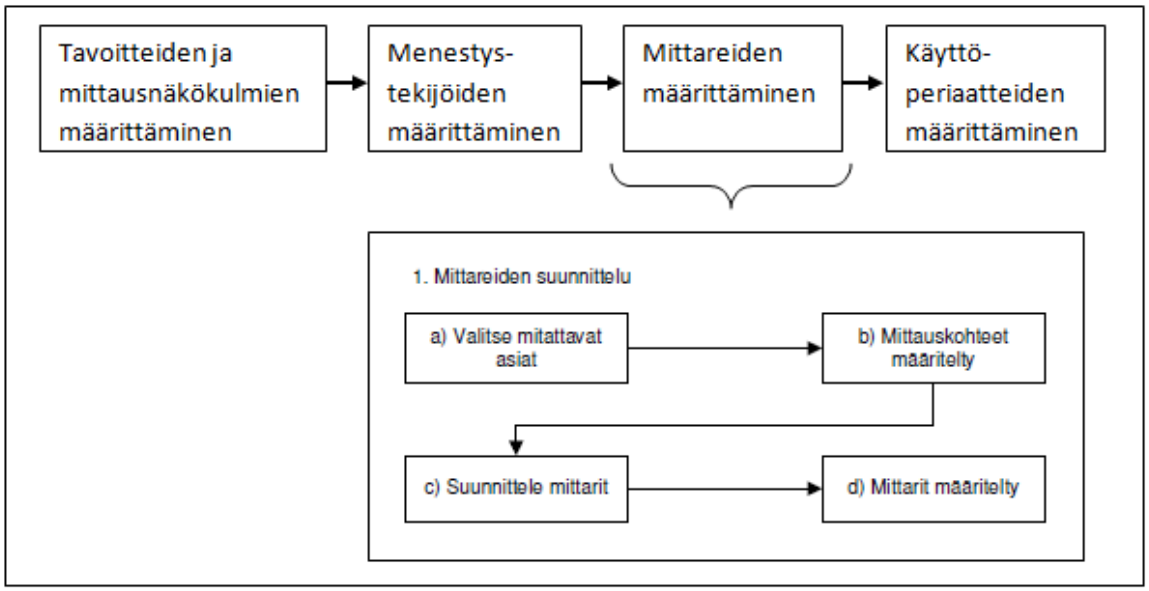
ISO/IEC 27004:2016 -standardissa kuvataan, miten tietoturvallisuuden hallintajärjestelmän prosessien ja hallintakeinojen toteuttaminen sekä tietoturvallisuuden tason varmistaminen voivat tarjota organisaation toimintaan ja talouteen liittyviä hyötyjä:

1. *Parantunut vastuullisuus:* Seuranta, mittaus, analysointi ja arviointi voivat lisätä tietoturvallisuutta koskevaa vastuullisuutta, koska ne avustavat tun-

nistamaan tietoturvaprosessit tai hallintakeinot, jotka on toteutettu virheellisesti, joita ei ole toteutettu ollenkaan tai jotka ovat tehottomia.

2. *Parantunut tietoturvallisuuden taso ja parantuneet tietoturvallisuuden hallintajärjestelmän prosessit:* Seuranta, mittaus, analysointi ja arviointi voivat tarjota organisaatioille mahdollisuuden määrittää tietojen turvaamisen parannusten suuruus tietoturvallisuuden hallintajärjestelmän puitteissa ja osoittaa määrällisesti ilmaistavissa olevaa edistymistä organisaation tietoturvatavoitteiden saavuttamisessa.
3. *Näyttö vaatimusten täyttämisestä:* Seuranta, mittaus, analysointi ja arviointi voivat tarjota dokumentoitua näyttöä, joka auttaa osoittamaan standardissa ISO/IEC 27001 (sekä muissa standardeissa) esitettyjen vaatimusten täyttämisen. Lisäksi ne voivat tarjota näyttöä organisaatiota koskevien lakien, sääntöjen ja viranomaisten vaatimusten täyttymisestä.
4. *Tuki päätöksenteolle:* Seuranta, mittaus, analysointi ja arviointi voivat tukea riskit huomioon ottavaa päätöksentekoa tarjoamalla riskienhallintaprosessiin määrällisesti ilmaistavaa tietoa. Se voi tarjota organisaatioille keinon mitata nykyisten ja aiempien tietoturvallisuuteen tehtyjen investointien onnistumista ja epäonnistumista. Siitä olisi saatava määrällisesti ilmaistavaa tietoa, josta voi olla apua tulevien investointien resurssien kohdentamisessa.

Kohdeorganisaation mittareiden suunnittelu etenee kuvan 17 mukaan, jossa on hyödynnetty luvussa 5.2 esitettyjä suunnittelu- ja mittausprosessin kuvia.



Kuva 17. Mittareiden suunnittelun eteneminen (mukailtu lähteistä Lönnqvist & Mettänen 2003, 84 ja Lönnqvist 2004, 143).

Mittariston suunnittelun alkuvaiheessa valitaan mittausnäkökulmat, joiden määrittäminen voidaan tehdä monella eri tavalla. Mittausnäkökulmat voidaan ottaa suoraan jostakin valmiista mittaristomallista. Esimerkiksi tasapainotetussa mittauksessa, joka esitettiin kappaleessa 4.3, pyritään kokonaisuuteen, jossa valitut mittausnäkökulmat muodostavat järkevän ja tasapainotetun kokonaisuuden. (Lönnqvist & Mettänen 2003, 89.)

Mittausnäkökulmien valinnassa on huomioitava tietoturvallisuuden kytkeytyminen organisaation johtamiseen ja tietoturvallisuuden tulosjohtamiseen, jonka periaatteena on kehittää tietoturvakulttuuria osana organisaation riskienhallintaa. Tietoturvatoiminnan tavoitteena on vähentää toimintaan kohdistuvia häiriöitä ja tietoturvariskejä sekä aikaansaada toiminnallista laatua minkä vuoksi toimintaa ja tavoitteita on perusteltua tarkastella organisaation toiminnan jatkuvuuden, asiakaspalvelujen, sidosryhmien, muutoksen hallinnan ja säädösnäkökulmista. Keskeisessä asemassa johtamisen näkökulmasta on tietoturvallisuuden johtamis- ja hallintajärjestelmä, joka toimii sateenvarjona ja määrittää tietoturvallisuuden johtamismenettelyt. (Tietoturvatavoitteiden asettaminen ja mittaaminen 2006, 16-18.)

Tutkimuksessa käytetään tasapainotetun mittaristomallin periaatetta, jota tarkastellaan tietoturvallisuuden menestystekijöiden näkökulmasta. Tietoturvamittariston suunnittelussa painotetaan ei-taloudellisia menestystekijöitä, joten Kaplanin ja Nortonin Balanced Scorecard -mallista jätetään pois taloudellinen näkökulma ja työssä huomioidaan siten seuraavat mittausnäkökulmat:

1. Asiakasnäkökulma
2. Sisäinen näkökulma
3. Oppimisen ja kasvun näkökulma.

Lönnqvistin ja Mettäsen (2003, 40) mukaan Balanced Scorecardin neljä näkökulmaa eivät ole ehdottomia ja niitä voi muokata sopiviksi kuhunkin tilanteeseen. Painoarvo voi määräytyä esimerkiksi organisaation strategisten arvojen mukaan. Edellä lueteltuja tietoturvallisuuden johtamisen näkökulmia painotetaan tietoturvamittariston suunnittelussa ja ne sisältyvät luvussa 4.3 (kuva 13) esitetyn tasapainotetun tuloskortin näkökulmiin seuraavasti:

- Asiakaspalvelujen näkökulma → Asiakasnäkökulma
- Sidosryhmien näkökulma → Asiakasnäkökulma
- Toiminnan jatkuvuuden näkökulma → Sisäinen näkökulma
- Muutoksen hallinnan näkökulma → Sisäinen näkökulma
- Säädösnäkökulma → Sisäinen näkökulma.

Mittausnäkökulmien ja menestystekijöiden määrittelyssä otetaan myös huomioon ISO/IEC 27004:2016 -standardin tietotarpeiden suunnittelun prosessi, josta on hyötyä tietoturvallisuuden hallintajärjestelmän toiminnallisten ominaisuuksien ja suorituskyvyn ymmärtämisessä.

6.2 Menestystekijöiden määrittäminen

Määriteltyihin mittausnäkökulmiin valitaan seuraavaksi kunkin näkökulman osalta suorituskyvyn ja tavoitteiden kannalta tärkeimmiksi koetut menestystekijät eli mitattavat asiat. Tietoturvallisuuden tilaa kuvaavien menestystekijöiden määrittämiseen liittyy oleellisena osana tietotarpeiden tunnistaminen ja kartoittaminen, mikä voidaan toteuttaa esimerkiksi ISO/IEC 27004:2016 -standardin mukaan. Tietotar-

peiden tunnistamisella on hyötyä mm. tietoturvallisuuden hallintajärjestelmän toiminnallisten ominaisuuksien ja suorituskyvyn ymmärtämisessä.

Kuhunkin mittausnäkökulmaan voidaan valita esimerkiksi kahdesta viiteen menestystekijää. Menestystekijät voidaan määrittää organisaation strategian perusteella ja/tai käyttäen apuna sidosryhmien tarpeita, päämääränä tunnistaa organisaation toiminnan kannalta tärkeimmät tavoitteet. Menestystekijöiden määrittäminen vaatii usein kompromisseja, sillä kaikkea ei voi mitata. Ne ovat usein organisaatiokohtaisia sen mukaan, mitä organisaatiossa halutaan painottaa. Asiantuntijaorganisaatiossa korostuvat usein ei-taloudelliset, aineettomat menestystekijät. (Lönnqvist & Mettänen 2003, 90 - 92.)

Menestystekijöiden määrittelyn jälkeen tarkastetaan vielä kokonaisuus ja tavoitteena on, että jokaiseen mittausnäkökulmaan sisältyy yksi tai useampi menestystekijä. Näkökulmien painotuksesta ja valinnasta sekä valituista menestystekijöistä riippuu, kuinka monta menestystekijää kukin näkökulma sisältää. Yleisperiaatteena voidaan pitää, että eri näkökulmissa on suunnilleen saman verran menestystekijöitä, joten tässä yhteydessä mittariston suunnittelua mahdolliset päällekkäisyydet poistetaan ja menestystekijöitä yhdistetään mahdollisuuksien mukaan. (Lönnqvist & Mettänen 2003, 92.)

Tavoitteena on, että menestystekijät määritetään kerralla ja lopulliseen muotoonsa, mutta käytäntö on osoittanut, että näin tapahtuu harvoin. Usein menestystekijöitä joudutaan tarkentamaan suunnitteluprosessin edetessä ja tulevissa vaiheissa, jos se koetaan tarpeelliseksi. Näin voi käydä esimerkiksi mittaria määritettäessä, jolloin voidaan huomata, että valittua menestystekijää on mahdoton mitata, ja menestystekijää joudutaan muokkaamaan sopivampaan muotoon. (Lönnqvist & Mettänen 2003, 94.)

Työssä tietoturvallisuuden menestystekijöitä määriteltiin kahdessa suunnitteluvaiheessa, jonka jälkeen määriteltyjä menestystekijöitä pyrittiin yhdistämään kokonaisuuksiksi. Ensin kuhunkin kolmeen mittausnäkökulmaan määriteltiin menestystekijöitä mahdollisimman kattavasti ja päällekkäisyyksiin ei tässä vaiheessa puututtu.

Alla on luettelo ensimmäisen suunnitteluvaiheen menestystekijöistä:

1. Asiakasnäkökulma
    - Asiakasvaatimukset
    - Sidosryhmien vaatimukset
    - Strategian ja sidosryhmälupausten mukainen toiminta
        - Asiakkuuslupaus
        - Kumppanuuslupaus
        - Henkilöstölupaus
        - Yhteiskuntalupaus
    - Tietoturvallisten järjestelmien ja palvelujen tuottaminen
        - Järjestelmän laatu
        - Informaation laatu
        - Palvelun laatu
2. Sisäinen näkökulma
    - Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta
    - Säädösperusteisen tietoturvatason toteutuminen
    - Tietoturvallisuuden tulostavoitteiden toteutuminen
    - Tietoturvatoiminnan tuloksellisuus ja tehokkuus
    - Tietoriskien havaitseminen ja niihin reagoiminen
    - Tietoturvatapahtumien ja -poikkeamien havaitseminen
    - Tietoturvallisten järjestelmien ja palvelujen tuottaminen
        - Järjestelmän laatu
        - Informaation laatu
        - Palvelun laatu
    - Tietoturva-arkkitehtuurin tavoitteiden toteutuminen
    - Tietoturva- ja tietosuojapolitiikan mukainen toiminta
    - Yhtenäinen tietoturvanäkemys ja -kulttuuri
    - Tietoturvallisuuden arviointi ja auditointi
    - Tietoturvallisuuden hallintajärjestelmän kehittyneisyys ja laatu
    - Toiminnan jatkuvuuden toimenpiteiden toteutuminen
    - Tietoturvallisuuden muutoksenhallinnan toteutuminen
    - Tietoturvallisuuden tason arviointi
    - Kriittisten tietoprosessien ja järjestelmien hallinta

- Tietoturvallisuuden dokumentoinnin toteutuminen

3. Oppimisen ja kasvun näkökulma
   - Tietoturvatietoisuus
   - Tietoturvavaatimukset tiedossa
   - Tietoturvaosaaminen
   - Perehdyttäminen
   - Toimintatavat

Toisessa suunnitteluvaiheessa tietoturvallisuuden menestystekijöitä arvioitiin ja tärkeysluokiteltiin ensi sijassa riskienhallinnan ja normatiivisten velvoitteiden kannalta sekä arvioitiin, kuinka helposti menestystekijöihin liittyviä mittareita on käyttöönotettavissa nykyisessä toimintaympäristössä. Toisessa suunnitteluvaiheessa käsiteltiin uudelleen ensimmäisessä suunnittelussa kirjatut menestystekijät ja arvioitiin kunkin menestystekijän kohdalla, miten niiden johtaminen mittareiksi voidaan toteuttaa, ottaen huomioon kohdeorganisaation nykytila sekä lähitulevaisuuden tavoitetila.

Määrittelytyössä apuna käytettiin ISO/IEC 27004:2016 -standardin (2016, 15) tietotarpeiden tunnistamisen ja määrittelyn prosessia, jonka mukaan pyritään tunnistamaan:

1. Sidosryhmien tarpeet
2. Organisaation strateginen suunta
3. Tietoturvapolitiikka ja tavoitteet
4. Riskienkäsittelysuunnitelma.

