Jarmo Simi

TIEDON LUOKITTELU OSANA ORGANISAATION KOKONAISARKKITEHTUURIN RISKIENHALLINTA-PROSESSIA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2017

TIIVISTELMÄ

Simi, Jarmo Juhani
Tiedon luokittelu osana organisaation kokonaisarkkitehtuurin riskienhallinta-prosessia
Jyväskylä: Jyväskylän yliopisto, 2017, 85 s.
Tietojenkäsittelytiede, pro gradu -tutkielma
Ohjaaja: Seppänen, Ville

Tutkimuksen tavoitteena oli kehittää menetelmä, jonka avulla voidaan tunnistaa organisaation kokonaisarkkitehtuuri- tai tietojärjestelmäprojektien tietoturvallisuusvaatimukset. Menetelmän tulisi tukea liiketoimintajohdon, tietojärjestelmäarkkitehtien ja -asiantuntijoiden välistä kommunikaatiota. Menetelmän tulisi myös tukea organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista. Menetelmän kehitys perustui kohdejärjestelmissä käsiteltävän tiedon tunnistamiseen ja luokitteluun tietoturvallisuuden osa-alueiden luottamuksellisuuden, saatavuuden ja eheyden perusteella. Tutkimuksessa sovellettiin suunnittelutieteellistä menetelmää. Tutkimuksen artefaktia testattiin ja kehitettiin viidessä erillisessä tutkimustapauksessa. Tutkimustapausten havainnot dokumentoitiin tutkimuskyselyn ja haastatteluiden avulla. Tulosten perusteella kehitetty menetelmä todettiin soveltuvaksi suunniteltuun tehtäväänsä. Menetelmää pidettiin loogisena ja helppokäyttöisenä ja kaikki osallistujat suosittelivat menetelmän jatkotestausta laajemmin tietojärjestelmäprojekteissa. Tutkimuksen näkökulma, tiedon tunnistaminen ja luokittelu osana kokonaisarkkitehtuuri- tai tietojärjestelmäprojektia oli kaikille tutkimukseen osallistuneille uusi. Näkökulman etuna pidettiin sen antamaa kokonaisvaltaista näkemystä kohteena olevista projekteista. Tutkimustapausten yhteydessä kyettiin menetelmän avulla vertailemaan tietoturvallisuuden eri osa-alueiden merkitystä kohdejärjestelmälle ja tuottamaan perusteltuja ratkaisuesityksiä. Tutkimustapauksen päätteeksi tuotettiin tutkijan johdolla esitys kohteena olevan projektin tietoturvallisuuden jatkotoimenpiteistä ja niiden vaihtoehdoista. Esitys perustui menetelmän käytön yhteydessä koottuihin tietoihin sekä riskienarviointiin ja siinä huomioitiin yleiselle tasolla vaadittavat resurssit.

Asiasanat: luokitus, kokonaisarkkitehtuuri, riskienhallinta, tietojärjestelmät, tietoturva, johtaminen

ABSTRACT

Simi, Jarmo
Information Categorization as a Part of Organization´s Enterprise Architecture Risk Management Processes
Jyväskylä: University of Jyväskylä, 2017, 85 p.
Information Systems, Master's Thesis
Supervisor: Seppänen, Ville

The aim of the study was to create a method for organizations' enterprise architecture and information system management. The management method should recognize information security requirements for the organizations and support organizations' risk management. It should also support communication and coordination between business managers and information system professionals. At the same time, the method should endorses information security requirements in communication between organizations. Recognition and categorization of information in the information system creates the foundations of developing the method.. Categorization is based on three sections of the information security; confidentiality, integrity and availability. Design Science Research Methodology was chosen to be the research method. The artifact was tested and further developed in five different cases. The findings of the study are documented with research surveys and interviews. According to the results of the research, the method was found applicable for its purpose. The method was considered to be logical and easy to use by the study partisipants. All participants recommended testing the method further in various information system projects. The method perspective, recognition and categorization of information, was new viewpoint for all of the participants. The method was useful and it offered comprehensive view to the projects. In the study cases it was possible to compare the areas of information security in the information systems by using the method. Moreover, it was possible to produce proposed decisions.

Keywords: Categorization, Enterprise Architecture, Risk Management, Information System, Information Security, Management

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kesällä 2016 Yleisradion julkaisi verkkosivuillaan uutisen "Sydänpotilas hengenvaarassa teho-osastolla - kirurgia ei voitu Soneran heikon mobiiliverkon takia tavoittaa HUS:ssa" (Fagerström & Nelskylä, 2016). Uutisessa esitetään kritiikkiä HUS Meilahden sairaalassa tapahtuneen tilanteen johdosta mobiiliverkon palvelutuotannosta vastannutta Soneraa kohtaan. Vanhan 2G-verkon johdosta päivystävää sydänkirurgia ei tavoitettu viiveettä. Oliko vika pelkästään Soneran? Vastasiko HUS päivystävän lääkärin 2G-verkossa toimivan puhelimen saatavuus päivystystehtävän kriittistä tavoitettavuutta? Oliko HUS arvioinut päivystävän lääkärin tavoitettavuuspalvelun saatavuuteen kohdistuvia vaatimuksia ja vastasiko valittu tekninen ratkaisu vaatimuksia?

Tämän pro gradu -työn aiheena on "Tiedon luokittelu osana organisaation kokonaisarkkitehtuurin riskienhallintaprosessia". Tavoitteena on tutkia tietoturvallisuuden luokittelumenetelmien hyödyntämismahdollisuuksia tunnistettaessa ja arvioitaessa organisaatioiden kokonaisarkkitehtuurissa käsiteltäviä tietovarantoja. Näistä tietovarannoista käytetään työssä nimitystä tietotyyppi. Tutkielman tavoitteena on kehittää tietoturvallisuuden analyysimenetelmä, jota voidaan hyödyntää tietojärjestelmien suunnittelun, kehittämisen ja toteutuksen yhteydessä. Tietoturvallisuuden analyysimenetelmän kautta voidaan tunnistaa erilaiset tietotyypit ja arvioida niihin kohdistuvia vaatimuksia tietoturvallisuuden osa-alueiden luottamuksellisuuden, saatavuuden ja eheyden kautta. Analysointimenetelmällä pyritään myös tukemaan liiketoimintajohdon ja ICT-alan asiantuntijoiden välistä kommunikaatiota sekä tukemaan organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista.

1.1 Tutkielman keskeiset käsitteet

Tutkielman keskeisiä käsitteitä ovat tieto, tietojärjestelmä, kokonaisarkkitehtuuri, tietoturvallisuus ja riskienhallinta. Tieto käsitteenä ja sen jakautuminen dataan, informaatioon sekä tietämykseen muodostaa tutkimuksen käsitteiden

pienimmän yksikön. Tutkimuksessa pohditaan tiedon merkitystä organisaatioille ja sitä miten tieto "virtaa" eri muodoissaan tietojärjestelmissä ja organisaatioiden kokonaisarkkitehtuureissa. Tietoturvallisuuden tehtävänä on turvata tiedon luottamuksellisuus, saatavuus ja eheys. Tietoa ja sen suojaamista tarkastellaan näiden tietoturvallisuuden eri osa-alueiden, luottamuksellisuuden, saatavuuden ja eheyden vaatimusten näkökulmasta. Tietojärjestelmät ja kokonaisarkkitehtuurit perustuvat teknologian, ihmisen ja prosessien muodostamaan kokonaisuuteen. Riskienhallinta muodostaa organisaation johdolle "työvälineen", jonka avulla organisaation kokonaisarkkitehtuurissa ja sen osana olevia tietojärjestelmissä olevaa ja prosessoitavaa tietoa voidaan tietoturvallisuuden näkökulmasta johtaa.

1.2 Menetelmä ja tutkimuskysymykset

Kyseessä on konstruktiivinen tutkimus, jossa käytetään suunnittelutieteellistä menetelmää. Tutkimustehtävänä on etsiä ja kehittää käytännön johtamistyössä sovellettavaa menetelmää tunnistaa organisaation kokonaisarkkitehtuuri- tai tietojärjestelmäprojektien tietoturvallisuusvaatimukset. Menetelmän tulisi tukea liiketoimintajohdon, tietojärjestelmäarkkitehtien ja -asiantuntijoiden välistä viestintää ja kommunikaatiota. Menetelmän tulisi myös tukea organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista. Tutkimuksen kohteena oleva menetelmä rakentuu tutkimuksessa käsiteltävän kirjallisuuden ja tutkimuksen suunnittelutieteellisen menetelmän soveltamisen myötä saatavien havaintojen mukaisesti. Menetelmän rakentumista tukee tutkijan työelämästä saamat kokemukset. Tutkimustehtävään haetaan vastausta seuraavien tutkimuskysymyksien kautta:

- Miten luokittelua voidaan hyödyntää organisaatioiden kokonaisarkkitehtuurin projekti- ja tietojärjestelmäsuunnittelussa?
- Miten luokitteluprosessi vaiheistetaan ja määritellään parhaan kustannustehokkuuden saavuttamiseksi?
- Miten luokitteluprosessissa varmistetaan tietoturvallisuuden eri osa-alueiden, luottamuksellisuuden, saatavuuden ja eheyden vaatimusten huomioiminen?

Tutkimuksen empiirisen materiaalin kokoamiseksi muodostetaan määritetty luokittelun testiprosessi, jota toistetaan viidessä erillisessä tutkimustapauksessa. Kussakin tapauksessa on tavoitteena tutkia luokitteluprosessin soveltuvuutta ja vaiheistusta sekä havainnoida kehittämistarpeita. Tutkimustapauksista kerätään empiiriset havainnot kyselylomakkeella ja täydentävällä haastattelulla. Luokittelun testiprosessia kehitetään kunkin tutkimustapauksen kokemusten perusteella. Tutkimustapausten havainnot analysoidaan kunkin tutkimustapauksen päätteeksi ja niiden perusteella raportoidaan tutkimuksen kokonaistulokset.

1.3 Pro gradu tutkimuksen rakenne

Johdannossa käsitellään työn tavoitteet, toteutus, keskeiset käsitteet, tutkimuskysymykset ja rakenne. Toisessa ja kolmannessa luvussa käsitellään kirjallisuuteen perustuen tutkimuksen keskeiset määritelmät ja miten ne liittyvät tässä tutkimuksessa toisiinsa. Lukujen päätavoitteena on rakentaa tutkimuksen teoreettinen viitekehys. Neljännessä luvussa käsitellään suunnittelutieteellisen tutkimusmenetelmän perusteet ja miten menetelmää tässä tutkimuksessa sovelletaan. Luvussa käsitellään yksityiskohtaisesti tutkimuksen toteutus ja empiirisen aineiston kokoaminen. Viidennessä luvussa käsitellään työn tulokset. Luvussa kuvataan mihin muotoon tutkimuksen kohteena ollut menetelmä iterointikierrosten tuloksena muotoutui, miten menetelmää eri tapauksissa testattiin ja millaista palautetta tapausten käsittelyn yhteydessä saatiin sekä miten kukin tapaus vaikutti lopputulokseen. Viimeisessä kuudennessa luvussa tutkimuksen tulokset kootaan yhteen johtopäätösten ja pohdinnan muodossa.

2 KOKONAISARKKITEHTUURISTA TIETÄMYKSEEN

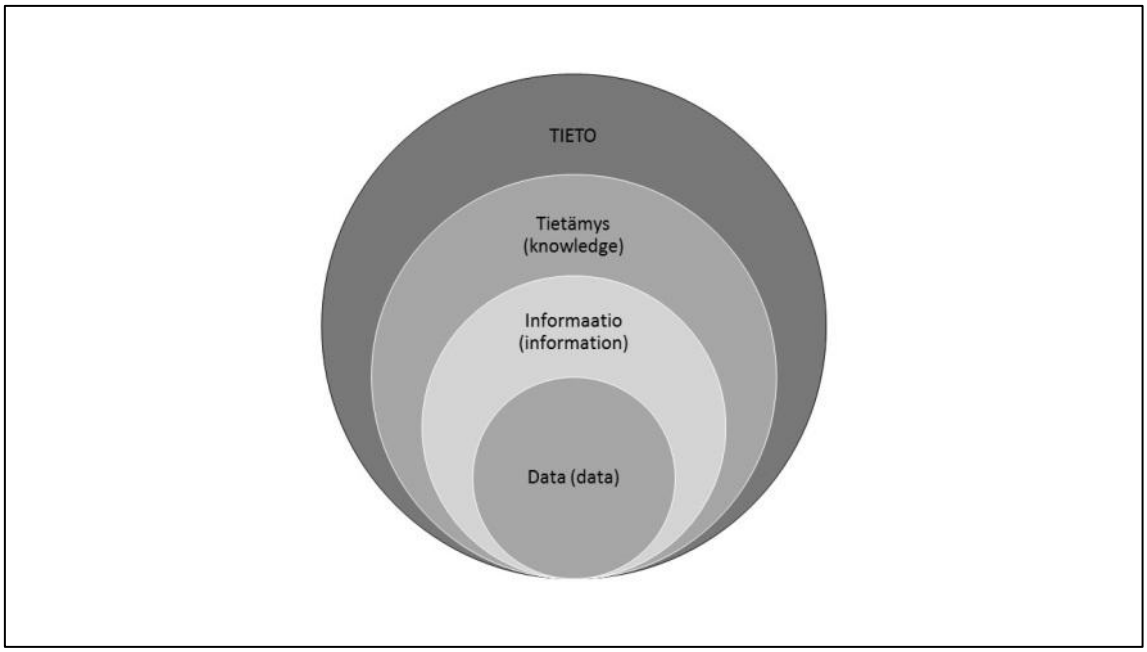
Kirjallisuuskatsauksen tehtävänä on muodostaa tutkimuksen käsitteellinen viitekehys (Hirsijärvi, Remes & Sajavaara, 2013). Tämän toisen ja seuraavan kolmannen luvun tavoitteena on määritellä kirjallisuuteen perustuen tutkimuksen viitekehys ja rajaukset sekä keskeiset käsitteet. Toisessa luvussa käsitellään tiedon, tietojärjestelmän sekä kokonaisarkkitehtuurin määritelmät ja merkitys tässä tutkimuksessa.

2.1 Data, tieto ja tietämys – tietojärjestelmästä kokonaisarkkitehtuuriin

Tutkimuksen aihe ”Tiedon luokittelu osana organisaation kokonaisarkkitehtuurin riskienhallintaprosessia” on moniselitteinen. Tämän luvun tavoitteena on rakentaa perusta tutkimuksen viitekehykselle ja esitellä siihen liittyvät kokonaisarkkitehtuurin, tietojärjestelmän sekä tiedon käsitteet ja niiden määritelmät tässä tutkimuksessa.

2.1.1 Tiedosta tietämykseen

Hytönen ja Kolehmainen (2003) käsittelevät tieto-sanan määrittelyä ja merkitystä. He vertaavat näitä määrittelyitä myös englannin kielen terminologiaan ja sanastoon. Englanninkielen sanat data, information ja knowledge käännetään usein suomenkielessä tieto-sanaksi. Tämä käännös on kuitenkin vajavainen eikä ole yksiselitteinen. Yksiselitteisen tuloksen saavuttamiseksi he esittävät kuvion 1 mukaisen kolmitasoisen luokittelun, jonka yläkäsitteenä toimiva tieto jakautuu kolmeen alaluokkaan. Alaluokat he ovat kääntäneet suomenkieleen seuraavasti data (data), informaatio (information) ja tietämys (knowledge). Englanninkieliset termit ovat suluissa. (Hytönen & Kolehmainen, 2003.)



Kuvio 1 Tiedon alaluokat

Ensimmäinen tason tieto, data, kuvaa yksityiskohtaisesti jotain reaalimaailman kohdetta. Data on yleensä helposti jäsennettävää ja käsiteltävää. Dataa voidaan muokata merkkitietona ja tallentaa fyysiselle tallenteelle. Data toimii seuraavan tason tiedon, eli informaation raaka-aineena. Dataan ei liity analyysia tai tulkintaa. (Trakman & Desouza, 2012.)

Informaatio eroaa datasta siinä, että sillä on merkitys, esimerkiksi osoitekirja. Informaatiota muodostuu käsiteltäessä ja analysoitaessa dataa. Analyysi voi tapahtua tietojärjestelmien sovellusten matemaattisten, tilastollisten ja loogisten prosessien kautta. (Trakman & Desouza, 2012.)

Tiedon korkein taso on tietämys. Tietämys muodostuu informaation ja datan pohjalta henkilön tai organisaation kokemukseen ja ymmärrykseen perustuen. Tietämykseen liittyy ajattelua, tulkintaa ja se liittyy johonkin kontekstiin. Tietämykseen liittyy muutakin kuin arkistojen asiakirjoja; se on myös organisaation rutiineja, prosesseja, käytänteitä ja normeja. (Trakman & Desouza, 2012.)

Tutkimuksessa noudatetaan Hytösen ja Kolehmaisen (2003) esittämää suomenkielistä käännöstä tiedon määritelmästä ja luokittelusta. Tutkimuksen kannalta on merkityksellistä ymmärtää tiedon, datan, informaation ja tietämyksen määritelmät sekä ymmärtää tiedon merkityksen moninaisuus ja pohtia sitä, miten organisaatiot voivat tunnistaa ja hallita tietoresurssejaan. Tutkimuksen otsikossa ”tiedon luokittelulla” tarkoitetaan pääasiassa ”tietämyksen luokittelua”. Yksittäisissä rajatuissa kohteissa luokittelu voi kohdistua myös dataan sekä informaatioon.

2.1.2 Tietojärjestelmä ja kokonaisarkkitehtuuri

Luvun tavoitteena on määritellä tietojärjestelmän ja kokonaisarkkitehtuurin termit sekä niiden suhteet tässä tutkimuksessa. Suomen kyberturvallisuusstrategia määrittää tietojärjestelmän:

> Tietojärjestelmällä tarkoitetaan ihmisistä, tietojenkäsittelylaitteista, tiedonsiirtolaitteista ja ohjelmista koostuvaa järjestelmää, jonka tarkoituksena on informaatiota käsittelemällä tehostaa tai helpottaa jotakin toimintaa tai tehdä toiminta mahdolliseksi. (Suomen kyberturvallisuusstrategia, 2013, 13.)

Yksittäinen laite, esimerkiksi matkapuhelin ja sitä käyttävä ihminen muodostavat tietojärjestelmän. Yrityksen toiminnanohjausjärjestelmä, siihen liittyvät tietokoneet, tietoverkot ja sitä käyttävät ihmiset muodostavat tietojärjestelmän. Käytämme vapaa-ajallamme ja työssämme jatkuvasti useita tietojärjestelmiä. Nykypäivän organisaatioiden tulee hallinnoida jatkuvasti muuttuvaa, useiden tietojärjestelmien verkostoa.

Sosiotekninen lähestymistapa tarkastelee tietojärjestelmien suunnittelua ja kehittämistä kokonaisvaltaisesti sosiaalisen ja teknisen komponentin kautta. Molempia komponentteja tarvitaan organisaation liiketoiminnan tavoitteiden saavuttamiseksi. Sosiotekninen lähestymistapa syntyi alkujaan 1950-luvulla tutkimaan ihmisten, organisaatioiden ja teknologian vuorovaikutukseen liittyviä haasteita. Tietojärjestelmien kehittyessä sitä on käytetty myös niiden tutkimiseen. (Mumford, 2006.) Sosioteknisessä lähestymistavassa pyritään näkemään tietojärjestelmän kompleksisuus eri näkökulmista. (Mumford, 2000.)

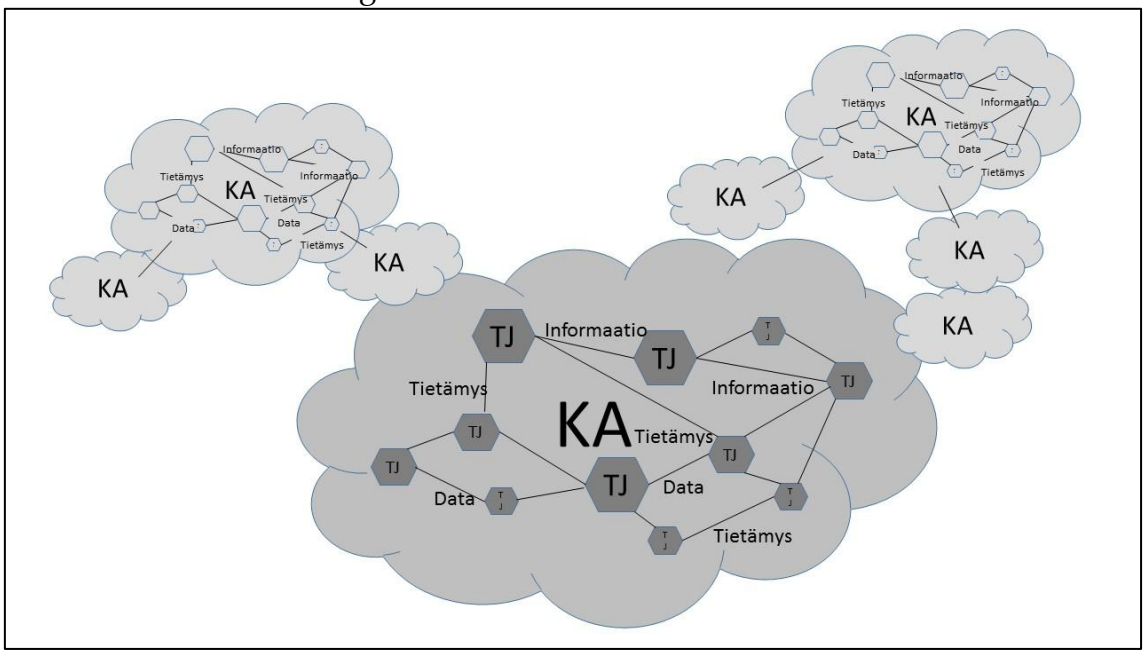
Tämän tutkimuksen kannalta on tärkeää ymmärtää tietojärjestelmien kompleksinen luonne ja se, ettei niitä voi tarkastella ainoastaan teknologisesta näkökulmasta. Sosioteknisen lähestymistavan periaatteiden mukaisesti tulee huomioida sekä sosiaalinen että tekninen näkökulma.

Kokonaisarkkitehtuurin käsite kokoaa yhteen organisaation liiketoiminta- ja johtamisprosessit sekä tietojärjestelmät. Kaisler, Armour ja Valivullah (2005) määrittävät kokonaisarkkitehtuurin (enterprise architeture) seuraavasti (tutkijan käännös):

> Kokonaisarkkitehtuurilla tarkoitetaan organisaation keskeisiä komponentteja ja tietojärjestelmiä sekä kuvausta siitä, miten näiden keskeisten komponenttien ja tietojärjestelmien yhteisenä tuloksena saavutetaan organisaation liiketoiminnalliset tavoitteet ja tuetaan organisaation liiketoimintatavoitteiden saavuttamista. Organisaation keskeisiä komponentteja ovat henkilöstö, liiketoimintaprosessit, teknologia, tieto, taloudelliset ja muut resurssit yms. (Kaisler, Armour & Valivullah, 2005, 1.)

Seppänen (2014) kuvaa kokonaisarkkitehtuuria liiketoiminta- ja tietojärjestelmästrategian, organisaation yleisen- ja tietojärjestelmäinfrastruktuurin sekä prosessien vuorovaikutukseksi (Seppänen, 2014). Kokonaisarkkitehtuuri näkökulma on näin ollen laajempi kuin yksittäisen tietojärjestelmän näkökulma vaikka molemmissa on mukana ihmisen ja johtamisen sekä teknologian viitekehys.

Tässä tutkimuksessa kokonaisarkkitehtuuri (KA) toimii viitekehyksenä, joka kokoaa kuvion 2 mukaisesti sisään organisaation eri tietojärjestelmät (TJ) sekä organisaation käsittelemän datan, informaation ja tietämyksen. Organisaation kokonaisarkkitehtuuri ei myöskään ole yksittäinen saareke, vaan se vuorovaikutuksessa muiden organisaatioiden kokonaisarkkitehtuurien kanssa.



Kuvio 2 Kokonaisarkkitehtuuri ja tietämys

Organisaation kokonaisarkkitehtuurissa käsitellään tietoa sen eri tasoilla. Kuvion 2 mallissa kukin pilvi kuvaa yksittäistä organisaatiota. Kullakin organisaatiolla on mallissa useita sen liiketoimintaa tukevia sosioteknisiä tietojärjestelmiä. Organisaation kokonaisarkkitehtuurissa sen eri sosioteknisissä tietojärjestelmissä käsitellään, tuotetaan ja prosessoidaan tietoa sen kaikissa muodoissa. Tietojärjestelmät käsittelevät dataa ja tuottavat informaatiota, jota organisaation henkilöstö tulkitsee tietämykseksi. Organisaatiot käyttävät tätä tietojärjestelmien prosessoimaa tietoa liiketoiminnassaan ja ollessaan vuorovaikutuksessa muiden organisaatioiden kanssa. Organisaatioiden välisessä vuorovaikutuksessa eri organisaatioiden kokonaisarkkitehtuurit muodostavat rajapintoja, joissa tietoa käsitellään, prosessoidaan ja vaihdetaan. Organisaatioiden kokonaisarkkitehtuurien muodostama verkko on jatkuvassa muutoksessa oleva kompleksinen rakenne.

2.2 Tieto-, tietoteknisen- ja kyberturvallisuuden käsitteistä

Luvussa esitellään tieto-, tietoteknisen- ja kyberturvallisuuden käsitteet sekä rajapinnat tässä tutkimuksessa. Tietoturvallisuuden osa-alueet luottamuksellisuus, saatavuus ja eheys ovat peruskäsitteitä joiden merkitys on

ymmärrettävä. Edellä mainitut termit käsitellään tässä luvussa, ja määritetään niiden asema osana tämän tutkimuksen viitekehystä.

Tietoturvallisuuden eri osa-alueista käytetään englanninkielessä termejä confidentiality, availability sekä integrity. Suomenkielessä vastaavat käännökset ovat luottamuksellisuus (confidentiality), saatavuus (availability) ja eheys (integrity). Suomenkieliset käännökset ovat ”availability” sanaa lukuun ottamatta kiistattomat. ”Availability” sanan käännöksenä käytetään tietojärjestelmätieteessä vakiintuneesti ”saatavuus” sanaa. VAHTI-ohjeissa ja turvallisuusalan keskusteluissa availability voidaan kääntää myös ”käytettävyydeksi”.

Tässä tutkimuksessa sovelletaan Valtionhallinnon tietoturvasanaston (2008) määritelmää tietoturvallisuudesta. Tutkija on korvannut alkuperäisen määritelmän ”käytettävyys” sanan ”saatavuudella”.

> Tietoturvallisuus: Järjestelyt, jolla pyritään varmistamaan tiedon saatavuus, eheys ja luottamuksellisuus. Saatavuus tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta. (VAHTI 8/2008, 109.)

Luottamuksellisuuden, eheyden ja saatavuuden tarkkoina määrityksinä käytetään Federal Information Processing Standards Publication 199:ssa (2004) esitettyjä määritelmiä (tutkijan käännös).

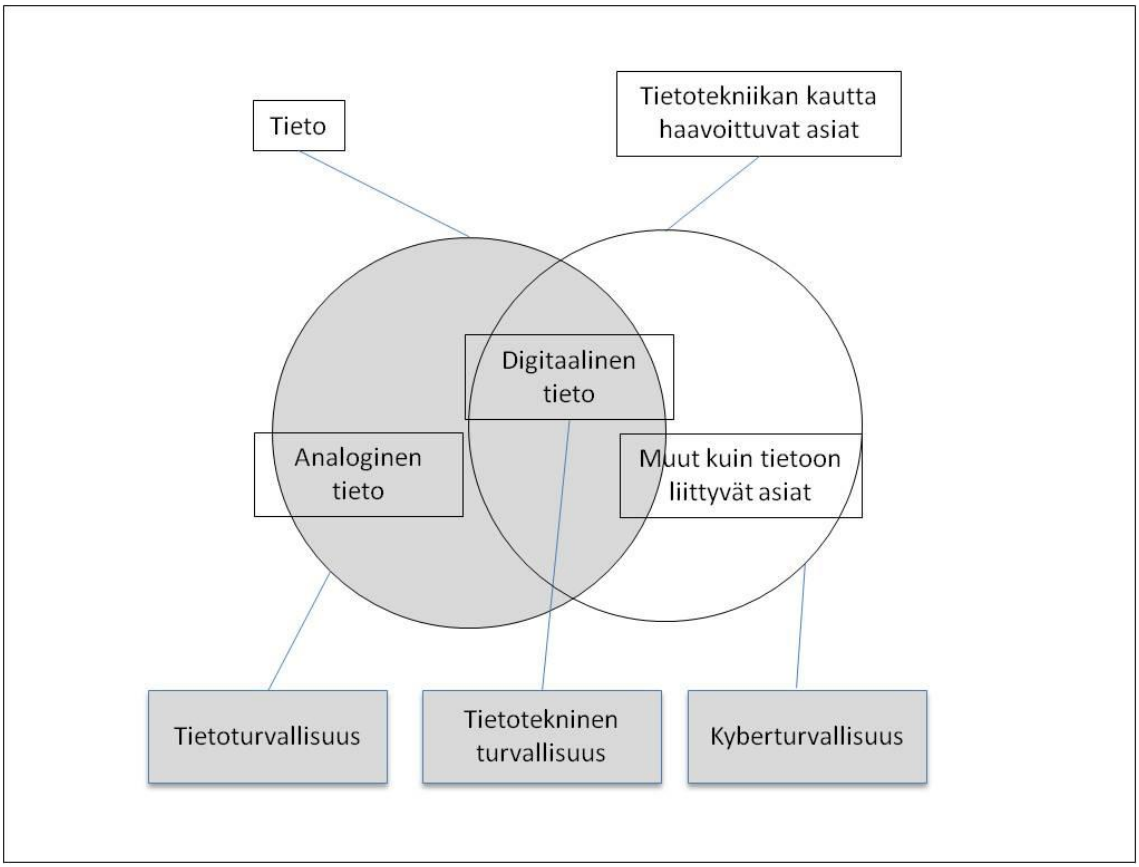
> Luottamuksellisuudella (confidentiality) tarkoitetaan tietojen suojaamista niiden luvattomalta käytöltä tai paljastumiselta. Tietojen suojaaminen kohdistuu myös henkilötietoihin ja yksityisyyden suojaan. Tiedon luottamuksellisuuden menetys tarkoittaa tietojen luvatonta käyttöä. (FIPS PUB 199, 2.)