Tietotarpeita tarkasteltiin ja määriteltiin edelleen ISO/IEC 27004:2016 -standardin (2016, 15) prosessin mukaan seuraavasti:

1. Tarkastellaan tietoturvallisuuden hallintajärjestelmää, sen prosesseja ja muita osia
2. Asetetaan tärkeysjärjestykseen tunnistetut tietotarpeet
3. Valitaan tärkeysjärjestykseen asetetuista tietotarpeista ne tiedot, joille tarvitaan mittaustoimintoja
4. Dokumentoidaan valitut tietotarpeet ja viestitään niistä kaikille olennaisille sidosryhmille.

Lönnqvist ja Mettänen (2003, 92) ohjeistavat, että jokaiseen valittuun mittausnäkökulmaan on tarkoituksenmukaista sisällyttää yksi tai useampi menestystekijä. Suunnitteluvaiheiden ja kartoitusten tuloksena valittiin kolmeen mittausnäkökulmaan yhteensä 7 menestystekijää, jotka sisältävät useita päällekkäin ja limittäin olevia menestystekijöitä. Ensimmäisen suunnitteluvaiheen menestystekijöiden luetteloa on tarkoitus hyödyntää mittariston testikäytön jälkeen, jolloin mahdolliset korjaustarpeet selviävät. Lisäksi menestystekijöiden luetteloa voidaan hyödyntää mittariston jatkokehittämisessä, jolloin suunnittelua voidaan jatkaa sujuvasti olemassa olevalla materiaalilla.

Alla on lueteltu yhteenveto ensimmäisen ja toisen suunnitteluvaiheiden kartoituksista. Määrittelyn tuloksena on valittu menestystekijöitä, joihin liittyvien mittareiden vaiheittainen toteuttaminen arvioitiin mahdolliseksi lähitulevaisuudessa, ottaen huomioon kohdeorganisaation nykyinen käyttöympäristö ja infrastruktuuri sekä kehittämissuunnitelmat. Kaikkia suunnitteluvaiheissa saatuja tuloksia hyödynnetään tietoturvamittariston suunnittelussa ja jatkokehittämisessä sekä mittariston käyttöönoton yhteydessä, mikäli työssä määriteltyä mittaristoa arvioidaan uudelleen esimerkiksi mittarien testauksen jälkeen.

1. Asiakasnäkökulma
    - Tietoturvallisten järjestelmien ja palvelujen tuottaminen
2. Sisäinen näkökulma
    - Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta
    - Tietoriskien havaitseminen ja niihin reagoiminen
    - Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu
    - Tietoturvallisuuden arviointi ja auditointi
3. Oppimisen ja kasvun näkökulma
    - Tietoturvatietoisuus
    - Tietoturvaosaaminen ja koulutus

6.3 Mittareiden määrittäminen

Menestystekijöiden valinnan jälkeen kullekin menestystekijälle määritellään sopiva mittari tai useampia mittareita. Mittarin valintaan vaikuttaa ensisijaisesti mittarin käyttötarkoitus, joten jokaisen mittarin kohdalla on pohdittava, mihin mittaria käytetään eli valitaan ne asiat, joista halutaan mittausinformaatiota, ja jotka vastaavat menestystekijän tietotarpeisiin. Luvussa 4.1 kuvattiin mittareiden luokituksen periaatteita ja mittausteoreettisia ominaisuuksia, kuten validiteetti, reliabiliteetti, relevanssi ja käytännöllisyys, jotka kuvastavat hyvän mittarin ominaisuuksia, ja joiden mukaan tietoturvallisuuden mittareita pyritään määrittämään.

6.3.1 Mitattavien asioiden valinta

Tietoturvamittareiden suunnittelun alkuvaiheeseen kuuluu mitattavien asioiden valinta. ISO/IEC 27004:2016 -standardin (2016 6, 9) mukaan mittausten on vastattava organisaation tietotarpeisiin ja mittareiden laatimiseen liittyy ensivaiheessa tietotarpeiden määrittäminen. Tämän jälkeen päätetään, mitä mittareita tarvitaan kunkin erillisen tietotarpeen tueksi ja mitä dataa tarvitaan mittareiden luomiseen.

Työssä tarkasteltiin valittuja tietoturvallisuuden menestystekijöitä ja kuvattiin ensivaiheessa mitattavia asioita mahdollisimman laajasti, jotta saatiin riittävä näkemys kunkin menestystekijän mitattavuudesta ja aineistoa mittariston laajentamiseen myöhemmässä vaiheessa.

Mitattavien asioiden kartoituksessa käytiin läpi tietoturva-asetuksen ja Vahti-ohjeiden perustason vaatimuksia sekä Vahti-suosituksia. Tietoturvallisuusasetuksen 5 §:ssä säädetään kymmenen vaatimusta tietoturvallisuuden perustasolle, joita täsmentää ja täydentää Vahti-ohje 2/2010, jossa vaatimukset on kuvattu yksityiskohtaisesti. Lisäksi käytiin läpi muita julkaistuja Vahti-ohjeita, joissa on kuvattu vaatimuksia tai suosituksia tietoturvallisuuden mittaamiseksi. Mitattavien asioiden kartoituksessa huomioidaan myös luvussa 6.2 esitetyt ISO/IEC 27004:2016 -standardin mukaiset tietotarpeet.

Työ eteni siten, että ensivaiheessa käytiin läpi tietoturvallisuuden perustason vaatimuksia ja niihin liittyviä tietotarpeita sekä arviotiin vaatimusten mitattavuutta. Perustason vaatimusten mitattavuuden arvioinnissa huomioitiin suorituskykyyn ja vaikuttavuuteen sekä määrälliseen ja laadulliseen mittaamiseen liittyviä vaatimuksia. Kartoituksen yhteydessä Vahti-ohjeista kerättiin perustason vaatimusten lisäksi myös muuta tietoturvallisuuden mittaamiseen liittyvää aineistoa, josta arvioitiin saatavan lisähyötyä mittariston suunnittelussa. Arvioinnissa tuotetusta materiaalista muodostettiin taulukko (liite 1), jossa tietoturvavaatimuksia ja tietoturvamittareita on luokiteltu luvuissa 6.1 ja 6.2 kuvattujen mittausnäkökulmien ja menestystekijöiden vaatimusten mukaan. Arvioinnissa karsittiin pois asioita, joista on vaikeaa tai mahdotonta saada mittausinformaatiota, jotka arvioitiin hankalaksi toteuttaa nykyisessä ympäristössä tai joiden tärkeys ei nouse riittävän korkealle.

ISO/IEC 27004:2016 -standardin (2016, 16) mukaan mittarien on vastattava tietotarpeisiin ja mittarien määrittelyssä voidaan turvautua nykyisiin käytäntöihin tai niitä varten voidaan tarvita uusia käytäntöjä. Tietotarpeita määritettäessä on myös otettava huomioon, että organisaation täytyy kerätä asianmukainen määrä dataa ennen analyysiä ja arviointia, jotta arviointia ja vertailua voidaan pitää merkitsevinä.

ISO/IEC 27004:2016 -standardissa (2016, 16) on lueteltu esimerkkejä turvallisuuteen liittyvien mittarien tueksi kerättävästä datasta, jota hyödynnetään myös tässä työssä:

- Erilaisten lokien ja skannausten tulokset
- Koulutuksen ja muiden henkilöresursseihin liittyvien toimien tilastot
- Asianmukaiset kyselyt ja kyselylomakkeet
- Häiriötilanteisiin liittyvät tilastot
- Sisäisten auditointien tulokset
- Liiketoiminnan jatkuvuuteen ja katastrofeista toipumiseen liittyvien harjoitusten tulokset
- Johdon katselmusten raportit.

Mittareiden suunnittelun tueksi kerättiin myös dataa ja hyödynnettiin soveltuvin osin Barabanovin ym. (2001, 38-39) tuottamaa listaa tutkimuksen informaatiolähteistä:

- Riskianalyysien tulokset
- Omaisuuden- ja varainhoidon järjestelmät
- Järjestelmien konfiguraationhallinta
- Ohjelmistopäivitysten hallintajärjestelmät
- Verkkojen skannauksen työkalut
- Muutoksenhallinnan prosessit ja seuranta
- Tietoturvatapahtumien ja poikkeamien hallintajärjestelmät
- Tietoturvapoikkeamaraportit
- Järjestelmien ja sovellusten seurantatiedot
- Penetraatiotestien tulokset
- Asiakkuuden hallintajärjestelmät
- Talouden hallintajärjestelmät
- Julkaistut budjetit
- Identiteetin hallintajärjestelmät
- Sisäisten tai ulkoisten auditointien raportit
- Henkilöstökyselyt ja henkilöhaastattelut
- Sosiaalisen hakkeroinnin testausraportit
- Tietoturvatietoisuuden harjoitusten tulokset

6.3.2 Mittauskohteiden määrittely

Menestystekijöiden valitsemisen ja tietotarpeiden arvioinnin jälkeen määritetään mittauskohteet ja kullekin menestystekijälle sopiva mittari tai useampi mittari. Mittarin käyttötarkoitus vaikuttaa ensisijaisesti soveltuvan mittarin valintaan ja jokaisen mittarin kohdalla tulee pohtia, mihin mittaria käytetään. Yleensä mittari kannattaa valita mittaristoon, jos sen käyttö on edullista ja helppoa. Tätä periaatetta noudatetaan ensisijaisesti myös tässä työssä. (Lönnqvist & Mettänen 2003, 94.)

Yleisimmät syyt tietoturvan mittaamiseen ovat vaatimuksenmukaisuuden ja tietoturvallisuuden hyödyn osoittaminen ja yleisimmin käytetyt mittarit liittyvät haittaoh-

jelmiin, tietoturvakorjauksiin, ulkoisiin tietoturvavaatimuksiin, tarkastustuloksiin ja kustannuksiin. Tietoturvallisuuden mittaamisen kohteet valittiin hyödyntäen perustason tietoturvavaatimuksia, Vahti-ohjeita, ISO/IEC 27004:2016 -standardin suosituksia sekä ydinjärjestelmien BIA-vaikutusanalyysejä, joiden tuloksia havainnollistetaan kappaleessa 6.5. Työssä tehdyt ydinjärjestelmien BIA-vaikutusanalyysit tuottivat informaatiota, jonka avulla priorisoitiin ja tärkeysluokiteltiin järjestelmiä kriittisyysluokkiin, joka on lähtökohtaisesti ensimmäisiä tehtäviä järjestelmiin liittyvän tietoturvallisuuden mittaamisessa. Tietojärjestelmien tärkeysluokittelu edesauttaa ”kruununjalokivien” tunnistamisessa ja edelleen tietojärjestelmiin liittyvien mittauskohteiden valinnassa ja mittareiden suunnittelemisessa.

Tietoturvallisuuden mittaaminen sekä BIA-vaikutusanalyysit tuottavat myös informaatiota, jolla kohdeorganisaatio voi arvioida tietosuoja-asetuksen (GDPR) säännösten toteutumista ja huolehtia osaltaan tietosuoja-asetukseen liittyvän osoitusvelvollisuuden noudattamisesta. Tietoturva on yksi tietosuojan toteuttamisen keino, minkä tarkoituksena on suojata tietoaineisto ja tietojärjestelmät asianmukaisilla organisatorisilla ja teknisillä toimenpiteillä (Tietosuojavaltuutetun toimisto).

Mittauskohteiden määrittelyssä hyödynnettiin ja arvioitiin kappaleessa 6.3.1 (mitattavien asioiden valinta) tuotettua materiaalia sekä ISO/IEC 27004:2016 -standardissa (2016, 9) esitettyä seurattavien järjestelmien, prosessien ja toimintojen listaa, joiden mukaan valittiin menestystekijöihin liittyvien mittauskohteiden seuranta:

1. Tietoturvallisten järjestelmien ja palvelujen tuottaminen
    - Järjestelmien ja palvelujen sopimukseen liitettävät tietoturvavaatimukset yhteistyön ja hankinnan kohteesta
    - Järjestelmien tietoturvapoikkeamien hallinta
    - Järjestelmien tietoturvahäiriöiden hallinta
    - Järjestelmien haavoittuvuuksien hallinta
    - Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta
    - Järjestelmien ja palvelujen jatkuvuudenhallinta ja toipuminen
    - Järjestelmien riskienhallinta ja tärkeysluokittelu
    - Järjestelmien konfiguraationhallinta ja tietoturvatestaus
    - Järjestelmien pääsyoikeuksien hallinta

2. Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta
    - Lainsäädäntö ja tietoturvavelvoitteet
3. Tietoriskien havaitseminen ja niihin reagoiminen
    - Tietoturvapoikkeamien hallinta
    - Tietoriskien hallinta
4. Tietoturvallisuuden arviointi ja auditointi
    - Tietoturvallisuuden arviointi
    - Tietoturvallisuuden auditointi
5. Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu
    - Tietoturvatoiminnan tehokkuus
    - Käyttövaltuuksien hallinta
    - Jatkuvuudenhallinta
6. Tietoturvatietoisuus
    - Viestintä ja ohjeistus
    - Perehdyttämisprosessi
7. Tietoturvaosaaminen ja koulutus
    - Tietoturvakoulutus

6.3.3 Mittareiden suunnittelu

Varsinainen mittareiden suunnittelu ja yksityiskohtainen dokumentointi työstettiin menestystekijöiden, tietotarpeiden ja mittauskohteiden määrittelyn jälkeen. Mittariston kokonaismäärä ja ominaisuudet on koostettu liitteeseen 1, josta valittiin jatkosuunnittelua ja -työstämistä varten seuraavat 21 tietoturvamittaria:

1. Tietojärjestelmien tietoturvallisuuden tila
2. Käyttöpalveluiden tietoturvallisuuden tila
3. Tietojärjestelmien turvakuvaukset
4. Tietojärjestelmien BIA-vaikutusanalyysit
5. Hälytysrajojen ja kriittisyyden arvojen ylittävät tapahtumat
6. Toteutetut torjuntaohjelmien päivitykset
7. Toteutetut tietoturvapäivitykset
8. Tietojärjestelmien tietoriskianalyysit

9. Tietojärjestelmien käyttöoikeuksien arviointi ja tarkastaminen
10. Tietoturvahäiriöiden lukumäärä mittausjaksolla
11. Rekisteriselosteiden/tietosuojaselosteiden lukumäärä
12. Tietojärjestelmäkuvausten lukumäärä
13. Tietoturvapoikkeamien lukumäärä
14. Havaitut virus- ja muut haittaohjelmat
15. Varkauksien ja kadotettujen laitteiden lukumäärä
16. Priorisoitujen ja kriittisten tietoriskien käsittelyn eteneminen kokonaisriskien hallinnassa
17. Tietoturvakatselmointien lukumäärä
18. Tietoturva- ja tietosuojaryhmän kokousten lukumäärä
19. Tietoturva- ja tietosuojainfot sekä henkilöstölle suunnattujen tiedotteiden lukumäärä
20. Perehdyttämisprosessin tietoturva- ja tietosuoja-asioiden läpikäynti
21. Allekirjoitettujen salassapitosopimusten lukumäärä

6.4 Määriteltyjen mittareiden käyttöperiaatteet

Koska mittareita, mittauksen käyttötilanteita ja mittauksen käyttäjiä on hyvin monenlaisia, on mittareiden määrittämisen jälkeen valittava jokaiselle valitulle mittarille käyttöperiaatteet. Mittareiden käyttöperiaatteet voidaan dokumentoida usealla tavalla. Esimerkiksi Lönnqvist ja Mettänen (2003, 99, 101) ovat esittäneet käyttöperiaatteiden lomakkeen ja dokumentointimenettelyn, jota organisaatiot voivat hyödyntää käytön kuvaamisessa, jolloin mittarin käytöstä tai tuloksista kiinnostuneet henkilöt ymmärtävät helpommin keskeiset mittariin liittyvät asiat.

Käyttöperiaatteet tulisi ratkaista mittari- ja tapauskohtaisesti pääosin jo mittareiden suunnitteluvaiheessa ja ensisijaisesti mittarin kohdalla tulee vastata seuraaviin kysymyksiin:

- Kuinka usein tulos kerätään?
- Kuka vastaa datan keräämisestä?
- Mistä data saadaan?
- Mikä on tavoitearvo?

Lisäksi voidaan pohtia kenelle ja missä mittarin tulos raportoidaan. Mittaustulosten tulkinnan helpottamiseksi on hyvä, jos käyttöperiaatteet ovat nähtävissä myös mittausraportin yhteydessä. (Lönnqvist & Mettänen 2003, 100.)

Usein mittarin yksityiskohtainen määrittäminen tuottaa mittarin käyttöperiaatteet, jotka dokumentoidaan lopuksi. Tämä toteutui myös tässä työssä, sillä aineiston keräämisen ja tuottamisen yhteydessä saatiin luontevasti aineistoa myös liitteen 1 mittari-tietokenttiä varten, joissa kuvataan kussakin mittauskohteessa käytettyjä tietoturvamittareita. Tällöin mittarin määrittämisvaiheella ja käyttöperiaatteiden määrittämisellä ei ole käytännön kannalta suurta eroa. Vaikka mittareille määritetään käyttöperiaatteet ne saattavat Lönnqvist & Mettänen (2003, 100) mukaan muuttua tai tarkentua myöhemmin, sillä voidaan esimerkiksi huomata, että mittariin tarvittavaa informaatiota ei saada riittävän helposti kyseisestä lähteestä. Lisäksi tulosten raportoinnin yhteydessä voidaan myös havaita, että mittarin tuloksia on tarpeetonta kerätä aikaisemmin suunnitellulla aikavälillä. Työssä on tämä otettu huomioon siten, että mittareita on pyritty kuvaamaan mahdollisimman laajasti, jolloin mittareita voidaan muuttaa tai ottaa tarvittaessa käyttöön muita liitteessä 1 kuvattuja mittareita, joita ei valittu tuotantokäyttöön kappaleessa 5.3.3 kuvatun mittariston valinnassa.

Osa luetelluista mittareista on osaltaan jo käytössä ja liittyvät esimerkiksi nykyisen tietojärjestelmän tai palvelun prosessiin. Niiden osalta tavoitteena on tässä yhteydessä yhdenmukaistaa mittauksen käyttöperiaatteita ja seurantaa sekä tuottaa mittausdataa ja -tietoa tarkoituksenmukaisesti mm. raportoinnin kannalta. Kukin tuotantokäyttöön valittu mittari on kuvattu taulukossa 1 hyödyntäen edellä kuvattua käyttöperiaatteiden dokumentointimenettelyä:

Taulukko 1. Tietoturvamittareiden käyttöperiaatteet.

Mittari	**Kuinka usein tulos raportoidaan**	**Kuka vastaa raportoinnista**	**Mistä tarvittava informaatio saadaan**	**Mikä on tavoitearvo**
Tietojärjestelmien tietoturvallisuuden tila	1 / kk, 1 / vuosi	Järjestelmän vastuuhenkilö	Palveluntarjoajan raportointi, tietoturvallisuuden tilaraportointi	Ydinjärjestelmien kk ja vuosiraportointi tuotettu
Käyttöpalveluiden tietoturvallisuuden tila	1 / 3kk	Palvelusopimuksen mukaan	Palveluntarjoajan raportointi	Sopimuksen mukainen raportointi tuotettu

Tietojärjestelmien turvakuvaukset	1 / vuosi	Järjestelmän vastuuhenkilö	Järjestelmän toimittajan turvakuvaus -dokumentti, järjestelmädokumentaatio	Kuvaus tuotetaan osana uuden järjestelmän käyttöönottoa
Tietojärjestelmien BIA-vaikutusanalyysit	1 / vuosi	Järjestelmän vastuuhenkilö, tietoturva-asiantuntija	Asianhallinta, järjestelmädokumentaatio	BIA-vaikutusanalyysi tuotetaan uusista ydinjärjestelmistä
Hälytysrajojen ja kriittisyyden arvojen ylittävät tapahtumat	1 / kk	Palvelusopimuksen mukaan, järjestelmän vastuuhenkilö	Järjestelmien lokitiedot, tikettijärjestelmä, jolla käsitellään turvallisuustapahtumia, torjuntaohjelmien hälytykset	100% kaikissa mitattavissa tapahtumissa
Toteutetut torjuntaohjelmien päivitykset	1 / kk	Palvelusopimuksen mukaan, järjestelmän vastuuhenkilö	Palveluntarjoajan raportointi, tietoturvallisuuden tilaraportointi	Kriittiset 100% seuraavassa päivitysaikaikkunassa, kk-raportointi tuotettu
Toteutetut tietoturvapäivitykset	1 / kk	Palvelusopimuksen mukaan, järjestelmän vastuuhenkilö	Palveluntarjoajan raportointi, tietoturvallisuuden tilaraportointi	Kriittiset 100% seuraavassa päivitysaikaikkunassa, kk-raportit tuotettu
Tietojärjestelmien riskianalyysit	1 / vuosi	Järjestelmän vastuuhenkilö	Riskianalyysi -dokumentaatio, tietoturvallisuuden tilaraportointi	Riskianalyysi tuotetaan osana uuden järjestelmän käyttöönottoa, jatkossa riskienhallintamenettelyn mukaan
Tietojärjestelmien käyttöoikeuksien arviointi ja tarkastaminen, vanhentuneiden tunnusten lukumäärä	1 / vuosi	Järjestelmän/prosessin omistaja, esimies	Käyttöoikeuksien arvioinnin ja tarkastamisen menettely	Ydinjärjestelmien tarkastaminen tehty, arvioinnin ja tarkastamisen dokumentointi tuotettu
Tietoturvahäiriöiden lukumäärä mittausjaksolla	1 / kk	Palvelusopimuksen mukaan, järjestelmän vastuuhenkilö	Palveluntarjoajan raportointi, tietoturvallisuuden tilaraportointi	Verrataan häiriöluetteloa edelliseen jaksoon, trendiviivan kehityssuunta, kk-raportit tuotettu
Rekisteriselosteiden/ tietosuojaselosteiden lukumäärä	1 / vuosi	Järjestelmän vastuuhenkilö	Dokumentit, asianhallinta, järjestelmät	100%, selosteet tuotettu
Tietojärjestelmäkuvausten lukumäärä	1 / vuosi	Järjestelmän vastuuhenkilö	Dokumentit, asianhallinta, järjestelmät	100%, kuvaukset tuotettu
Tietoturvapoikkeamien lukumäärä	1 / kk	Palvelusopimuksen mukaan, tietoturva-asiantuntija	Tietoturvapoikkeamamenettely ja ilmoituslomake, raportti poikkeamista, palveluntarjoajan	Verrataan poikkeamia edelliseen jaksoon, trendiviivan kehityssuunta,

			raportointi, tietoturvallisuuden tilaraportti	poikkeamaraportit tuotettu
Havaitut virus- ja muut haittaohjelmat	1 / kk	Palvelusopimuksen mukaan, tietoturva-asiantuntija	Palveluntarjoajan raportointi, tietoturvallisuuden tilaraportointi, virus- ja haittaohjelmien torjuntajärjestelmän ilmoitukset, tiketöintijärjestelmä	Verrataan 1kk häiriöluetteloa edelliseen 3kk jaksoon, trendiviivan kehityssuunta, yhteenvetoraportti tuotettu
Varkauksien ja kadotettujen laitteiden lukumäärä	1 / kk	Tietoturva-asiantuntija	Tietoturvapoikkeamamenettely ja ilmoituslomake, raportti poikkeamista	Verrataan poikkeamia edelliseen jaksoon, trendiviivan kehityssuunta, raportti tuotettu
Priorisoitujen ja kriittisten tietoriskien käsittelyn eteneminen kokonaisriskien hallinnassa	1 / 6kk	Kokonaisriskien vastuuhenkilö, riskin omistaja, tietoturva-asiantuntija, tietosuojavastaava	Tietoriskien analyysin dokumentaatio, kokonaisriskien hallinnan dokumentaatio	Kriittisten riskien korjaaminen on aloitettu, seurantadokumentaatio tuotettu
Tietoturva- ja tietosuojaryhmän kokousten lukumäärä	1 / vuosi	Tietoturva-asiantuntija, tietosuojavastaava	Kokouspöytäkirjat	Vuosikellon suunnitelman mukaan 100%
Tietoturvakatselmointien lukumäärä	1 / vuosi	Tietoturva-asiantuntija	Raportit, pöytäkirjat, dokumentaatio	Vuosikellon suunnitelman mukaan 100%
Tietoturva- ja tietosuojainfot sekä henkilöstölle suunnattujen tiedotteiden lukumäärä	1 / vuosi	Tietoturva-asiantuntija, tietosuojavastaava	Ohjeet, esitysmateriaali ja tukidokumentaatio, sähköpostiviestit, intranet, videotallenteet, asianhallinta	Vuosikellon suunnitelman mukaan 100%
Perehdyttämisprosessin tietoturva- ja tietosuoja-asioiden läpikäynti	1 / vuosi	HR, koulutuspäällikkö, tietoturva-asiantuntija, tietosuojavastaava	Perehdyttämisen tietoturva/tietosuoja-asioiden suoritusmerkintä lokista tai rekisteristä	100% kaikilla uusilla työntekijöillä
Allekirjoitettujen salassapitosopimusten lukumäärä	1 / vuosi	HR, tietopalveluasiantuntija, tietoturva-asiantuntija	Asianhallintajärjestelmä	100% kaikilla uusilla työntekijöillä

Mittariston suunnittelun jälkeen mittarit implementoidaan ja otetaan käyttöön, johon voi sisältyä esimerkiksi tietojärjestelmien määrittelyä ja konfigurointia, jotta ne voivat tuottaa mittareihin tarvittavaa informaatiota. Lisäksi valittu mittaristo täytyy testata ja mittausprosessiin liittyvää avainhenkilöstöä täytyy kouluttaa mittareiden käyttöön. Mittariston käyttöönoton suunnittelussa arvioidaan myös valittujen mittareiden käyttöönoton helppous ja muodostetaan käyttöönottoaikataulu sen mukaan. Nämä seuraavat tehtävät jäävät tämän tutkimuksen ulkopuolelle ja mittariston varsinaisen tuotantokäytön aikataulutus määräytyy testaamisen jälkeen, johon kuuluu

mm. datan keräämistä sekä tulosten laskemista, raportoimista ja analysointia. Mittareiden käyttöönoton aika vaihtelee ja todennäköistä on, että osa mittareista voidaan ottaa käyttöön hyvinkin nopeasti. Joidenkin mittarien osalta tuotantokäyttöön saattaminen voi kestää kuukausia, riippuen siitä onko esimerkiksi testauksen yhteydessä ilmennyt tarvetta mittarin muuttamiselle tai poistamiselle riittämättömän tuloksen vuoksi.

6.5 BIA-vaikutusanalyysi mittariston suunnittelun tukena

Luvussa 2.8 on kerrottu BIA-vaikutusanalyysin taustatiedot. Työssä BIA-vaikutusanalyysissä kerättiin tietoa kohdeorganisaation ydinjärjestelmistä, haastattelemalla järjestelmästä vastaavia henkilöitä ja käymällä läpi järjestelmädokumentaatiota. Analyysin onnistumisen varmistamiseksi keskeistä on järjestelmän tuntemus, jolloin vaikutusanalyysiin ja arviointiin saadaan mahdollisimman yksityiskohtaista tietoa tarkasteltavasta kohteesta. Näin saadaan kartoitettua erilaisten riskien toteutumisen vaikutuksia ja voidaan valita oikeat ja riittävät jatkotoimenpiteet.

Analyysin avulla luokiteltiin tarkasteltavat tietojärjestelmät tärkeysindeksin mukaan ja tuotettua taulukkoa käytettiin järjestelmien keskinäisen tärkeyden vertaamiseen ja tehtiin priorisointia järjestelmien välillä. BIA-vaikutusanalyysin raportin yhteenveto-osuudessa tuotettiin ydinjärjestelmien tärkeysindeksit ja tärkeysluokat, minkä mukaan valittiin tärkeimmät tietojärjestelmät tietoturvallisuuden mittausprosessiin.

6.5.1 BIA-vaikutusanalyysien toteutus

Vaikutusanalyysityökalu (BIA-työkalu) on tuotettu Valtiovarainministeriön (VM) päätöksellä Valtorin (Valtion tieto- ja viestintätekniikkakeskus) ohjauksessa ja yhteistyössä Valtorin asiantuntijoiden kanssa. Liitteessä 2 on malli käytetystä BIA-vaikutusanalyysilomakkeesta, jota voidaan käyttää mm. toiminnan jatkuvuuden ja järjestelmien toipumisen ja tärkeysluokittelun tukityökaluna. Lisäksi analyysillä voidaan selvittää tietoturvan merkitystä ja arvioida häiriöiden (käyttökatkokset, tietojen menetys tai päivittymättömyys) vaikutusta tietojärjestelmän luottamuksellisuuteen, eheyteen ja käytettävyyteen.

Työssä BIA-vaikutusanalyysien tekemisen keskeisenä tavoitteena oli ydinjärjestelmien tärkeysluokittelun tuottaminen ja tuloksena saadun kriittisten järjestelmien luettelon hyödyntäminen tietoturvamittareiden kohdentamisessa. Vaikutusanalyysien tekeminen ajoittui keväälle ja syksylle 2017 ja niitä tehtiin yhteensä 18 ydinjärjestelmälle. Arviointiin osallistui kustakin järjestelmästä kohteen/järjestelmän omistaja (palvelupäällikkö), sovellusvastaava, sovellusasiantuntija ja tietoturva-asiantuntija. Yhteensä arviointeihin osallistui 29 henkilöä.