> Eheydellä (integrity) tarkoitetaan tietojen suojaamista virheellisiltä muutoksilta tai tuhoamiselta sekä tietojen käsittelyketjun kiistämättömyyden ja autenttisuuden varmistamisesta. Tiedon eheyden menetys tarkoittaa oikeudettomien muutoksien tekoa tietoon tai sen rakenteisiin. (FIPS PUB 199, 2.)

> Saatavuudella (availability) tarkoitetaan luotettavaa sekä oikea-aikaista mahdollisuutta päästä käyttämään tarvittavaa tietoa. Tiedon saatavuuden menetys tarkoittaa tietoon tai tietojärjestelmään pääsyn estymistä. (FIPS PUB 199, 2.)

Tieto-, tietojärjestelmä- ja kyberturvallisuuden käsitteet edellyttävät täsmällistä määrittelyä. Julkisessa keskustelussa ja tiedotusvälineissä käsitteitä käytetään yleisesti ristiriitaisesti. Norjalainen Center for Cyber and Information Security (CCIS) esittää artikkelissaan Cyber security versus information security kuvion 3 mukaisen määritelmän ja rajauksen (CCIS, 2014).

CCIS:n artikkelin mallissa kyberturvallisuus liittyy teknologiaan ja voi käsittää muitakin osa-alueita kuin tietoa. Kyseessä voi olla esimerkiksi teknologiaperusteinen haavoittuvuus, jolla on vaikutusta organisaation toimintaan. Tietotekninen turvallisuus käsittää teknologian ja digitaalisen tiedon. Esimerkkinä voi olla organisaation sisäverkossa liikkuva data.



Kuvio 3 Tietoturvallisuuden ja kyberturvallisuuden rajapinnat (CCIS, 2014)

Tietoturvallisuus käsittää artikkelin mukaan myös analogisen tiedon, voidaan puhua esimerkiksi organisaatioon henkilöstölle vuosien saatossa muodostuneesta kokemuksesta ja suullisesti vaihdettavasta tiedosta ja niistä menetelmistä miten tällaista tietoa suojataan.

Tutkimuksen näkökulmasta artikkelin malli kuvaa organisaation sisältä katsottuna tieto-, tietoteknisen- ja kyberturvallisuuden rajapintaa. Organisaation johtamisen ja riskienhallinnan näkökulmasta tieto-, tietoteknisen- ja kyberturvallisuuden rajapinnat kietoutuvat toisiinsa. Organisaation toimintaan kohdistuvien riskienarviointi edellyttää tieto-, tietoteknisten sekä kyberturvallisuuden uhkien arviointia. Organisaation tehtävä ja koko vaikuttavat siihen miten eri osa-alueet eriytyvät organisaation johtamisen näkökulmasta. Riskienhallintaa käsittelevässä alaluvussa (3.1.3) pohditaan sitä, miten edellä mainittu kokonaisuus kytkeytyy riskienhallinnan kokonaisuuteen.

2.3 Organisaation tietämyksen hallinta

Tämän luvun tavoitteena on käsitellä tarkemmin tietämystä. Luvussa tarkastellaan miten tietämys rakentuu. Tietojärjestelmien kehittyessä organisaatioiden tietämyksen hallinta on nykypäivänä entistä tärkeämpää. Organisaatioissa käsi-

tellään erityyppistä tietämystä, osa tietämyksestä on täsmällistä dokumentoitua, osa hiljaista dokumentoimatonta. Tarkastelemalla tietämyksen rakennetta, sen hallintaa ja johtamista voidaan arvioida syvällisemmin kokonaisarkkitehtuurissa käsiteltävän tiedon merkitystä ja luonnetta.

2.3.1 Tietämyksen lajit

Organisaatioilla on erityyppistä tietämystä. Virallinen dokumentoitu ja täsmällinen tietämys sisältyy yrityksen arkistoihin, nettisivuille ja muille virallisesti ylläpidetyille foorumeille. Tämän lisäksi jokaisella organisaatiolla on yksilöiden ja organisaatio kulttuurin kokemusten perusteella muotoutunutta hiljaista tietoa. Edellä mainitun jaon perusteella puhutaan täsmällisestä tietämyksestä (explicit knowledge) ja hiljaisesta tiedosta (tacit knowledge). Hiljaisen ja täsmällisen tietämyksen jako ei ole yksiselitteinen eikä tietämystä voida jakaa jompaankumpaan ryhmään, vaan se virtaa näiden ryhmien välillä. (Sheden, Scheepers, Smith & Ahmad, 2011.)

Täsmällisen tietämyksen hallinta perustuu organisaation virallisiin prosesseihin ja hallintajärjestelmiin. Hiljaisen tiedon hallinta on organisaatiolle vaikeampaa. Miten hallita ja kontrolloida tietämystä, jonka olemassa olosta ei ole varmuutta. Internetin ja sosiaalisen median sekä erilaisten yhteistyövälineiden (collaboratio) käyttö aiheuttaa organisaatiolle tässä suhteessa kasvavan haasteen. Yksittäisillä ihmisillä on käytössään viestintä- ja vuorovaikutuskanavat, joilla tietoa voidaan jakaa nopeasti jopa maailman laajuisesti. (Ilvonen, Jussila, Kärkkäinen & Päivärinta, 2015.)

Organisaation tietämyksen hallinta ei tietämyksen luonteesta johtuen ole myöskään pelkästään teknologisesti hallittavissa. Teknologialla ei voida hallita ihmisten ”mieliin” jäsentynyttä hiljaista tietoa. Täsmällisenkin tiedon hallinta yhä kompleksisemmissa tietojärjestelmissä on vaikeaa. Organisaation tietämyksen hallinta edellyttää kokonaisvaltaista organisaation ihmisten ja teknologian tarkastelua. (Padyab, Päivärinta & Harnesk, 2014.)

Freeze ja Kulkarni (2005) käsittelevät organisaation tietämyksen rakentumista eri näkökulmista. Tutkimuksessaan he tunnistavat ihmis- ja teknologia näkökulman lisäksi tietämyksen elinkaaren. He pohtivat tutkimuksessaan täsmällisen ja hiljaisen tiedon elinkaarien pituuksien eroja. Tutkimuksen mukaan ihmisten ja organisaation muistissa oleva hiljainen tieto säilyy pitempään kuin virallinen täsmällinen tieto. Tämä näkökulma korostaa hiljaisen tiedon hallinnan haasteellisuutta. (Freeze & Kulkarni, 2005.)

2.3.2 Tietämyksen hallinta ja johtaminen

Luvun tavoitteena on avata tietämyksen hallintaan ja johtamiseen liittyvää kirjallisuutta. Luvussa tarkastellaan miten organisaatiot tunnistavat ja hallinnoivat tietämystään. Miten organisaatiot tunnistavat tietämyksen eri prosessien avulla sekä millaisia hyviä käytänteitä organisaatiot ovat kehittäneet.

Gold, Malhotra ja Segars (2001) kuvaavat organisaation tietämyksen hallintaprosessien jakautuvan neljään osaan. Ensimmäinen on tietämyksen hankinta, sisältäen ne toimenpiteet joiden kautta organisaatio hankkii ja jakaa tietämystä organisaation sisällä ja organisaatioiden välillä. Toinen osa on uuden tietämyksen jakaminen käyttöön. Miten uutta tietämystä tulee prosessoida, tallentaa tai jakaa, jotta organisaatio voi sitä hyödyntää. Kolmas osa on tietämyksen soveltaminen käytäntöön todellisissa työtehtävissä. Gold ym. (2001) arvioivat, että tämä näkökulma monesti ohitetaan. He esittävät kritiikkiä sellaista näkemystä kohtaan, jossa uusi tietämys vapaasti leviää organisaation käyttöön, ilman erityisiä toimenpiteitä. Neljäs ja viimeinen osa on tietämyksen suojaamisen näkökulma. Organisaatioiden tulee suojata kriittinen tietämys muutoinkin kuin lainsäädäntöön perustuvin liiketoimintapatenttien kautta. Gold:n ym. (2001) näkemyksen mukaan kaksi jälkimmäistä näkökulmaa, tietämyksen käytäntöön soveltaminen ja tietämyksen suojaaminen, ovat herättäneet vähiten mielenkiintoa. Niistä löytyy heidän mukaan myös vähiten akateemista kirjallisuutta. (Gold, Malhotra & Segars, 2001.)

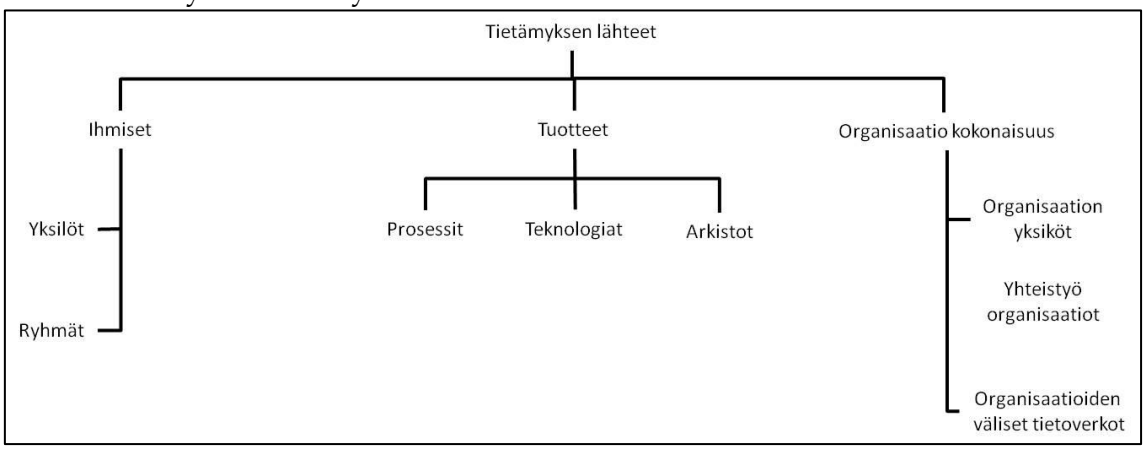
Ahmad, Bosua ja Scheepers (2014) käsittelevät tietämyksen suojaamista kolmesta näkökulmasta. Ensimmäinen on strategisen johtamisen näkökulma, jonka mukaan organisaation tulee suojata tietämystä kuten yrityksen muitakin kriittisiä menestystekijöitä. Toinen on tietojohtamisen näkökulma, jossa tietämys toimii kilpailutekijänä. Kolmas tietoturvallisuuden näkökulma tarkastelee tietämystä enemmän staattisena datana, joka voidaan turvata erilaisin auditointi- ja dokumentointimenetelmin. Tietoturvallisuusnäkökulma tunnistaa liiketoimintavaatimukset, mutta tietoturvallisuutta ei pidetä kilpailutekijänä. Tietointensiivisten organisaatioiden haasteena he pitävät sitä, miten tietoturvallisuuden eri elementit, luottamuksellisuus, saatavuus ja eheys, otetaan tasapainoisesti huomioon. Tutkimuksen perusteella strategisen ja operatiivisen tason tietämyksen hallinnan osaaminen on puutteellista. Strategisella tasolla he määrittävät tavoitteeksi tunnistaa suojattava tieto. Suojausmenetelmät ja tiedon käsittely prosessit tulee myös tunnistaa, jotta voidaan määrittää tiedon suojaamisesta vastaavat ”portinvartijat”. (Ahmad, Bosua & Scheepers, 2014.)

Manhart ja Thalman (2013) pitävät tietämyksen hallinnan tavoitteena tuottaa päätöksentekijöille läpinäkyvät perusteet tehdä tietoturvaan kohdistuvia päätöksiä. (Manhart & Thalman, 2013.)

Barney (1999) mukaan resurssit, jotka kehittävät organisaation liiketoiminnan tehokkuutta ja vaikuttavuutta, ovat sille arvokkaita resursseja (Barney, 1999). Aljafari ja Sarnikar (2009) korostavat organisaation tiedon tunnistamisen merkitystä liiketoiminta- ja arvoketjujen perusteella. He esittävät kuvion 4 mukaisen Beccerra-Fernandez ym. (2004) näkemykseen perustuvan jäsennyksen tietämyksen lähteistä. Tietämyksen organisaatioresursseina he tunnistavat ihmiset, tuotteet ja tuotannon sekä sisäiset ja ulkoiset organisaatiot. (Aljafari & Sarnikar, 2009.)

Iivari, Hirschheim ja Klein (2004) esittävät artikkelissaan tietojärjestelmien viisi tietämyksen lähdettä. Ensimmäinen on tietojärjestelmiin, verkkoihin ja so-

velluksiin liittyvää teknologista tietämystä. Toinen on tietojärjestelmien kehittämiseen liittyvää tietämystä.



Kuvio 4 Tietämyksen lähteet (Aljafari & Sarnikar, 2009, 5)

Kolmas on tietämystä siitä mihin toimintaympäristöön tietojärjestelmää suunnitellaan. Voidaan puhua kohdeympäristön tuntemisesta. Neljäs on tietämys tietojärjestelmää käyttävän organisaation sosiaalisesta ja taloudellista toimintaympäristöstä. Viides tietojärjestelmien tietämyksen lähde on yleinen tietojärjestelmien sovellustietämys. Miten sovellukset toimivat, miten niitä käytetään, millainen rakenne niillä on. (Iivari, Hirschheim & Klein, 2004.)

Ahmad ym. (2014) käyttävät organisaation maineelle ja liiketoiminnalle merkittävästä tietämyksestä termiä sensitiivinen tietämys. Sensitiivistä tietämystä tulisi ohjata ja johtaa heidän mukaan kuin mitä tahansa liiketoiminta-resurssia, sitä tulisi tarkastella myös kokonaisvaltaisesti, ei ainoastaan teknologisesta näkökulmasta. Sensitiivisellä tietämyksellä on myös oltava heidän mukaan omistaja, joka ohjaa käytännössä sensitiiviseen tietämykseen liittyvää organisaation prosessia tai muuten on keskeisessä roolissa suhteessa sensitiiviseen tietämykseen. Sensitiivisen tietämyksen omistajan ja organisaation tulee kommunikoida yhteisten tavoitteisen saavuttamiseksi. Esimerkkinä käytännön organisaatioiden tietämyksen hallinnan ongelmista he kuitenkin nostavat esille sen, että johto yleisesti ulkoistaa tietämyksen hallinnan johtamisen tiedon omistajille. Toimivien johtamismenetelmien puuttuessa asiaa ei osata käsitellä strategisella tasalla. Ratkaisuvalta ohjataan ”tiedon omistajille”, joilla taas ei välttämättä ole organisaation kokonaisliiketoimintaan riittävää näkökulmaa tai osaamista. (Ahmad, Bosua & Scheepers, 2014.)

Trkman ja Desouza (2012) nostavat esille samat edellä kuvatut tietämyksen johtamisen haasteet organisaatioissa. He korostavat tietämyksen merkitystä yhtenä organisaation liiketoiminnan perusedellytyksenä, sekä tietämyksen johtamisen merkitystä kustannustehokkuuden näkökulmasta. Heidän näkemys on, etteivät perinteiset vaikuttavuuden ja todennäköisyyden arviointiin perustuvat riskienarviointimenetelmät sovellu tietämyksen hallintaan ja johtamiseen. Haasteena on miten johto ja johtajat kykenevät tunnistamaan organisaation kannalta kriittisen tietämyksen. Mitä yleensä tarkoitetaan tietämysriskillä? (Trkman & Desouza, 2012.)

Organisaation tiedon tunnistamisen merkitystä, tiedon priorisoinnin tärkeyttä sekä erityyppisten luokittelumenetelmien hyödyntämistä korostetaan monissa artikkeleissa. Desouza ja Vanapalli (2005) pitävät merkittävänä tietämystyyppien tunnistamista ja priorisointia organisaation tiedon suojaamisen toimenpiteenä. He myös yhdistävät tietämyksen ja teknologian, jossa tietämystä käsitellään. Käytettävän teknologian tulee vastata tietämyksen tietoturvallisuusvaatimuksia. (Desouza & Vanapalli, 2005.) O'Donoghue ja Croasdell (2009) pitävät myös tietämyksen tunnistamista merkityksellisenä ja he jaottelevat hiljaisen tiedon inhimilliseen, rakenteelliseen ja innovaatioita käsittelevään tietämykseen. Jaottelu on karkeampi kuin Aljafari ja Sarnikar:n esittämä, mutta perustaltaan yhtenevä. (O'Donoghue & Croasdell, 2009.)

Järvenpää ja Majchrzak (2008) korostavat organisaatioiden välisen tiedon vaihdon riskiä, henkilöstö voi tietämättään luovuttaa organisaation sensitiivistä tietoa. Organisaatioiden tulee tunnistaa sensitiivinen tieto, ja koko organisaation henkilöstön tulee tietää, miten sensitiivistä tietoa käsitellään. Tiedon luokittelu eri ryhmiin ja tyyppeihin auttaa organisaatiota muodostamaan käsityksen siitä, mitä tietoa se omistaa. Organisaatio yhteisen käsityksen myötä on mahdollista muodostaa henkilöstölle oma tietoisuus siitä mitä tietoa he käsittelevät sekä miten ja missä he voivat sitä käsitellä. Tämä näkökulma korostaa tiedon omistajan ja yksilön vastuuta, jota organisaatio tukee. (Järvenpää & Majchrzak, 2008.)

2.3.3 Yhteenveto

Tietämyksen hallinnasta itsessään on runsaasti akateemista kirjallisuutta. Perinteisessä näkökulmassa kyseinen kirjallisuus tarkastelee organisaation toimintaa tukevan tietämyksen saatavuutta, läpinäkyvyyttä ja tunnistamista. Miten tietämys saadaan organisaation käyttöön, miten varmistetaan hiljaisen tiedon periytyminen organisaatiossa tuleville työntekijöille tai miten parhaat käytänteet jalkautetaan organisaatiossa. Sosiaalisen median ja erilaisten yhteistyö (collaboratio) työkalujen laajamittainen käyttöönotto organisaatioissa on nostanut esille tarpeen suojata ja rajoittaa tietämyksen jakamista. Tästä suojaamisen näkökulmasta kirjoitettua akateemista kirjallisuutta on rajallisesti. Olemassa olevan kirjallisuuden perusteella tietämyksen tunnistaminen ja suojaaminen on organisaatioille haasteellista. Tietämyksen hallintaa pidetään kuitenkin olemassa olevan kirjallisuuden perusteella merkittävänä organisaatioiden liiketoiminnan kannalta ja sen johtamista pidetään yhtä tärkeänä kuin mitä tahansa muuta liiketoimintaresurssia. Internetin, sosiaalisen median sekä erilaisten yhteistyövälineiden (collaboratio) kehittyminen lisää asian merkittävyyttä. Tiedon jakaminen laajasti organisaation sisällä ja ulkopuolella on erittäin helppoa ja nopeaa. Tämä korostaa yksittäisen henkilön vastuuta, ymmärrystä ja osaamista.

Tietämyksenhallinnan ja -johtamisen tulee ottaa huomioon tietojärjestelmien kokonaisvaltaisuus. Tietämyksen hallinnan tai -johtamisen haasteita ei voi ratkaista vain inhimillisestä tai teknologisesta näkökulmasta, tarvitaan molempia näkökulmia. Tietämystä tulee myös johtaa kuten mitä tahansa liiketoimin-

nan osa-aluetta. Tavoitteena tulee olla kustannustehokas ja läpinäkyvä tietämyksenhallinnan johtaminen. Keskeinen sensitiivinen tietämys tulee tunnistaa ja luokitella. Sensitiivistä tietämystä käsitellessä tulee arvioida, millaisessa tietojärjestelmässä sitä voidaan käsitellä. Tietämyksen sensitiivisyys ja tietojärjestelmän teknisten sekä toiminnallisten ratkaisujen välille muodostuu näin sidos.

Kirjallisuuden perusteella perusta organisaation tietämyksen hallintaan on tietämyksen tunnistaminen ja erityyppisten luokittelutyökalujen käyttö. Organisaation tietämyksen hallinnan on oltava läpinäkyvää kaikille organisaatioiden henkilöille. Organisaation pitää tunnistaa erityisesti sen liiketoiminnan kannalta kriittinen tietämys ja määrittää kyseiselle kriittiselle tietämykselle omistaja. Tunnistettua tietämystä voidaan hallita ja johtaa.

Organisaatioiden arvo- ja prosessiketjujen tunnistaminen sekä niiden omistajien määrittäminen mahdollistaa näissä ketjuissa liikkuvan tietämyksen omistajien määrittämisen. Tietämyksen omistajien tehtävänä on ohjata ja koordinoida omistamansa tietämyksen hallintaa. Tietämyksen omistajan rooli arvo- ja prosessiketjuissa kytkee liiketoiminnan ja tietämyksen johtamisen yhteen. Näin voidaan kehittää organisaation koko johdon vaikuttavuutta ja mahdollisuutta johtaa organisaation tietämystä.

Tietoturvallisuuden eri osa-alueiden, luottamuksellisuuden, saatavuuden, ja eheyden implementointi tietointensiivisten organisaatioiden osalta on haasteellista. Kaikkien kolmen osa-alueen tasapuolinen huomioiminen edellyttää pohdintaa.

3 Riskienhallintamenetelmät osana organisaation johtamisprosessia

Tutkimuksen tavoitteena on kehittää organisaation tietämyksen johtamista tukeva menetelmä. Tästä syystä tässä luvussa kiinnitetään huomio johtamisen näkökulmaan. Organisaation johtamisen näkökulma tutkimuksessa perustuu riskienhallintaan. Luvussa määritetään riskienhallinnan, tieto- ja kyberturvallisuuden suhteet tässä tutkimuksessa. Riskienhallinnan näkökulmaa täydennetään viranomaisten riskienhallintaa ohjaavilla normeilla. Viranomaisten normien tarkastelun tavoitteena on löytää tutkimuksen kehityskohteena olevaa menetelmää tukevia käytänteitä. Luvun päätteeksi esitellään tutkimuksen viitekehys. Viitekehys kokoaa yhteen toisen ja kolmannen luvun tulokset. Viitekehyksessä esitellään miten kokonaisarkkitehtuuri, tietojärjestelmät, tieto sekä riskienhallinnan johtaminen jäsentyvät tutkimuksen viitekehyksessä yhteen.

3.1 Riskienhallintamenetelmät

Luvussa esitellään tutkimuksen lähteenä käytetty Yhdysvaltain kansallisen teknologia ja standardointi järjestön (National Institute of Standards and Technology, NIST) riskienhallinnan johtamismalli. Luvussa esitellään myös riskienhallintamenetelmien perusteet ja riskienhallintamenetelmien suhde organisaation johtamiseen sekä tieto-, tietotekniseen- ja kyberturvallisuuteen.

3.1.1 NIST riskienhallinnan johtamismalli

Peruste NIST riskienhallinnan johtamismallin käyttöön liittyy tiedon luokittelun näkökulmaan. Tutkimuksen kehityskohteena oleva menetelmä ja NIST:n riskienhallinnan johtamismalli perustuvat molemmat tiedon luokitteluun. NIST:n ohjeissa esitetään kokonaisvaltainen ja hyvin yksityiskohtainen riskienhallinnan johtamisprosessi, joka käynnistyy tietotyyppien tunnistamisella ja luokittelulla. Luokittelussa NIST:n prosessi huomioi tietoturvallisuuden osa-

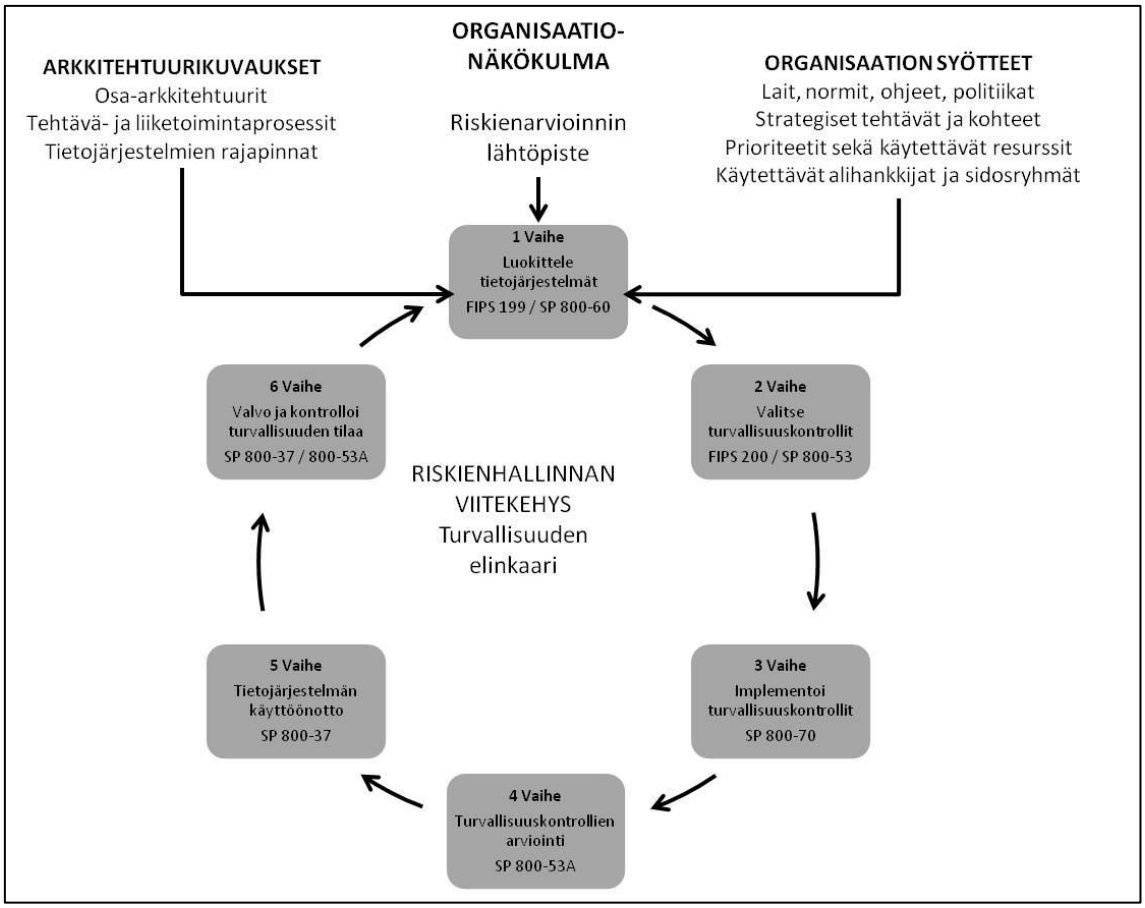
alueet: luottamuksellisuuden, saatavuuden ja eheyden. Periaate on sama kuin tutkimuksen kohteena olevassa menetelmässä.

Yhdysvalloissa vuonna 2002 voimaanastunut *"The E-Government Act of 2002"* perustui Yhdysvalloissa tunnistettuun tietoturvallisuuden merkitykselliseen rooliin liiketoiminnan ja kansallisen turvallisuuden näkökulmasta. Lain edellyttämien kansallisten ohjeiden, standardien ja turvallisuuden minivaatimusten määrittäminen määrättiin Yhdysvaltojen kansallisen teknologia ja standardointi järjestön, NIST:n tehtäväksi. (FIPS Publication 199, 2004.)

NIST-ohjeistuksen perusajatuksena on kuvion 5 mukainen Riskienhallinnan johtamisen kuusivaiheinen prosessi. Prosessin lähtösyötteenä ovat arkkitehtuurikuvaukset sekä organisaatioon kohdistuvat vaatimukset. Arkkitehtuurikuvauksilla tarkoitetaan kohteena olevan tietojärjestelmän arkkitehtuurin ja siihen liittyvien liiketoimintaprosessien sekä niiden rajapintojen määrittelyä. Organisaation vaatimuksia ovat ohjaavat lait, normit, politiikat, liiketoiminnan tavoitteet ja prioriteetit sekä käytettävissä olevat resurssit. (NIST Special Publication 800–37, 2010.)