6.5.2 Analyysien hyödyntäminen mittariston suunnittelussa

Analyysien tuloksena saatiin kustakin tietojärjestelmästä yhteenvetoraportti, joka on kuvattu liitteen 2, BIA-vaikutusanalyysin täyttöpohjan viimeisessä kohdassa. Yhteenveto-osuuteen on kerätty keskeiset arvioinnissa läpikäydyt havainnot raportoitavaksi:

- Perustiedot arvioinnin kohteesta, omistajasta ja organisaatiosta
- Arvioinnin toteuttamisajankohta
- Yhteiskunnan turvallisuusstrategian (YTS 2010) näkökulman kannalta sekä tärkeys yhteiskunnalle että YTS:n vakavin uhkataso
- Odottamattoman katkoksen suurimmat vaikutukset oman organisaation, kumppaneiden/alihankkijoiden, asiakkaiden/loppukäyttäjien ja esimerkiksi yhteiskunnan kannalta
- Odottamattoman katkoksen mahdolliset suurimmat menetykset terveyden ja hengen menetyksen, lakisääteisten tehtävien viivästymisen, taloudellisten menetysten ja maineen menettämisen näkökulmista
- Tärkeysluokka ja tärkeysindeksi, joita voidaan käyttää esimerkiksi kuvaamaan eri järjestelmien keskinäistä tärkeyttä
- Keskeisimmät tietoturvallisuuden ja varautumisen luokitukset sekä palvelutasosopimuksen taso
- Yleisimmät suositukset, mikäli käytettyjen mittareiden perusteella näin on esitettävissä
- Graafinen osuus havainnollistamaan eri osapuolille mahdollisesti kohdistuvien odottamattomien katkosten vaikutuksia

Kustakin analysoitavasta järjestelmästä vietiin edelleen jatkokäsiteltäväksi keskeiset tiedot, joista muodostettiin yhteenvetotaulukko suojaustasoluokan, tietoturvatason, ICT-varautumistason, palvelutasosopimuksen (SLA) ja tärkeysluokan (indeksin) mukaan. Järjestelmien yhteenvetotaulukkoa muokattiin edelleen siten, että tärkeysindeksin luvun suuruus määrää kriittisyysjärjestyksen järjestelmien tärkeysluokittelussa. Tietojärjestelmien kriittisyysluokittelu otetaan huomioon tietoturvallisuuden hallinnassa sekä jatkuvuus- ja toipumistoimenpiteiden suunnittelussa, millä mm. priorisoidaan järjestelmiä toipumisprosessiin liittyen.

Alla on lueteltu taulukosta 1 irrotettuja tietoturvamittareita, joita voidaan kohdentaa ja implementoida tietojärjestelmien seurantaan:

- Tietojärjestelmien tietoturvallisuuden tila
- Tietojärjestelmien turvakuvaukset
- Hälytysrajojen ja kriittisyyden arvojen ylittävät tapahtumat
- Toteutetut tietoturvapäivitykset
- Tietojärjestelmien tietoriskianalyysit
- Tietojärjestelmien käyttöoikeuksien arviointi ja tarkastaminen, vanhentuneiden tunnusten lukumäärä
- Käyttöpalveluiden tietoturvallisuuden tila.

Yllä olevan listan viimeisenä kohtana on käyttöpalveluiden tietoturvallisuuden tila, mikä otetaan myös huomioon tietoturvamittareiden kohdentamisessa. Valtaosa ydinjärjestelmistä tuotetaan keskitetyn käyttö- ja kapasiteettipalvelun kautta, mikä asettaa vaateita käyttöympäristön ja palvelinalustan tietoturvallisuuden hallinnalle.

7 YHTEENVETO JA JOHTOPÄÄTÖKSET

7.1 Yhteenveto

Tämä työ sijoittuu toiminta-analyyttisen tutkimuksen prosessin eri vaiheisiin. Lähtökohdan muodosti tutkimusongelmaan liittyvä kysymyksenasettelu, minkä perusteella selvitettiin miten tietoturvallisuuden mittaaminen parantaa tietoturvallisuuden hallintajärjestelmän toimivuutta sekä tietoturvallisuuden tilaa. Lisäksi alun käsiteanalyyttisiä piirteitä sisältävän teoriaosuuden kautta selvitettiin tietoturvamittareiden olemusta ja mittausprosessin vaiheita sekä mitä tietoa mittausprosessista tuotetaan ja miten saatua tietoa hyödynnetään päätöksenteossa. Laajan teoriaosuuden tavoitteena oli muodostaa ymmärrys tietoturvallisuuden mittaamisesta, jonka kautta muodostettiin näkemys ongelman tunnistamiseksi sekä sen määrittelyn selvittämiseksi.

Kirjallisuuden ja aineistolähtöisen analyysin avulla tuotiin esille yleisesti tunnetut haasteet mittaamisen ja erityisesti tietoturvallisuuden mittaamisen kontekstissa. Lisäksi tunnistettiin, miten tietoturvallisuuden mittaaminen tulee huomioida osana julkishallinnon organisaation velvoitteita, tulosvastuuta sekä päätöksentekoa, mikä muodostaa osaltaan myös keskeisen työhön liittyvän viitekehyksen.

Työn diagnosointi toteutettiin käsiteanalyyttisen tutkimuksen jälkeen, jolloin kirjallisuudesta saadun tiedon hyödyntäminen auttoi kerätyn aineiston käyttöä työn empiirisen osion ja kohdeorganisaation mittareiden suunnittelussa. Lisäksi diagnosointivaiheessa hyödynnettiin BIA-vaikutusanalyysejä, joiden tuloksien perusteella luokiteltiin keskeisten tietojärjestelmien tärkeysjärjestys, jota hyödyntäen voidaan edelleen kohdentaa mittareiden suunnittelu järjestelmille asetettujen tarpeiden perusteella. Saadun aineiston avulla määriteltiin runkoa tietoturvan mittaamiselle sekä tunnistettiin tietoturvallisuuden hallintajärjestelmään liittyviä tietotarpeita.

Diagnosointivaiheen aineistoa analysoitiin aineistolähtöisen sisällönanalyysin periaatteilla. Sisällönanalyysissä aineistoa tarkastellaan eritellen, yhtäläisyyksiä ja eroja etsien ja tiivistäen. Sisällönanalyysi on tekstianalyysiä, jossa tarkastellaan tekstimuotoista aineistoa, jonka tavoitteena on muodostaa tutkittavasta ilmiöstä tiivis-

tetty kuvaus, joka kytkee tulokset ilmiön laajempaan kontekstiin ja aihetta koskeviin muihin tutkimustuloksiin. (Saaranen-Kauppinen & Puusniekka 2012, 97.)

Diagnosointivaiheessa aineistosta eriteltiin julkishallinnon organisaatiolle kohdistuvia tietoturvallisuuden arviointiin ja mittaamiseen liittyviä velvoitteita, joiden perustan muodostaa tietoturvaa ja tietosuojaa (GDPR) ohjaava lainsäädäntö. Mittaamisella kehitetään myös tietoturvallisuuden hallintajärjestelmää, joten analyysissä käsiteltiin ISO/IEC 27004:2016 -standardiin liittyviä suosituksia. Tavoitteena oli saada muodostettua ensivaiheessa keskeinen mittaristo kohdeorganisaation tarpeisiin.

Siirryttäessä tietoturvamittariston suunnitteluvaiheeseen tietotarpeita ryhmiteltiin ja niistä etsittiin kokonaisuuksia ja yhtäläisyyksiä tietoturvallisuuden perustasoon sekä tietoturva-asetukseen liittyvien vaatimusten mukaan. Kerättyä aineistoa ja tietotarpeita vertailtiin määriteltyihin mittausnäkökulmiin, joihin valittiin suorituskyvyn ja tavoitteiden kannalta tärkeimmät menestystekijät eli mitattavat asiat. Mittariston suunnittelussa otettiin myös huomioon tietosuoja-asetus (GDPR), jonka säännösten toteutumisen ja osoitusvelvollisuuden noudattamisen arvioimiseen tuotetaan tietoa sekä mittaristolla että BIA-vaikutusanalyyseillä.

7.2 Tulosten tarkastelua tutkimuskysymyksiä vasten

Työn keskeisiä tuloksia tarkastellaan myös vastaamalla luvussa 1.3 esitettyihin tutkimuskysymyksiin:

1. Miten tietoturvallisuuden mittaaminen parantaa tietoturvallisuuden hallintajärjestelmän toimivuutta ja ylläpitoa sekä ymmärrystä koskien tietoturvajärjestelmiä, tietoprosesseja ja tietoturvallisuuden tilaa?
2. Miksi tietoturvadataa ja -informaatiota kerätään ja mitä ovat keskeiset tietoturvamittarit ja mistä mittausprosessi muodostuu?
3. Mitä tietoa mittausprosessista tuotetaan ja miten kerättyä dataa ja informaatiota organisoidaan edelleen tietämykseksi ja käytännön soveltamiseksi?

Kohtaan 1 vastataan kirjallisuusselvityksen ja työn alun käsiteanalyyttisen tutkimuksen aikana kerätyn materiaalin perusteella. Kohtiin kaksi ja kolme vastataan sekä kirjallisuusselvityksen että työn empiirisen osion perusteella.

Miten tietoturvallisuuden mittaaminen parantaa tietoturvallisuuden hallintajärjestelmän toimivuutta ja ylläpitoa sekä ymmärrystä koskien tietoturvajärjestelmiä, tietoprosesseja ja tietoturvallisuuden tilaa?

Organisaation tietoturvaa johdetaan ja hallitaan periaatteilla ja käytännöillä, jotka on julkishallintoa ohjaavassa Vahti-ohjeistuksessa määritelty tietoturvallisuuden hallintajärjestelmän alle. Käytännössä jokaisella organisaatiolla voidaan sanoa olevan hallintamenettely, jolla tietoturvaa johdetaan; kypsyystaso voi toki vaihdella aloittavasta optimoituun. Luvussa 3.1 on esitetty tietoturvallisuuden hallintajärjestelmän tavoitteet sekä kuvissa 9 ja 10 hallintajärjestelmän malli ja prosessi, joiden mukaan hallintajärjestelmä sisältää tietoturvatoiminnan säännöllisen mittaamisen sekä kehittämisen ja ylläpitämisen prosessin.

Tietoturvallisuuden mittaamisella saadaan tietoa tietoturvallisuuden hallintajärjestelmän eri osa-alueiden toimivuudesta. Tuotettu mittausinformaatio analysoidaan ja koostetaan tarvittaessa muotoon, jota voidaan hyödyntää hallintajärjestelmän kehittämiseen tähtäävässä päätöksenteossa. Mittaamisen tavoitteena on parantaa ISO/IEC 27001 PDCA -prosessimallin mukaisesti tietoturvallisuuden hallintajärjestelmää jatkuvana menettelytapana. Mittausprosessiin ja päätöksentekoon osallistuvien tahojen ymmärrys tietoturvallisuuden prosessien toiminnasta lisääntyy kehittämistoimenpiteiden edistyessä sekä organisaation kypsyystason parantuessa.

Tietoturvallisuuden mittaamisella saadaan tietoa tietoturvatoiminnan nykytilasta ja kypsyystasosta. Näiden perusteella voidaan asettaa kehittämisen tavoitetaso linjatuille vaatimuksille. Tietoturvatoiminnan seuraamisessa systemaattinen ja jatkuva mittaaminen mahdollistaa tietoturvallisuuden hallintajärjestelmän jatkuvan kehittämisen sekä hallintaprosessien toiminnan.

Julkishallinnon palvelujen digitalisoinnin sekä organisaatioiden järjestelmien automatisointiin kohdennettujen resurssien myötä myös kohdeorganisaatiolla on lisääntyvää kiinnostusta saada spesifistä tietoa tietojärjestelmien ja niihin liittyvien tietoprosessien tietoturvallisuuden tilasta. Oikein kohdennetulla mittaamisella ta-

voitteena on saada informaatiota, jota voidaan hyödyntää yhä tehokkaammin tietoturvallisuuden kehittämisessä ja päätöksenteossa. Lisäksi analysoitu mittausinformaatio tuo kokonaisnäkemystä prosessien toiminnasta ja niiden tietoturvallisuuden tilasta. Pidemmällä aikajänteellä iteratiivisesti toteutettu mittaaminen lisää siihen osallistuvien tahojen ymmärrystä paitsi kyseisten mittareiden toiminnasta ja tavoitteista, myös mittaamisen roolista ja merkityksestä koko tietoturvallisuuden hallintajärjestelmän toiminnassa.

Miksi tietoturvadataa ja -informaatiota kerätään ja mitä ovat keskeiset tietoturvamittarit ja mistä mittausprosessi muodostuu?

Järjestelmien ja prosessien toiminnan seurauksena tietoa kertyy ehtymättömänä virtana ja digitalisaation myötä informaation määrä kasvaa koko ajan. Kerääntyneestä datasta saadaan tietoa moneen tarkoitukseen ja tutkimuksessa tietoturvan mittaamisen lähtökohtana on tuottaa tietoturvan kannalta spesifinen tieto päätöksentekoa ja tietoturvallisuuden hallintajärjestelmän kehittämistä varten. Tavoitteena mittareiden tuottamalla tietoturvadatalla ja -informaatiolla on mm. vähentää ja poistaa toimintaan kohdistuvia häiriöitä ja uhkatekijöitä sekä huolehtia tietoturvallisuudesta lainsäädännön asettamien vaatimusten mukaan tekemällä mm. säännönmukaisesti tietoturvallisuuden arviointia.

Johtaminen ja päätöksenteko ilman mittaamista on vaikeaa tai lähes mahdotonta, kohdeorganisaation tietoturvallisuuden johtaminen ei tee tähän poikkeusta. Tehokas mittaaminen ja raportointi on oleellista toimittaessa lainsäädännön mukaisten määräysten ehdoilla, parannettaessa tehokkuutta ja valvonnan vaikuttavuutta sekä varmistettaessa strategian mukaisten toimien kohdentamista luotettavalla ja tarkoituksenmukaisella tavalla. Tietoturvallisuuden mittaamisella pyritään luomaan selittävyyttä ja läpinäkyvyyttä tietoturvallisuuden hallintaan, joka johtaa toimintaan ja päätöksentekoon.

Tietoturvallisuuden mittaus on prosessimuotoista ja se on osa johtamisen ja tietoturvallisuuden hallintaprosessia. Jatkuvasti kehittyvällä mittaamisella ja mittausprosessilla saavutetaan merkittävää hyötyä tietoturvallisuuden parantamisessa. Toiminnan ohjausta ja organisaation onnistumisen arviointia tehdään monella tasolla, joten tarvitaan mittareita eri ohjaustasojen ja tavoitteenasettelujen tarpeisiin.

Esimerkiksi osa mittareista tuo informaatiota tapahtumista, joiden analysoinnin jälkeinen toiminta suoritetaan reaktiivisesti, jotta varmistetaan asianmukainen tietoturvallisuus kyseiseen mittariin liittyvän käyttöperiaatteen mukaan. Toisaalta mittarit, joiden tavoitteena on esimerkiksi arvioida henkilöstön tietoturvatietoisuutta, voivat edesauttaa tietoturvakoulutuksen kohdentamisessa ja kehittämisessä kohdeorganisaation henkilöstöhallinnon ja koulutuksen johtamisen prosesseissa. Tutkimuksen tavoitteena on, että mittaamisesta muodostuu kohdeorganisaatiossa jatkuvaa toimintaa ja aikaansaadaan aikasarjoja, joten käytettävän mittareiden on oltava riittävän selkeitä.

Tietoturvamittarien suunnittelemisessa ja kehittämisessä kohdataan erilaisia haasteita, joskin ne ovat pääpiirteissään samanlaisia kuin muidenkin organisaatiossa tapahtuvien mittareiden suunnittelussa. Kohdeorganisaatiossa suunnittelun haasteet liittyivät mittareiden ja mittaamisen tavoitteiden määrittelyyn, jotka ovat sidoksissa mm. organisaation tietoturvallisuuden hallinnan kypsyystasoon sekä yhteiskunnallisiin ja lainsäädännöllisiin velvoitteisiin. Tutkimuksen edetessä tavoitteet selkiintyivät ja viitekehyksen mukaisesti tietoturvamittareiden suunnittelu rakentuu tietoturva-asetuksen perustason vaatimusten ja niitä tukevien Vahti-ohjeiden mukaan. Lisäksi mittareiden suunnittelussa huomioitiin ISO/IEC 27004:2016 -standardi, joka on tarkoitettu avuksi tietoturvan tason ja tietoturvallisuuden hallintajärjestelmän vaikuttavuuden arviointiin. Mittareiden suunnittelussa otettiin huomioon myös kohdeorganisaation riskienhallinnan menettelyt, joilla voi olla vaikutusta uusien mittareiden suunnitteluun tai olemassa olevien määrittelyyn.

Tässä työssä tuotettiin kohdeorganisaatiolle soveltuvat keskeiset mittarit, huomioiden ensi sijassa tietoteknisen infrastruktuurin ja tietoprosessien tällä hetkellä tuottama aineisto. Työssä suunniteltiin tietoturvamittareita, joihin tarvittava tieto on pääosin valmiina olemassa, ja jotka voidaan ottaa käyttöön ilman mittavaa työpanosta. Ensivaiheessa otetaan käyttöön muutama keskeinen mittari, joiden implementoinnin jälkeen voidaan tehdä jatkosuunnitelmia mittariston edelleen kehittämiseksi ja laajentamiseksi. Näin toimien toteutetaan myös yleisiä suosituksia, joiden mukaan mittareita tulee olla mieluummin liian vähän ja niiden tulee olla kuvaavia ja ohjaavia, kuin paljon ja kaiken kattavia. Kun mittaristo ja mittausprosessi

on testattu ja otettu käyttöön, tavoitteena on myöhemmässä vaiheessa kehittää edelleen mittaristoa osana tietoturvallisuuden hallintaprosessia.

Tutkimuksessa käytetään Kaplanin ja Nortonin tasapainotetun mittaristomallin periaatetta, jota tarkasteltiin tietoturvallisuuden menestystekijöiden näkökulmasta. Tietoturvallisuuden menestystekijöitä määriteltiin kahdessa suunnitteluvaiheessa, jonka jälkeen niitä yhdistettiin kokonaisuuksiksi. Ensin mittausnäkökulmiin määriteltiin menestystekijöitä mahdollisimman kattavasti, päällekkäisyyksiin ei tässä vaiheessa puututtu. Toisessa suunnitteluvaiheessa menestystekijöitä arvioitiin ja tärkeysluokiteltiin ensi sijassa riskienhallinnan ja normatiivisten velvoitteiden kannalta sekä arvioitiin, kuinka helposti menestystekijöihin liittyviä mittareita on käyttöönotettavissa nykyisessä toimintaympäristössä. Toisessa suunnitteluvaiheessa käsiteltiin uudelleen ensimmäisessä suunnitteluvaiheessa kirjatut menestystekijät ja arvioitiin kunkin menestystekijän kohdalla, miten niiden johtaminen mittareiksi voidaan toteuttaa, ottaen huomioon kohdeorganisaation nykytila sekä lähitulevaisuuden tavoitetila. Määrittelytyössä käytettiin apuna ISO/IEC 27004:2016 -standardin (2016, 15) tietotarpeiden tunnistamisen ja määrittelyn prosessia.

Menestystekijöiden valitsemisen ja tietotarpeiden arvioinnin jälkeen määritettiin mittauskohteet ja kullekin menestystekijälle sopiva mittari tai useampi mittari. Mittarin käyttötarkoitus vaikuttaa ensisijaisesti soveltuvan mittarin valintaan. Jokaisen mittarin kohdalla pohdittiin, mihin mittaria käytetään. Yleensä mittari kannattaa valita mittaristoon, jos sen käyttö on edullista ja helppoa. Tätä periaatetta noudatettiin ensisijaisesti myös tässä työssä.

Varsinainen mittareiden suunnittelu ja yksityiskohtainen dokumentointi työstettiin menestystekijöiden, tietotarpeiden ja mittauskohteiden määrittelyn jälkeen. Mittariston kokonaismäärä ja ominaisuudet on koostettu liitteeseen 1, josta valittiin jatkosuunnittelua ja -työstämistä varten 21 tietoturvamittaria. Käyttöperiaatteet-taulukossa (taulukko 1) on kuvattu tietoturvamittarit, jotka katsottiin olevan perusteltua ottaa tuotantokäyttöön joko kriittisyysarvion tai helpohkon käyttöönoton vuoksi. Tässä tutkimuksessa ei priorisoitu tietoturvamittareiden käyttöönottojärjestystä, joskin osa työssä suunniteltujen mittareiden tietotarpeesta kerätään jo nykyisellään tietoturvallisuuden seuraamiseksi ja päätöksenteon pohjaksi. Käytännössä työssä tuotetun mittariston implementoinnissa ja käyttöönotossa ensimmäi-

siä jatkotehtäviä on kohdeorganisaation nykyisen mittaustiedon tarkastaminen, jonka laajentamiseksi on syytä tehdä lisämäärittelyä yhdenmukaisen mittausprosessin ja mittariston luomiseksi.

Mitä tietoa mittausprosessista tuotetaan ja miten kerättyä dataa ja informaatiota organisoidaan edelleen tietämykseksi ja käytännön soveltamiseksi?

Mittarin valintaan vaikuttaa ensisijaisesti mittarin käyttötarkoitus, joten jokaisen mittarin kohdalla on pohdittava, mihin mittaria käytetään eli valitaan ne asiat, josta halutaan mittausinformaatiota, ja jotka vastaavat menestystekijän tietotarpeisiin. Tässä työssä keskeinen mittausprosessista tuotettava data liittyy julkishallintoon kohdistuviin tietoturvallisuuden perustason vaatimuksiin sekä ISO/IEC 27004:2016 -standardin tietotarpeiden tunnistamiseen liittyvään prosessiin.

Työssä tuotettiin yhteensä 21 tietoturvamittaria. Koska mittareita, mittauksen käyttötilanteita ja mittauksen käyttäjiä on hyvin monenlaisia, valittiin mittareiden määrittämisen jälkeen jokaiselle valitulle mittarille käyttöperiaatteet. Osa luetelluista mittareista liittyy esimerkiksi nykyisen tietojärjestelmän tai palvelun prosessiin ja on siten jo käytössä. Niiden osalta tavoitteena on jatkossa yhdenmukaistaa mittausprosessia ja seurantaa sekä tuottaa mittausdataa ja -tietoa tarkoituksenmukaisesti mm. raportoinnin kannalta.

Kukin tuotantokäyttöön valittu mittari on kuvattu taulukossa 1. Jatkosuunnittelussa tulee myös määritellä kenelle ja missä tulos raportoidaan ja mittaustulosten tulkinnan helpottamiseksi on suositeltavaa viedä käyttöperiaatteet myös mittausraporttiin. Nämä seuraavat toimenpiteet voidaan tehdä tutkimuksen jälkeisen mittareiden käyttöönoton suunnittelun yhteydessä, samoin kuin valitaan priorisoidut tietoturvamittarit, ensin testattavaksi ja sen jälkeen tuotantokäyttöön.

Mittaristolla kerättyä informaatiota on tavoitteena hyödyntää kohdeorganisaation useaan tietotarpeeseen. Johdon päätöksentekoa varten tuotetaan tarkoituksenmukaisia raportteja ja yhteenvetoja, joista osa on säännönmukaisesti ja osa tarveharkinnan jälkeen tuotettavia, esimerkiksi poikkeamatilanteen arvioinnin yhteydessä. Mittaristolla tuotettu informaatio ja yhteenvetotieto edesauttaa tietoturvallisuuden hallintajärjestelmän kehittämistä sekä toimenpidesuunnitelman ja vuosikellon suunnittelua. Osa mittareista on tarkoitus kohdentaa tietojärjestelmien tietoturvalli-

suuden mittaamiseen. Työssä tuotettiin ydinjärjestelmistä BIA-vaikutusanalyysit ja saatujen analyysitulosten mukaan järjestelmät luokiteltiin tärkeysindeksin mukaisesti kriittisyysluokkiin. Tuotettua taulukkoa käytetään kohdistamaan tietoturvallisuuden mittareita priorisoiduille tietojärjestelmille. Kriittisyysluokittelua käytetään myös kohdeorganisaation jatkuvuus- ja toipumissuunnittelussa mm. resurssien kohdentamisen suunnittelussa ydinjärjestelmien ongelmatilanteissa.

Jatkuvuutta tietoturvallisuuden kehittämiseen ja kypsyystason arviointiin tuo tietoturvallisuuden hallintaprosessi, johon mittaaminen ja arviointi kuuluvat oleellisena osana. Ajantasainen ja kehittyvä mittausprosessi tuottaa tietoa päätöksentekoa sekä tietoturvallisuuden hallintajärjestelmän ylläpitoa, kehittämistä ja käytännön toimenpiteitä varten. Siihen osallistuvien tahojen tietoturvatietämys kehittyy väjäämättä tietoturvallisuuden kypsyystason kehittymisen mukana ja keskeisenä tavoitteena on, että kohdeorganisaation tietoturvatietämys syvenee ja laajenee edelleen tietoturvallisuuden mittaamiseen liittyvän iteratiivisen toiminnan kautta.

7.3 Jatkotutkimusaiheet

Tämän työn jatkotutkimusaiheiksi muodostuu mittareiden käyttöönotto, joka Lönnqvistin (2004, 143) mittausprosessin mukaan sisältää seuraavat vaiheet:

1. Mittareiden käyttöönotto
   a) Mittarit otetaan käyttöön
   b) Mittarit implementoitu
2. Mittareiden käyttö
   a) Käytetään mittareita käytännön työssä
   b) Mittareiden käyttö osana organisaation toimintaa

Lönnqvistin ja Mettäsen (2003, 101) mukaan käyttöönottoon voi myös sisältyä tietojärjestelmien muokkausta, jotta ne tuottaisivat mittareihin tarvittavaa informaatiota. Lisäksi käyttöönottoon liittyvää henkilöstöä täytyy kouluttaa mittareiden käyttöön ja mittaristo on myös testattava, johon kuuluu mm. dataan keräämistä sekä tulosten laskemista. Jatkotutkimuksen keskeisiä asioita on myös mittaustulosten asianmukaiseen analysointiin ja raportointiin liittyvät menettelytavat.

LÄHTEET

Aaltio, I. 2014. Case-tutkimus metodisena lähestymistapana. Metodix – metoditietämystä kaikille. [Verkkojulkaisu]. Helsinki: Metodix Oy. [Viitattu 13.2.2018]. Saatavana: https://metodix.fi/2014/05/19/aaltio-marjosola-casetutkimus/

Aineettoman pääoman johtaminen 2004. Työkirja. Aineeton pääoma projekti. Helsinki: IC Partners Oy.

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma Oy.

Anttila, P. 2014. Tutkimisen taito ja tiedon hankinta. Metodix - metoditietämystä kaikille. [Verkkojulkaisu]. Helsinki: Metodix Oy. [Viitattu 6.2.2018]. Saatavana: https://metodix.fi/2014/05/17/anttila-pirkko-tutkimisen-taito-ja-tiedon-hankinta/

Barabanov, R., Kowalski, S. & Yngström, L. 2011. Information Security Metrics. DSC Report series No. 11-007.

ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin 2009. Vahti 2/2009.

ICT-varautumisen vaatimukset 2012. Vahti 2/2012.

Information Security Forum 2016. The Standard of Good Practice for Information Security 2016. [Verkkojulkaisu]. Information Security Forum. [Viitattu 24.3.2018]. Saatavana: https://www.securityforum.org/tool/the-isf-standardrmation-security

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

ISO/IEC 27004:2016. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Seuranta, mittaus, analysointi ja arviointi. Helsinki: Suomen Standardisoimisliitto SFS ry.

Johdon tietoturvaopas 2011. Vahti 2/2011.

Johnson, E. 2015. Kehittämistutkimusta ja ongelmanratkaisua YAMK-opinnäytetyössä: [Verkkosivu]. Kokkola: Centria ammattikorkeakoulu. [Viitattu 28.1.2018]. Saatavana: https://centriaamk.wordpress.com/2015/12/18/kehittamistutkimusta-ja-ongelmanratkaisua-yamk-opinnaytetoissa/

Kananen, J. 2014a. Laadullinen tutkimus opinnäytetyönä. Jyväskylä: Jyväskylän ammattikorkeakoulun julkaisuja -sarja.

Kananen, J. 2014b. Toimintatutkimus kehittämistutkimuksen muotona. Jyväskylä: Jyväskylän ammattikorkeakoulun julkaisuja -sarja.

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas. Jyväskylä: Jyväskylän ammattikorkeakoulun julkaisuja -sarja.

Kananen, J. 2017. Kehittämistutkimus interventiotutkimuksen muotona. Jyväskylä: Jyväskylän ammattikorkeakoulun julkaisuja -sarja.

Kaplan, S & Norton, P. 1996. The balanced scorecard 1996. Translation strategy into action. Boston, Massachucetts: Harvard business school.

Kaplan, S & Norton, P. 2004. Strategiakartat. Aineettoman pääoman muuttaminen mitattaviksi tuloksiksi. Helsinki: Talentum.