Ensimmäinen vaihe prosessissa on informaation ja tietojärjestelmien luokittelu. Luokittelun lähtökohtana on tietojärjestelmän käytön myötä rakentuvan ja itse tietojärjestelmän systeemi informaation tietotyyppien (Information Type) tunnistaminen. Tietotyypit voivat olla sähköisessä tai ei-sähköisessä muodossa. Tietotyyppien kautta arvioidaan informaatioon tai tietojärjestelmään kohdistuvat riskit ja tietoturvallisuuden vaatimukset. Riskien- ja tietoturvallisuuden vaatimusten arviointi perustuu tietotyyppien luokitteluun. Tietotyypit luokitellaan tietoturvallisuuden osa-alueiden (luottamuksellisuus, saatavuus ja eheys) mukaisesti. Kukin tietoturvallisuuden osa-alue arvioidaan asteikolla matala (low), normaali (moderate) tai korkea (high). (NIST Special Publication 800–60, 2008.)

Toinen vaihe alkaa alustavien turvallisuuskontrollien valinnalla. Turvallisuuskontrollien valintaan liittyy turvallisuuskontrollien suhteuttaminen kohteen erityispiirteisiin, arvioituihin riskeihin, kustannusvaikutusten arviointiin sekä liiketoiminnan vaatimuksiin. Turvallisuuskontrollien valintaa ohjaa yksityiskohtainen ja erittäin laaja ohje. Tätä turvallisuuskontrollien suhteellisuusarviointia kutsutaan turvallisuusvaatimusten räätälöinniksi. Kolmannessa vaiheessa valitut turvallisuuskontrollit implementoidaan osaksi tietojärjestelmää. Implementointi edellyttää turvallisuuskontrollien dokumentointia ja suunnitelmaa, miten ne liitetään osaksi tietojärjestelmää. Neljännen vaiheen tavoitteena on varmistaa turvallisuusvaatimusten toteutuminen soveltuvien menetelmien ja prosessien avulla: vaikuttavatko turvallisuuskäytännöt suunnitellulla tavalla, onko niiden implementointi onnistunut suunnitellusti. Viidennessä vaiheessa tietojärjestelmä hyväksytään käyttöön valtuutetun viranomaisen toimesta. Kuudennen, viimeisen vaiheen tavoitteena on tietojärjestelmän ja sovittujen kontrollien valvonta. Kuviossa 5 esitetään prosessi kokonaisuudessaan. Kunkin vaiheen yhteydessä on viittaus kyseistä vaihetta koskevaan NIST:n ohjeistukseen. (NIST Special Publication 800–60, 2008.)



Kuvio 5 Riskienhallintaprosessi NIST mukaan (NIST SP 800–37, 2010, 8)

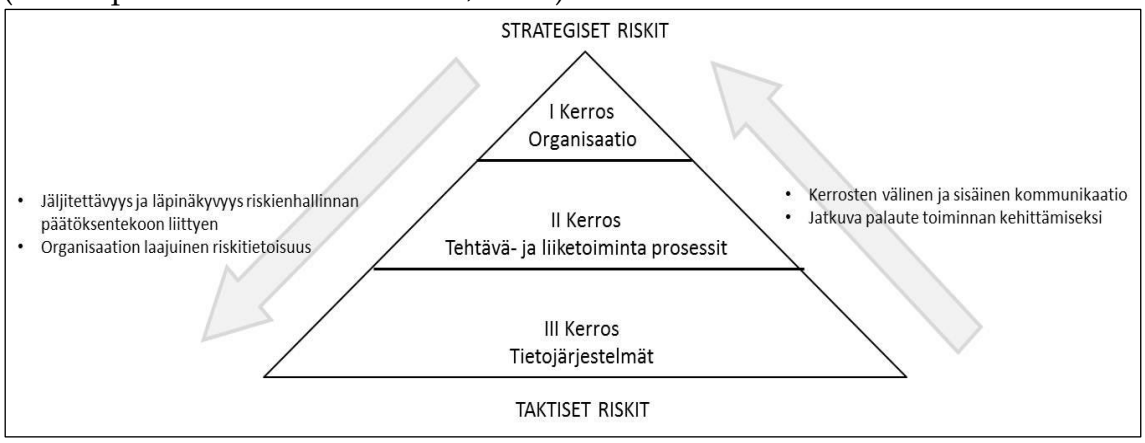
Edellä esitetty NIST:n prosessin tavoitteena on tietojärjestelmien sekä niiden sisältämän tiedon luokittelu. Luokittelun avulla arvioidaan tietojärjestelmiin kohdistuvat riskit. Riskienarviointiin perustuen turvallisuuden minimivaatimukset kyetään määrittämään kohteena olevalle tietojärjestelmälle. Riskienarviointiin pohjautuvaa johtamista pidetään parhaana menetelmänä riittävän tietoturvallisuuden saavuttamiseksi. (Hulit & Vaughn, 2009.)

Prosessin lähtösyötteenä mainittu liiketoimintatavoitteiden tunnistaminen ja priorisointi sekä käytettävien resurssien arviointi yhdistettynä vaiheen kaksi turvallisuuskontrollien räätälöintiin nostavat esille inhimillisen harkinnan ja pohdinnan merkityksen. Turvallisuusvaatimusten valinta ei mallin mukaan ole mekaanisesti suoritettua absoluuttisen turvallisuuden tavoittelua, vaan turvallisuusvaatimuksia ja -kontrolleja valitessa tulee huomioida toimintaympäristön riskit, vaatimukset sekä resurssit. Voidaan puhua ”riittävän” turvallisuustason tunnistamisesta.

Allen pohtii 2009 julkaistussa artikkelissaan "How Much Security Is Enough" kuinka paljon turvallisuutta on riittävästi. Artikkelissa pohditaan riittävän ja hyväksyttävän turvallisuuden tason määrittämistä sekä sitä, miten varmistetaan se, että johtajat ymmärtävät riskienhallintapäätösten jälkeen jäävän jäännösriskin merkityksen. Artikkelissaan Allen korostaa sitä, ettei absoluuttista turvallisuutta voida saavuttaa. Organisaation koko, liiketoiminnan

tavoitteet ja tietojärjestelmien kompleksisuus tulee ottaa suunnittelussa huomioon. Organisaation kriittiset suojattavat kohteet tulee tunnistaa sekä pohtia miten ja millä resursseilla suojattavia arvoja on järkevää suojata. Organisaation tulee myös päättää miten jäljelle jäävät riskit otetaan huomioon. Allen määrittää riittävän turvallisuuden seuraavasti (tutkijan käännös). "Olosuhteet, joissa organisaation kriittisten arvojen ja liiketoimintastrategian turvallisuus- ja jatkuvuusstrategiat ovat oikeassa suhteessa organisaation riskin sietokykyyn." Riittävän turvallisuuden arviointi on Allenin mukaan oltava osa organisaation päivittäistä päätöksentekoprosessia. (Allen, 2009.)

NIST:n riskienhallinnan johtamismalli tukee myös organisaation kokonaisarkkitehtuurin johtamista. NIST ohjeistus jakaa riskienarvioinnin johtamisprosessin organisaatio-, liiketoiminta- ja tietojärjestelmätasoihin kuvion 6 mukaan. Ylimmällä kerroksella on vastuu organisaation riskienhallinnasta sekä organisaation johtamis- ja hallintajärjestelmän kehittämisestä. Keskimmäinen kerros vastaa liiketoimintaprosessien johtamisesta sekä niihin liittyvästä informaatiosta. Alimmalla tietojärjestelmätasolla on vastuulla toimintaympäristöt. Alempien kerrosten toiminta perustuu ylempien kerroksien ohjaukseen sekä molempiin suuntiin kulkevaan riskienarviointi informaatioon. Mallin tavoitteena on monikerroksinen organisaation laajuinen riskienhallinta ja -johtaminen. Mallilla on tiukka kytkös organisaation kokonaisarkkitehtuuriin. Malli korostaa riskienhallinnan ja liiketoimintatiedon liikkumisen tarvetta eri tasojen välillä. (NIST Special Publication 800–30, 2012.)



Kuvio 6 Riskienhallinnan organisaatio kerrokset (NIST SP 800–30, 2012, 17)

Organisaation kokonaisarkkitehtuurissa eri tietojärjestelmien luokittelut ja niiden määritetyt rajapinnat tukevat osaltaan kokonaisarkkitehtuurin riskienhallinnan johtamista sekä tietojärjestelmien elinkaaren hallintaa. Turvallisuusvaatimukset voidaan kohdentaa kunkin tietojärjestelmän luokitteluvaatimusten perusteella ja eri tietojärjestelmien rajapintoja voidaan tarkastella siihen liittyvien tietojärjestelmien määritettyjen luokitteluiden perusteella. (NIST Special Publication 800-100, 2006.)

3.1.2 Riskienhallinnan menetelmät ja riskienhallinnan johtaminen

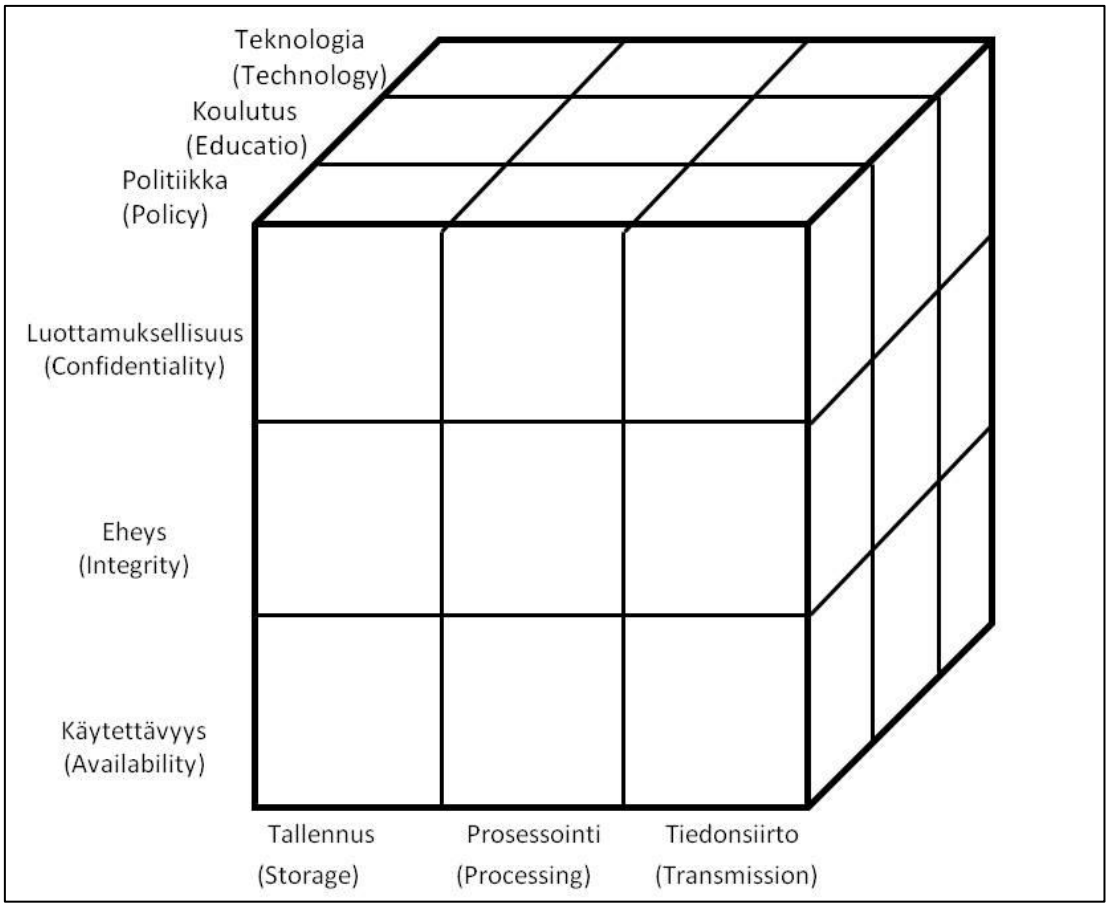
Luvussa avataan kirjallisuuteen perustuen riskienhallinnan menetelmien ja -johtamisen käsitteet. Riskienhallinnalla tarkoitetaan yleisesti ottaen menetelmiä, joiden avulla voidaan arvioida ennalta organisaatioon, toimintaan tai prosesseihin kohdistuvia uhkia. Ennakoivan suunnittelun tavoitteena on tuottaa informaatiota, jonka perusteella voidaan varautua, ennalta ehkäistä tai torjua arvioituja sekä tunnistettuja riskejä. Erilaisia riskienhallintamenetelmiä on lukemattomia. Niiden perusrakenne on kuitenkin samantyyppinen. Lähtötilanteessa määritetään ja rajataan riskienhallinnan kohde, mihin tietojärjestelmään tai organisaation osa-alueeseen riskienarviointi kohdistetaan. Seuraavassa vaiheessa tunnistetaan millaisia uhkia kohteena olevaan tietojärjestelmään tai organisaation kohdearkkitehtuuriin kohdistuu. Päätösvaiheessa arvioidaan tunnistettujen uhkien ja haavoittuvuuksien vaikuttavuus ja todennäköisyys. Itse arviointi suoritetaan yleensä valitun riskienarviointityökalun hallitsevan asiantuntijan johdolla ja arviointiin osallistuu arviointikohteen hyvin tuntevia asiantuntijoita. (Shedden, Scheepers, Smith & Ahmad, 2011.)

Riskienarviointimenetelmien etuina pidetään myös niiden antamaa tukea johdon ja ICT-alan ammattilaisten väliseen viestintään (Baskerville, 1991). Tämä näkökulma on myös merkittävä tämän tutkimuksen kohteena olevan menetelmän tavoitteiden kannalta.

Riskienhallinnan johtamisprosesseilla tai -menetelmillä tarkoitetaan yleisemmin organisaation liiketoiminnan- tai osaprosessien johtamiseen liitettyjä riskienhallinnan ja turvallisuuden johtamisprosesseja ja -menetelmiä. Tällöin riskienhallinnalla on laaja-alaisempi näkökulma.

Jennex ja Zyngier (2007) esittävät raportissaan kuvion 7 mukaisen esimerkin jossa organisaation resurssit, tietojärjestelmien toimintaprosessit ja tietoturvallisuuden osa-alueet on kytketty yhteen. Mallin mukaan tietoturvallisuuden johtamiseen kuuluvat tietoturvallisuuden luottamuksellisuuden, saatavuuden ja eheyden lisäksi tietojärjestelmien prosessit, joita ovat tallennus, prosessointi ja tiedonsiirto. Kolmas kokonaisuus muodostuu organisaation resursseista, joita ovat käytettävät teknologiat, olemassa olevat politiikat sekä henkilöstön osaaminen. Malli perustuu The National Security Telecommunications and Information System Security Committeen esitykseen vuodelta 1994. Malli on kattava ja sitä voidaan soveltaa erilaisiin organisaatioihin ja teknologioihin. Malliin sisältyy mahdollisuus erilaisten riskienhallintamenetelmien ja johtamisprosessien käyttämiseen. (Jennex & Zyngier, 2007.)

Pohjimmiltaan malli kuvaa tietämyksen hallinnan ja tietoturvallisuuden johtamisen kokonaisviitekehyksen. Kuution eri ruudut yhdistävät hallinnon, tietoturvallisuuden sekä teknologian eri vaatimukset ja niiden kombinaatiot. Tietämyksenhallinta ja tietoturvallisuus muodostavat mallissa ehjän hallittavan ja johdettavan kokonaisuuden. (Jennex & Zyngier, 2007.)

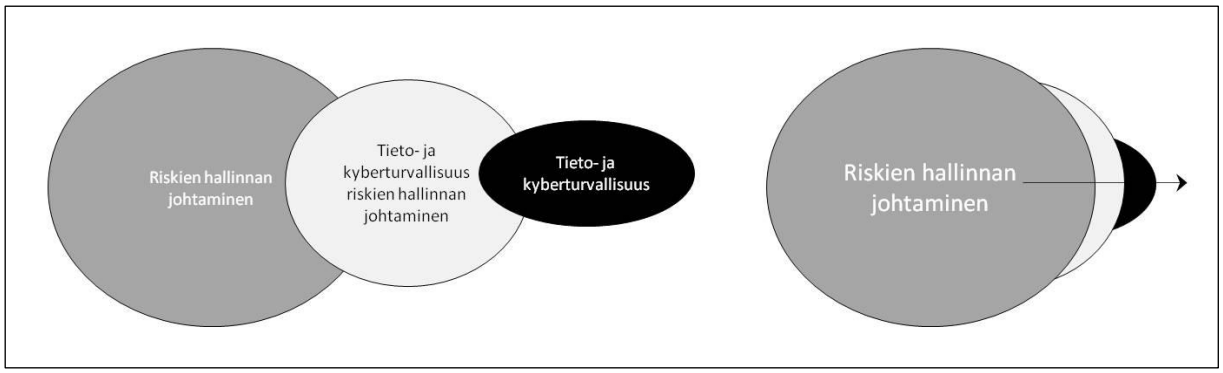


Kuvio 7 Turvallisuusmalli (Jennex & Zyngier, 2007, 498)

3.1.3 Riskienhallinnan, tieto- ja kyberturvallisuuden käsitteiden suhteesta

Luvun tavoitteena on esittää miten tieto- ja kyberturvallisuuden käsitteet ja riskienhallinnan johtaminen liittyvät tämän tutkimuksen viitekehyksessä yhteen. National Defense Universityn luennolla 8.2.2016 Professori Roxanne B. Everetts esitti kuvion 8 mukaisen rakenteen (Everetts, 2016). Alkuperäisessä kuvassa ei mainita kyberturvallisuutta. Tutkija täydensi kuvaa liittämällä aiemmin käsitellyin (luku 2.2) perusteluin tietoturvallisuuden yhteyteen kyberturvallisuuden. Tieto- ja kyberturvallisuuden tehtävät ovat organisaatiosidonnaisia riippuen organisaation tehtävistä ja asemasta. Valtionhallinnon ja kansainvälisten konsernien toimintaympäristössä tieto- ja kyberturvallisuuden rajapinta voi olla hyvinkin selvä. Toisaalta pienemmissä organisaatioissa tietoturvallisuuden ja kyberturvallisuuden rajapinnat hämärtyvät ja voi olla vaikea organisaation johtamisen näkökulmasta erottaa niitä toisistaan.

Tieto- ja kyberturvallisuuden toimintaa ja riskejä tulisi arvioida yhteisillä läpinäkyvillä mittareilla. Kuvion 8 mukainen malli ”Riskienhallinnan johtamisen silmä” tarjoaa mahdollisuuden tarkastella tieto- ja kyberturvallisuuden johtamista yhteisillä perusteilla ilman niiden siiloutumista omiksi saarekkeiksi.



Kuvio 8 Riskienhallinnan suhde tieto- ja kyberturvallisuuteen

3.1.4 Yhteenveto

Riskienhallinnan viitekehys tarjoaa toimivan johtamisrakenteen organisaatiolle. Riskienhallinta toimii kokoavana yläkäsitteenä organisaation tieto- ja kyberturvallisuuden riskien johtamiselle.

Riskienhallinnan, tietoturvallisuuden ja kyberturvallisuuden suhde on kuvion 8 mukainen. Riskienhallinta on kokonaismalli, jolla ohjataan tieto- ja kyberturvallisuuden kokonaisuutta. Riskienhallinta toimii organisaation johdon ja asiantuntijoiden työkaluna tavoiteltaessa organisaation liiketoiminnan tavoitteita. Riskienhallinnan tavoitteena on tuottaa organisaatiolle riittävä turvallisuuden taso ja menetelmät hallita päivittäisessä työssä organisaatioon kohdistuvia riskejä.

Tässä tutkimuksessa keskitytään tarkemmin NIST:n riskienhallinnan johtamismalliin ja erityisesti sen prosessin ensimmäiseen vaiheeseen, luokitteluun. NIST riskienhallintamallin rakennetta verrataan kansalliseen normistoon ja näiden yhdistelmänä tuotetaan menetelmä, jota testataan tutkimuksen yhteydessä.

3.2 Kansalliset turvallisuuden johtamista ohjaavat normit ja ohjeet

Luvussa käsitellään keskeisimmät Suomen kansalliset tietoturvallisuutta ohjaavat normit ja ohjeet. Peruste näiden käsittelyyn on tutkimuksen kansallinen viitekehys. Tutkimus toteutettiin puolustusvoimissa, jossa toiminta perustuu näihin kansallisiin normeihin ja ohjeisiin. Käsiteltäviä normeja ovat julkisuuslaki ja tietoturva-asetus. Valtionvarainministeriön tietoturvallisuuden johtoryhmän VAHTI -ohjeet sekä kansallisen turvallisuusviranomaisen koordinointivastuulla olevan Kansallinen turvallisuusauditointikriteeristö (KATAKRI).

Suomen kansallinen tietoturvaohjaus perustuu keskeisiltä osin lakiin viranomaisen toiminnan julkisuudesta (621/1999, jatkossa julkisuuslaki) ja valtioneuvoston asetukseen tietoturvallisuudesta valtionhallinnossa (681/2010,

jatkossa tietoturva-asetus). Julkisuuslaki ja tietoturva-asetus velvoittavat lähtökohtaisesti valtionhallinnon viranomaisia, mutta yhteiskunnan eri toimijoiden verkostoitumisen takia vaatimukset säteilevät laajalti myös muun julkishallinnon ja yksityisen sektorin toimijoihin.

Valtionvarainministeriön johdolla toimiva tietoturvallisuuden VAHTI-johtoryhmä valmistelee ja julkaisee tietoturvallisuusohjeita. VAHTI-johtoryhmän tavoitteena on kehittää kansallista hallinnon tietoturvallisuuden ohjausta ja koordinointia (Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010).

Ulkoministeriössä toimiva Kansallinen turvallisuusviranomainen (NSA) ylläpitää ja hallinnoi Kansallista turvallisuusauditointikriteeristöä (KATAKRI). KATAKRI on viranomaisen auditointityökalu auditoitaessa viranomaisten sidosryhmiä. KATAKRI:n päivitys ja ylläpito on toteutettu eri hallinnonalojen ja yrityselämän laajassa yhteistyössä. (KATAKRI 2015 Tietoturvallisuuden auditointityökalu viranomaisille, 2015.)

3.2.1 Julkisuuslaki ja tietoturva-asetus

Julkisuuslailla säädetään kansalaisten oikeudesta saada tieto viranomaisten julkisista asiakirjoista sekä viranomaisten vaitiolovelvollisuudesta ja asiakirjojen salassapidosta. Lain tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa. Laissa asiakirjan määritelmä on hyvin laaja.

> ”Asiakirjalla tarkoitetaan tässä laissa kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville automaattisen tietojenkäsittelyn tai äänen- ja kuvantoistolaitteiden taikka muiden apuvälineiden avulla.”

Laki määrittää salassapitovelvoitteisiin liittyen viranomaisten asiakirjojen salassapidon perusteet sekä vaatimuksen merkitä salassa pidettävät asiakirjat (Julkisuuslaki, 1999.)

Tietoturva-asetuksella säädetään viranomaisten asiakirjojen tietoturvallisuusvaatimuksista, asiakirjojen luokittelusta ja luokittelua vastaavista tietoturvallisuusvaatimuksista. Tietoturva-asetus määrittää salassa pidettävien asiakirjojen neliportaisen suojaustaso luokittelun (ST), luokitusmerkintöjä koskevat säännöt sekä suojaustasoihin liittyvät käsittelysäännöt. Suojaustasoja ovat KÄYTTÖRAJOITETTU (STIV), LUOTTAMUKSELLINEN (STIII), SALAINEN (STII) sekä ERITTÄIN SALAINEN (STI). (Tietoturva-asetus, 2010.) Tietoturva-asetukseen liittyy kiinteästi VAHTI-ohje 2/2010, ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta.

3.2.2 VAHTI-ohjeet

Tässä alaluvussa tarkastellaan yhteenvetotyyppisesti VAHTI-ohjeiden yleisiä tietoturvavaatimuksia sekä millaisia perusperiaatteita niissä esitetään. Tarkaste-

lu kohdistuu seuraaviin tietoturva-asetuksen voimaantulon jälkeen julkaistuihin VAHTI-ohjeisiin:

- Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta VAHTI 2/2010
- Sisäverkko-ohje VAHTI 3/2010
- Valtion ICT-hankintojen tietoturvaohje VAHTI 3/2011
- ICT-varautumisen vaatimukset VAHTI 2/2012
- Teknisen ICT-ympäristön tietoturvataso-ohje VAHTI 3/2012
- Sovelluskehityksen tietoturvaohje VAHTI 1/2013
- Toimitilojen tietoturvaohje VAHTI 2/2013
- Päätelaitteiden tietoturvaohje VAHTI 5/2013
- Tietoturvallisuuden arviointiohje VAHTI 2/2014
- Ohje salauskäytännöistä VAHTI 2/2015

Kaikissa tarkastelun kohteena olevissa VAHTI-ohjeissa viitataan tietoturva-asetuksen asiakirjan luokitteluvaatimuksiin. Luokittelun merkitystä pidetään tietoturvallisuuden hallinnan kannalta keskeisenä vaatimuksena. Käsiteltävän tiedon suojaustaso linkitetään päätelaitteisiin, tietoverkkoihin ja tiloihin. Päätelaitteet, tietoverkot ja tilat tulee olla hyväksyttäjä niissä käsiteltävän tiedon suojaustason vaatimuksien mukaisesti.

Ohjeissa yleisesti toistuva periaate on myös määrittää tiedolle, palvelulle tai esimerkiksi tietoverkolle omistaja, joka vastaa kyseisen resurssin hallinnasta, luokittelusta ja ylläpidosta. Organisaation pitää tunnistaa ja luetteloida resurssinsa sekä määrittää näiden resurssien tärkeysjärjestys. Omistajuus tulee olla organisaatiolla itsellään eikä sitä saa ulkoistaa esimerkiksi palveluntoimittajalle.

Omistajuuden kautta viranomaiselle syntyy edellytykset kohdistaa palveluntoimittajaan tietoturvallisuuteen liittyviä vaatimuksia. Viranomaisvaatimusten tulee näin ollen liittyä palveluntoimittajan kanssa sovittuun palveluun. Ulkoistettavien ICT-palveluiden hankintaan, tietojärjestelmien tai -sovellusten kehitykseen liittyen korostetaan tietoturvallisuusvaatimusten huomioinnin oikea-aikaisuuden merkitystä. Tietoturvavaatimukset on huomioitava suunnitteluvaiheen alusta alkaen, jotta saavutetaan toimivin ja kustannustehokkain lopputulos.

Suunnittelun yhteydessä korostetaan riskienhallinnan merkitystä. Tietoturvavaatimukset tulee suhteuttaa organisaation tehtävään, toimintaympäristöön ja olemassa oleviin tietoturvariskeihin. Suunnittelun yhteydessä on myös huomioitava tietoturvallisuuden eri osa-alueiden sekä palvelutuotannon vaatimukset.

Teknisen ICT-ympäristön tietoturvataso-ohjeessa (VAHTI 3/2012) on käytännönläheisiä luokitteluohjeita teknisten tietojärjestelmien suunnitteluun liittyen. Luokitteluohjeet sisältävä taulukkomalleja ja tarkastelevat luokittelua tietoturvallisuuden lisäksi palvelutuotannon ja varautumisen näkökulmasta. Luokitteluohje on laaja-alainen ja antaa mahdollisuuden arvioida tietojärjestelmän merkittävyyttä yhteiskunnan palveluidenkin kannalta. (Tekninen ICT-

ympäristön tietoturvataso-ohje, VAHTI 3/2012.) Ohjeistuksesta saa käsityksen, että se on tarkoitettu eri hallinnonalojen ylätason luokittelumenetelmäksi.

3.2.3 Kansallinen turvallisuusauditointikriteeristö (KATAKRI)

KATAKRI on tarkoitettu viranomaisille avuksi heidän auditoidessa yrityksiä, jotka käsittelevät viranomaisen salassa pidettävää tietoa. KATAKRI:n vaatimukset perustuvat voimassa olevaan lainsäädäntöön ja Suomea sitoviin kansainvälisiin tietoturvallisuusvelvoitteisiin. Keskeisimpinä normeina ovat tietoturva-asetus sekä kansainvälisten vaatimusten osalta EU:n neuvoston turvallisuussääntö (2013/488/EU). KATAKRI jakautuu kolmeen osa-alueeseen, joita ovat turvallisuusjohtaminen (T), fyysinen käyttöympäristö (F) sekä tekninen tietojenkäsittely-ympäristö (I). Turvallisuusjohtamisen vaatimuksissa kuvataan perustason vaatimukset kohdeorganisaatiolle. Fyysisen käyttöympäristön vaatimukset jakaantuvat salassa pidettävän tiedon käsittely- tai säilytystarpeesta johtuen hallinnolliseen, turva- tai tekniseen turva-alueeseen. Tekninen tietoturvallisuuden vaatimukset jakautuvat käsiteltävän tiedon mukaan kolmeen suojaustasoon, joita ovat ST IV, STIII ja STII. Esitetyt vaatimukset mahdollistavat erilaisia toteutusvaihtoehtoja. Vaatimusten yhteydessä on viittaukset niiden perustana olevaan lainsäädäntöön, VAHTI-ohjeisiin sekä tietoturvallisuuden standardeihin. (KATAKRI 2015 Tietoturvallisuuden auditointityökalu viranomaisille, 2015.)