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

Koppa 2015. Toimintatutkimus. [Verkkosivu]. Jyväskylän Yliopisto. [Viitattu 13.2.2018]. Saatavana: https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/toimintatutkimus

KvantiMOTV menetelmätietovaranto 2003. Mittaaminen: Tilastoyksikkö ja muuttujat. [Verkkojulkaisu]. Yhteiskuntatieteellinen tietoarkisto. Menetelmäopetuksen tietovaranto. [Viitattu 18.3.2018]. Saatavana: http://www.fsd.uta.fi/menetelmaopetus/mittaaminen/tilastoyksikko.html

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen Tietoturvakäsikirja. Helsinki: Edita Publishing Oy.

Laitinen, E. K 2003. Yritystoiminnan uudet mittarit. Jyväskylä: Talentum Media Oy.

L 10.6.2011/634. Laki julkisen hallinnon tietohallinnon ohjauksesta. [Verkkosivu]. Oikeusministeriö. Edita Publishing Oy. [Viitattu 6.5.2018]. Saatavana: https://www.finlex.fi/fi/laki/ajantasa/2011/20110634

L 6.5.2011/418. Laki Suomen metsäkeskuksesta. [Verkkosivu]. Oikeusministeriö. Edita Publishing Oy. [Viitattu 2.8.2018]. Saatavana: https://www.finlex.fi/fi/laki/ajantasa/2011/20110418

L 21.5.1999/621. Laki viranomaisen toiminnan julkisuudesta. [Verkkosivu]. Oikeusministeriö. Edita Publishing Oy. [Viitattu 15.4.2018]. Saatavana: https://www.finlex.fi/fi/laki/ajantasa/1999/19990621

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Jyväskylä: Talentum Media Oy.

Lundholm, K., Hallberg, J. & Granlund, H. 2011. Design an Use of Information Security Metrics: Application of the ISO/IEC 27004 standard. Report no. FOI-R-3189-SE. FOI, Swedish Defence Research Agency. Lindköping.

Lukka, K. 2014. Konstruktiivinen tutkimusote. Metodix - metoditietämystä kaikille. [Verkkojulkaisu]. Helsinki: Metodix Oy. [Viitattu 11.2.2018]. Saatavana: https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Lönnqvist, A. 2004. Measurement of Intangible Success Factors: Case Studies on the Design, Implementation and Use of Measures. Väitöskirja. Tampere, Tampereen teknillinen yliopisto. Julkaisu 475.

Lönnqvist, A. & Mettänen P. 2003. Suorituskyvyn mittaaminen - Tunnusluvut asiantuntija -organisaation johtamisvälineenä. Helsinki: Edita Prima Oy.

Metsäkeskus 2018. [Verkkosivu]. Lahti: Suomen metsäkeskus. [Viitattu 2.8.2018]. Saatavana. https://www.metsakeskus.fi/metsakeskus

Neilimo, K. & Näsi, J. 1980. Nomoteettinen tutkimusote ja Suomalaisen yrityksen taloustiede. Tutkimus positivismin soveltamisesta. Tampereen yliopisto, Yrityksen taloustieteen ja yksityisoikeuden laitoksen julkaisuja, Sarja A2: Tutkielmia ja raportteja 12. Tampere 1980.

Ohje riskienhallintaan 2017. Valtiovarainministeriön julkaisuja 22/2017. Valtiovarainministeriö. Julkisen hallinnon ICT. Helsinki.

Olkkonen, T. 1993. Johdatus teollisuustalouden tutkimustyöhön. Teknillinen korkeakoulu. Teollisuus ja työpsykologia. Report No 152. Otaniemi.

Puusa, A. 2008. Tieteellinen artikkeli. Käsiteanalyysi tutkimusmenetelmänä. Premissi 4/2008, 36-43.

Saaranen-Kauppinen, A., Puusniekka, A., Kuula, A. & Rissanen, R. 2012. Menetelmäopetuksen tietovaranto KvaliMOTV. Kvalitatiivisten menetelmien verkko-oppikirja. [Verkkojulkaisu]. Tampere: Yhteiskuntatieteellisen tietoarkiston julkaisuja. [Viitattu15.2.2018]. Saatavana: http://www.fsd.uta.fi/fi/julkaisut/motv_pdf/KvaliMOTV.pdf

Saari, S. 2006. Tuottavuus. Teoria ja mittaaminen liiketoiminnassa. Tuottavuuden käsikirja. Vantaa: Mido Oy.

Savola, R. 2009. A security Metrics Taxonomation Model for Software-Intensive Systems. Journal of Information Processing Systems, Vol. 5, No.4, December 2009, 197-206.

Savola, R. 2010. On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems. IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1, January 2010, 230-239.

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

Teknisen ICT-ympäristön tietoturvataso-ohje 2012. Vahti 3/2012.

Tietohallinnon ohjaus 2011. [Verkkosivu]. Helsinki: Valtiovarainministeriö. [Viitattu 23.1.2018]. Saatavana: https://vm.fi/tietohallinnon-ohjaus

Tietosuojavaltuutetun toimisto 2018. Tietosuoja. [Verkkosivu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 22.8.2018]. Saatavana: https://tietosuoja.fi/tietosuoja

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

Tietoturvallisuuden arviointiohje 2014. Vahti 2/2014.

Tietoturvallisuus ja tulosohjaus 2004. Vahti 2/2004.

Tietoturvatavoitteiden asettaminen ja mittaaminen 2006. Vahti 6/2006.

Toiminnan jatkuvuuden hallinta 2016. Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä. Vahti 2/2016.

Vaikutusanalyysi (BIA, Business Impact Analysis) käyttäjän ohje 2016. Tuotettu Valtiovarainministeriön päätöksellä.

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 2004. Vahti 5/2004.

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

A 1.7.2010/681. Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa. [Verkkosivu]. Oikeusministeriö. Edita Publishing Oy. [Viitattu 5.4.2018]. Saatavana: https://www.finlex.fi/fi/laki/ajantasa/2010/20100681

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

LIITTEET

Liite1. Tietoturvamittaristo ja ominaisuudet.

Liite 2. BIA-vaikutusanalyysin täyttöpohja.

LIITE 1. Tietoturvamittaristo ja ominaisuudet.

Näkökulma	Menestystekijä	Vaatimus	Mittauskohde	Mittari
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Kumppanin kanssa tehdään kirjallinen sopimus, jossa määritellään yhteistyön tai hankinnan kohteen tietoturvavaatimukset sekä miten tietoturvallisuuden valvonta, seuranta, auditointi ja raportointi tapahtuu (Vahti 2/2010)	Järjestelmien ja palvelujen sopimukseen liitettävät tietoturvavaatimukset yhteistyön ja hankinnan kohteesta	Sopimusten lukumäärä, joissa tietoturvavaatimukset
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Tietoturvallisuuden valvonta sekä poikkeamien kirjaaminen ja raportointi on organisoitu ja vastuutettu yhteistyön kohteeseen liittyen (Vahti 2/2010)	Järjestelmien tietoturvapoikkeamien hallinta	Toimittajalla on (sopimuksessa sovitusti) tietoturvallisuuden valvonnasta ja poikkeamien kirjaamisesta dokumentaatio, joka raportoidaan tietoturvavastaavalle säännöllisesti
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Säännöllinen raportointi IT-järjestelmien ja niiden hallinnan tietoturvallisuuden tilasta tietoturvavastaavalle on organisoitu ja vastuutettu (Vahti 2/2010)	Järjestelmien tietoturvapoikkeamien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Toimittaja reagoi hankinnan kohteeseen liittyviin vakaviin tietoturvapoikkeamiin viivytyksettä, pitää niistä kirjaa ja raportoi ne asiakkaalle (Vahti 3/2011)	Järjestelmien tietoturvapoikkeamien hallinta	Toimittajan ilmoittamat tietoturvapoikkeamat, lukumäärä
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Toimittajan tietoturvallisuuden vastuuhenkilö lähettää tietoturvaraportin asiakkaan tietoturvallisuuden vastuuhenkilöille aina ongelmatilanteiden ilmetessä, kuitenkin vähintään puolivuosittain (Vahti 3/2011)	Järjestelmien tietoturvapoikkeamien hallinta	Vakavista tietoturvapoikkeamista ilmoittaminen/aika suhteessa havaintoon

Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Toimittaja valvoo hankittavan palvelun tietoturvallisuuden toteutumista, kirjaa poikkeamat ja raportoi ne asiakkaalle välittömästi sekä aloittaa korjaustoimet sovitusti. Toimittaja velvoittaa myös alihankkijansa myötävaikuttamaan tämän vaatimuksen toteutumiseen (Vahti 3/2011)	Järjestelmien tietoturvapoikkeamien hallinta	Tietojärjestelmien tilan raportointi tuotetaan määrävälein
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Toimittaja raportoi palveluun liittyvien tietojärjestelmien ja niiden hallinnan tietoturvallisuuden tilasta asiakkaalle säännöllisesti, vähintään kerran vuodessa ja aina kun tietoturvallisuudessa esiintyy poikkeamia (Vahti 3/2011)	Järjestelmien tietoturvapoikkeamien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Toimittaja raportoi palveluun liittyvistä vakavista tietoturvatapahtumista asiakkaalle välittömästi (Vahti 3/2011)	Järjestelmien tietoturvapoikkeamien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Mittaaminen, raportoidaanko turvallisuustapahtumat ja käsitelläänkö ne muodollisesti (ISO/IEC 27004:2016)	Järjestelmien tietoturvapoikkeamien hallinta	Tietoturvahäiriöiden vasteryhmälle (Sirt) raportoitujen turvallisuustapahtumien lukumäärä suhteessa organisaation kokoon
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Laitteiden ja tietojärjestelmien päivitysten tarpeen seuranta, päivityspäätösten teko ja päivitysten asennus on vastuutettu ja organisoitu erityisesti tietoturvapäivitysten osalta (Vahti 2/2010)	Järjestelmien tietoturvahäiriöiden hallinta	Järjestelmillä on turvakuvaus
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Laitteiden ja tietojärjestelmien muutostarpeen seuranta, muutospäätösten teko ja muutosten toteutus on vastuutettu ja	Järjestelmien tietoturvahäiriöiden hallinta	

		organisoitu (Vahti 2/2010)		
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Ainakin sovelluksen käsittelemät tiedot ja sovelluksen konfiguraatiot on varmuuskopioitava säännöllisesti (Vahti 1/2013)	Järjestelmien tietoturvahäiriöiden hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti (Vahti 2/2010)	Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta	Sovellukset ja järjestelmät tekevät riittäviä lokeja
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Laitteet, ohjelmistot sekä tietojärjestelmät tekevät riittäviä lokeja ja kirjausketjuja toiminnastaan (Vahti 2/2010)	Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Sovelluksen tulee tuottaa riittävästi lokia virhetilanteista sekä tietoturvapoikkeamista (Vahti 1/2013)	Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta	Hälytysrajat ja kriittisyyden arvojen ylittävät tapahtumat
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Epäonnistuneet kirjautumisyritykset sekä muut valtuuksien puutteeseen kariutuvat toimenpideyritykset kirjataan (Vahti 3/2010)	Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta	Epäonnistuneiden kirjautumisyritysten lukumäärä
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Laitteiden lokiasetukset on määritetty sellaisiksi, että lokeista saadaan riittävästi tietoa verkon toiminnasta (Vahti 3/2010)	Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Kriittisten järjestelmien lokitiedostojen säännöllisten katselmointien vaatimuksenmukai-	Järjestelmän- ja tapahtumienhallinta, seuranta sekä lokienhallinta	Tarvittaessa katselmoitujen tapahtumalokitietojen prosenttiosuus ajanjaksoa kohden

		suuden arviointi (ISO/IEC 27004:2016)		
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Haittaohjelmakuvaukset päivittyvät säännöllisesti ja automaattisesti (Vahti 2/2010)	Järjestelmien haavoittuvuuksien hallinta	Haittaohjelmien automaattisten päivitysten asennusaika suhteessa päivityksen julkiseen jakeluaikatauluun/lanseeraus sekä onnistuminen ja läpimenoaika Toteutetut torjuntaohjelmien päivitykset Toteutetut tietoturvapäivitykset, jatkuvaluontoisten päivitysten raportit Sovellusten tietoturvapäivitysten ja korjausten dokumentoinnin katselmointi, tietoturvallisuuden tilaraportit Toteutetut sovellusten tietoturvapäivitykset, tietoturvallisuuden tilaraportit
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Sovellusten tietoturvapäivitykset pidetään ajan tasalla (Vahti 3/2010)	Järjestelmien haavoittuvuuksien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Toimittaja vastuuttaa ja organisoi hankinnan kohteen tuottamisessa käytettävien laitteiden ja tietojärjestelmien päivitys- ja muutostarpeen seurannan, päivityspäätösten teon ja päivitysten asennuksen erityisesti tietoturvapäivitysten osalta (Vahti 3/2011)	Järjestelmien haavoittuvuuksien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Kriittiset tietoturvapäivitykset tunnistetaan ja asennetaan (Vahti 1/2013)	Järjestelmien haavoittuvuuksien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Sovelluksen tietoturvapäivitysten ja korjauksien asennus on dokumentoitu (Vahti 1/2013)	Järjestelmien haavoittuvuuksien hallinta	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Organisaatiossa on yleinen toipumisstrategia ja suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille (Vahti 2/2010)	Järjestelmien ja palvelujen jatkuvuudenhallinta ja toipuminen	BIA-vaikutusanalyysien vuosittainen tarkistaminen tehty, tietoturvallisuuden tilaraportit Jatkuvuus- ja toipumissuunnitelmat on tarkastettu määrävälein, tietoturvallisuuden tilaraportit
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Järjestelmään kohdistetaan riskianalyysi, jolla pyritään löytämään tietoturvavaatimukset tarjouspyyntöön, vaatimus-	Järjestelmien riskienhallinta ja tärkeysluokittelu	Uusien järjestelmien riskianalyysi tehty