KATAKRI muodostaa loogisen jatkumon Suomen kansalliselle tietoturvallisuutta ohjaavalle lainsäädännölle ja VAHTI-ohjeille. KATAKRI:ssa noudatetaan samaa luokittelua kuin VAHTI ohjeissa. KATAKRI:n vaatimukset noudattavat yleisesti käytössä olevia tietoturvallisuuden vaatimuksia. KATAKRI ei kuitenkaan suoraan sovellu käytettäväksi tietojärjestelmien tai -sovellusten suunnittelun tai hankintojen vaatimusmäärittelytyökaluna. KATAKRI:ssa ei myöskään käsitellä tiedon tunnistamista tietämysnäkökulmasta.

3.2.4 Yhteenveto

Julkisuuslaissa esitetystä laajasta asiakirjan määritelmästä johtuen lailla on vaikutusta tietojärjestelmien suunnitteluun ja käyttöön valtionhallinnossa. Tietoturva-asetuksen luokitteluvaatimukset muodostavat pohjan kansallisesti noudatettavalle tietoturvaluokittelulle. Suomen kansallinen luokittelu on yhteneväinen yleisesti kansainvälisesti noudatettavaan tietoturvaluokitteluun neliportaisen jaottelun suhteen. Merkinnöissä ja käsittelysäännöissä on kuitenkin eroavaisuuksia.

VAHTI-ohjeet muodostavat hyvän perustan tietoturvallisuuden johtamiseen ja hallintaan. VAHTI-ohjeiden pääperiaatteet voidaan tiivistää seuraavasti:

- Tiedon, palveluiden ja resurssien luokittelu ja priorisointi
- Tiedon, palveluiden ja resurssien omistajien määrittäminen

- Tietoturvavaatimusten oikea-aikaisuudesta huolehtiminen hankintojen, tietojärjestelmien ja -sovellusten suunnittelun yhteydessä
- Riskienhallintatoimenpiteiden merkitys tietoturvavaatimuksia määritettäessä
- Tietoturvallisuuden eri osa-alueiden mukaisten vaatimusten tasapuolinen huomioiminen

KATAKRI täydentää kansallista tietoturvallisuuden ohjeistusta. KATAKRI noudattaa samaa logiikkaa kuin kansallinen lainsäädäntö ja VAHTI-ohjeet. KATAKRI:n käyttötarkoitus eroaa VAHTI-ohjeista ja kohdistuu viranomaisen salassa pidettävää tietoa käsitteleviin yrityksiin VAHTI-ohjeiden kohdistuessa valtionhallinnon viranomaisiin. VAHTI-ohjeiden ja KATAKRI:n soveltaminen vaatii perehtyneisyyttä ja ymmärrystä vaatimusten kokonaistavoitteesta. Niissä ei myöskään esitetä niin yksityiskohtaisia turvallisuusvaatimusten valintaa ohjaavia vaatimuksia kuin NIST:n ohjeissa. VAHTI-ohjeiden ja KATAKRI:n vaatimukset sirpaloituvat tarkemmassa tarkastelussa ja ovat jossain määrin vaikeasti tulkittavissa.

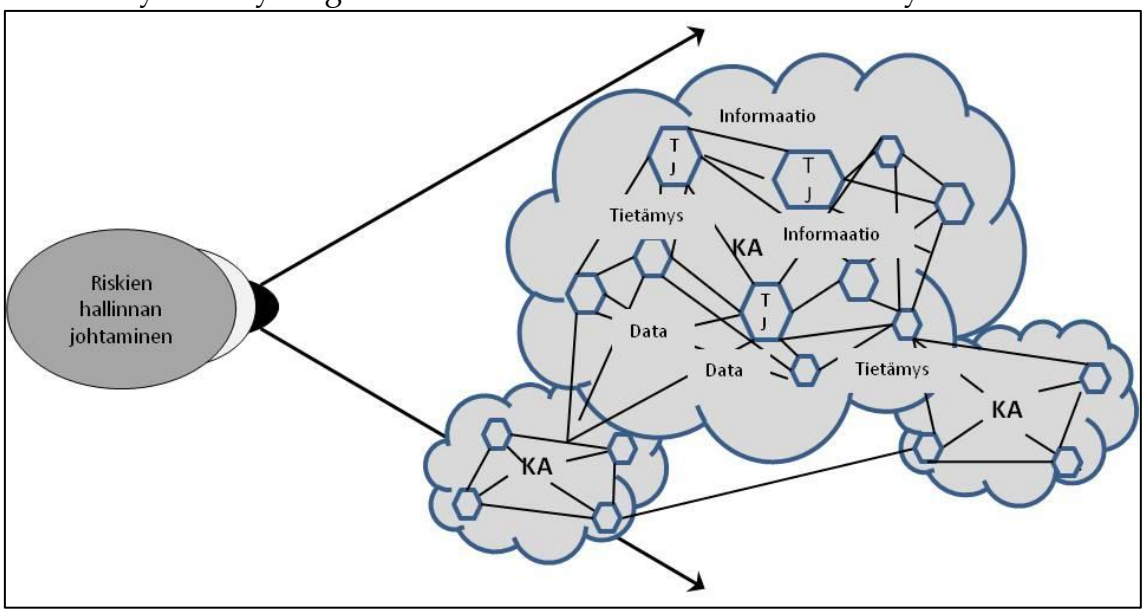
3.3 Tutkimuksen viitekehys

Toisen ja kolmannen luvun tavoitteena oli tutkimuksen viitekehyksen esittely ja keskeisten käsitteiden määrittely. Tutkimuksen viitekehys perustuu kuvion 9 näkemykseen. Organisaation riskienhallinnan keinot sisältävät tieto- ja kyberturvallisuuden osa-alueet organisaation liiketoiminnan vaatimusten mukaisessa laajuudessa. Riskienhallinnalla johtaminen kohdistuu organisaation kokonaisarkkitehtuuriin (KA). Kokonaisarkkitehtuurilla on organisaation toimintaan ja liiketoimintatavoitteisiin liittyvä kokonaisvaltainen tehtävä. Kokonaisarkkitehtuuri rakentuu toimintaa ohjaavista prosesseista, ihmisistä sekä teknologioista. Kokonaisarkkitehtuuri on tietojärjestelmiensä (TJ) summa, jossa tieto eri muodoissaan virtaa. Kokonaisarkkitehtuuri rajapintoineen on kompleksinen ja moniuloitteinen kokonaisuus, josta alla oleva kuvio 9 antaa varsin pelkistetyn näkemyksen.

Kirjallisuuslähteinä tarkasteltiin kahden tyyppistä kirjallisuutta, akateemisia lähinnä tietämyksen hallintaan ja johtamiseen liittyviä artikkeleita sekä Yhdysvaltain ja Suomen viranomaislähteiden ohjaavia normeja. Akateemisiin lähteisiin perustuen voidaan todeta, että tietämyksen hallinnan tutkiminen tietämyksen suojaamisen näkökulmasta on uusi tutkimusalue. Tietämyksenhallinnan tutkimuksen herätteenä ovat toimineet sosiaalisen median ja tietojärjestelmien erilaisten yhteistyömenetelmien (collaboration) kehittyminen. Organisaatioiden ja yksilöiden tiedon jakamisen mahdollisuudet ja nopeus ovat huomattavasti kasvaneet tämän kehityksen myötä.

Kirjallisuutta kokonaisuutena katsoen nousee esille tietämyksen hallinnan ja -johtamisen merkitys. Tietämystä on johdettava kuten kaikkia muitakin organisaation keskeisiä osa-alueita. Sensitiivisen tietämyksen tunnistaminen ja eri-

laiset luokittelumenetelmät luovat perustan tietämyksen johtamiselle. Tunnistamisen ja luokittelun kautta tietämykselle voidaan määrittää omistajuus kuten muillekin organisaation resursseille. Tietämys voidaan näin konkretisoida ja tehdä siitä johdettavaa. Viimeisenä voidaan mainita tietämyksen johtamisen läpinäkyvyysvaatimus. Organisaatioiden johdolla ja yksilöillä täytyy olla yhteinen ymmärrys organisaation tiedosta ja sen hallintaan liittyvistä vaatimuksista. Organisaation kannalta yksittäinen ihminen ja hänen ratkaisunsa ovat kuitenkin viimekädessä vastuussa organisaation tiedosta. Yksittäisen ihmisen ja organisaation ymmärrys organisaation tiedosta on näin ollen oltava yhtenevä.



Kuvio 9 Tutkimuksen viitekehys

Riskienhallinnan näkökulmasta kirjallisuudesta voidaan nostaa esille riittävä turvallisuuden periaate. Absoluuttista turvallisuutta ei voida saavuttaa, vaan organisaation tulee jatkuvasti osana päivittäistä työtä arvioida riskejä ja pohtia järkeviä organisaation resursseihin suhteutettavia riskienhallintatoimia. Organisaation tulee varautua myös jäännösriskien laukeamiseen, johdolla tulee olla tietoisuus näistä mahdollisuuksista sekä tarvittavaa kriisinsietokykyä ongelmatilanteiden hallintaan. Riskienhallintatoimenpiteiden tulee myös olla oikea-aikaisia, ne tulee huomioida eri prosessien suunnitteluvaiheesta alkaen ja niiden tulee elää eri prosessien kanssa niiden koko elinkaaren ajan.

Tietoturvallisuuden osa-alueet, luottamuksellisuus, saatavuus ja eheys, nousevat kirjallisuudessa esille. Yhteisenä haasteena kirjallisuus tunnistaa tietointensiivisten organisaatioiden osalta tietoturvallisuuden osa-alueiden tasapuolisen soveltamisen. Haasteena on tarkastella tietoturvallisuutta luottamuksellisuuden kautta ja lukita samalla saatavuuden ja eheyden vaatimukset.

Saatavuuden ja eheyden merkitys ei nouse Suomen kansallisissa ohjeissa samalla tavalla esille kuin luottamuksellisuus. Suojaustason määrittäminen perustuu luottamuksellisuuden vaatimuksiin, mutta samalla ohjaavat normit määrittävät tarkasti myös saatavuuden ja eheyden vaatimukset.

4 TUTKIMUSMENETELMÄT

Tässä tutkimuksessa on tavoitteena kehittää tietoturvallisuuden analyysimenetelmä, jota voidaan hyödyntää organisaatioiden kokonaisarkkitehtuurien ja tietojärjestelmien suunnittelu- ja kehittämisprosesseissa. Tutkimuksessa sovelletaan suunnittelutieteellistä Design Science Research Methodology (DSRM) -menetelmää. Tässä luvussa esitellään suunnittelutieteellisen menetelmän perusperiaatteet sekä se, miten menetelmää tässä tutkimuksessa sovelletaan käytäntöön.

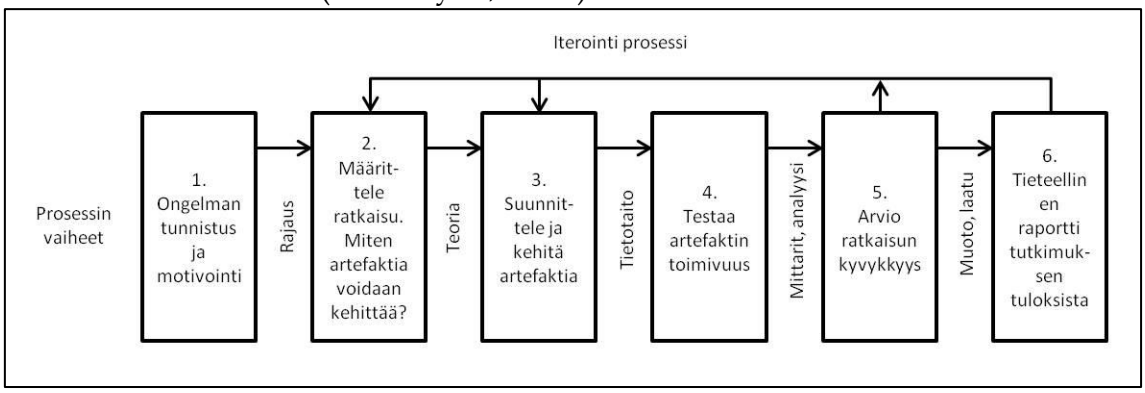
4.1 Suunnittelutieteellinen menetelmä

Tietojärjestelmien tarkoituksena on tehostaa ja helpottaa niitä käyttävien organisaatioiden työtä. Työ- ja johtamisprosessien tehostamisella kehitetään organisaatioiden tuloksellisuutta ja helpotetaan organisaatiossa työskentelevien ihmisten työkuormaa. Tietojärjestelmien tutkimus edellyttää tästä syystä kokonaisvaltaista liiketoimintastrategioiden, organisaatioiden infrastruktuurin, tietojärjestelmästrategioiden ja infrastruktuurien tutkimusta. (Hevner, March, Park & Ram, 2004.)

Suunnittelutieteellisen tutkimusmenetelmän tavoitteena on tuottaa ratkaisuja tunnistettuihin ja tarkasti määritettyihin organisaation tietojärjestelmäongelmiin. Hevner ym. (2004) käyttävät tällaisesta määritetyn ongelman ratkaisusta nimitystä artefakti. Artefaktin perusteellinen, tarkka ja täsmällinen määrittäminen on suunnittelutieteellisessä tutkimuksessa olennainen tekijä ja sen määrittäminen käynnistää tutkimusprosessin. Artefaktin määrittäminen ja sen perustelut osoittavat myös tutkittavan ongelman merkityksellisyyden. Hevnerin ym. (2004) esittelemässä tutkimusprosessissa korostetaan artefaktin määrittämisen lisäksi teknologiaperusteisen ratkaisuehdotuksen tuottamista ja sen testausta sekä arviointia liiketoiminta- ja tietojärjestelmäinfrastruktuurissa tunnustaen kuitenkin organisaatioiden, politiikkojen sekä työprosessien tutkimuksen merkityksen. (Hevner, ym., 2004.)

Suunnittelutieteellisen tutkimusmenetelmän tavoitteena on kehittää ja evaluoida organisaatioiden määritettyihin tietojärjestelmäongelmiin ratkaisuja (Peffers, Tuunanen, Rothenberg & Chatterjee, 2007).

Peffers ym. (2007) korostavat Hevnerin ym. (2004) tavoin tutkimusongelman ratkaisun, artefaktin, merkitystä. Artefaktin selkeä ja tarkka määrittely sekä sen merkityksen kuvaaminen organisaatioille ovat suunnittelutieteellisen tutkimuksen kulmakiviä. Tutkimusprosessin vaiheet he esittävät alla olevan kuvion 10 mukaisesti. (Peffers ym., 2007.)



Kuvio 10 Suunnittelutieteellinen tutkimusprosessi

Suunnittelutieteellinen tutkimusprosessi etenee seuraavissa vaiheissa:

1. Tutkimuksen aluksi on tunnistettava sekä määritettävä tutkimusongelma ja perusteltava tutkimuksen merkitys.
2. Suunnitellaan toteuttamiskelpoinen ratkaisu tutkimusongelmaan. Miten artefaktia muuttamalla tai kehittämällä voidaan tuottaa tutkimusongelmaan ratkaisu.
3. Jatketaan artefaktin suunnittelua ja kehittämistä.
4. Käytetään artefaktia erilaisissa ympäristöissä, tilanteissa tai tapauksissa. Arvioidaan artefaktin toimivuutta.
5. Arvioidaan, mitataan ja analysoidaan kuinka artefakti toimii. Tuottaako artefakti tuloksia tunnistettuun ongelmaan? Palataan tarvittaessa edellisiin vaiheisiin ja jatketaan artefaktin kehittämistä.
6. Raportoidaan tuloksista akateemiselle tiedeyhteisölle.

Perinteisen ongelmalähtöisen tutkimuksen sijaan tutkimus voi alkaa esimerkiksi suoraan vaiheesta neljä. Ratkaisu voisi olla perusteltua tilanteessa, jossa tavoitteena on testata asiakasyrityksen toiminnallista tuotetta suoraan tuotannossa. (Peffers ym., 2007.)

4.2 Menetelmä artefaktina

Artefaktin tehtävänä on tuottaa ratkaisu tunnistettuihin ja tarkasti määritettyihin organisaation tietojärjestelmäongelmiin (Hevner ym., 2004). Tutkimuksen tavoitteena on kehittää menetelmä, jonka avulla voidaan tunnistaa organisaation kokonaisarkkitehtuuri- tai tietojärjestelmäprojektien tietoturvallisuusvaatimukset. Menetelmän tulee tukea liiketoimintajohdon, tietojärjestelmäarkkitehtien ja -asiantuntijoiden välistä viestintää ja kommunikaatiota. Menetelmän tulee myös tukea organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista.

Kehitettävän menetelmän tavoitteena on auttaa organisaatioita tunnistamaan mitä tietoa niiden käyttämissä tai suunnittelemissa tietojärjestelmissä käsitellään, prosessoidaan tai tallennetaan. Tutkimuksessa käytetään näistä tiedon eri lajeista käsitettä tietotyyppi. Tunnistettuja tietotyyppejä arvioidaan ja analysoidaan tietoturvallisuuden eri osa-alueiden perusteella. Tietoturvallisuuden osa-alueita ovat luvussa 2.2 määritellyt luottamuksellisuus, saatavuus sekä eheys.

4.2.1 Menetelmä

Nykysuomen sanakirja määrittelee menetelmän järjestelmälliseksi, suunnitelmalliseksi menettelytavaksi (Nykysuomensanakirja, 1985). Tolvanen määrittää menetelmän tutkimuksessaan (tutkijan käännös): *"Systemaattiseksi ja ennalta suunnitelluksi ohjeeksi, joka tuottaa vähintäänkin yhden valmiin tietojärjestelmän suunnitteluprojektin tehtävän."* (Tolvanen, 1998, 12).

Tolvanen käsittelee väitöskirjassaan menetelmän tietorakennetta. Menetelmän tietorakenne esitetään kuvion 11 mukaisena solumallina. (Tolvanen, 1998, 35.)

Menetelmän tietorakenne on tarkoitettu tietojärjestelmän suunnittelun työkaluksi. Tämän tutkimuksen kohteena on kehittää menetelmä, joka palvelee organisaation johdon ja tietojärjestelmiä kehittävien sekä suunnittelevien henkilöiden vuorovaikutusta. Tutkimuksen kohteena ei siis ole tietojärjestelmän suunnittelumenetelmä. Ongelmakenttä ja rajapinnat tietojärjestelmäsuunnittelun kanssa ovat kuitenkin siinä määrin yhtenevät, että Tolvasen esittelemä menetelmän rakennetta kuvaava malli soveltuu myös tähän tutkimukseen.

Solumallissa menetelmän eri osien tietosisällöllä ja keskinäisillä riippuvuussuhteilla on oma merkityksensä.

- *Arvot ja odotukset,* menetelmä perustuu yleensä organisaation perustehtävään tai arvoperusteiseen tavoitteeseen. Arvot ja odotukset voivat olla myös näkymättömiä. Menetelmän kohteena olevan tuotteen tai palvelun kannalta on tärkeää tunnistaa ja avata myös piilossa olevat arvot ja odotukset.

- *Kehittämistavoitteet ja päätökset,* menetelmän tulee tuottaa muutakin kuin kuvaus olemassa olevasta järjestelmästä. Menetelmän tulee kehittää olemassa olevaa järjestelmää ja saada aikaiseksi muutoksia prosesseissa. Menetelmän tulee kuvata vaihtoehtoisia ratkaisuja ja arvioita mahdollisista tuloksista. Järjestelmän kehittäminen ja siihen liittyvät vaatimukset on pystyttävä kuvaamaan tavalla, joka mahdollistaa eri vaihtoehtojen erittelyn ja arvioinnin sekä päätöksen tekemisen.

Kuvio 11 Menetelmän rakenne (Tolvanen, 1998, 35)

- *Osallistujien roolit,* tietojärjestelmän kehittämiseen osallistuu useista ihmisiä eri rooleissa: johtajia, suunnittelijoita, ohjelmoijia ja loppukäyttäjiä. Yleensä roolit ja tehtävät on kuvattu osallistuvien ICT-ammattilaisten roolien osalta. Tietojärjestelmien käyttäjien roolit kuvataan yleensä epäsuorasti järjestelmän vaatimusmäärittelyn yhteydessä. Mitä rajoitetumpaan käyttöön tietojärjestelmä on tarkoitettu, sitä suurempi merkitys käyttäjien ja sidosryhmien roolilla on.
- *Prosessit,* tietojärjestelmän suunnittelu ja toteutus kuvataan prosesseina. On olemassa kahden tyyppisiä prosesseja; itse tekemistä ja suunnittelua kuvaavia työtapaprosesseja tai tietojärjestelmän suunnitteluun ja johtamiseen liittyviä johtamisprosesseja. Työtapaprosessit kuvaavat menetelmän syötteitä ja tuloksia. Johtamisenprosessit kuvaavat projektin suunnittelua, organisointia ja johtamista. Prosessien tehtävänä on kuvata ne tekniikat ja menetelmät, joilla päästään haluttuihin tuloksiin. Jotta edellä mainittuihin tuloksiin päästään, tulee prosesseilla olla vahva side menetelmän käsitteelliseen rakenteeseen.
- *Notaatio,* käsitteellinen rakenne tulee kuvata ja esittää määritetyn notaation mukaisesti. Notaation ja käsitteellisen rakenteen välinen suhde tulee kuvata ja määrittää. Notaatio voi perustua muodolliseen, puolimuodolliseen tai vapaaseen rakenteeseen. Joissain tilanteissa notaatiota ei käytetä. Tilanteessa, jossa notaatio ei kata koko tietojärjestelmän kä-

sitteellistä rakennetta, voidaan hyödyntää eri notaatioita ja mallintamismenetelmiä.

- *Käsitteellinen rakenne,* tietojärjestelmän suunnittelun ja toteutuksen yhteydessä on mahdotonta esittää tietojärjestelmään yksityiskohtaisena tarkkana kokonaiskuvauksena. Tietojärjestelmän käsitteellinen rakenne tarkoittaa tietojärjestelmä jakamista pienempiin käsiteltävissä oleviin määriteltyihin kokonaisuuksiin. Tällöin on mahdollista keskittää huomio näiden määriteltyjen osakokonaisuuksien toiminnollisuuksien ja niiden välisten suhteiden tarkasteluun (Tolvanen, 1998.)

4.2.2 Tutkimuksen artefakti

Edellä kuvattu menetelmän rakennemalli mahdollistaa tutkimuksen artefaktin täsmällisen määrittämisen. Määritettyä artefaktia tutkitaan, testataan ja kehitetään tutkimuksen kussakin tapauksessa. Tutkimuksen päätteeksi voidaan arvioida artefaktin merkityksellisyys ja arvo.

Tämän tutkimuksen arvojen ja odotusten tavoitteena on tuottaa johtamismenetelmä, joka mahdollistaa eri tietojärjestelmäprojektien tietoturvallisuusvaatimusten tunnistamisen. Sen tavoitteena on tukea johdon ja ICT-asiantuntijoiden välistä kommunikaatiota ja viestintää sekä organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista.

Kehitystavoitteena on tuottaa luokittelumenetelmä, jota voidaan hyödyntää organisaatioiden kokonaisarkkitehtuurin projekti- ja tietojärjestelmäsuunnittelussa. Luokittelumenetelmän tavoitteena on varmistaa tietoturvallisuuden eri osa-alueiden vaatimusten huomioiminen projekti- ja tietojärjestelmäsuunnittelussa. Menetelmä tulee vaiheistaa, määritellä tarkoituksenmukaisella tavalla parhaan kustannustehokkuuden saavuttamiseksi.

Luokittelumenetelmä on johtamismenetelmä ja sijoittuu kokonaisarkkitehtuurissa organisaation johtamisen ja teknisen suunnittelun rajapintaan. Luokittelumenetelmää käyttävät organisaation johdon edustajana tietoturvallisuuden asiantuntija tai konsultti sekä projektin omistaja. Luokittelumenetelmä soveltuu myös perehdytyksen jälkeen projektin itsearviontityökaluksi.

Luokittelumenetelmä toteutetaan kuvion 12 mukaisena prosessina. Prosessi alkaa kohteena olevan projektin määrittämisellä ja kuvauksella sekä luokittelumenetelmän esittelyllä. Luokittelumenetelmän keskeisin kohta on eri tietotyyppien tunnistaminen ja luokittelu sekä niiden analysointi. Prosessi päättyy projektin tietoturvallisuusvaatimusten määrittämiseen. Luokittelumenetelmän prosessin vaiheittainen toteutus toteutetaan ja ohjataan määrämuotoisella lomakkeella.

Luokittelumenetelmän notaatio noudattaa soveltuvin osin Suomen kansallisia määritelmiä. Luokittelumenetelmässä sovelletaan johtamisen ja tietojärjestelmäprojektien eri menetelmiä, joten yksiselitteistä vain luokittelumenetelmän käyttöön soveltuvaa notaatiota ei ole olemassa. Tutkimuksen aikana kehitetään suosituksina hyviä käytänteitä notaatioiksi.

Kuvio 12 Luokittelumenetelmän prosessi

Luokittelumenetelmää pyritään soveltamaan hyvin erityyppisiin tietojärjestelmäprojekteihin. Projektit voivat olla laajoja organisaatioiden kokonaisarkkitehtuurien tietoturvallisuusvaatimusten kartoituksia tai yksittäisten ohjelmistoprojektien tietoturvallisuusvaatimusten arviointeja. Luokittelumenetelmää käytettäessä tulee hyvin tarkkaan määrittää kohteena oleva projekti ja sen rajaukset. Laajoissa projekteissa tarkastelunäkökulma on laaja-alaisempi, karkeampi, yksittäisissä projekteissa voidaan mennä hyvinkin tarkkoihin yksityiskohtiin. Luokittelumenetelmää voidaan myös käyttää useina eri iterointikierroksina, edetään yleisestä kohti yksityiskohtaisempaa tai tarkennetaan luokittelua tietojärjestelmäprojektin elinkaaren aikana. Luokittelumenetelmän käsitteellinen rakenne perustuu tietoturvallisuuden osa-alueisiin, luottamuksellisuuteen, saatavuuteen ja eheyteen. Kohteena olevan tietojärjestelmän rakenne, käyttötarkoitus ja käyttäjät luovat perustan arvioida millaista tietoa (tietotyyppejä) tietojärjestelmässä käsitellään, tallennetaan ja prosessoidaan. Tietotyypillä tarkoitetaan tässä tutkimuksessa näitä tietojärjestelmien eri tietovarantoja. Tietotyyppien tunnistaminen on luokittelumenetelmän perusta. Tietotyyppejä arvioidaan suhteessa tietoturvallisuuden osa-alueisiin. Kullekin tietoturvallisuuden osa-alueelle annetaan arvo, korkea (K), normaali (N) tai matala (M). Arvon määrityksen tueksi on määritetty ohjaavia esimerkkejä, joita voidaan käyttää arvioinnin tukena. Tutkimuksen aikana voidaan vain kehittää kuvailevia arviointiesimerkkejä. Tietotyyppien tunnistamisen ja luokittelun jälkeen analysoidaan tulokset. Analyysissä tulee kiinnittää huomio tuloksen johdonmukaisuuteen sekä mahdollisiin ongelmakohtiin. Analyysissä voi kiinnittää huomiota esimerkiksi tietotyyppeihin, jotka ovat kaikkien tietoturvallisuuden osa-alueiden osalta korkealla tasolla.

4.3 Tutkimuksen toteutus

Kyseessä on konstruktiivinen tutkimus, jossa käytetään suunnittelutieteellistä menetelmää. Tutkimuksen vaiheet on esitetty kuviossa 13.

Kuvio 13 Tutkimuksen vaiheet

Tutkimusprosessi noudattaa Peffersin ym. (2007) määrittelemää tutkimusprosessia. Malli on sovitettu Suomen kansalliseen toimintaympäristöön. Suunnittelutieteellistä menetelmää sovelletaan seuraavalla tavalla.

- *Tunnistetaan ja määritetään tutkimustehtävä, perustellaan tutkimuksen tarve.* Tutkimuksessa etsitään käytännön johtamistyössä sovellettavaa menetelmää tunnistaa organisaation kokonaisarkkitehtuurin tietoturvallisuusvaatimukset. Menetelmän tulisi tukea liiketoimintajohdon, tietojärjestelmäarkkitehtien ja – asiantuntijoiden välistä viestintää ja kommunikaatiota sekä organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista. Tutkimustehtävään haetaan vastausta seuraavien tutkimuskysymysten kautta.
  1. Miten luokittelua voidaan hyödyntää organisaatioiden kokonaisarkkitehtuurin projekti- ja tietojärjestelmäsuunnittelussa?
  2. Miten luokitteluprosessi vaiheistetaan ja määritellään parhaan kustannustehokkuuden saavuttamiseksi?
  3. Miten luokitteluprosessissa varmistetaan tietoturvallisuuden eri osa-alueiden, luottamuksellisuuden, saatavuuden ja eheyden, vaatimusten huomioiminen?
- *Suunnitellaan tutkimustehtävään ratkaisumalli.* Tutkimustehtävän ratkaisumallina testataan ja kehitetään liitteen 1 mukaista luokitteluprosessia. Luokitteluprosessi ja siihen liittyvät ohjeet esitetään liitteessä lo-

makemuodossa. Kehitetty ratkaisumalli perustuu toisessa luvussa esitettyyn kirjallisuuteen. Kirjallisuudessa esitettyjä malleja on pelkistetty ja kevennetty tavoitteena saada aikaiseksi helpommin erilaisiin tapauksiin ja Suomen kansalliseen ympäristöön sopeutuva malli. Ratkaisumalli perustuu lomakkeen täyttämisen yhteydessä tehtävään tiedon kokoamiseen ja analysointiin. Lomakkeen tietojen kokoamiseen ja analysointiin osallistuvat organisaation tai projektin omistaja sekä mahdolliset asiantuntijat. Tutkimuksen tekijä vastaa näiden tilaisuuksien ohjauksesta ja osallistuu aktiivisena toimijana. Tutkija toimii tilanteessa organisaation turvallisuuden asiantuntijan roolissa. Ratkaisumallin tavoitteena on tuottaa organisaatiolle tai projektille yhteneväinen ja läpinäkyvä käsitys kohteena olevan tapauksen tietoturvavaatimuksista.

- *Testataan ratkaisumallia erilaisissa tutkimustapauksissa.* Ratkaisumallia testataan viidessä erillisessä tutkimustapauksessa. Tutkimustapaukset on valittu tutkijan työtehtäviin liittyvistä ajankohtaisista tehtävistä. Valitut tapaukset jakautuvat opetustehtävään liittyvään harjoitukseen, yrityselämään kohdistuvaan kokonaisarkkitehtuurin taustaselvitykseen, kahteen eri tietojärjestelmäprojektin vaatimusmäärittelyyn sekä yhteen tietojärjestelmän tutkimushankkeeseen. Valitut tapaukset ovat hyvin erityyppisiä ja mahdollistavat aidon vertailun kehitettävän menetelmän suhteen. Kussakin tapauksessa tutkitaan menetelmän soveltuvuutta ja kehittämistarpeita. Tutkimustapauksista kerätään empiiriset havainnot kyselylomakkeella ja täydentävällä haastattelulla.
- *Jatketaan menetelmän suunnittelua ja kehittämistä tutkimustapauksesta saatujen havaintojen perusteella.* Menetelmän suunnittelua ja kehittämistä jatketaan tutkimustapausten välillä. Jokaisen tutkimustapauksen kokemusten perusteella menetelmään voidaan tehdä tarvittavia muutoksia. Tutkimuksen päätteeksi alkuperäistä menetelmää on testattu ja kehitetty viidessä erillisessä toisistaan poikkeavassa tutkimustapauksessa. Tapausten poikkeavuus vahvistaa johtopäätöksiä ja on tärkeä tässä tutkimuksessa, koska itse tutkittava prosessi on varsin yksinkertainen.
- *Arvioidaan ja analysoidaan tutkimustulokset.* Tutkimustapausten käsittelyn päätteeksi analysoidaan koottu empiirinen aineisto. Kyselyiden ja haastatteluiden yhteenveto on koostettu liitteen 2 taulukkoon. Tulosten käsittelyssä ja analyysissa on noudatettu Pulkkisen ja Kapraalin (2015, s 69) artikkelissa sovellettua tekniikkaa. Tulosten perusteella liitteen 1 luokitteluprosessi kirjoitetaan ohjeineen lopulliseen muotoon.
- *Tulosten raportointi.* Tulokset raportoidaan tiedeyhteisölle tässä Pro gradu -tutkielmassa. Kommunikointi tiedeyhteisölle mahdollistaa tutkimuksen tulosten asettamisen kriittisen arvioinnin ja mahdollisen jatkokehityksen kohteeksi.

4.4 Empiirisen materiaalin keräys ja haastattelukysymykset

Pääesikunta myönsi tutkimukselle tutkimusluvan hallintopäätöksellä AM10032 24.5.2016 (Pääesikunta, 2016). Tutkimus kohdistuu organisaatioihin, jotka joutuvat liiketoimintaprosesseihin ja tietojärjestelmiin liittyen käsittelemään ja pohtimaan tiedon luottamuksellisuuden, saatavuuden ja eheyden vaatimusten huomioimista. Tutkimusongelman testaus reaalimaailman ilmiöiden yhteydessä aiheutti väistämättä tilanteen, jossa tutkija joutui prosessin aikana käsittelemään salassa pidettävää tietoa. Tästä seurasi se että, tutkittavien tapausten sisältöä ja aihetta voitiin käsitellä vain yleisellä tasolla. Tämä korostaa ja nostaa esille tutkimuksen varsinaisena kohteena olevan prosessin. Tutkimus itsessään on julkinen eikä siihen liity salassa pidettävää materiaalia

Salassa pidettävän tiedon käsittelystä aiheutui riski tutkimuksen empiirisen aineiston kokoamiselle. Tutkija ei voinut dokumentoida käsiteltävää tietoa itsessään vaan dokumentointi tuli kohdistaa tutkittavaan prosessiin, prosessin vaiheisiin ja sen määritelmiin. Empiirisen aineiston kokoamisen kannalta tämä rajoitti haastatteluiden tallentamista. Tutkija dokumentoi kunkin tapauksen vaiheet tutkimuspäiväkirjaan. Tapauksen päätteeksi tutkija haastatteli kunkin tapauksen osallistujat. Haastattelu toteutettiin puoliavoimena teemahaastatteluna. Haastatteluita ei tallennettu, koska tapauksen havaintojen käsittelyyn ja keskusteluun liittyi salassa pidettävien tietojen käsittelyä. Tutkimuksen yhteydessä ei haluttu tuottaa salassa pidettävää dokumentaatiota.

Tutkimustapausten haastatteluihin osallistuivat kyseiseen tapaukseen osallistuneet henkilöt. Tutkimustapaukset esitellään luvussa 5.2. Laajimmillaan haastateltavien määrä oli ensimmäisessä opetustapauksessa, seitsemän henkilöä. Muissa tapauksissa osallistujia oli kussakin yksi henkilö. Kussakin tapauksessa käsiteltiin samat kysymykset. Haastateltavien motivointia helpotti se, että opetustapausta lukuun ottamatta mielenkiinto ongelmanratkaisuun oli molemminpuolinen. Haastateltavien henkilöiden valintaan ja motivointiin liittyvät haasteet ratkaistiin tutkimuksessa tutkimustapausten valintavaiheessa.

Tutkimustapauksia rajasi tutkimusekonomia, aineisto tuli olla kerättynä syksyyn 2016 mennessä. Tapausten valinta perustui tutkijan työelämässä olemassa oleviin tapauksiin ja aikatauluihin.

Materiaalin reliabiliteettiin vaikuttaa kunkin tapauksen ominaispiirteet ja vastaajien mieliala ja muut satunnaisvirheet. Tutkija pyrkii tukemaan reliabiliteettia toteuttamalla haastatteluvaiheen pragmaattisen yhdenmukaisesti. Tutkimuksen validisuus perustuu itse tutkimuksen rakenteeseen ja erityisesti tutkimustapausten valintaan.

Haastattelukysymysten tavoitteena oli selvittää kokemusperäisesti tutkimuksen kohteena olevan menetelmän soveltuvuutta suunniteltuun käyttötarkoitukseen. Haastattelukysymyksiin vastaaminen perustui haastateltavien kokemuksiin menetelmästä tutkimustapauksessa, jonka käsittelyyn he osallistuivat. Opetustapauksessa tutkimustapaus on kuvitteellinen harjoitustilanne, jon-

ka haastateltavat toteuttivat kahden tai kolmen hengen työryhmissä. Haastattelukysymykset olivat seuraavat:

1. Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuusvaatimusten tunnistamiseen?
2. Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturvavaatimusten tunnistamiseen? Mitä nämä uudet käytännöt ovat?
3. Voitko tunnistaa tekijöitä tai kohtia prosessista, jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen? Mitä nämä tekijät tai kohdat ovat?
4. Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat?
5. Miten prosessia voisi kehittää?
6. Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen?

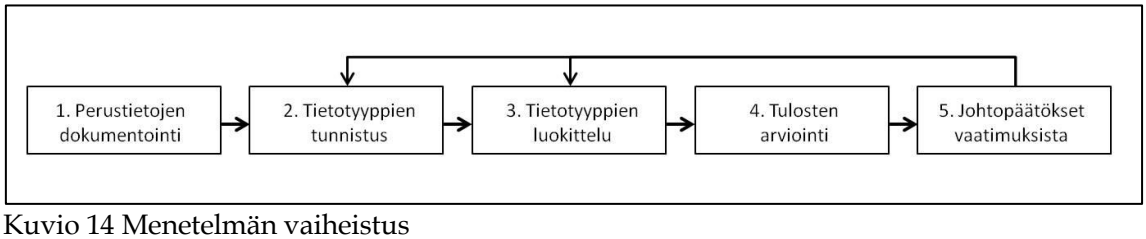
Haastattelumateriaali koottiin haastattelulomakkeille, jotka haastateltavat täyttävät. Lomakkeiden täytön jälkeen tutkija haastatteli osallistujat ryhmänä. Ryhmähaastatteluvaiheessa tutkija tekee kuhunkin kysymykseen liittyvästä keskustelusta vielä omat muistiinpanot.

5 TULOKSET

Tässä luvussa käsitellään tutkimuksen tulokset. Tulosten käsittely on jaettu neljään erilliseen alalukuun. Ensimmäisessä alaluvussa esitellään tutkimuksen tuloksena syntynyt valmis menetelmä. Toisessa alaluvussa käsitellään tutkimustapausten toteutus ja niistä saadut havainnot. Kolmannessa alaluvussa tutkimustapausten havaintoihin, tutkimuksen kirjallisuuteen sekä tutkijan ammatilliseen kokemukseen pohjautuen perustellaan valmiin menetelmän ratkaisut. Viimeisessä alaluvussa tutkimustulokset vedetään yhteen ja arvioidaan vastauksia suhteessa esitettyihin tutkimuskysymyksiin. Tutkimuksen liitteissä esitellään menetelmän perustyövälineet sekä tutkimuskyselyiden analysoidut sekä alkuperäiset vastaukset.

5.1 Tutkimuksen kohteena olevan menetelmän esittely

Tässä luvussa kuvataan menetelmä sellaisena, joksi se muodostui tutkimuksen iterointikierrosten tuloksena. Menetelmän vaiheet esitetään kuviossa 14. Tutkimuksen tavoitteena oli kehittää menetelmä, jonka avulla voidaan tunnistaa organisaation kokonaisarkkitehtuuri- tai tietojärjestelmäprojektien tietoturvallisuusvaatimukset.



Kuvio 14 Menetelmän vaiheistus

Menetelmän tulisi tukea liiketoimintajohdon, tietojärjestelmäarkkitehtien ja –asiantuntijoiden välistä viestintää ja kommunikaatiota. Menetelmän tulisi myös tukea organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamis-

ta. Menetelmän käyttöä tukemaan kehitettiin liitteessä 1 oleva lomake. Lomakkeessa on menetelmän käyttöä tukevat ohjeet. Ideaalitilanteessa menetelmää on suunniteltu käytettävän projektien esiselvitys- ja valmisteluvaiheessa.

5.1.1 Menetelmän ensimmäinen vaihe, perustietojen dokumentointi

Menetelmän käyttöön osallistuvat menetelmän käytön hallitseva asiantuntija, ohjaaja, jonka vastuulla on johtaa ryhmän työskentelyä ja perehdyttää osallistujat menetelmän käyttöön. Hänen lisäksi työhön osallistuu organisaation kokonaisarkkitehtuurin tai tietojärjestelmäprojektin omistajan edustaja sekä mahdolliset tietojärjestelmäprojektin suunnitteluun osallistuvat toimittajien edustajat. Osallistujia valittaessa on huomioitava, että heillä on riittävät kokonaistiedot menetelmän kohteesta. Heidän tulee ymmärtää kohteen vaatimukset sekä teknisten että johdon asettamien toiminnallisten vaatimusten näkökulmasta. Osallistujilla tulee myös olla riittävät vaikuttamismahdollisuudet havaintojen viemiseksi osaksi kohteen vaatimusmäärittelyä.

Ensimmäinen tehtävä on tunnistaa perustiedot sekä rajata kohteena oleva alue. Perustietoja ovat kohteena olevan kokonaisarkkitehtuurin tai tietojärjestelmän nimi, käyttötarkoitus, käyttäjät sekä kohteen rajapinnat muihin järjestelmiin ja arvio kohteen merkittävyydestä sen käyttäjille. Merkittävyyden arviointi perustuu VAHTI-ohjeissa käytettyyn saatavuusluokitteluun. Luokittelun tarkoituksena on muodostaa ryhmälle yhteinen käsitys kohteen tärkeydestä ja mahdollistaa jatkossa eri tietojärjestelmien keskinäinen vertailu.

Perustiedot dokumentoidaan liitteen 1 mukaiselle lomakkeelle. Lomakkeen liitteeksi voidaan lisätä mahdollisia tietojärjestelmän rakennetta selventäviä dokumentteja tai kuvia.

Perustietojen tunnistamisella ja dokumentoinnilla, sekä sillä onko menetelmää käyttävällä työryhmän edustajilla tieto ja ymmärrys kohteena olevan tietojärjestelmän tai organisaation kokonaisarkkitehtuurin tehtävistä ja tavoitteista, on suuri merkitys lopputulokselle. Mikäli lähtötietoja ja rajausta ei voida dokumentoida tai osallistujat eivät edusta tietojärjestelmän tai kokonaisarkkitehtuurin omistajaa, ei menetelmän tavoitetta saavuteta.

5.1.2 Menetelmän toinen vaihe, tietotyyppien tunnistus

Perus- ja lähtökohtatietojen dokumentoinnin jälkeen vuorossa oli menetelmän toinen vaihe, eri tietotyyppien tunnistaminen. Tietotyypillä tarkoitetaan kohteena olevan tietojärjestelmän tai organisaation kokonaisarkkitehtuurin sisältämää ja prosessoimaa tietoa. Tieto voi olla tietämystä, informaatiota tai dataa.

Tietotyyppien tunnistaminen edellyttää menetelmän ohjaajalta alustusta. Tietotyypin määritelmä pitää avata ja osallistujien perehtymistä tulee tukea kohteeseen soveltuvilla esimerkeillä.

Tietotyyppien tunnistamista helpottaa luvussa 2 esitetty kuvio 4, tietämyksen lähteet. Kuvio helpottaa osallistujia tunnistamaan tietotyypit johdon-

mukaisesti ja kokonaisvaltaisesti. Perustietojen yhteydessä käsitellyt rajaukset sekä mahdolliset kohteen kuvaukset tukevat tietotyyppien tunnistamista.

Tietotyyppien tunnistaminen kannattaa toteuttaa iterointikierroksina, edeten yleisestä kohti yksityiskohtaisempaa. Tyypillisesti ensimmäisellä kerralla tulos on varsin pelkistetty, mutta menetelmän tullessa tutuksi ja työn edetessä tulos tarkentuu.

5.1.3 Menetelmän kolmas vaihe, tietotyyppien luokittelu

Menetelmän kolmannessa vaiheessa kukin tietotyyppi arvioidaan ja luokitellaan tietoturvallisuuden osa-alueiden luottamuksellisuuden, saatavuuden ja eheyden suhteen. Luokittelussa käytetään kolmiportaista asteikkoa, korkea (K), normaali (N) tai matala (M). Luokittelun tavoitteena oli arvioida, miten tietotyypin tietoturvallisuuden vaatimukset tulisi huomioida. Esimerkiksi, onko tunnistetun tietotyypin oltava erityisen saatavilla kokonaisarkkitehtuurin liiketoimintavaatimusten toteutumisen kannalta, vai onko luottamuksellisuuden turvaaminen tärkeämpää.

Luokitteluvaiheen aluksi menetelmän ohjaaja esittelee liitteessä 2 olevan luokittelun aputaulukon. Taulukon esittelyn tavoitteena on, että ryhmällä on yhteinen käsitys luokitteluasteikosta. Taulukon perustiedot pohjautuvat VAHTI-ohjeisiin, mutta ryhmän tehtävänä on rakentaa esimerkin pohjalta kyseisen tapauksen erityispiirteet huomioiva oma luokittelun aputaulukko.

Tietotyyppien tunnistaminen ja luokittelu perusteluineen dokumentoidaan liitteen 1 taulukkoon. Perusteluiden dokumentoinnin tavoitteena oli luokittelun läpinäkyvyyden parantaminen. Dokumentoinnilla on merkitystä projektityössä yhteisen näkemyksen muodostamisessa ja osana johdonmukaista päätöksentekoa. Tulosten analysoinnin helpottamiseksi kuhunkin luokkaan liittyy värikoodi, punainen (K=korkea), keltainen (N=normaali) ja vihreä (M=matala). Viimeisenä kohtana luokittelun yhteydessä kirjattiin mahdolliset kansainvälisten tietoturvallisuusvaatimusten perusteet.

5.1.4 Menetelmän neljäs vaihe, tulosten arviointi

Neljännessä vaiheessa arvioidaan luokittelun tulos. Arvioinnissa tulee huomioida seuraavan tyyppisiä asioita. Onko kaikki tietotyypit tunnistettu? Syntyykö tietotyyppejä, joihin pitää kiinnittää erityisesti huomiota? Onko jokin tietotyyppi esimerkiksi kaikkien tietoturvan osa-alueiden mukaan korkealla tasolla? Onko kyseinen ratkaisu toteutettavissa vai pitääkö kyseinen tietotyyppi jakaa useampaan osaan? Jakautuvatko tietotyypit useampaan ryhmään? Syntyykö erillisiä korkean luottamuksellisuuden ja korkean saatavuuden tietotyyppiryhmiä? Pitäisikö näitä eri ryhmiä käsitellä eri tietojärjestelmissä?

Tietotyypit, jotka kaikilta tietoturvallisuuden osa-alueilta ovat korkealla tasolla, ovat kriittisiä koska niiden toteuttamiseen liittyy yleensä teknisiä ja toiminnallisia haasteita. Korkean saatavuuden, eheyden ja luottamuksellisuuden yhdistäminen edellyttää yleensä organisaation ja tietojärjestelmän teknisten

vaatimusten lisäksi niitä ohjaavien hallinnollisten prosessien, kontrollien ja toimintaympäristöjen kriittistä tarkastelua. Ratkaisujen kustannusvaikutukset ovat myös yleensä varsin korkeat ja mikäli muutokset kohdistuvat jo olemassa oleviin ratkaisuihin, voi niiden toteuttaminen olla varsin haastavaa. Tavoitteena tulisi olla tietotyyppien jakaminen osiin, jotta kyseisiä korkeantason luokitteluri-vejä ei syntyisi.

Tietotyyppien jakamista tehtäessä itse luokitteluun tulee suhtautua kriittisesti ja keskustella tosiasiallisista tavoitteista. Luokittelussa tulee arvioida myös sitä, mikä on riittävä tietoturvallisuuden taso. Voidaan myös arvioida, voidaanko joltain osalta tietotyypin sisältämää tietoa pelkistää ja/tai sanitoida, jolloin sen luottamuksellisuusvaatimusta voitaisiin laskea.

Arviointi käydään keskusteluna tapauksen käsittelyyn osallistuneen ryhmän kesken. Keskustelun ja arvioinnin myötä tehtyä luokittelua tarvittaessa täsmennetään. Arviointivaiheen tavoitteena on, että ryhmälle muodostuu yhteinen käsitys kohteena olevan kokonaisarkkitehtuurin tai tietojärjestelmäprojektin tietoturvallisuusvaatimuksista.

5.1.5 Menetelmän viides vaihe, johtopäätökset vaatimuksista

Työn päätteeksi viidennessä vaiheessa kirjoitetaan esitys kohteen tietoturvallisuusvaatimuksista. Esityksessä huomioidaan eri vaihtoehdot ja mahdolliset erityishuomiota vaativat kriittiset tekijät. Esitys on hyvä muotoilla ajallisesti vaiheistaen ja arvioiden vaatimusten resurssitarpeet.

Tavoitteena on huomioida vaatimukset tietoturvallisuuden suhteen kokonaisvaltaisesti. Esityksessä tulee ottaa kantaa niin hallinnollisiin kuin teknisiin tietoturvallisuusvaatimuksiin sekä tilaturvallisuusratkaisuihin. Esityksessä tulee huomioida myös mahdollisten eri organisaatioiden väliseen tiedon vaihtoon liittyvät tietoturvallisuusvaatimukset.

Esityksestä tulee käydä selkeästi ilmi vaihtoehtoihin sisältyvät jäännösriskit. Esityksen perusteella johdon tulee kyetä arvioimaan vaihtoehtojen tulokset, resurssitarpeet sekä kuhunkin vaihtoehtoon sisältyvät riskit. Esityksen perusteella johto tekee vaadittavat päätökset ja kohteen jatkokehitykseen.

Menetelmän tulokset liitetään osaksi kohteen projektisuunnitelmia ja tuloksia pidetään yllä projektin eri vaiheissa.

5.2 Tutkimustapauksien käsittely

Tässä luvussa esitellään tutkimustapaukset, niiden toteutus sekä saadut havainnot. Kukin tutkimustapaus esitellään omassa alaluvussaan. Tutkimustapauksien raportointi on jäsennelty neljään osaan. Aluksi perustiedoissa kerrotaan tapauksen numero ja nimi, kuvaus tapauksen kohteesta ja tapauksen käsittelyyn osallistuneet henkilöt ja heidän henkilöiden roolit. Toisessa osassa kerrotaan tutkimustapauksen toiminnallinen toteutus ja

sen aikana mahdollisesti tehdyt artefaktia koskevat välittömät kehitystoimenpiteet. Kolmannessa osassa käsitellään haastatteluiden ja tapauksen toteutuksen perusteella saadut havainnot. Neljännessä osassa esitetään lyhyt analyysi tapauksesta ja mahdollisesti esille nousseet menetelmän kehityskohteet. Tutkimustapauksia oli viisi kappaletta:

- Tapaus 1, Harjoitus
- Tapaus 2, Puolustusvoimien operatiivinen tietojärjestelmäprojekti
- Tapaus 3, Yrityksen kokonaisarkkitehtuurin arviointi
- Tapaus 4, Puolustusvoimien tietojärjestelmäprojekti
- Tapaus 5, Tutkimushanke Mobile Urban Area Situational Awareness System (MUSAS)

Liitteessä 3 on tutkijan taulukkoon koostama analyysi tutkimustapauksista. Analyysi perustuu tutkimuskyselyyn, haastatteluihin sekä tutkijan omaan näkemykseen kustakin tapauksesta. Tutkimuskyselyyn vastanneiden vastaukset on koottu tapauksittain liitteeseen 4.

5.2.1 Tutkimustapaus 1, Harjoitus

Tutkimustapaus toteutettiin Jyväskylän Ammattikorkeakoulussa kolmipäiväisessä riskienhallinnan- ja tietoturvallisuuden opetustilaisuudessa huhti-toukokuun vaihteessa 2016. Tutkimustapaukseen osallistui seitsemän opiskelijaa, joilla oli kaikilla pitkä ICT-alan koulutus ja kokemus. Koulutustasoltaan opiskelijoilla oli joko ylempi tai alempi korkeakoulututkinto. Opiskelijoilla ei ollut erityistä riskienhallinnan tai hallinnollisen tietoturvallisuuden kokemusta. Tutkija toimi opetustilaisuuden vastuullisena suunnittelijana ja opettajana.

Opetustilaisuus jakautui kahteen vaiheeseen. Ensimmäisessä vaiheessa käsiteltiin riskienhallinnan- ja tietoturvallisuuden perusteet ja toisen vaiheessa harjoiteltiin case-harjoituksessa menetelmän käyttöä. Harjoituksessa opiskelijat muodostivat kolme työryhmää, jotka kukin edustivat kuvitteellista yritystä. Harjoituksen tavoitteena oli laatia yrityksen kokonaisarkkitehtuurin tietotyyppien kuvaus. Kukin työryhmä sai harjoituksen tehtävän perusteissa kuvauksen yrityksen toimialueesta, johon perustuen heidän tuli ensimmäisenä tehtävänään laatia yritysesittely. Tehtävän tavoitteena oli perehtyä ja eläytyä tilanteeseen. Seuraavassa vaiheessa työryhmät saivat tehtäväkseen tunnistaa ja luokitella yrityksen kokonaisarkkitehtuurin tietotyyppit. Viimeisesssä vaiheessa laadittua kuvausta tarkennettiin yksityiskohtaisemman ja rajatumman tehtävän puitteissa. Kukin työryhmä laati tietotyyppien kuvauksen kahteen kertaan, ensin karkeammalla tasolla harjoitellen ja harjoituksen päätteeksi jaettuun case-tehtävään liittyen yksityiskohtaisemmin.

Tehtävän perustuminen kuvitteelliseen toimintaympäristöön ja tilanteeseen vaikeutti opiskelijoiden tehtävää. Menetelmää sovellettiin tästä syystä muihin tapauksiin verrattuna poikkeavasti. Menetelmän rakenne ei

myöskään ensimmäisen tapauksen kyseessä ollen ollut täysin valmis. Perustietojen dokumentoinnin korvasi opiskelijoiden ryhmätyönä tekemä yritysesittely, jossa he kuvasivat yrityksen liiketoiminnan rakenteen, laajuuden, tavoitteet ja tuotannon karkeat tunnusluvut. Itse tietotyyppien tunnistaminen toteutetiin vastaavalla tavalla kuin muissakin tapauksissa. Loppuanalyysia ja turvallisuusvaatimusten suunnittelua ei myöskään toteutettu.

Tapauksen kokemusten perusteella tutkija lisäsi lomakkeeseen perustieto-osion. Tapaus nosti myös esille sen, että menetelmää käytettäessä osallistujilla tulee olla hyvä käsitys kohteena olevasta tietojärjestelmästä, organisaation kokonaisarkkitehtuurista sekä organisaation kohteeseen liittyvistä liiketoimintavaatimuksista.

Tutkimustapauksen aikana nousi selkeästi esille, että menetelmässä sovellettava näkökulma oli opiskelijoille uusi. Eräs opiskelija esitti työn lomassa kommentin "tämä on niin filosofista ja vaikeaa". Kommenttiaan hän perusteli sillä, että perinteinen tietojärjestelmäsuunnittelu on hyvin täsmällistä ja selkeästi määriteltyä. Termien ja määritelmien tarkentaminen nousi myös tämän tapauksen vastauksissa korostetusti esille. Tutkijan näkökulmasta opiskelijan kommentin taustalla oli myös uusi tiedon tunnistamisen näkökulma ja tarve tarkastella asioita myös laajemmasta organisaation johdon, ei teknisen asiantuntijan näkökulmasta.

Näkökulman uutuudesta johtuen menetelmän käyttö edellyttää harjoittelua ja osaavaa ohjaajaa. Tietotyyppien tunnistamista ja luokittelua pidettiin vaikeana tehtävänä. Palautteen perusteella luokittelu olisi hyvä jakaa useampaan iterointikierrokseen, edetä yleisestä kohti yksityiskohtaisempaa. Luokittelua helpottamaan tutkija laati seuraavia tapauksia varten liitteessä 2 olevan taulukon. Taulukossa on VAHTI-ohjeisiin perustuvia luokitteluesimerkkejä, jotka tutkija jakoi eri tasoille (korkea, normaali, matala). Palautteen perusteella myös liitteen 1 mukainen taulukko kehittyi lähelle lopullista muotoaan.

Kokonaisuutena ottaen menetelmä sai positiivisen palautteen. Uutta tiedon tunnistamisen näkökulmaa pidettiin hyvänä ja sen koettiin tukevan organisaation johtamista ja tietoturvallisuuden ohjausta. Menetelmän rakennetta pidettiin loogisena. Tiedon tunnistamisesta nähtiin hyötyä tuotantojärjestelmien suunnittelulle ja vastauksissa pidettiin tarpeellisena liittää menetelmä osaksi tietojärjestelmien suunnitteluprosessia, erityisesti suunnitteluprosessin alkuvaiheeseen. Eräässä vastauksessa todettiin että, "ohjelmistosuunnittelijan olisi hienoa saada tällainen valmiina". Huomioiden osallistujien ammattillisen kokemuksen ja koulutuksen, voidaan vastausta pitää hyvinkin rohkaisevana.

Yhteenvetona tapauksesta voidaan todeta menetelmän käytön ohjauksen ja tarkemman termien määrittelyn tarve sekä perustietojen dokumentoinnin tärkeys. Positiivinen palaute kannusti jatkamaan seuraavaan tapaukseen liittyvää valmistelua.

5.2.2 Tutkimustapaus 2, Puolustusvoimien operatiivinen tietojärjestelmäprojekti

Tutkimustapaus toteutettiin puolustusvoimissa puolen päivän aikana kesäkuussa 2016. Tapaukseen osallistui kohteena olevan tietojärjestelmän tekninen projektihenkilö ja tutkija. Projektihenkilöllä on pitkä kokemus puolustusvoimien tietojärjestelmäprojekteista ja hän hallitsi hyvin tietoturvallisuuden perusteet. Kohteena oleva tietojärjestelmä on tarkoitettu puolustusvoimien operatiiviseen käyttöön. Operatiivinen käyttö tarkoittaa sitä, että järjestelmä on suunniteltu käytettäväksi mahdollisen sodan ajan olosuhteissa. Tietojärjestelmää on tarkoitus käyttää myös normaaleissa rauhan ajan harjoituksissa. Tietojärjestelmäprojekti on ollut käynnissä useamman vuoden ja sen tulokset ovat jo pitkälti käytössä.

Tutkimustapaus toteuttiin kahdessa vaiheessa, ensimmäisessä vaiheessa projektihenkilö esitteli tutkijalle kohteena olevan tietojärjestelmäprojektin tavoitteet ja tietojärjestelmänteknisen toteutuksen. Samassa yhteydessä keskusteltiin projektin yleisistä tietoturvallisuusvaatimuksista. Lopuksi dokumentoitiin tutkijan johdolla tietojärjestelmän perusteet, tietotyyppien tunnistus ja luokittelu sekä johtopäätökset liitteen 1 mukaan.