		määrittelyyn tai uuden version asennuksen projektisuunnitelmaan (Vahti 2/2010)		
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Laitteiden, rekistereiden ja tietojärjestelmien omistajuus on organisoitu ja vastuutettu (Vahti 2/2010)	Järjestelmien riskienhallinta ja tärkeysluokittelu	Järjestelmien omistajat -taulukko/katselmointi
Sisäinen näkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Sovelluksen tietoturvavaatimukset tulee ottaa huomioon jo suunnitteluvaiheessa kohdistamalla sovellukseen riskianalyysi (Vahti 1/2013)	Järjestelmien riskienhallinta ja tärkeysluokittelu	Sovelluksista tehty riskianalyysi suunnitteluvaiheessa
Sisäinen näkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Sovelluksen aiheuttamat riskit organisaation toiminnalle tulee viimeistään tässä vaiheessa viedä osaksi organisaation laajuista riskienhallintaprosessia ja riskikarttaa (Vahti 1/2013)	Järjestelmien riskienhallinta ja tärkeysluokittelu	
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Tietoturvatestit tulee suorittaa osana sovelluksen normaalia testausprosessia. Testauksesta valmistuu testiraportti, joka sisältää tiedon tietoturvatestien suorituksesta (Vahti 1/2013)	Järjestelmien konfiguraationhallinta ja tietoturvatestaus	Kriittisten järjestelmien testaus on tehty ja testausraportti tuotettu
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Arvioiminen, noudatetaanko muutoksenhallinnan parhaita käytäntöjä ja koventamispolitiikkaa (ISO/IEC 27001:2016)	Järjestelmien konfiguraationhallinta ja tietoturvatestaus	Prosenttiosuus uusista asennetuista järjestelmistä, joissa noudatettiin muutoksenhallinnan parhaita käytäntöjä ja koventamispolitiikkaa
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Kriittisten järjestelmien pääsyoikeuksien uudelleenarviointi ja tarkastaminen (ISO/IEC 27001:2016)	Järjestelmien pääsyoikeuksien hallinta	Niiden kriittisten järjestelmien prosenttiosuus, joissa pääsyoikeudet arvioidaan uudelleen säännöllisesti
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Suojausjärjestelmän vaikuttavuuden arvioiminen haittaohjelmien hyökkäykseltä suojaa-	Järjestelmien haavoittuvuuksien hallinta	Havaittujen ja torjumatta jääneiden hyökkäysten kehityssuunta useiden raportointijaksojen ajalla

		misessa (ISO/IEC 27004:2016)		
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Haittaohjelmille altistuneiden järjestelmien lukumäärä, joissa ei ole päivitettyä virustorjuntaohjelmaa (ISO/IEC 27004:2016)	Järjestelmien haavoittuvuuksien hallinta	Verkkoon kytkettyjen järjestelmien määrä, jotka ovat altistuneet haittaohjelmille ja joissa ei ole päivitettyjä torjuntaohjelmia
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Arviointi, ovatko arkaluonteista tietoa (luottamuksellisia, eheitä) käsittelevät tietojärjestelmät haavoittuvia haittaohjelmien hyökkäyksille (ISO/IEC 27004:2016)	Järjestelmien haavoittuvuuksien hallinta	Niiden kriittisten tietojärjestelmien prosenttiosuus, joille on suoritettu tunkeutumistestaus tai haavoittuvuuksien arviointi edellisen merkittävän päivityksen jälkeen
Asiakasnäkökulma	Tietoturvallisten järjestelmien ja palvelujen tuottaminen	Tietoturvahäiriöiden kehityssuunta (ISO/IEC 27004:2016)	Järjestelmien haavoittuvuuksien hallinta	Tietoturvahäiriöiden lukumäärä määritellyllä ajanjaksolla
Sisäinen näkökulma	Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta	Toteutetaan järjestelyt, joiden avulla voidaan varmistaa, että asetettuja tietoturvavaatimuksia noudatetaan myös silloin, kun viranomaisen asiakirjoja käsitellään toimeksiantosopimuksen perusteella esim. tietojenkäsittelyn palveluyrityksissä (Vahti 2/2010)	Lainsäädäntö ja tietoturvavelvoitteet	Perustason vaatimukset sopimuksissa, kuinka monessa sopimuksessa on mukana, tietoturvasopimusten lukumäärä
Sisäinen näkökulma	Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta	Perusvaatimuksena on, että kukin tiedonkäsittely-ympäristö sekä hallinnolliset toiminnot täyttävät tietoturvallisuuden perustasolle asetetut vaatimukset. Tämä koskee sekä viranomaisen omia järjestelyjä että niitä tahoja, jotka suorittavat tehtäviä viranomaisen toimeksiannosta (Vahti 2/2010)	Lainsäädäntö ja tietoturvavelvoitteet	

Sisäinen näkökulma	Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta	Organisaation omistamista henkilörekistereistä on Henkilötietolain 10§ mukainen rekisteriseloste ja se on asetettu rekisteröityjen nähtäville (Vahti 2/2010)	Lainsäädäntö ja tietoturvavelvoitteet	Rekisteriselosteiden/tietosuojaselosteiden lukumäärä
Sisäinen näkökulma	Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta	Kustakin tietojärjestelmästä on Julkisuuslain 18§ mukainen tietojärjestelmäkuvaus (Vahti 2/2010)	Lainsäädäntö ja tietoturvavelvoitteet	Tietojärjestelmäkuvausten lukumäärä
Sisäinen näkökulma	Lainsäädännön ja tietoturvavelvoitteiden mukainen toiminta	Sähköisten viestien, tunnistamistietojen sekä paikkatietojen luottamuksellisuudesta ja oikeasta käsittelystä huolehditaan myös lokitietojen käsittelyssä (Sähköisen viestinnän tietosuojalaki 4§ ja 5§) (Vahti 2/2010, perustaso)	Lainsäädäntö ja tietoturvavelvoitteet	Lokienhallinnan periaatteiden toteutuminen Käsittelyyn osallistuvien roolien katselmointi
Sisäinen näkökulma	Tietoturva- ja tietosuojapolitiikan mukainen toiminta	Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet. Tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu periaatteiden mukaisesti (Vahti 2/2010)	Käyttövaltuuksien hallinta	Käyttövaltuuksien tarkastus (esimiehet) tehty määrävälein/kehityskeskustelujen yhteydessä, asialistaan merkintä
Sisäinen näkökulma	Tietoturva- ja tietosuojapolitiikan mukainen toiminta	Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää (Vahti 3/2011)	Käyttövaltuuksien hallinta	
Sisäinen näkökulma	Tietoturva- ja tietosuojapolitiikan mukainen toiminta	Tietoturva-asioista raportoidaan organisaation johdolle säännöllisesti (Vahti 2/2010)	Tietoturvapoikkeamien hallinta	Raja-arvon ylittävistä ja kriittisistä tietoturvapoikkeamista raportoiminen Raportit ja dokumentaatio tehty linjausten ja vuosikellon mukaan

Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Toimintaan liittyvät tietoturvariskit on kartoitettu ja tietoturvallisuuden toteuttaminen on suunniteltua (Vahti 2/2010)	Tietoturvapoikkeamien hallinta	Riskianalyysit tehty vuosikellon mukaan Poikkeamat kirjattu ja niistä raportointi tehty
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Organisaatiossa tehdään säännöllisesti tietoturvallisuuteen liittyvien riskien arviointia (Vahti 2/2010)	Tietoturvapoikkeamien hallinta	Ilmoitetut/tietoon tulleet toimenpiteitä vaatineiden tietoturvatapahtumien lukumäärä Raportoitujen tietoturvapoikkeamien luonne ja määrä
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Vakavista tietoturvapoikkeamista kerrotaan johdolle viivytyksettä ja niistä pidetään kirjaa (Vahti 2/2010)	Tietoturvapoikkeamien hallinta	Virus- ja muut haittaohjelmavahingot ja torjuntaprosentti Havaitut virus- ja muut haittaohjelmat Roskapostitilanne
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Vakavista tietoturvatapahtumista kerrotaan tietoturvavastaavalle viivytyksettä (Vahti 2/2010)	Tietoturvapoikkeamien hallinta	Varkauksien ja kadotettujen laitteiden lukumäärä Havaitut tunkeutumisyritykset Havaitut palvelunestohyökkäykset
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Organisaatio ilmoittaa CERT-FI:lle vakavista tietoturvaloukkauksista ja niiden epäilyistä (Vahti 2/2012)	Tietoturvapoikkeamien hallinta	Epäonnistuneiden tunkeutumisyritysten lukumäärä järjestelmiin
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Riskien arvioinnin perusteella parannetaan tietoturvallisuutta liian suurten riskien osalta johdon päättämillä toimenpiteillä (Vahti 2/2010)	Tietoriskien hallinta	Priorisoitujen ja kriittisten tietoriskien käsittelyn eteneminen kokonaisriskien hallinnassa
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Organisaation johdolle raportoidaan riskianalyysin perusteella päätettyjen kehittämistoimenpiteiden edistymisestä	Tietoriskien hallinta	

		normaalin raportoinnin osana (Vahti 2/2012)		
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Tietoriskeille altistumisen arviointi (ISO/IEC 27004:2016)	Tietoriskien hallinta	Korkeat ja keskitason riskit, jotka ovat hyväksyttävän kynnysarvon yläpuolella
Sisäinen näkökulma	Tietoriskien havaitseminen ja niihin reagoiminen	Tietoriskeille altistumisen arviointi (ISO/IEC 27004:2016)	Tietoriskien hallinta	Korkeiden ja keskitasoisten riskien välitön katselmointi
Sisäinen näkökulma	Tietoturvallisuuden arviointi ja auditointi	Organisaatiossa tehdään säännöllisesti tietoturvallisuuden auditointeja tai arviointeja (Vahti 2/2010)	Tietoturvallisuuden auditointi	Auditoinnit tehty auditointisuunnitelman mukaan
Sisäinen näkökulma	Tietoturvallisuuden arviointi ja auditointi	Auditointien tai arviointien suosituksista pidetään koko organisaation tasolla kirjaa ja parannustoimenpiteiden toteutumista seurataan (Vahti 2/2010)	Tietoturvallisuuden auditointi	Tietoturvakatselmointien lukumäärä kohteittain
Sisäinen näkökulma	Tietoturvallisuuden arviointi ja auditointi	Auditoinnit tai itsearvioinnit toteutetaan suunnitelmallisesti ja ne ovat johdon hyväksymiä (Vahti 2/2012)	Tietoturvallisuuden auditointi	
Sisäinen näkökulma	Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu	Tietoturvatoiminnan tehokkuus ja suoritteet (Vahti 6/2006)	Tietoturvatoiminnan tehokkuus	Tietoturvaryhmän kokousten lukumäärä Tietosuojaryhmän kokousten lukumäärä Hallinnonalan tietoturvaryhmän kokousten lukumäärä
Sisäinen näkökulma	Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu	Tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä (Vahti 2/2010)	Käyttövaltuuksien hallinta	Käyttövaltuudet tarkastetaan säännöllisesti, vanhentuneiden tunnusten lukumäärä

Sisäinen näkökulma	Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu	Organisaatiossa on yleinen toipumisstrategia ja suunnitelma tärkeimpien omien järjestelmien häiriöille, jossa on mm. johdon hyväksymä tärkeysjärjestys ICT-palveluille (Vahti 2/2010)	Jatkuvuudenhallinta	BIA-vaikutusanalyysien vuosittainen tarkistaminen tehty, tietojärjestelmien tilaraportit Jatkuvuus- ja toipumissuunnitelmat on tarkastettu, tietojärjestelmien tilaraportit Suoritetut jatkuvuustestaukset
Sisäinen näkökulma	Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu	Jatkuvuuden hallinnan seuranta ja mittaaminen tehdään yleensä harjoitusten yhteydessä ja testien yhteydessä, sekä toteutuneita häiriötilanteita jälkikäteen arvioimalla (Vahti 2/2016)	Jatkuvuudenhallinta	Reagointi-, vaste- ja läpimenoajat (oma henkilöstö, palveluntarjoaja jne.) vs. luvatut Tapahtuneet merkittävät virhe- ja häiriötilanteet vs. skenaariot joihin on varauduttu Vuosikellon mukaisten toimenpiteiden toteutuminen Dokumenttien ajantasaisuus, tietojärjestelmien tietoturvallisuuden tilaraportit
Sisäinen näkökulma	Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu	Vyöhykkeelle tulee nimetä avainvastuuhenkilö, jonka tehtävänä on säilyttää avainkortit, tehdä avainten lisätilaukset, ylläpitää lukostokaaviot sekä huolehtia avainten ja kulkutunnisteiden kuittauksista ja jakamattomien avainten säilytyksestä (Vahti 2/2013)	Fyysisen turvallisuuden ja ympäristön turvallisuuden hallinta	Kaikilla toimistoilla avaintenhallinta kunnossa/vastuuhenkilö nimetty
Sisäinen näkökulma	Tietoturvallisuuden hallintajärjestelmän prosessi, kehittyneisyys ja laatu	Hävitettäväksi tarkoitetut asiakirjat tuhotaan niin, että luottamuksellisuus ja tietosuoja on varmistettu (Vahti 2/2010)	Fyysisen turvallisuuden ja ympäristön turvallisuuden hallinta	Poistoista on raportit ja hävitystodistukset
Oppimisen ja kasvun näkökulma	Tietoturvatietoisuus	Annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan	Viestintä ja ohjeistus	Tietoturvatestit

		säännöllisesti (Vahti 2/2010)		
Oppimisen ja kasvun näkökulma	Tietoturvatietoisuus	Muuttuneista tietoturvaohjeista ja -käytännöistä tiedotetaan kaikille organisaatiossa toimiville (Vahti 2/2010)	Viestintä ja ohjeistus	Tietoturvainfot, infojen lukumäärä Henkilöstölle suunnattujen tiedotteiden lukumäärä
Oppimisen ja kasvun näkökulma	Tietoturvatietoisuus	Perehdyttämistilanteessa käsitellään myös tietoturva-asioita (Vahti 2/2010)	Perehdyttämisprosessi	Perehdyttämisprosessissa tietoturva-asioiden läpikäynti
Oppimisen ja kasvun näkökulma	Tietoturvatietoisuus	Osana organisaation perehdyttämisprosessia uusille työntekijöille järjestetään tietoturvakoulutus, jossa työntekijälle esitetään organisaation tietoturvasäännöt ja hänet perehdytetään organisaation tietoturvatoimintaan ja -tavoitteisiin (Vahti 1/2013)	Perehdyttämisprosessi	Perehdyttämisprosessin tietoturvallisuuden verkkokoulutus Salassapitosopimus allekirjoitettu
Oppimisen ja kasvun näkökulma	Tietoturvatietoisuus	Sovelluskehityksestä vastuussa oleville tulee järjestää tietoturva-koulutusta, ns. tietoisuuskoulutusta (awareness training) (Vahti 1/2013)	Tietoturvakoulutus	Tietoturvakoulutuksen toteutuminen
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä (Vahti 2/2010)	Tietoturvakoulutus	
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Pidetään huolta, että virkamiehet tietävät luokittelumerkintöjen merkityksen ja sen, että ne eivät vapauta viranomaista velvollisuudesta asiakirja- ja tapauskohtaisesti arvioida julkisuuslain ja sen ratkaisu-	Tietoturvakoulutus	

		käytännön mukaisesti asiakirjan julkisuutta siitä tietoja julkisuuslain nojalla pyydettäessä (Vahti 2/2010)		
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Tietoturvahenkilöstön osaamista kehitetään ja ylläpidetään (Vahti 2/2010)	Tietoturvakoulutus	Tietoturvakoulutuksen kohdentaminen ja toteutuminen määrävälein, koulutusten lukumäärä
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Organisaatiossa järjestetään säännöllisesti tietoturvakoulutusta henkilöstölle ja muille avainryhmille (Vahti 2/2010)	Tietoturvakoulutus	
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Työntekijät tietävät miten tietoaineistoja organisaatiossa käsitellään (Vahti 2/2010)	Tietoturvakoulutus	
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Käyttäjät koulutetaan ilmoittamaan havaituista puutteista, ongelmista ja niiden epäilyistä esimiehelle, tietoturvavastaavalle tai verkon vastuuhenkilölle (Vahti 3/2010)	Tietoturvakoulutus	
Oppimisen ja kasvun näkökulma	Tietoturvaosaaminen ja koulutus	Hallinnonalan koulutus ja roolin mukainen tietoturvaosaaminen	Tietoturvakoulutus	Hallinnonalan tietoturvakoulutukset, lukumäärä Hallinnonalan tietoturvaryhmän toiminta ja osallistuminen, lukumäärä

LIITE 2. BIA-vaikutusanalyysin täyttöpohja.