Palautteen perusteella tunnistettiin haasteeksi arvioida operatiiviseen käyttöön suunniteltua tietojärjestelmää samalla mittarilla kuin rauhanajan käyttöön tarkoitettuja tietojärjestelmiä. Menetelmä itsessään toimii myös operatiivisten järjestelmiä arvioitaessa, mittarin tulisi olla niitä arvioitaessa eri asteikolla. Edellisen tapauksen perusteella laadittua liitteen 2 luokittelun aputaulukkoa jouduttiin tapauksen aikana täydentämään laitteiden osalta, ohjelmistojen näkökulmasta käytetty luokittelun aputaulukko vastasi vaatimuksia. Täydennykset koskivat arvioita siitä kuinka hyvin varmentavat laitteet on oltava saatavilla.

Keskeisin havainto liittyy pohdintaan siitä, miten varmistetaan tietojärjestelmäprojekteissa menetelmää käytettäessä läpinäkyvä ja yhteinen dokumentointi. Asialla on erityistä merkitystä työn tehokkuuden ja yhteisen näkemyksen muodostamisen kannalta. Projektijohtamisen kannalta olisi tärkeää, että tietotyypit tunnistetaan ja luokitellaan yhteiseen näkemykseen perustuen ja että luokitteluun sitoudutaan. Yhteinen näkemys tietotyypeistä ja niiden luokittelusta mahdollistaa organisaation johdon ja tietojärjestämäprojektin henkilöstön välisen selkeän kommunikaation ja johtamisen. Käydyn keskustelun pohjalta liitteen 1 taulukkoon lisättiin luokittelusarakkeiden viereen sarake johon luokitelu lyhyesti perustellaan. Luokittelun visualisointia tukemaan otettiin käyttöön värikoodisto.

Projektihenkilö piti menetelmää hyödyllisenä ja soveltuvana käyttötarkoitukseensa. Menetelmä oli hänen mielestään myös helppo- ja nopeakäyttöinen verratuna moniin muihin projektityökaluihin. Edellisen tapauksen havaintoihin verratuna eroa selittänee projektihenkilön perehtyneisyys tietoturvallisuuden perusasioihin ja kokemus puolustusvoimien tietojärjestelmäprojekteista.

Menetelmä tuotti palautteen perusteella lyhyessä ajassa merkittävää lisätietoa projektin suunnittelun tueksi, nosti esille merkityksellisiä kokonaisuuksia ja auttoi avaamaan ongelmakohtia.

Projektihenkilön kokemuksella tutkimuksen aihealueesta oli merkitystä menetelmän käytön soveltamisen helppouteen. Toisaalta kokemus nosti esille erityyppisiä kehitystarpeita. Näistä merkittävin oli luokittelun dokumentoinnin läpinäkyvyyden vaatimus ja sen merkittävyys projektin johtamiselle. Yleisesti ottaen tapauksesta saatu palaute oli hyvin positiivinen.

5.2.3 Tutkimustapaus 3, Yrityksen kokonaisarkkitehtuuri arviointi

Tutkimustapaus toteuttiin yrityksen tiloissa kahden päivän aikana heinäkuussa 2016. Tapaukseen osallistui tutkijan lisäksi yrityksen toimitusjohtaja. Yritys hallinnoi asiakkaidensa informaatiota ja tuottaa niiden pohjalta palveluita yksityisille henkilöille, yrityksille ja julkisyhteisoille. Tutkimustapauksen tavoitteena oli arvioida yrityksen viranomaisasiakkaiden informaation korkeampien luottamuksellisuusvaatimusten vaikutusta yrityksen kokonaisarkkitehtuuriin. Arviointi ajoittui projektin valmisteluvaiheeseen.

Tutkimustapaus toteutettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa yrityksen toimitusjohtaja perehdytti tutkijan yrityksen liiketoimintaan ja siihen kohdistuviin vaatimuksiin. Toisessa vaiheessa dokumentoitiin tutkijan johdolla yrityksen kokonaisarkkitehtuuri tutkimusmenetelmän periaatteiden mukaisesti. Tähän dokumentointiin käytettiin aikaan noin neljä tuntia.

Tutkimustapauksen yhteydessä hyödynnettiin ensimmäisen kerran tietotyyppien tunnistamisen yhteydessä kuviota 4, tietämyksen lähteet. Kuvio helpotti tietotyyppien johdonmukaista ja loogista tunnistamista.

Palautteen perusteella nousi esille tarve hyödyntää menetelmää organisaation liiketoiminnan suunnittelun tukena. Menetelmän tulisi tarjota vaihtoehtoisia kustannusvaikutukset ja aikataulut huomioivia kehitysmalleja. Esitys huomioitiin johtopäätösvaiheessa kirjoitettaessa esitystä turvallisuusvaatimusten toteuttamisesta. Esitys jaettiin kahteen vaihtoehtoon, jossa huomioitiin yleisellä tasolla aikataulut sekä kustannusten suuruusluokka.

Palaute oli positiivinen ja menetelmän kokonaisvaltaisuutta pidettiin hyvänä. Toimitusjohtajan näkemyksen perusteella menetelmä nostaa esille prosessien välisiä riippuvuussuhteita, tukee yrityksen johtamista sekä riskienhallinnan suunnittelua. Riskienhallintaan menetelmä tuo mukaan uuden osan, tiedon turvaamisen huomioimisen.

Mielenkiintoisena kokonaisuutena tapaus nosti esille tietoturvallisuuden eri osa-alueiden merkittävyyden. Yrityksen liiketoiminnan menestyksellisyyden ja jatkuvuuden kannalta asiakaspalvelun tietojärjestelmien ja -prosessien korkea saatavuus sekä yrityksen hallinnoiman informaation eheys ovat yritykselle kriittisiä menestystekijöitä. Viranomaisten informaation korkeammalla luottamuksellisuus vaatimuksella ei sinällänsä ole yrityksen liiketoiminnalle vastaavaa merkitystä. Viranomaisen yritykseltä hankkima palvelu on myös riippuvainen yrityksen asiakaspalvelun korkeasta

saatavuudestä ja informaation eheysvaatimuksista, sillä ilman niitä yritys ei kykene tarjoamaan viranomaiselle sen tarvitsemaa palvelua. Informaation luottamuksellisuus ei siis tämän tapauksen yhteydessä noussut tärkeimmäksi merkitseväksi tekijäksi. Tässä mielessä tapaus haastoi perustellusti perinteisen tietoturvallisuuden luottamuksellisuus lähtöisen näkökulman.

5.2.4 Tutkimustapaus 4, Puolustusvoimien tietojärjestelmäprojekti

Tutkimustapaus toteutettiin puolustusvoimien tiloissa yhden päivän aikana heinäkuussa 2016. Tapaukseen osallistui tutkijan lisäksi tietojärjestelmäprojektin projektipäällikkö. Projektipäälliköllä on laaja- ja pitkäaikainen kokemus eri tietojärjestelmäprojekteista, niin puolustusvoimien kuin yksityisen sektorin palveluksessa.

Tietojärjestelmäprojektin tavoitteena on tuottaa palveluita eri viranomaisille. Projekti on käynnistynyt alkuvuodesta 2016 ja sen perusmäärittelyt oli tutkimustapauksen käsittelyvaiheessa tehty. Määrittelyissä tietoturvallisuuden määrittelyt perustuivat tietoturvallisuuden teknisiin vaatimuksiin.

Tutkimustapaus toteutettiin kahdessa vaiheessa. Ensimmäisessä vaiheessa projektipäällikkö esitteli yleisesti projektin sekä tarkemmin projektin tavoitteet ja vaiheen. Toisessa vaiheessa dokumentoitiin tutkijan johdolla menetelmän periaatteiden mukaisesti projektin perustiedot, tietotyypit, arviointi ja johtopäätökset.

Tietojärjestelmän käyttäjien moninaisuus ja erilaiset vaatimukset rajoittivat menetelmän käyttöä. Perustietojen dokumentointi jäi puutteelliseksi ja sen seurauksena tietotyyppien tunnistamista ja luokittelua ei voitu riittävällä tarkkuudella toteuttaa. Käytyjen keskustelujen pohjalta kyettiin kuitenkin laatimaan esitys projektin tietoturvallisuuden peruslinjoista ja -vaatimuksista.

Palautteen perusteella menetelmän näkökulma oli projektipäällikölle uusi, mutta hän piti menetelmää soveltuvana keskeisten tietojärjestelmäprojektin vaatimusten tunnistamiseen ja jäsentämiseen. Menetelmä tuki hänen mielestä projektin kokonaisvaltaista johtamista. Kehityskohteena projektipäällikkö piti tarpeellisena testata menetelmää tietojärjestelmäprojektien eri vaiheissa.

Yhteenvetona tapauksesta voidaan nostaa esille perustietojen dokumentoinnin merkitys, ilman niitä menetelmän käyttöön soveltaminen on vaikeaa. Perustietojen dokumentointi edellyttää eri käyttäjien vaatimusten koordinointia sekä kaikkien käyttäjien näkökulmien huomiointia tietotyyppejä tunnistettaessa ja erityisesti tietotyyppien luokittelun yhteydessä. Tapauksen kohteena olevassa tietojärjestelmähankkeessa näitä vaatimuksia ei tutkimuksen aikataulusyistä johtuen kyetty toteuttamaan.

5.2.5 Tutkimustapaus 5, Tutkimushanke MUSAS

Tutkimustapaus toteutettiin puolustusvoimissa puolen päivän aikana elokuussa 2016. Tutkimustapaus perustui TEKES:n rahoittamaan WISM II-

tutkimushankkeeseen, johon osallistui Aalto yliopisto ja Vaasan yliopisto sekä Maanpuolustuskorkeakoulu (MPKK). WISM II-hankkeen tavoitteena oli tuottaa rakennetun alueen tilannekuvajärjestelmän testiversio. Järjestelmästä käytetään englanninkielistä nimeä Mobile Urban Area Situational Awerness System (MUSAS). MUSAS-järjestelmän suunniteltu käyttö perustui sodanajan toimintaympäristön vaatimuksiin. WISM II-hanke on päättynyt ja MUSAS :n testiversion testaus on toteutettu. MUSAS :n esittelyvideo löytyy alaviitteessä olevasta osoitteesta[1] tai YouTube-palvelusta hakusanalla WISM II.

Tapaukseen osallistui WISM II hankkeeseen osallistunut MPKK:n tutkija ja tämän tutkimuksen tekijä. Tutkimustapaus toteutettiin kahdessa vaiheessa. Hankeeseen osallistunut tutkija esitteli WISM II -hankkeen ja MUSAS:n tavoiteet ja teknisen toteutuksen sekä toteutetun testauksen yleisellä tasolla. Toisessa vaiheessa dokumentoitiin tämän tutkimuksen tekijän johdolla MUSAS-tietojärjestelmän perusteet, tietotyyppien tunnistus ja luokittelu sekä johtopäätökset liitteen 1 mukaisesti.

Palautteen perusteella menetelmä tukee projektien teknisten henkilöiden ja johdon välistä vuorovaikutusta. Menetelmän oikea-aikainen soveltaminen tietojärjestelmäprojektissa on tärkeää. Liian varhainen tarkastelu on vaikeaa puutteellisista perustiedoista johtuen ja liian myöhään tehtynä vaadittavien korjausten suorittaminen voi olla vaikeaa ja kallista. Menetelmästä koettiin olevan myös hyötyä tilaaja-tuottaja -mallissa vaatimusten tunnistamisessa ja määrittämisessä. Kuten kaikissa aiemmissakin tapauksissa menetelmän näkökulmaa pidettiin uutena. Menetelmän katsottiin tukevan perinteistä tietojärjestelmäsuunnittelua turvallisuuden näkökulmasta.

Kehityskohteena tunnistettiin oikean tietojärjestelmäprojektin resurssien arvioinnin tarve. Menetelmää tulisi käyttää vaiheittain ja pitäisi myös pohtia menetelmän käytön rajapinnat yleiseen vaatimusten määrittelyprosessiin.

Yhteenvetona tapauksesta voidaan todeta palautteen positiivisuus ja kokonaisvaltaisuus. Palautteessa kiinnitettiin erityinen huomio tietojärjestelmien suunnitteluprosessiin yleisesti ottaen ja siihen miten menetelmää voitaisiin ko. suunnitteluprosessiin liittää. Palautteessa nousi myös selkeästi esille menetelmän teknisten asiantuntijoiden ja johdon välistä vuorovaikutusta tukeva rooli. Tapauksen palaute nosti esille tilaaja-tuotaja mallin vaatimusmäärittelyä tukeva vaikutus.

5.2.6 Yhteenveto tutkimustapauksista

Tutkimustapausten havainnot perustuvat tutkimustapauksen käsittelyn yhteydessä tehtyihin havaintoihin ja keskusteluihin. Tutkimustapauksen päätteeksi toteutettuun kyselyyn sekä kyselyn jälkeen tutkijan toteuttamaan haastatteluun. Tutkimustapauksen jälkeen tutkija koosti analyysin tapauksesta liitteessä 3 olevaan taulukkoon.

[1] https://www.youtube.com/watch?v=9v1fFIHRWGE&app=desktop

Tiivistelmä tutkimustapauksien havainnoista sekä toteutetuista kehitystoimenpiteistä on allaolevassa taulukossa 1(taulukko 1). Ensimmäisessä sarakkeessa on tutkimustapauksen numero, toisessa sarakkeessa tutkijan arvio tutkimustapauksen merkityksestä tutkimukselle sekä sanallinen kuvaus keskeisistä havainnoista. Viimeisessä sarakkeessa on listattu menetelmään toteutetut muutokset.

Taulukko 1 Tiivistelmä tutkimustapauksien havainnoista

Tapaus nro	**Arvio tutkimustapauksen merkityksestä ja keskeiset havainnot**	**Toteutetut muutokset**
1	Positiivinen palaute menetelmästä. Opetustilanne. Menetelmän näkökulma oli osallistujille uusi. Perustason kehitystarpeita: Menetelmän rakenne ja käsitteet tulee määritellä tarkemmin. Perusteet ja rajaus tulee dokumentoida yksiselitteisesti.	Laadittiin liitteen 1 mukainen taulukko ja huomioitiin siinä perustietojen dokumentointi, Määritettiin menetelmän rakenne ja käsitteet
2	Positiivinen palaute menetelmästä. Tietojärjestelmäprojekti. Osaava ja kokenut projektihenkilö, joka arvioi menetelmän tuottavan nopeasti projektille lisäperusteita. Menetelmän näkökulma oli projektihenkilölle uusi. Tapaus tuotti selkeitä projektityössä tarpeellisia kehitystarpeita: Tarve kehittää menetelmän dokumentaation läpinäkyvyyttä sekä visuaalisuutta.	Lisättiin tietotyyppien luokitteluun yhteyteen perustelut sarake. Lisättiin tietotyyppien luokitteluun värikoodit.
3	Positiivinen palaute menetelmästä. Toimintaympäristönä yritys ja sen kokonaisarkkitehtuuri. Menetelmän näkökulma uusi haastateltavalle toimitusjohtajalle. Tapaus tuotti selkeää lisäarvoa menetelmän johtopäätös osioon: Tarve huomioida eri vaihtoehtojen liiketoimintavaatimukset sekä resurssitarpeet. Tietotyyppien johdonmukaista tunnistamista helpotti tietämyksen lähteet kuvion (kuvio 4) käyttö.	otettiin käyttöön tietotyyppien tunnistamista helpottamaan tietämyksen lähteet kuvio (kuvio 4). Liiketoimintavaatimukset kirjoitettiin tapauksen johtopäätöksiin.

(jatkuu)

(Taulukko 1 jatkuu)

Tapaus nro	Arvio tutkimustapauksen merkityksestä ja keskeiset havainnot	Toteutetut muutokset
4	Positiivinen palaute menetelmästä. Tietojärjestelmäprojekti. Projektipäällikkö arvosti menetelmän tuottamaa kokonaiskuvaa projektista. Itse menetelmän näkökulma oli hänelle uusi. Tapaus nosti erityisesti esille perustietojen dokumentoinnin merkityksen. Projektipäällikkö nosti esille tarpeen testata menetelmää eri tietojärjestelmäprojekteissa.	Ei toteutettuja muutoksia. Tapaus korosti perustietojen merkitystä. Ilman niitä menetelmää ei voida hyödyntää. Eikä tietojärjestelmä projektin tietoturvallisuusvaatimuksia voida tietämyksen suojaamisen näkökulmasta tunnistaa.
5	Positiivinen palaute menetelmästä. Tutkimushanke. Tutkijalle menetelmän näkökulma oli uusi. Tutkija nosti esille: Menetelmän positiivisen vaikutuksen johdon ja teknisten henkilöiden väliseen vuorovaikutukseen. Menetelmän hyödynnettävyyden tietojärjestelmäprojektien vaatimusmäärittelyn yhteydessä. Menetelmän hyödyn tilaaja-tuottaja mallissa vaatimuksien määrittelyn yhteydessä.	Ei toteutettuja muutoksia mentelmään.

Ensimmäinen tapaus tarjosi mahdollisuuden testata menetelmää puhtaalta pöydältä. Tapaus osoittikin tutkijalle selkeitä perustason kehitystarpeita menetelmän rakenteen ja käsitteiden selkeän määrittelyn suhteen.

Toinen tapaus oli selkeä tietojärjestelmäprojekti, joka oli ollut käynnissä jo useamman vuoden. Tapaukseen osallistunut projektihenkilö oli osaava ja tunnisti nopeasti menetelmän perusajatuksen. Tapaus tuotti projektityössä tarvittavia havaintoja menetelmän kehittämiseen. Keskeisimpänä menetelmän läpinäkyvyyttä ja visuaalisuutta kehittävät havainnot.

Kolmannessa tapauksessa menetelmää sovellettiin selkeästi erilaisemmassa ympäristössä, yrityksessä. Tavoite oli myös soveltaa menetelmää arvioitaessa yrityksen kokonaisarkkitehtuurin kehittämistarpeita liiketoiminnallisesti uudessa tilanteessa. Menetelmää sovellettiin tapauksessa karkeammalla tarkastelutasolla. Tulokset ja kokemukset menetelmän soveltuvuudesta tapauksessa olivat erittäin hyvät ja kokonaisvaltaiset. Menetelmän avulla pystyttiin tuottamaan yrityksen käyttöön kokonaisvaltainen vaihtoehtoinen kehityssuunnitelma kyseiseen liiketoimintatilanteeseen. Kehityssuunnitelma ja sen vaihtoehdot kyettiin myös vaiheistamaan ja arvioimaan niiden riski-, resurssi ja kustannusvaikutukset.

Neljännessä tapauksessa käsiteltiin toisen tapauksen tyyppistä tietojärjestelmäprojektia. Erona nousi esiin erilaisten käyttäjien vaatimuksista

johtuvat haasteet tunnistaa riittävällä tarkkuudella projektin perustietoja. Tästä johtuen tietotyyppien tunnistamista ja luokittelua ei kyetty riittävällä tarkkuudella toteuttamaan. Käydyn keskustelun ja menetelmän soveltamisen tuloksena tutkija kykeni kuitenkin tukemaan projektipäällikköä tietoturvallisuusvaatimusten tunnistamisessa. Tarkastelutaso tosin oli yleisempi mihin perusteellisen tietotyyppien tunnistamisen ja luokittelun kautta olisi ollut mahdollisuus. Tapauksen keskeinen havainto liittyy perustietojen tunnistamisen tarpeeseen sekä siihen, että projektin omistajan vaatimukset on tunnistettu. Ilman niitä menetelmää ei voida soveltaa käyttöön, eikä tietojärjestelmäprojektin tietoturvallisuusvaatimuksia tietämyksen hallinnan näkökulmasta voida määrittää.

Viimeinen tutkimustapaus perustui jo päättyneeseen tutkimushankkeeseen ja sen kokemuksiin. Tutkimustapaus nosti esille tietojärjestelmäsuunnittelun kokonaisprosessin ja menetelmän hyödyn teknisten henkilöiden ja organisaation johdon välillä.

Tutkimustapausten keskeisimpinä havaintoina voidaan nostaa esille seuraavat:

- Menetelmän näkökulma oli kaikille tutkimukseen osallistuneille uusi.
- Menetelmän avulla yrityksen kokonaisarkkitehtuurista voitiin muodostaa tiivis kokonaiskuva tiedon suojaamisen näkökulmasta. Menetelmän avulla voitiin tarkastella yrityksen prosesseja ja niiden riippuvuussuhteita. Menetelmä tuki näin yrityksen riskienhallintaprosessia ja mahdollisti siihen perustuvan kehityssuunnitelman laatimisen vaihtoehtoineen.
- Yrityksen osalta nousi esille tietoturvallisuuden eri osa-alueiden merkittävyys. Menetelmän avulla voitiin vertailla eri tietotyyppejä, joita erotti toisistaan niiden merkittävyys yritykselle tiedon luottamuksellisuuden, saatavuuden ja eheyden kannalta. Lopputuloksena yrityksen liiketoiminnalle kriittisimmiksi tietotyypeiksi tunnistettiin saatavuuden ja eheyden asettamat vaatimukset. Luottamuksellisuuden osalta tunnistetut tietotyypit tulisi sovittaa näihin saatavuuden ja eheyden vaatimuksiin. Tapaus nosti myös selkeästi esille arviointivaiheessa riskienhallinnan ja riittävien turvallisuusvaatimusten arvioinnin merkityksen.
- Menetelmää pidettiin kokonaisuutena ottaen loogisena ja helposti käyttöön sovellettavana. Menetelmän koettiin myös tuottavan oleellista lisäarvoa tarkastelun kohteena olleisiin tutkimustapauksiin.
- Kaikissa tapauksissa, joissa kohteena oli tietojärjestelmäprojekti, menetelmästä koettiin olevan hyötyä ja menetelmää esitettiin laajemmin testattavaksi eri tietojärjestelmäprojekteissa. Kiinnostusta herätti myös menetelmän käytön vaiheistus suhteessa tietojärjestelmäprojektin vaiheistukseen.
- Viimeisessä tapauksessa nousi esille johdon ja teknisten projektihenkilöiden välisen vuorovaikutuksen kehittyminen. Menetelmä tuki myös projektin sisäistä vuorovaikutusta ja läpinäkyvyyttä vaatimusmäärittelyiden suhteen.

Tutkimustapauksiin osallistui tutkijan lisäksi yhteensä yksitoista henkilöä. Osallistuneet henkilöt erosivat taustoiltaan toisistaan. Yhteistä tutkimuksiin osallistuneille henkilöille oli tietojärjestelmäalan koulutus ja kokemus. Kaikilla osallistuneilla oli jo pitkä, vuosien kokemus alan työtehtävistä. Eroa osallistuneiden henkilöiden suhteen tuli siinä missä roolissa he tutkimukseen osallistuivat. Osallistujien rooleja oli opiskelija (7), projektipäällikkö (2), tutkija / projektipäällikkö (1) ja yrityksen toimitusjohtaja (1). Osallistujien roolit tarjosi tutkimukselle riittävän hajonnan osallistujien suhteen. Kehitettävää jäi siinä, ettei yhteenkään tapaukseen saatu erilaisella koulutus- ja kokemuspohjalla olevaa henkilöä. Tutkimuksen kannalta olisi ollut kehittävää saada menetelmän käytöstä kokemusta tilanteessa, jossa teknisen projektipäällikön lisäksi tilaisuuteen olisi osallistunut selkeästi organisaation johtoa edustava henkilö. Tässä tutkimuksessa tämä rooli jäi tutkijan vastuulle. Yleisestikin olisi ollut eduksi jos tutkimustapauksissa kaksi - viisi olisi ollut mukana useampi henkilö.

5.3 Menetelmän kehitysvaiheet ja niihin vaikuttaneet tekijät

Menetelmä rakentui tutkimuksen aikana vaiheittain. Menetelmän kehittymiseen vaikuttivat eri tekijät. Näitä tekijöitä olivat tutkimustapauksista saadut havainnot sekä tutkimuksen kirjallisuudessa esitetyt perusteet. Näiden tekijöiden vaikutus menetelmän kehittymiseen on kuvattu taulukossa 2.

Tutkija käytti lähteenä myös omaa ammatillista kokemustaan sekä tutkijan Teknilliselle korkeakoululle Turvallisuusjohdon koulutusohjelmaan liittyen vuonna 2010 laatimaa tutkielmaa. Tutkielmassa tutkija käsitellee suojattavan tiedon tunnistamisen merkitystä puolustusvoimien turvaluokitelluissa hankinnoissa. Tutkielman mukaan turvaluokitelluissa hankinnoissa suojattava tieto on tunnistettava ja luokiteltava kustannustehokkaan ja turvallisen lopputuloksen saavuttamiseksi. (Simi, 2010.)

Taulukko 2 Menetelmän kehittämiseen vaikuttaneet tekijät

Menetelmän vaihe	**Perustelu**	**Lähteet**
1. Perustietojen dokumentointi	Menetelmään aloitettaessa osallistujien on kyettävä rajaamaan kohteena oleva tietojärjestelmä (TJ). Osallistujilla tulee olla käytettävissä TJ:n keskeiset vaatimusmäärittelyt. Osallistujien tulee kyetä vaikuttamaan näihin vaatimusmäärittelyihin.	NIST-julkaisut, VAHTI-ohjeet, Ahmad ym. (2014) Tutkijan ammatillinen kokemus, Havainnot tutkimustapauksista, erityisesti tapaukset 1 ja 4.

(jatkuu)

(Taulukko 2 jatkuu)

2. Tietotyyppien tunnistus	TJ tulee kyetä jakamaan loogisiin kokonaisuuksiin, tietotyyppeihin (TT).	NIST-julkaisut, Luvun 2.3 kirjallisuus, Havainnot tutkimustapauksista, Tutkijan ammatillinen kokemus (Simi, 2010).
3. Tietotyyppien luokittelu	Tunnistetut TT:t tulee luokitella luottamuksellisuuden (L), saatavuuden (S) ja eheyden (E) perusteella eri tasoille.	NIST-julkaisut, VAHTI-ohjeet, Havainnot tutkimustapauksista, Tutkijan ammatillinen kokemus (Simi, 2010).
4. Tulosten arviointi	Tunnistettujen TT:en kriittisen arvioinnin tarve kasvaa. Pelkästään L arviointi ei riitä, myös S ja E on merkitystä.	NIST-julkaisut, Havainnot tutkimustapauksista, Tutkijan ammatillinen kokemus (Simi, 2010)
	TT:t tulee muokata, jakaa sekä sanitoida. Toimenpiteillä on vaikutusta TJ:n vaatimusmäärittelyyn sekä TJ-projektin johtamiseen.	
5. Johtopäätökset vaatimuksista	Johtopäätöksissä tunnistetaan kriittiset tekijät tietoturvallisuuden eri osa-alueiden mukaisesti (L,S ja E).	Luvun 2.3 ja 3 kirjallisuus, Allen (2009), NIST-julkaisut, VAHTI-ohjeet, KATAKRI, Havainnot tutkimustapauksista, erityisesti tapaus 3, Tutkijan ammatillinen kokemus (Simi, 2010)
	Johtopäätöksissä tunnistetaan vaihtoehtojen jäännösriskit ja luodaan TJ-projektin johdolle edellytykset niitä koskevaan päätöksen tekoon.	
	Johtopäätöksissä esitetään konkreettiset TJ-projektin tietoturvallisuusvaatimukset, huomioiden eri vaihtoehdot ja niiden resurssitarpeet.	

Menetelmän ensimmäisen vaiheen havainnot perustuvat erityisesti tutkimustapauksien 1 ja 4 esille nostamiin havaintoihin. Tutkimustapauksessa 1 osallistujilla oli puutteellisista perustiedoista johtuen vaikeuksia päästä menetelmään sisään kuvitteellisessa toimintaympäristössä. Tutkimustapauksessa 4 puutteelliset perustiedot estivät tietotyyppinen täsmällisen tunnistamisen ja luokittelun. Perustietojen tunnistaminen esitetään myös NIST:n riskienhallinnan prosessissa lähtösyötteenä. Osallistujien valintaan vaikuttaa myös Ahmad ym. (2004) esittämä prosessin omistajien tunnistamisvaatimus. Prosessin omistajat tunnistamalla voidaan tiedon suojaamisen vastuu osoittaa oikealle taholle.

Menetelmän toisen, kolmannen ja neljännen vaiheen toiminnallinen toteutus kehittyi tutkimustapauksien myötä. Toteutus perustui pitkälti tutkijan ammatilliseen kokemukseen sekä NIST:n julkaisuissa esitettyihin tietotyyppien tunnistamisen ja luokittelun periaatteisiin. Toisen vaiheen taustalla oli tutkimuksen luvussa 2.3 käsitelty kirjallisuus. Kyseisen luvun kirjallisuus käsittelee organisaation tietämyksen rakennetta, hallintaa ja johtamista. Kolmannen vai-

heen toteutukseen vaikuttivat myös VAHTI-ohjeissa esitetyt luokitteluesimerkit.

Menetelmän viimeisen viidennen vaiheen kehitykseen, johtopäätöksien kirjoittamiseen, vaikuttivat tutkimustapausten yhteydessä saadut havainnot, erityisesti tutkimustapauksen 3 yhteydessä käyty keskustelu yrityksen toimitusjohtajan kanssa. Keskustelussa nousi esille liiketoiminnan tarpeista lähtevät konkreettisten vaihtoehtojen sekä resurssien arvioinnin tarpeet. Vaiheen kehitykseen vaikutti myös luvun 2.3 tietämyksen rakennetta, hallintaa ja johtamista käsittelevät perusteet joita sovellettiin luvun 3 riskienhallinnan kirjallisuuden periaatteita mukaillen. Luvun 3 kirjallisuudesta tulee erityisesti nostaa esille Allenin (2009) esittämä riittävän turvallisuuden käsite ja sen vaikutus johtopäätösten vaihtoehtojen kirjoittamiseen.

5.4 Yhteenveto tutkimuksen tuloksista

Tutkimustehtävänä oli etsiä käytännön johtamistyössä sovellettavaa menetelmää tunnistaa organisaation kokonaisarkkitehtuurin tai tietojärjestelmäprojektien tietoturvallisuusvaatimukset. Menetelmän tuli tukea liiketoimintajohdon, tietojärjestelmäarkkitehtien ja – asiantuntijoiden välistä viestintää ja kommunikaatiota. Menetelmän tuli myös tukea organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista. Tutkimustehtävään haettiin vastauksia seuraavien tutkimuskysymyksien kautta:

- Miten luokittelua voidaan hyödyntää organisaatioiden kokonaisarkkitehtuurin projekti- ja tietojärjestelmä suunnittelussa?
- Miten luokitteluprosessi vaiheistetaan ja määritellään parhaan kustannustehokkuuden saavuttamiseksi?
- Miten luokitteluprosessissa varmistetaan tietoturvallisuuden eri osa-alueiden, luottamuksellisuuden, saatavuuden ja eheyden vaatimusten huomioiminen?

5.4.1 Tutkimustapausten valinta ja niistä saadut havainnot

Viisi tutkimustapauksta valittiin vuoden 2016 kevään ja kesän aikana tutkijan työtehtäviin liittyvistä soveltuvista projekteista. Tapaukset erosivat toisistaan ja mahdollistivat sitä kautta vertailun menetelmän käytön suhteen.

Jokainen tutkimustapaus kehitti menetelmää. Kaikkia kehitysehdotuksia ei voitu huomioida tutkimuksen resursseista johtuen. Tällaisia kehitysehdotuksia olivat pääasiassa aputaulukoihin liittyvät tarkemmat määrittelyesitykset. Tässä tutkimuksessa nämä taulukot toimivat ajatusten herättäjinä sekä tapauskohtaisina yhteisen näkemyksen muodostajina. Menetelmää laajemmin käytettäessä näitä taulukoita kannattaa tarkastella kriittisesti.

Kokonaisuutena palaute oli erittäin positiivista ja rakentavaa. Menetelmää pidettiin loogisena ja sen avulla koettiin saatavan tukea kohteen projektisuunnitteluun suhteellisen lyhyessä ajassa.

Menetelmän näkökulma oli kaikille osallistujille uusi ja vaati tutkijalta tarkaa alustusta sekä ohjausta menetelmää käyttöön sovellettaessa. Kaikissa tutkimustapauksissa esitettiin menetelmän laajempaa testausta ja kehittämistä eri tietojärjestelmäprojekteissa. Menetelmä tuotti palautteen perusteella kokonaisvaltaisen näkemyksen tietojärjestelmäprojektin vaatimusmäärittelystä sekä kehitti johdon ja ICT-asiantuntijoiden välistä vuorovaikutusta.

Menetelmän käytön kriittisinä vaatimuksina nousi esille perustietojen dokumentointi, osallistujien valinta sekä menetelmän käytön oikea-aikaisuus.

5.4.2 Tutkimuksen tulokset

Tutkimuksen tuloksena pystyttiin kehittämään menetelmä joka tukee organisaation kokonaisarkkitehtuuri- tai tietojärjestelmäprojektin tietoturvallisuusvaatimuksien tunnistamista. Asetetut tutkimuskysymykset kyettiin johdonmukaisesti toteuttamaan tutkimuksen eri vaiheissa ja ne tuottivat tutkimustehtävään vaaditut vastaukset.

Tutkimustapauksista saatujen havaintojen perusteella tutkimuksessa kehitetty menetelmä tukee organisaation johdon ja tietojärjestelmäasiantuntijoiden vuorovaikutusta. Menetelmästä on hyötyä organisaation kokonaisarkkitehtuurin ja tietojärjestelmäprojektien tietoturvallisuusvaatimusten tunnistamisessa. Organisaatioiden välisen viestinnän turvallisuusvaatimusten turvaamisesta menetelmän avulla ei tutkimuksen yhteydessä saatu suoria tuloksia. Välillisesti voidaan arvioida, että johdonmukaisesti ja dokumentoidusti toteutettujen tietoturvallisuusvaatimusten tunnistaminen edesauttaa organisaatioiden välisen viestinnän turvallisuutta. Tätä johtopäätöstä tukee myös tutkijan aiemmat työtehtävistä saamat kokemukset.

Menetelmää tärkeämpinä havaintoina nousi esille se, että tiedon tunnistaminen ja luokittelu osana kokonaisarkkitehtuuri- tai tietojärjestelmäprojektin vaatimuksia oli kaikille osallistujille uusi asia. Palautteen perusteella näkökulmaa pidettiin kuitenkin hyödyllisenä ja sen nähtiin tukevan kokonaisvaltaista johtamista. Tutkimustapausten yhteydessä eri tietotyyppejä arvioitaessa päästiin myös konkreettiseen vertailuun eri tietoturvallisuuden osa-aluiden suhteen. Tutkimustapauksessa 3 asia nousi erityisesti esille; yrityksen liiketoiminnan jatkuvuus perustuu saatavuuden ja eheyden vaatimuksiin, joihin luottamuksellistenkin tietojen käsittely tulee sopeuttaa.

Menetelmän viimeinen vaihe vaatii menetelmän ohjaajalta perehtyneisyyttä tietoturvallisuuden johtamiseen. Ohjaajan tulee kyetä muodostamaan menetelmän aineistoon perustuen ratkaisuesitys vaihtoehtoineen. Ratkaisuesityksessä tulee huomioida myös karkealla tasolla vaadittavat resurssit. Ratkaisuesityksessä tulee kyetä soveltamaan Suomen

kansallisia tietoturvallisuusohjeita käytäntöön ja kyettävä niiden perusteella tuottamaan kohteena olevan organisaation tai tietojärjestelmän kokonaisvaatimukset huomioiva riskienarviointiin perustuva ratkaisu. Tutkimuksessa ei huomioitu ratkaisuesitysten perusteita, vaan ne pohjautuivat tutkijan ammattitaitoon ja kokemukseen. Ratkaisuesitysten perustelu riskienarviointiin, ohjaaviin normeihin ja standardeihin perustuen on laaja oman erillisen tutkimuksen arvoinen laaja kokonaisuus.

6 JOHTOPÄÄTÖKSET JA POHDINTA

Tutkimuksen tavoitteena oli kehittää organisaation kokonaisarkkitehtuurin tai tietojärjestelmäprojektien tietoturvallisuuden johtamista tukeva menetelmä. Menetelmän avulla pyrittiin tunnistamaan organisaation kokonaisarkkitehtuurin tai tietojärjestelmäprojektin erilaiset tietotyypit ja arvioimaan niihin kohdistuvia tietoturvallisuuden vaatimuksia. Menetelmän tavoitteena oli tukea liiketoimintajohdon ja ICT-alan asiantuntijoiden välistä kommunikaatiota sekä tukea organisaatioiden välisen viestinnän turvallisuusvaatimusten tunnistamista.

Kyseessä oli konstruktiivinen tutkimus, jossa käytettiin suunnittelutieteellistä menetelmää. Tutkimustehtävän kohteena ollut menetelmä rakentui tutkimuksessa käsiteltävän kirjallisuuden ja tutkimuksen suunnittelutieteellisen menetelmän soveltamisen myötä saatujen havaintojen perusteella. Menetelmän rakentumista tukivat myös tutkijan työelämästä saamat kokemukset.

Tutkimuksen empiirinen materiaali koottiin viidestä erillisestä tutkimustapauksesta. Kussakin tapauksessa tutkittiin menetelmän soveltuvuutta ja vaiheistusta sekä havainnoitiin kehittämistarpeita. Tutkimustapauksista kerättiin empiiriset havainnot kyselylomakkeella ja sitä täydentävällä haastattelulla. Menetelmää kehitettiin kunkin tutkimustapauksen kokemusten perusteella. Tutkimustapausten havainnot koottiin yhteen ja analysoitiin tutkimuksen päätteeksi.

Tutkimustapaukset valittiin tutkijan ajankohtaisiin työtehtäviin liittyvistä projekteista. Projektien salassa pidettävästä materiaalista johtuen tutkimustapausten tarkkoja havaintoja ei voitu tässä pro gradu -tutkielmassa raportoida. Tästä aiheutui riski tutkimuksen luotettavuuden arvioinnille. Tätä riskiä pyrittiin vähentämään raportoimalla tutkimuksen liitteissä kaikki tutkimuskyselyyn vastanneiden vastaukset sekä niistä tehdyt johtopäätökset.

Tutkimuksen tulosten perusteella tutkimuksessa kehitetty menetelmä vastasi sille asetettuja vaatimuksia. Menetelmä kehittyi tutkimustapausten myötä ja tutkimustapausten erilaisuus tuki tätä kehitystyötä. Tutkimustapausten valintaa voi pitää onnistuneena.

Tutkimustapauksiin osallistui yhteensä 11 henkilöä joista seitsemän (7) ensimmäiseen tapaukseen. Muihin tapauksiin osallistui kuhinkin yksi (1) henki-

lö. Osallistuneet henkilöt edustivat pääsääntöisesti ICT-alan teknisen asiantuntijan tai projektipäällikön näkökulmaa. Ainoastaan tutkimustapauksessa 3 osallistuja tarkasteli menetelmää organisaation johtamisen näkökulmasta. Tutkimuksen luotettavuutta olisi parantanut se, että tutkimustapauksiin 2 - 5 olisi osallistunut useampia henkilöitä ja että he olisivat edustaneet tasapuolisesti molempia em. näkökulmia.

Ensimmäisessä tapauksessa menetelmän keskeneräisyys, puutteelliset termien määritelmät ja osin menetelmän soveltaminen kuvitteelliseen tietojärjestelmäprojektiin aiheuttivat haasteita. Myöhemmissä tutkimustapauksissa osallistuneet henkilöt pitivät menetelmän käyttöä helppona ja loogisena.

Menetelmän toiminnallisia ratkaisuja tärkeämmäksi havainnoksi tutkimuksessa nousi esille se, että itse tiedon tunnistamisen näkökulma oli kaikille tutkimukseen osallistuneille henkilöille uusi. Havainto tukee tietämyksen hallintaa koskevan kirjallisuuden havaintoja. Kyseissä kirjallisuudessa tietämyksen tunnistamista ja hallintaa organisaatioissa pidettiin uutena sosiaalisen median ja tietojärjestelmien mahdollistaman viiveettömän maailman laajuisen tiedonsiirron nostamana trendinä. Tietämyksen tunnistaminen ja hallinta tietojärjestelmäprojekteissa voisi olla tämän tutkimuksen havaintojen perusteella hyödyllinen jatkotutkimuksen aihe.

Tiedon tunnistamisen näkökulma ei herättänyt osallistujissa kritiikkiä vaan kaikki pitivät näkökulmaa hyödyllisenä ja jatkokehityksen arvoisena. Palautteessa toistuivat kokonaisvaltaista vaatimusmäärittelyä, -johtamista sekä ongelmanratkaisua tukevat kommentit.

Menetelmän käytön kannalta nousi myös esille menetelmän soveltamisen oikea-aikaisuus, riittävien perustietojen tunnistaminen sekä oikeassa roolissa toimivat osallistujat. Menetelmä tuottaa parhaan tuloksen, kun sitä hyödynnetään projektien alkuvaiheessa. Organisaatioiden kokonaisarkkitehtuuri- tai tietojärjestelmäprojektien vaatimusmäärittelyiden on oltava käytettävissä ja osallistujilla pitää olla tieto ja ymmärrys kohteena olevan järjestelmän kokonaistavoitteista. Ilman näitä perusteita menetelmä ei tuota riittävän yksityiskohtaisia tuloksia.

Tutkimustapauksissa nousi esille myös aito tietoturvallisuuden eri osa-alueiden vertailu. Erityisesti yrityksen kokonaisarkkitehtuuria arvioitaessa havainto tiedon saatavuuden ja eheyden kriittisestä merkityksestä yrityksen liiketoiminnan jatkuvuudelle oli mielenkiintoinen ja konkreettinen. Tutkimustapauksen yhteydessä yrityksen luottamuksellisten tietojen käsittelystä laadittiin esitys em. liiketoimintavaatimuksiin perustuen. Ratkaisuesityksessä kyettiin huomioimaan tietoturvallisuuden osa-alueet ja tutkimustapauksen yhteydessä menetelmä osoitti vahvuutensa.

Menetelmän käytön viimeinen vaihe eli johtopäätösten teko, perustui Suomen kansallisten turvallisuusvaatimusten VAHTI-ohjeiden, KATAKRIn ja näiden taustalla olevien standardien soveltamiseen sekä riskienarviointiin. Riskienarvioinnin tavoitteena oli räätälöidä kohteen eri vaatimukset huomioiden soveltuvat vaihtoehtoiset tietoturvallisuuden ratkaisuesitykset sekä arvioida karkealla tasolla vaihtoehtojen resurssitarpeet. VAHTI-ohjeet tai KATAKRI ei-

vät anna suoria vaatimuksia vaan niitä tulee kyetä soveltamaan. Niiden tietoturvallisuus vaatimukset ovat myös hyvin laaja-alaisia lähtien tietoturvallisuuden hallinnollisesta johtamisesta sekä tilaturvallisuudesta ja päätyen tekniseen tietoturvallisuuteen. Menetelmän soveltaminen edellyttää menetelmän käyttöön ja tietoturvallisuuteen perehtynyttä ohjaajaa. Erityisesti johtopäätösosio vaatii ohjaajalta kokemusta.

Tutkijan kannalta menetelmän keskeisin etu oli sen tarjoama kokonaisvaltainen näkökulma tarkastelun kohteena olevaan tietojärjestelmään. Kokonaisvaltainen näkökulma tukee myös organisaation johdon ja ICT ammattilaisten välistä viestintää.

Jatkotutkimuksissa menetelmää voisi soveltaa tietojärjestelmien vaatimusmäärittelyihin. Tässä tutkimuksessa ei syvennytty luokittelun ja riskienarvioinnin perusteella määritettävien turvallisuusvaatimuksien perusteluihin. Myöskään määritettävien turvallisuusvaatimusten mittaamista eri näkökulmista ei tässä tutkimuksessa tarkasteltu. Nämä aiheet voisivat myös soveltua jatkotutkimusaiheiksi.

LÄHTEET

Ahmad, A., Bosua, R., & Scheepers, R. (2014). Protecting organizational competitive advantage: A knowledge leakage perspective. *Computers & Security,* 42, 27-39.

Aljafari, R., & Sarnikar, S. (2009). A framework for assessing knowledge sharing risks in interorganizational networks. Teoksesta *AMCIS 2009, (s.* 572).

Allen, J.H. (2009). *How Much Security Is Enough.* Haettu 26.5.2016 osoitteesta http://resources.sei.cmu.edu/asset_files/WhitePaper/2013_019_001_295906.pdf.

Barney, J. (1991). Firm resources and sustained competitive advantage. *Journal of management, 17(1),* 99-120.

Baskerville, R. (1991). Risk analysis: an interpretive feasiblity tool in justifying information systems security. *European Journal of Information Systems,* 1(2), 121-130.

Becerra-Fernandez, I., Gonzales, A., & Shabherwal, R. (2004). *Knowledge Management and KM Software Packages.* Prentice Hall.

Center for Cyber and Information Security. (2014). *Cybersecurity versus information security.* Haettu 20.06.2016 osoitteesta https://ccis.no/cyber-security-versus-information-security/.

Desouza, K. C., & Vanapalli, G. K. (2005). Securing knowledge in organizations: lessons from the defense and intelligence sectors. *International Journal of Information Management*, 25(1), 85-98.

O'Donoghue, N., & Croasdell, D. T. (2009). Protecting knowledge assets in multinational enterprises: a comparative case approach. *VINE, 39(4),* 298-318.

Everetts, R. (2016). Enterprise Information security and Risk Management kurssi [luento] Information Resources Management Collage/ National Defence University 8.2.2016.

Fagerström, N. & Nelskylä, L. (2016). Sydänpotilas hengenvaarassa teho-osastolla - kirurgia ei voitu Soneran heikon mobiiliverkon takia tavoittaa HUS:ssa. *Yleisradio verkkouutinen 8.6.2016.* Haettu 10.6.2016 osoitteesta http://yle.fi/uutiset/sydanpotilas_hengenvaarassa_teho-osastolla__kirurgia_ei_pystytty_soneran_heikon_mobiiliverkon_takia_tavoittamaan_husssa/8939118.

Federal Information Processing Standards Publication, Computer Security Division. (2004). *Standards for Security Categorization of Federal Information and Information Systems.* Gaithersburg: MD. Haettu 25.5.2016 osoitteesta http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

Freeze, R., & Kulkarni, U. (2005, January). Knowledge management capability assessment: validating a knowledge assets measurement instrument. Teoksesta *38th Annual Hawaii International Conference on System Sciences* (s. 251a-251a). IEEE.

Gold, A., Malhotra, A. & Segars, A. (2001). Knowledge Management: An Organizational Capabilities Perspective. *Journal of Management Information Systems,* 18(1), 185-214.

Hevner, A. , March, S. , Park, J., & Ram, S. (2004). Design science in information systems research. *MIS quarterly,* 28(1), 75-105.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2013). *Tutki ja kirjoita* (15.-17. uud. painos). Porvoo: Bookwell.

Hulitt, E. & Vaughn, R. (2010). Information system security compliance to FISMA standard: a quantitative measure. *Telecommunication Systems*, 45(1-2), 139-152.

Hytönen, S., & Kolehmainen, J. (2003). *Tietämyksenhallinta uusmedia-ja ohjelmistoyritysten innovaatiotoiminnassa.* Tampereen yliopisto.

Iivari, J., Hirschheim, R. & Klein. H. (2004). Towards a distinctive body of knowledge for Information Systems experts: coding ISD process knowledge in two Is journals. *Information systems journal* 14.4 (2004): 313-342.

Ilvonen, I., Jussila, J., Kärkkäinen, H. & Päivärinta, T. (2015). Knowledge security risk management in contemporary companies - toward a proactive approach. Teoksesta *System Sciences (HICSS), 2015 48th Hawaii International Conference on* (s. 3941-3950). IEEE.

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers,* 9(5), 493-504.

JUHTA - Julkisen hallinnon tietohallinnon neuvottelukunta. (2012). *JHS 174 ICT-palvelujen palvelutasoluokitus.* Haettu 5.6.2016 osoitteesta http://www.jhs-suositukset.fi/suomi/jhs174.

Jarvenpaa, S. L., & Majchrzak, A. (2008). Knowledge collaboration among professionals protecting national security: Role of transactive memories in ego-centered knowledge networks. *Organization Science,* 19(2), 260-276.

Kaisler, S.H., Armour, F. & Valivullah, M. (2005). Enterprise Architecting: Critical Problems. Teoksessa *38th Hawaii International Conference on System Sciences, (s.* 224b) IEEE.

National Institue of Standards and Technology, Computer Security Division. (2004). *Standards for Security Categorization of Federal Information and Information Systems. Federal Information Processing Standards Publication 199.* Gaithersburg: MD. Haettu 23.11.2016 osoitteesta http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

National Institue of Standards and Technology, Computer Security Division. (2006). *Information Security Handbook: A Guide for Managers. Recommendations of the National Institute of Standards and Technology. Special Publication 800-100.* Gaithersburg: MD. Haettu 24.5.2016 osoitteesta http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

National Institue of Standards and Technology, Computer Security Division. (2008). *Guide for Mapping Types of Information and Information Systems to Security Categories. Special Publication 800-60 Volume I Revision 1.* Gaithersburg: MD. Haettu 25.5.2016 osoitteesta

http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf.

National Institue of Standards and Technology, Computer Security Division. (2008). *Appendices to Guide for Mapping Types of Information and Information Systems to Systems Categories. Special Publication 800-60 Volume II Revision 1.* Gaithersburg: MD. Haettu 25.5.2016 osoitteesta http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf.

National Institue of Standards and Technology, Computer Security Division. (2010). *Guide for Applying the Risk Management Framework to Federal Information Systems. A Security Life Cycle Approach. Special Publication 800-37 Revision 1.* Gaithersburg: MD. Haettu 25.5.2016 osoitteesta http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf.

National Institue of Standards and Technology, Computer Security Division. (2011). National Checklist Program for IT Products-Guidelinses for Checklist Users and Developpers. Special Publication 800-70 Revision 2. Gaithersburg: MD. Haettu 25.8.2016 osoitteesta http://csrc.nist.gov/publications/nistpubs/800-70-rev2/SP800-70-rev2.pdf.

National Institue of Standards and Technology, Computer Security Division. (2011). Assessing Security and Privacy Controls in Federal Information Systems and Organizations. Special Publication 800-53A Revision 4. Gaithersburg: MD. Haettu 25.8.2016 osoitteesta. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf.

National Institue of Standards and Technology, Computer Security Division. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations. Special Publication 800-53 Revision 4.* Gaithersburg: MD. Haettu 25.5.2016 osoitteesta http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

Manhart, M., & Thalmann, S. (2013). An integrated risk management framework: measuring the success of organizational knowledge protection.

Mumford, E. (2000). A socio-technical approach to systems design. *Requirements Engineering*, 5(2), 125-133.

Mumford, E. (2006). The story of socio-technical design: Reflections on its successes, failures and potential. *Information Systems Journal*, 16(4) 317-342.

Padyab, A. M., Päivärinta, T., & Harnesk, D. (2014). Genre-based assessment of information and knowledge security risks. Teoksessa *2014 47th Hawaii International Conference on System Sciences* (s. 3442-3451). IEEE.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chatterjee, S. (2007). A design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems,* 24(3) s. 45-77.

Peffers, K., Tuunanen, T., Gengler, C.E., Rossi, M., Hui, W., Virtanen, V. & Bragge, J. (2006). The Design Science Research Process: A Model for Producing and Presenting Information Systems Research. Teoksessa *1st International Conference on Design Science in Information Systems and Technology* (DESRIST 2006) (s. 83-106).

Pulkkinen, M. & Kapraali, L. (2015). Collaborative EA Information Elicitation Methdo: The IEM for Business Architecture. Teoksessa *2015 IEEE 17ht Conference on Business Informatics* (s. 64-71). IEEE.

Puolustusministeriö (2015). *KATAKRI 2015 - Tietoturvallisuuden auditointityökalu viranomaisille.* Haettu 24.5.2016 osoitteesta http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf .

Puolustusvoimat *WISM II projektin esittely video*. Haettu 5.8.2016 osoitteesta https://www.youtube.com/watch?v=9v1fFIHRWGE&app=desktop

Pääesikunta (2016). *Hallintopäätös Majuri Jarmo Simin tutkimuslupahakemukseen AM10032 24.5.2016.*

Sadeniemi, M., & Vesikansa, J (1985). *Nykysuomen sanakirja.*(9. painos). Porvoo, Helsinki: Werner Söderström Osakeyhtiö.

Seppänen, V. (2014). *From Problems to Critical Success Factors of Enterprise Architecture Adoption.* Jyväskylän yliopisto. Väitöskirja.

Shedden, P., Scheepers, R., Smith, W., & Ahmad, A. (2011). Incorporating a knowledge perspective into security risk assessments. *Vine, 41(2),* 152-166.

Simi, J. (2010). Puolustusvoimien turvaluokiteltua tietoa sisältävien kotimaisten hankintojen turvallisuus. *Turvallisuusjohdon koulutusohjelma, Teknillinen korkeakoulu. Tutkielma.*

Suomen eduskunta (1999). *Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa* 1.7.2010/681 haettu 30.8.2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/2010/20100681.

Suomen eduskunta, (2010). *Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta* 12.11.1999/1030 haettu 30.8.2016 osoitteesta http://www.finlex.fi/fi/laki/ajantasa/1999/19991030.

Tolvanen, J-P. (1998). *Incremental Method Engineering with Modeling Tools, Theoretical Principles and Empirical Evidence.* Jyväskylän yliopisto. Väitöskirja.

Trkman, P., & Desouza, K. C. (2012). Knowledge risks in organizational networks: An exploratory framework. *The Journal of Strategic Information Systems, 21(1),* 1-17.

Turvallisuuskomitean sihteeristö (2013). *Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013.* Haettu 10.10.2016 osoitteesta http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit.

Valtionvarainministeriö (2008). *VAHTI -ohje 8/2008 - Valtionhallinnon tietoturvasanasto.* VM/47/01/2008. Helsinki: Edita Prima.

Valtionvarainministeriö (2010). *VAHTI -ohje 2/2010 - Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta.* VM/2029/00.00.00/2010. Tampere: Juvenes Print.

Valtionvarainministeriö (2010). *VAHTI -ohje 3/2010 - Sisäverkkoohje.* VM/2312/00.00.00/2010. Tampere: Juvenes Print.

Valtionvarainministeriö (2011). *VAHTI -ohje 3/2011 - Valtion ICT-hankintojen tietoturvaohje.* VM/1982/00.00.00/2011. Tampere: Juvenes Print.

Valtionvarainministeriö (2012). *VAHTI -ohje 2/2012 - ICT -varautumisen vaatimukset.* VM/1619/00.00.00/2012. Tampere: Juvenes Print.

Valtionvarainministeriö (2012). *VAHTI -ohje 3/2012 - Teknisen ICT-ympäristön tietoturvataso-ohje.* VM/1991/00.00.00/2012. Tampere: Juvenes Print.

Valtionvarainministeriö (2012). *Suojattavien kohteiden (tietojärjestelmien) tärkeysluokittelijan käyttöohje 1.11.2012 VAHTI 3/2012.* Haettu 31.5.2016 osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=4769e61c-e581-40c2-bf71-dd4cd80d6b5f&groupId=10128.

Valtionvarainministeriö (2012). *Tärkeysjärjestys apuväline - exel työkalu.* Versio 1.0 01.11.2012. Haettu 31.5.2016 osoitteesta https://www.vahtiohje.fi/web/guest/tyokalut-ja-muut-ohjeen-kayttoonottoa-tukevat-apuvalineet.

Valtionvarainministeriö (2012). *Järjestelmien väliset riippuvuudet - exel työkalu.* Versio 1.0 01.11.2012. Haettu 31.5.2016 osoitteesta https://www.vahtiohje.fi/web/guest/tyokalut-ja-muut-ohjeen-kayttoonottoa-tukevat-apuvalineet.

Valtionvarainministeriö (2013). *VAHTI -ohje 1/2013 - Sovelluskehityksen tietoturvaohje.* VM/144/00.00.00/2013. Juvenes Print.

Valtionvarainministeriö (2013). *VAHTI -ohje 2/2013 - Toimitilojen tietoturvaohje.* VM/1041/00.00.00/2013. Tampere: Juvenes Print.

Valtionvarainministeriö (2013). *VAHTI -ohje 5/2013 - Päätelaitteiden tietoturvaohje.* VM/2723/00.00.00/2013. Juvenes Print.

Valtionvarainministeriö (2014). *VAHTI -ohje 2/2014 - Tietoturvallisuuden arviointiohje.* VM/2423/00.00.00/2014. Juvenes Print.

Valtionvarainministeriö (2015). *VAHTI -ohje 2/2015 - Ohje salauskäytännöistä.* VM/2204/00.00.00/2015. Lönnberg Print & Promo.

LIITE 1 MENETELMÄLOMAKE

Menetelmä toteutettiin seuraavalla sivulla olevan lomakkeen avulla. Etenemisjärjestys oli seuraava:

1. Tapauksen perustietojen dokumentointi
    a. Tietojärjestelmän nimi
    b. Käyttötarkoitus
    c. Käyttäjät
    d. Rajapinnat
    e. Merkitys organisaatiolle
2. Tietotyyppien tunnistus
    a. Tunnistetaan tietotyypit
    b. Luokitellaan tietotyypit
    c. Huomioidaan mahdolliset kansainväliset tietoturvavaatimukset
3. Tarkastetaan ja analysoidaan luokittelun lopputulokset
    a. Tarkastetaan erityisesti kokonaisuudessaan korkealle tasolle luokiteltujen tietotyyppien rakenne. Analysoidaan mahdollisten uusien tietotyyppien tarve.
    b. Tarkastetaan tietotyyppien harmonisuus. Analysoidaan mahdollinen tarve jakaa tietojärjestelmän tietotyypit useampaan järjestelmään.
4. Kirjoitetaan johtopäätökset ja analyysi tietojärjestelmän tietoturvavaatimuksista.

Tietojärjestelmän tärkeyttä arvioitaessa käytettiin seuraavaa VAHTI 3/2012 ohjeeseen sekä JHS174 perustuvia määritelmiä:

- 1-Vähäinen merkitys käyttökatkos voi kestaa viikon tai pitempään,
- 2-Jonkin verran tärkeä käyttökatkos voi kestää 3 vrk - viikon,
- 3-Tärkeä käyttökatkos voi kestää 7 tunnista - vrk:teen,
- 4-Erittäin tärkeä käyttökatkos voi kestää 2 - 7 tuntia,
- 5-Elintärkeä käyttökatkos voi kestää enintään 2 tuntia.