Vaikutusanalyysin (BIA, Business Impact Analysis) täyttöpohja

BIA-analyysin/-arvioinnin tiedot kirjataan tähän lomakkeeseen. Yhteenveto sekä yksityiskohtainen raportti voidaan tulostaa eri välilehdeltä.

1. Kohde, kohteen omistaja, arvioinnin tekijä, arviointiin osallistujat sekä dokumentin muutoshistoria

BIA-analyysin kohde:	
Kohteen sijainti:	
Palvelun tarjoaja:	

Arvioinnin teettäjä:	
Työrooli:	
Organisaatio:	

Kohteen omistaja:	
Työrooli:	
Organisaatio:	

Arvioinnin suorittamisajankohta:			
Arviointi alkoi:		**kello**	
Arviointi päättyi:		**kello**	

Muut arviointiin/arviointitilaisuuteen osallistujat:		
Osallistujan nimi:	**Työrooli:**	**Organisaatio:**

Dokumentin versiointi, muutoksen tekijä ja muutos:			
Ver.	**Päivämäärä**	**Päivittäjä/muuttaja**	**Muutos**

2. Kohteessa käsiteltävien tietojen sekä kohteen tietoturva- ja ICT-varautumisen luokitukset

Suojaustaso luokitus:	
5	**Suojaustaso I (ST I)**
4	**Suojaustaso II (ST II)**
3	**Suojaustaso III (ST III)**
2	**Suojaustaso IV (ST IV)**
1	**Julkinen / ei luokitusta**

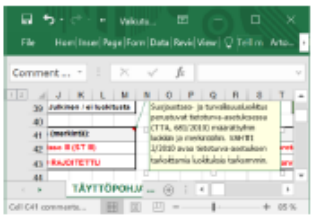
Turvallisuusluokitus:	
5	**ERITTÄIN SALAINEN**
4	**SALAINEN**
3	**LUOTTAMUKSELLINEN**
2	**KÄYTTÖ RAJOITETTU**
1	**Julkinen / ei luokitusta**

Täyttövinkkinä seuraavaa:
- useimmiten järjestelmässä tai palvelussa on käytössä vain jompi kumpi eli suojaustaso tai turvallisuusluokitus
- tietoturvaluokkaan tulee arvo automaattisesti tietojen tason perusteella (tarvittaessa arvoa voi muuttaa manuaalisesti)

Kohteen tietoturvataso ja/tai ICT-varautumistaso vaihtoehdot:	
4	**Korkea taso**
3	**Korotettu taso**
2	**Perustaso**
1	**Ei tasoluokittelua**

Korkein kohteen sisältämien tietojen luokitus (merkintä):		
Suojaustaso (ST...):		Ei arvioitu
Turvallisuusluokitus:		Ei arvioitu

Kohdetta koskevat luokitukset:			**Lisätietoja:**
Tietoturvataso:	0	Ei arvioitu	
ICT-varautumistaso:		Ei arvioitu	



Vinkki: Joissakin ruuduissa on kyseiseen kohtaan lisätietoja antamassa 'Kommentti'-kenttä, joka aktivoituu hiiren päälle viemisellä.

3. Tietoturvallisuuden tärkeys, palvelutasotavoitteet

Tietoturvallisuuden tärkeys (käytä arvoja 1-4):		
Luottamuksellisuus:		Ei arvioitu
Eheys:		Ei arvioitu
Saatavuus:		Ei arvioitu

Käytettävät vaihtoehdot:		Esimerkiksi luottamuksellisuudessa:
4	Erittäin tärkeä	ST II tai ST I luokiteltua aineistoa.
3	Tärkeä	ST III luokiteltua aineistoa.
2	Jonkin verran merkitystä	ST IV luokiteltua aineistoa.
1	Vähäinen merkitys	Julkista/luokittelematonta aineistoa.

Muu mahdollinen tärkeys, mikä (vapaamuotoinen selitys):

Eheys: Esim. digitaalinen tiedotuskanava, lupapalvelu tai myyntisovellus.
Saatavuus: Esim aikakriittisyys, tietty palveluaika tai palvelutasosopimukse

Kohteen osalta sovittu palvelutaso (SLA, Service Level Agreement) kuvataan valitsemalla vaihtoehdoista 1-6:

Sopimukseen perustuva käytössä oleva SLA-taso:		
Täytä vaihtoehto 0-6:		Ei sovittu
Palveluaikatavoite		Ei sovittu
Käytettävyystavoite		Ei sovittu
Palveluvastetavoite		Ei sovittu
Ratkaisuaikatavoite		Ei sovittu

SLA-tasojen vaihtoehdot (tarvittaessa täytä oma asteikko):		Palveluaika	Käytettävyys	Palveluvaste	Ratkaisuaika
Erittäin kriittinen	5	24/7	99,9 % (99,95 %)	15 minuuttia	3 tuntia
Kriittinen	4	24/7	99,5 % (99,9 %)	30 minuuttia	4 tuntia
Laajennettu	3	arkisin 7-21, la-su 9-18	99 % (99,5 %)	2 tuntia	1 työpäivä
Normaali	2	arkisin 7-19	99 % (99,5 %)	2 tuntia	1 työpäivä
Lähtötaso	1	arkisin 8-16 tai huonompi	97 % (99 %) tai huonompi	4 tuntia tai enemmän	2 työpäivää tai enemmän
Oma asteikko:	6				

4. Odottamattoman käyttökatkoksen, tietojen menetyksen ja vanhenemisen vaikutukset

Arvioinnissa valinnoissa käytettävät vaihtoehdot 0-5:					
5	Sietämättömät	3	Merkittävät	1	Ei vaikutusta
4	Kohtuuttomat	2	Jonkin verran	0	Ei arvioitu

Odottamattoman katkoksen vaikutukset arviointialueille:	Painotus	oma	Omalle organisaatiolle	Kumppaneille tai alihankintatahoille	Asiakkaille tai loppukäyttäjille	Muulle osapuolelle... Yhteiskunnalle
Terveyden tai hengen vaara	1,20	1,20	Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Lakisääteiset tehtävät	0,80	0,80	Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Taloudelliset vahingot	1,00	1,00	Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Mainevaikutukset	1,00	1,00	Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Tärkeysindeksi:		0,00				
Tärkeysluokka:		Ei kriittinen				

Häiriön kesto vs. vaikutuksen pienuus / suuruus:		Kesto, jolla pienin vaikutus: Kesto		Vaikutus	Kesto, jolla suurin vaikutus: Kesto		Vaikutus
Palvelun toiminnan täysin keskeyttävä odottamaton ja suunnittelematon häiriö:	palveluaikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
	ns. virka-aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
	muuna aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
Palvelu on erityisen kriittinen:							
Keskeytyksen aiheutuminen:	kriittisenä aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
Lisätietoja / muu häiriön kuvaus							

Tietojen menettämisen ja vanhenemisen vaikutukset:		Kesto, jolla pienin vaikutus: Kesto		Vaikutus	Kesto, jolla suurin vaikutus: Kesto		Vaikutus
Aika ja vaikutukset sen mukaan, miten pitkältä ajalta tiedot voidaan menettää:	palveluaikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
	ns. virka-aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
	muuna aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
Lisätietoja:							
Aika ja vaikutukset sen mukaan, miten pitkään voidaan toimia ilman tietojen päivittymistä:	palveluaikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
	ns. virka-aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
	muuna aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
Lisätietoja:							
Tiedot ovat erityisen kriittisiä:							
Keskeytyksen aiheutuminen:	kriittisenä aikana		h	Täytä arvo 1-5		h	Täytä arvo 1-5
Lisätietoja / muu häiriön kuvaus							

5. Keskeiset riippuvuudet

Käytettävissä olevat vaihtoehdot (tässä ensisijaisesti vaihtoehdot 3-5):			
5	Elintärkeä	2	Jonkin verran merkitystä
4	Erittäin tärkeä	1	Vähäinen merkitys
3	Tärkeä	0	Vähäinen merkitys

Huom! Luokkiin 1-2 kuuluvat jätetään pääsääntöisesti listaamatta.

Tässä kohdassa luetellaan tärkeimmät riippuvuudet.

Arviointikohteen toiminta riippuu seuraavista:

Riippuvuuden tärkeys:		Palvelu/järjestelmä:	Vastuuorganisaatio:	Riippuvuus:	Lisätietoja
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
Muita riippuvuuksia (tarvittaessa):					

Toiminnot, jotka riippuvat arviointikohteesta:

Riippuvuuden tärkeys:		Palvelu/järjestelmä:	Vastuuorganisaatio:	Riippuvuus:	Lisätietoja
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
Muita riippuvuuksia (tarvittaessa):					

6. Yhteiskunnan turvallisuusstrategian (YTS 2010) uhkakuvien vaikutukset

Yleiset velvoitteet valmiussuunnitteluun ja/tai varautumiseen:		
Valmiuslaki (1552/2011) velvoittaa varautumaan (tämän kohteen osalta):		Ei arvioitu
Varautumisvelvollisuus tulee jostakin muusta säädöksestä tai viranomaisohjeesta:		Ei arvioitu
Kohde liittyy yhteiskunnan turvallisuusstrategiassa (YTS 2010) kuvattuihin tehtäviin:		Ei arvioitu
Kohteeseen liittyviä tehtäviä täytyy suorittaa myös häiriö-/poikkeusoloissa:		Ei arvioitu

Käytettävissä olevat vaihtoehdot:	
1	Kyllä
2	Ei
0	Ei arvioitu

Huom! Mikäli jokaisen viereisen kohdan valinta on 2 eli ei varautumisvelvollisuutta, jätä elintärkeät tehtävät arvioimatta ja siirry uhkien tarkasteluun.

Yhteiskunnan elintärkeät tehtävät (jätetään käsittelemättä, mikäli em. kaikkiin kohtiin tuli valinta 2 Ei).

Kohteen merkitys yhteiskunnan elintärkeille tehtäville (katso tarvittaessa tarkemmin yhteiskunnan turvallisuusstrategiasta):		
Valtion johtaminen		Ei arvioitu
Kansainvälinen toiminta		Ei arvioitu
Suomen puolustuskyky		Ei arvioitu
Sisäinen turvallisuus		Ei arvioitu
Talouden ja infrastruktuurin toimivuus		Ei arvioitu
Väestön toimeentuloturva ja toimintakyky		Ei arvioitu
Henkinen kriisinkestävyys		Ei arvioitu

Käytettävissä olevat vaihtoehdot:			
5	Elintärkeä	2	Jonkin verran merkitystä
4	Erittäin tärkeä	1	Vähäinen merkitys
3	Tärkeä	0	Ei arvioitu

Yhteiskunnan turvallisuusstrategiassa kuvatut uhkamallit. Arvioidaan uhkien merkitys arvioinnin kohteelle.

Käytettävissä olevat vaihtoehdot 0-5 (Huom! Avaa tarvittaessa yksityiskohtaisempi arviointiruudukko):											
5	Sietämättömät	4	Kohtuuttomat	3	Merkittävät	2	Jonkin verran	1	Ei vaikutusta	0	Ei arvioitu

Mitkä näistä uhkista voivat häiritä kohteen toimintaa?			
	Voimahuollon vakavat häiriöt		Julkisen talouden rahoituksen saatavuuden häiriintyminen
	Tietoliikenteen ja tietojärjestelmien vakavat häiriöt - kyberuhkat		Väestön terveyden ja hyvinvoinnin vakavat häiriöt
	Kuljetuslogistiikan vakavat häiriöt		Suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhkat
	Yhdyskuntateknikan vakavat häiriöt		Terrorismi ja muu yhteiskuntajärjestystä vaarantava rikollisuus
	Elintarvikehuollon vakavat häiriöt		Rajaturvallisuuden vakavat häiriöt
	Raholtus- ja maksujärjestelmän vakavat häiriöt		Poliittinen, taloudellinen ja sotilaallinen painostus
			Sotilaallisen voiman käyttö

Huom! Alla on tarvittaessa avattavissa yksityiskohtaisempi ruudukko YTS 2010 uhkakuvien vaikutusten arviointia varten:

Vaikutusanalyysi yhteenveto 20.1.2016

Arvoitu kohde:	Tietojärjestelmä XYZ
Kohteen omistaja:	Pekka Palvelujohtaja
Omistajan organisaatio:	Virasto ABC
Arvioinnin toteutusaika:	19.1.2016 - 20.1.2016

Tärkeysluokka	2,70	Merkittävä

Tiedot suojaustasoluokka:	3	Suojaustaso III (ST III)
Tiedot turvallisuusluokka:	2	KÄYTTÖ RAJOITETTU
Kohde, tietoturvataso:	3	Korotettu taso
Kohde, ICT-varautuminen:	0	Ei arvioitu
Palvelutasosopimus (SLA):	0	Ei sovittu

Yhteiskunnan turvallisuusstrategia (YTS 2010) mukaan

Kohteen tärkeys yhteiskunnalle:	3	Tärkeä
Suurin uhkan/riskin vaikutus:	5	Sietämätön

Odottamattoman katkoksen suurimmat vaikutukset:

Oman organisaation toiminnalle	3	Merkittävät
Kumppaneille tai alihankintatahoille:	2	Jonkin verran
Asiakkaille tai loppukäyttäjille:	3	Merkittävät
Yhteiskunnalle	3	Merkittävät

Odottamattomassa katkoksessa suurimmat menetykset:

Terveyden tai hengen menetys	2	Jonkin verran
Lakisääteisten tehtävien viivästys	3	Merkittävät
Taloudellisina menetyksinä	3	Merkittävät
Maineen menetyksenä	3	Merkittävät

Suositeltavat jatkotoimet/kommentit arvioinnin tuloksista:

Tarkasta/laadi jatkuvuussuunnitelmat.

Arvioi ICT-varautumisen tarpeet.