(jatkuu)

(Liite 1 jatkuu)

TIETOJÄRJESTELMÄN LUOKITTELUMATRIISI (tietoturvallisuus)

1) Dokumentoi tietojärjestelmän perustiedot

Tietojärjestelmän nimi	
Tietojärjestelmän käyttötarkoitus	
Tietojärjestelmän käyttäjät	
Tietojärjestelmän rajapinnat	
Tietojärjestelmän tärkeys organisaatiolle tai palvelua käyttävälle kumppanille.	*(Nro 1 - 5)*

2) Tunnista ja luokittele tietojärjestelmän tietotyypit

Tietotyyppi		L	Kuvaus	S	Kuvaus	E	Kuvaus	KV
Tietotyyppi 1		N		K		M		esim. EU
Tietotyyppi 2		K		N		M		
Tietotyyppi …n		M		K		N		

3) Luokittelun arviointi

Tarkastetaan laadittu luokittelu. Onko kaikki tietotyypit tunnistettu? Arvioidaan tunnistetut tietotyypit. Kiinnitetään huomio erityisesti niihin tietotyyppeihin jotka ovat kaikkien osa-alueiden suhteen korkealla tasolla. Pitääkö näitä tietotyyppejä jakaa tai sanitoida. Ovatko tunnistetut tietotyypit jakautuneet selkeästi korkean ja matalan tason tietotyyppeihin. Sisältyykö samaan tietojärjestelmään sekä hallinnollinen, että operatiivinen tietojärjestelmä. Onko ratkaisu toteuttamiskelpoinen?

4) Johtopäätökset tietojärjestelmän turvallisuusvaatimuksista

Laaditaan esitys järjestelmän tietoturvallisuuden jatkosuunnitteluun. Jatkosuunnittelun perusteina ovat kansalliset normit ja ohjeet (VAHTI, KATAKRI) sekä mahdolliset KV sopimukset, Standardit ja muut vaatimukset. Esitykset mahdollisista tietoturvallisuusauditointi tai akreditointi tarpeista. Esitetään perusteet yhteistoimintaan kumppanien kanssa. Esitetään eri vaihtoehdot ja arvioidaan vaihtoehtojen resurssitarpeet. Esitetään ja arvioidaan eri vaihtoehtoihin sisältyvät jäännösriskit.

LIITE 2 TIETOTYYPPIEN LUOKITTELUN APUTAULUKKO

Alla olevaan taulukkoon on koottu luokittelun apuna käytetyt esimerkit.

	Luottamuksellisuus - (L)	Saatavuus - (S)	Eheys - (E)
Korkea (K), esimerkkejä	Tieto julkista - STI. Paljastuessaan tuottaa riskin yhteiskunnan infrastruktuurin, tietovarannon jatkuvuudelle, luottamuksellisuudelle tai maineelle.	Palvelu käytössä 24/7/365. Varalaitteet on oltava välittömästi saatavilla.	Aiheuttaa vakavan riskin useamman ihmisen terveydelle, aiheuttaa organisaation päätehtävän jatkuvuudelle tai maineelle tai resursseille erittäin vakavan riskin. Palvelun suoritukseen liittyy merkittävä vaikutusalueelliselle palvelutoiminnalle.
Normaali (N), esimerkkejä	Tieto julkista - STIII. Nopeasti vanheneva < STII tieto. Paljastuessaan tuottaa riskin yrityksen liiketoiminnan jatkuvuudelle, luottamuksellisuudelle tai maineelle. Toteutuessaan aiheuttaa laaja-alaisia tai ajallisesti pitkävaikutteisia liiketoiminnan menetyksiä.	Palvelu on käytössä laajemmin arkipäivinä ja myös viikonloppuisin, esimerkiksi arkisin 7-21,la-su 9-18. Laitteen tai palvelun normaali käyttövarmuus riittää kun varaosien, saatavuus tai palveluvaste sekä tietojen varmennus on varmistettu.	Aiheuttaa riskin yhden tai useamman henkilön terveydelle, aiheuttaa huomattavan riskin organisaation toiminnalle, maineelle tai resursseille. Palvelun suoritukseen liittyy merkittävä rajatulle alueelle riski tilatulle palvelutoiminnalle.
Matala (M), esimerkkejä	Tieto julkista - STIV. Nopeasti vanheneva < STIII tieto. Paljastuessaan tuottaa riskin yrityksen liiketoiminnalle yksittäisen kumppanin tai liiketoimintasektorin jatkuvuudelle, luottamuksellisuudelle tai maineelle. Toteutuessaan aiheuttaa riskin yksittäisen hankkeen kilpailutukselle tai organisaation liiketoiminta osa-alueelle.	Palvelu käytössä virka/toimistoaikana. Esimerkiksi arkipäivinä 7 - 17. Laitteen tai palvelun normaali käyttövarmuus on riittävä, ei erityisiä varmennus-, palautus- tai ylläpitovaatimuksia.	Ei merkittävää henkilöstö vaikutusta tai merkitystä organisaation toiminnalle, maineelle tai resursseille. Palvelun suoritus ei aiheuta merkittävää riskiä tilatulle palvelutoiminnalle.
Kansainväliset tietoturvavaatimukset (KV)	Kirjataan sopimuksen tiedot ja mihin kansainväliseen yhteisöön tai maahan viitataan (esim. EU)		
Ei voida valita (N/A)	Perustelu	Perustelu	Perustelu

Esimerkkejä valitessa on hyödynnetty VAHTI-ohjeita. Taulukko päivitettiin kunkin tapauksen luokittelun yhteydessä. Taulukon tavoitteena oli ohjata menetelmän käyttäjää valitsemaan tapaukseen soveltuvia luokittelutasoja. Luokittelut eivät eri tapausten välillä ole eksaktisti vertailukelpoisia.

LIITE 3 ANALYYSI TUTKIMUSTAPAUKSISTA

Tähän liitteeseen on koottu analyysi tutkimustapauksista. Analyysi perustuu tutkimuskyselyyn, -haastatteluun sekä tutkijan näkemykseen tutkimustapauksesta.

Tutkimustapaus 1 Harjoitus

Kokonaisarvio

- Positiivinen palaute ja rakentavia kehitysehdotuksia. Toteutettiin ryhmätyönä joten tutkijan osallistuminen ja ohjaus oli kaikkein vähäisin. Tällä oli selkeästi vaikutusta menetelmän käytön hallintaan. Tästä syystä palautteessa nousi esille selkeitä menetelmän käyttöä kehittäviä esityksiä.

Vahvuudet

- Nostaa esille uusia näkökulmia ja tukee johtamisen sekä tietoturvallisuuden prosessien ohjausta. Auttaa tunnistamaan suojattavan tiedon.
- Menetelmän rakenne on looginen sekä selkeä ja tuki osaltaan menetelmän käyttöä.
- Tietorakenteiden tunnistamisesta koettiin olevan hyötyä soveltuvien tuotantoympäristöjen suunnittelussa ja valinnassa.

Kehityskohteet

- Käsitteet ja termit tulee avata ja määritellä tarkemmin.
- Menetelmän perustietojen rajaaminen on tärkeää, kohteena olevasta liiketoimintaosa-alueesta tulee olla kokemusta.
- Menetelmän käyttö edellyttää harjoittelua ja kokemusta. Luokittelu on hyvä vaiheistaa ja syventää sitä useissa iterointikierroksissa. Käyttö edellyttää menetelmän hallitsevaa ohjaajaa.
- Menetelmä tulisi liittää tietojärjestelmien suunnitteluprosesseihin ja käyttää prosessien kaikissa vaiheessa. Erityisesti suunnitteluprosessin alku on tärkeä.

Toteutetut muutokset

- Lomakkeeseen lisättiin perustieto osiot ja laadittiin luokittelua helpottava esimerkkitaulukko. Taulukossa on esimerkkejä tietoturvallisuuden eri osa-alueiden luokittelusta.

(jatkuu)

(Liite 3 jatkuu)

Tutkimustapaus 2 Puolustusvoimien operatiivinen (OP) tietojärjestelmäprojekti

Kokonaisarvio

- Positiivinen palaute ja rakentavia kehitysehdotuksia. Projektihenkilö hallitsi tietoturvallisuuden peruskäsitteet ja oli perehtynyt aiheeseen. Helpotti menetelmän käyttöä.

Vahvuudet

- Menetelmä on hyödyllinen ja verrattuna moniin muihin "projektityökaluihin" helppo- ja nopea soveltaa käyttöön. Käsitteet olivat selkeitä. Menetelmä tuotti lyhyessä ajassa merkittävää lisätietoa projektin suunnitteluun.
- Prosessi nosti esille merkityksellisiä kokonaisuuksia. Auttoi avaamaan ongelmakohtia.

Kehityskohteet

- Rauhan- ja sodanajan tietojärjestelmien arviointi on vaikeaa samalla mittarin asteikolla.
- Tietojärjestelmä rakentuu ohjelmistoista, sovelluksista ja laitteista "raudasta". Arvioinnin aputaulukko huomioi ohjelmistojen ja sovellusten osuuden, mutta soveltuu huonosti laitteiden arviointiin. Arvioinnin aputaulukkoa tulee tältä osin kehittää.
- Perustelut tietotyyppien luokitteluiden osalta tulisi kirjata näkyviin. Tällöin kehitetään työkalun läpinäkyvyyttä ja hyödyllisyyttä viestittäessä perusteluita laajemmin projektihenkilöille.

Toteutetut muutokset

- Lomakkeeseen lisättiin sarake johon kirjataan luokittelun perusteet. Luokittelussa käytetään jatkossa värikoodia (liikennevaloja) helpottamaan visuaalista tarkastelua ja tulosten analyysia.

(jatkuu)

(Liite 3 jatkuu)

Tutkimustapaus 3 Yrityksen kokonaisarkkitehtuuri

Kokonaisarvio

- Positiivinen palaute ja rakentavia kehitysehdotuksia. Tuotti tutkijan näkökulmasta kokonaisvaltaisimman lopputuloksen.

Vahvuudet

- Menetelmä antoi hyvän kokonaiskuvan yrityksen toiminnan kriittisistä kohdista. Menetelmä nosti esille prosessien riippuvuusketjuja ja vuorovaikutussuhteita.
- Menetelmä tuki yrityksen johtamista, ja sen riskienhallinnan suunnittelua.
- Menetelmä toi yrityksen riskienhallintaan uuden näkökulman.

Kehityskohteet

- Arvioitaessa kokonaisarkkitehtuuria kokonaisuutena, voisi tutkia mahdollisuutta lisätä menetelmään kehityssuunnitelman näkökulma. Menetelmä voisi tarjota arvioita eri vaihtoehtojen näkökulmasta, niiden vaikuttavuudesta, kustannuksista ja aikatauluista.

Toteutetut muutokset

- Tapauksessa dokumentoinnissa hyödynnettiin ensimmäisen kerran "tietämyksen virrat" organisaatio kuvaa (kuvio 4) helpottamassa tietotyyppien tunnistamista.

(jatkuu)

(Liite 3 jatkuu)

Tutkimustapaus 4 Puolustusvoimien tietojärjestelmäprojekti

Kokonaisarvio

- Positiivinen palaute ja rakentavia kehitysehdotuksia. Perustietojen jäsentymättömyys esti menetelmän täysimääräisen soveltamisen. Tästä huolimatta projektipäällikkö näki menetelmästä olevan hyötyä. Tutkijan näkökulmasta nostaa esille perustietojen ja taustalla olevan arkkitehtuuri rakenteen merkityksen.

Vahvuudet

- Soveltuva menetelmä keskeisten tietojärjestelmäprojektin osa-alueiden tunnistamiseen ja jäsentämiseen
- Menetelmä antaa perusteet vieraan osa-alueen vaatimusten huomioimiseen.
- Menetelmä tukee kokonaisvaltaista käsittelyä ja eri osa-alueiden tunnistamista.

Kehityskohteet

- Menetelmää tulisi hyödyntää tietojärjestelmien suunnitteluprosessien eri vaiheissa.
- Laajempi käyttö sekä testaus tietojärjestelmäprojekteissa antaa lisää palautetta ja kertoo menetelmän soveltuvuudesta tehtäväänsä.
- Palautteessa esitettiin kuvion 4 "tietämyksen virrat" täydentämistä valmiilla asiasana listalla. Näin voitaisiin helpottaa menetelmän itsenäistä käyttöä.

Toteutetut muutokset

- ”Tietämyksen virrat” kuviota 4 ei lähdetty tämän tutkimuksen yhteydessä täydentämään. Havainto on varmastikin pohdinnan arvoinen, mutta tutkijan resurssit eivät tässä yhteydessä mahdollistaneet työn toteutusta.

(jatkuu)

(Liite 3 jatkuu)

Tutkimustapaus 5 Tutkimushanke MUSAS

Kokonaisarvio

- Positiivinen palaute ja rakentavia kehitysehdotuksia. Kokonaisvaltaisin palaute.

Vahvuudet

- Tukee projektien teknisten henkilöiden ja johdon välistä vuorovaikutusta.
- Tietojärjestelmäprojekteissa menetelmää tulisi käyttää oikea-aikaisesti. Liian varhain toteutettuna perustiedot ovat puutteellisia ja liian myöhään tehtynä vaikutukset projektin toteutukseen ja kustannuksiin ovat negatiiviset.
- Menetelmästä voisi olla apua myös tilaaja-tuottaja mallissa vaatimusten tunnistamisessa.
- Menetelmä ohjaa tunnistamaan tietojärjestelmän tietotyypit uudesta näkökulmasta. Menetelmä tukee perinteistä tietojärjestelmä suunnittelua turvallisuuden näkökulmasta.

Kehityskohteet

- Oikeassa tietojärjestelmäprojektissa ajan ja muiden resurssien tarve kasvaa. Menetelmää voisi käyttää vaiheittain. Pitäisi myös pohtia rajapinnat yleiseen vaatimusten määrittelyprosessiin.

Toteutetut muutokset

- Ei muutoksia

LIITE 4 TUTKIMUSKYSELYN TULOKSET

Tähän liitteeseen on koottu tutkimukseen osallistuneiden henkilöiden vastaukset. Tutkimustapauksia oli viisi kappaletta joihin osallistui tutkijan lisäksi yhteensä yksitoista henkilöä. Ensimmäiseen tutkimustapaukseen osallistui seitsemän (7) henkilöä, muihin tapauksiin osallistui jokaiseen yksi (1) henkilö.

Vastaajat on erotettu kussakin tutkimustapauksessa kirjaimella ja juoksevalla numerolla. Vastauksissa käytetty lyhenne CIA viittaa tietoturvallisuuden englanninkieliseen lyhenteeseen, Confidentiality (C), Integrity (I) ja Availability (A).

Tutkimuskyselyn kysymykset olivat seuraavat:

1. Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuusvaatimusten tunnistamiseen?
2. Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturva vaatimusten tunnistamiseen. Mitä nämä uudet käytännöt ovat?
3. Voitko tunnistaa tekijöitä tai kohtia prosessista jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai kohdat ovat?
4. Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat?
5. Miten prosessia voisi kehittää?
6. Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen?
7. Muuta?

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 1:

Kysymys	Vastaukset
1) Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuus vaatimusten tunnistamiseen?	*A1: Kyllä, Tietotyyppien kautta auttaa hahmottamaan suojattavan tiedon.*
	A2: Koska prosessi auttaa hahmottamaan asioita tarkemmin ja ehkä uusilla näkökulmilta puolustaa se paikkansa osana johtamisen ja tietoturvallisuuden työkaluja.
	A3: Prosessi on toimiva ja siitä olisi ollut hyötyä minun aikaisemmin johtamissani projekteissa. Sain uusia menetelmiä vaatimusten luokitteluun. Jos olisi ollut kokemusta tehtävän liiketoiminnasta, olisi saanut enemmän irti.
	A4: Kyllä
	A5: On hyvä rakenne looginen lähestymistapa
	A6: On, Nähtävästi toimii eri aloilla. Luennot antoivat pohjaa prosessille, ja selkeästi huomasi, että on tehty projekteja ja mietitty käytännön juttuja.
	A7: 5-kohtainen tietotyyppeihin perustuva vaatimusten tunnistus prosessi oli selkeä ja vaikutti hyvältä.
2) Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturva vaatimusten tunnistamiseen. Mitä nämä uudet käytännöt ovat?	*A1: Kyseinen prosessi on hyvä käydä läpi projektin/hankkeen **alkuvaiheessa** sen tunnistamiseksi mitä tietoa on tarve suojata ja millä tasolla. Prosessi voisi olla osa "projektimetodia". Mielestäni prosessi soveltuu käytettäväksi sekä julkishallinnon että yksityisen puolen projekteissa.*
	A2: Katso edellinen vastaus. Käytäntönä voisi olla lisätä prosessi räätälöitynä projektikohtaisesti osaksi projektin elinkaaren tapahtumia.
	A3: Ei välttämättä työkaluja, mutta menetelmiä ja ajattelutapoja.
	A4: Käytetty CIA -vaikuttavuusluokittelu haastaa "ankarasti" liiketoiminnan näkökulmasta.
	A5: Tietojärjestelmissä tallennetaan iso määrä tietoa ja jo järjestelmän määritysvaiheessa olisi hyvä purkaa auki tietotyyppejä, rakenteita ja miettiä niiden "CIA". Jälkeenpäin on vaikea korjata väärin suunniteltua tietovarastoa.
	A6: Vaikutus, 5 vaihetta antaa hyvän suuntaviitan tarkentaa asioita pikkuhiljaa. Excel on nähtävästi hyvä apuväline, eri "lajin" tai "lähteen" asioita voi käsitellä omilla sivuilla.
	A7: Edelleen 5 -kohtainen prosessi, jossa tietotyyppien kautta tunnistetaan vaatimuksia.

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 1 (jatkuu):

Kysymys	Vastaukset
3) Voitko tunnistaa tekijöitä tai kohtia prosessista jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai kohdat ovat	*A1: Erityisesti kohdat 1,2, 4 ovat tehokkaita. Tietorakenteiden tunnistaminen ja luokittelu auttavat suunnittelemaan tarkoitukseen sopivia tuotantoympäristöjä.*
	A2: Luokittelu on vaikeaa. Voi johtaa huomattavaankin tehottomuuteen riippuen kokoonpanosta. Luokittelu lisää panoksia.
	A3: Tietotyypin rakenteet hankalia.
	A4: Tietotyyppien tunnistaminen sopii prosessin tulokulmaksi. Rajaaminen auttaa eteenpäin.
	A5: Vaikka olen tehnyt ohjelmistosuunnittelua niin siksi tai siitä huolimatta tietotyyppien ja rakenteiden tunnistus vaikeata. Toisaalta yhä enemmän järjestelmiä liitetään yhteen niin rakenteiden määrittely auttaa eteenpäin.
	A6: Luokittelun vaikeuksia tuli näkökulman "pitämisessä" kuvitteellisessa yrityksessä. Asioiden vaikuttavuus on osassa vaikea arvioida.
	A7: Tehokkuutta paransi selkeä työjärjestys.
4) Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat	*A1: Tyhjä*
	A2: Paikka SW-tuotekehityksen elinkaareessa/prosesseissa.
	A3: Tyhjä
	A4: Tyhjä
	A5: Prosessien kuvaus esimerkein.
	A6: Aika: mitkä asiat pitää heti olla kunnossa, mitkä myöhemmin. Lähtökohta: tunnistetaanko lähtökohta (onko lähtökohtatietoja)
	A7: Tyhjä.
5) Miten prosessia voisi kehittää	*A1: Sanallinen kuvaus prosessin eri osista. Termien "avaaminen".*
	A2: Heittä se erilaisiin projekteihin ja hankkia mahdollisimman tarkkaa palautetta. 100 projektin jälkeen voi olla, että sitä ei enää tunnista samaksi.
	A3: Terminologian selkeytys
	A4: Toistoilla päästään optimaaliseen vaikuttavuuteen.
	A5: Ehkä prosessi olisi helpommin ymmärrettävissä jos tällainen analyysi tehtäisiin jokaiselle yksittäiselle käyttötapaukset koostamalla alhaalta ylös saataisiin koko tietojärjestelmän tietotyypit, rakenteet ja "CIA".
	A6: Vaikutti, että luokitteluun pitää oppia. --> luokittelun tasoesimerkit, --> painota asioiden täydentymistä työn kuluessa. Luokittelu: 1st draft --> 2nd esitys --> 3rd: eka luokitusdokumentti.
	A7: Tyhjä.

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 1 (jatkuu):

Kysymys	Vastaukset
6) Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen	*A1: Kyllä on. Prosessia tukevaa materiaali löytyy myös. Tietotyyppi Excel ohjaa prosessin toteutusta.*
	A2: On varauksin, katso edelliset vastaukset.
	A3: Ei ole kokemusta tietoturvallisuusluokittelua vaativista projekteista, mutta mielestäni toimiva.
	A4: Luokittelu-, sitouttamis- ja sanitointiharjoittelua oivallisesti.
	A5: Prosessi ainakin jossain määrin pakottaa ajattelemaan että kuka saa käyttää ja mitä tietoa. Prosessin avulla löytää kyllä syyt miksi jotain tietoa pitää suojella vaikka lopputulos saattaa olla liian tiukka. Ohjelmistosuunnittelijan olisi hienoa saada tämmöinen valmiina.
	A6: On soveltuva, "vaikeus" tulee siitä, milloin lopettaa. Nähtävästi teen ”yrityksen nimi” ensin karkean tämän tyyppisen jutun ja katson myöhemmin (syksyllä) miten toimii
	A7: Ilmeisestikin, koska harjoitustyöstämmekin tuli jotain konkreettista tulosta.
7) Muuta	*A1: Tyhjä*
	A2: Hieno homma että työkaluja suunnitellaan. Ne vain helposti eskaloituvat liian vaikeiksi käytännön projekteihin joiden aikataulut on lähes poikkeuksetta laskettu liian tiukoiksi. Loogisesti toimivia. "Pakko mennä siitä missä aita on matalin" -projektissa ei ole. Vaatii käyttäjien kokemusta yleensä ja kokemusta itse prosessista, siten että on henkilökohtaisesti saanut palautetta prosessin hyödyistä ja paikkansa pitävyydestä.
	A3: Tyhjä
	A4: Tyhjä
	A5: Tyhjä.
	A6: Tyhjä (kommentti opetustilaisuuden rakenteeseen ja toteutukseen ei itse prosessiin)
	A7: Tyhjä (kommentti opetustilaisuuden rakenteeseen ja toteutukseen, ei itse prosessiin).

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 2:

Kysymys	Vastaukset
1) Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuus vaatimusten tunnistamiseen?	*B1: Prosessi tuotti realistisen kuvan järjestelmän tietotyypeistä sekä niiden luottamuksellisuudesta, käytettävyydestä ja eheydestä. Prosessi ei ota yhtä hyvin huomioon laitteisiin sidottuja ominaisuuksia kuin tietojärjestelmiin.*
2) Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturva vaatimusten tunnistamiseen. Mitä nämä uudet käytännöt ovat?	*B1: Itselle hyötyä oli mm, tietotyyppien erittelyssä, epäselvien / monitulkintaisten kohtien erottelusta omille riveilleen. --> Tärkeimpien kohtien nosto esille menetelmän avulla.*
3) Voitko tunnistaa tekijöitä tai kohtia prosessista jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai kohdat ovat	*B1: TEHOKAS: rivien vaatimusten värikoodaus, TEHOTON: operatiivisen käytettävyys aina kriittistä, SOVELTUVA: tiedonhallinnan elementit --> vaikeampi laitteille. (haastattelijan kommentti, ra - sa järjestelmien arviointi tulee toteuttaa eri asteikolla).*
4) Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat	*B1: Meni keskustelun kautta jouhevasti*
5) Miten prosessia voisi kehittää	*B1: Tietotyyppien rajauksen määrittely pitäisi dokumentoida johonkin. Tietotyyppien luokitteluvaatimukset tarkentuvat kun useita testitapauksia käydään läpi. (Haastattelija kommentti, lisätään sarake luokittelusarakkeen viereen)*
6) Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen	*B1: Prosessi on lupaava*
7) Muuta	*Menetelmä oli helppokäyttöinen ja poiketen monesta muusta "projektityökalusta" käsitteet olivat selkeitä. Menetelmä myös tuotti lyhyessä ajassa oleellista käytännön hyötyä projektin suunnitteluun.*

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 3:

Kysymys	Vastaukset
1) Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuus vaatimusten tunnistamiseen?	*C1: Prosessi kuvaa hyvin läpileikkauksen "yrityksen nimi" toimintamalliprosessista ja sen vaativuuden arvioinnista. Käsittelymenetelmä oli hyvä ja loi visuaalisesti kuvauksen toiminnan kriittisistä kohdista ja niiden vaikuttavuudesta.*
2) Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturva vaatimusten tunnistamiseen. Mitä nämä uudet käytännöt ovat?	*C1: Prosessin kuvaus tukee yrityksen riskipolitiikkaa ja laajentaa entisestään tarkastelukulmia, myös laajempaan seurantaan liittyen. Yrityksen johtamisen tukityökaluna soveltuu hyvin sekä mahdollistaa rekrytoinnin osalta tehtävien vaativuusarviointeja.*
3) Voitko tunnistaa tekijöitä tai kohtia prosessista jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai kohdat ovat	*C1: Tehokkuus näkyy riippuvuuspuumaisesti ja tukee tieto/toimintaprosessin kehittämistä. Prosessin aikana tuli näkökulmia jotka lisäävät varmennuksen tärkeyttä kun toimintaa edelleen kehitetään.*
4) Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat	*C1: Seurannan näkökulmasta olisi hyvä määräajoin edellyttää asioiden arviointia ja muutosten kirjaamista.*
5) Miten prosessia voisi kehittää	*C1: Voisiko prosessiin luoda herkkyysindikaattorin sekä voisiko yhtenä arviointinäkökulmana olla variaatioiden tarkastelu / kustannusarvio / aikataulutus*
6) Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen	*C1: Mielestäni kyllä, prosessikuvausta on helppo jatkaa kehittämistä. Prosessi kuvaa ja täydentää uutta osa-aluetta yrityksen riskien arvioinnissa.*
7) Muuta	*C1: Tyhjä*

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 4:

Kysymys	Vastaukset
1) Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuus vaatimusten tunnistamiseen?	*D1: Soveltuu ja on hyödyllinen pohjustus keskeisiin huomioitaviin aiheisiin ja niiden jäsentämiseen.*
2) Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturva vaatimusten tunnistamiseen. Mitä nämä uudet käytännöt ovat?	*D1: Vaatimusten perusjäsennys auttaa erittelemään suoraan aiheita ja toisaalta takaa että aihealue tulee käsiteltyä kattavasti*
3) Voitko tunnistaa tekijöitä tai kohtia prosessista jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai kohdat ovat	*D1: Prosessi ohja suoraan yhteen menettelyyn jäsentää tekijälle useimmiten jossain määrin vierasta aihealuetta.*
4) Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat	*D1: Käytännön hyödyntäminen tuonee lisää palautetta.*
5) Miten prosessia voisi kehittää	*D1: Puolustusvoimien tietohallintopäätösten käsittely ja sen uudempi PVLOGL:n teknisten elinjaksojen hallinnon tietoturvaosiot voisi olla hyvä kohde tekniikan/mallin hyödyntämiseen.*
6) Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen	*D1: On*
7) Muuta	*D1: Tyhjä*

(jatkuu)

(Liite 4 jatkuu)

Tutkimustapaus 5:

Kysymys	Vastaukset
1) Oliko kehitetty prosessi soveltuva projektin johtamiseen ja tietoturvallisuus vaatimusten tunnistamiseen?	*E1: Kyllä. Vahvuuksia on "nörttien" ja esimiesportaan yhteisen ymmärryksen löytämisen mahdollistaminen.*
2) Tuoko kehitetty prosessi mielestäsi uusia käytännön työkaluja projektin johtamiseen ja tietoturva vaatimusten tunnistamiseen. Mitä nämä uudet käytännöt ovat?	*E1: Mielestäni luokitteluun perustuva malli pakottaa ajattelemaan järjestelmän tietotyypit eri näkökulmista, joka tukee hyvin perinteistä vaatimusmäärittelyä erityisesti turvallisuuden näkökulmasta.*
3) Voitko tunnistaa tekijöitä tai kohtia prosessista jotka tekivät siitä tehokkaan/tehottoman tai soveltuvan/soveltumattoman suunniteltuun käyttötarkoitukseen. Mitä nämä tekijät tai kohdat ovat	*E1: Uskon, että keskeistä on oikea ajoitus projektissa. Liian aikaisin toteutettaessa ei tuota riittävän tarkkaa tietoa ja myöhään muutosten tekeminen olisi liian kallista. Voisi toimia tuotteistamisen alussa myös tilaaja-tuottaja työn apuvälineenä.*
4) Puuttuiko prosessista joitain oleellisia kohtia? Mitä nämä kohteet ovat	*E1: Mielestäni ei. Kun tutkittava järjestelmä paisuu, on myös määrittelytyö isompi ja haastavampi.*
5) Miten prosessia voisi kehittää	*E1: Jos kyseessä olisi oikea tuote niin lisää aikaa ja resursointi voisi olla kaksiosainen (ehkäpä jopa ennakkotehtäviä). Olisiko liittymäpintoja vaatimusmäärittelyprosessiin?*
6) Onko prosessi soveltuva suunniteltuun käyttötarkoitukseen	*E1: Mielestäni on.*
7) Muuta	