LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Case Study: Tietojärjestelmien kriittisyyden arviointi valtioneuvoston kansliassa

Vento, Eero

2017 Laurea

Laurea-ammattikorkeakoulu

Case Study: Tietojärjestelmien kriittisyyden arviointi valtioneuvoston kansliassa

Eero Vento
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2017

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusala
Tradenomi (AMK)

Eero Vento

Case Study: Tietojärjestelmien kriittisyyden arviointi valtioneuvoston kansliassa

Vuosi 2017 Sivumäärä 60

Valtioneuvoston kanslian keskeinen rooli yhteiskunnallisessa varautumisessa ja valtion johtamisessa edellyttää varautumiselta laadukkaasti toimivaa kokonaisuutta, joka perustuu parhaisiin mahdollisiin käytänteisiin. Osana jatkuvuudenhallintaa ja siihen kuuluvaa ICT-varautumista valtioneuvoston kanslian valmiusyksikön tehtävänä on koordinoida ja ohjata ministeriön tietojärjestelmien kriittisyyden arviointia tietoturvallisuuden asiantuntijuutta sekä yhteisiä menetelmiä tarjoamalla. Muutokset valmiusyksikön hallinnollisen tietoturvallisuuden asiantuntijaorganisaatiossa ja tietojärjestelmien kriittisyyden arvioinnissa havaitut puutteet edellyttävät prosessin kehittämistarpeen tutkimista.

Opinnäytetyöllä vastattiin tutkimustarpeeseen selvittämällä tapaustutkimuksen keinoin tietojärjestelmien kriittisyyden arvioinnin nykytilaa ja vertaamalla sitä jatkuvuuden hallinnan teoreettiseen viitekehykseen. Teoreettinen viitekehys muodostettiin kirjallisuuslähteiden, kansallinen lainsäädännön ja toimintatapoihin ohjaavien standardien sekä ohjeiden perusteella. Työn tavoitteena oli muodostaa käsitys siitä, mitä toimiva tietojärjestelmien kriittisyyden arvioinnin prosessi valtioneuvoston kansliassa edellyttää ja luoda kehittämisehdotuksia sekä -ideoita siitä, miten tietojärjestelmien kriittisyyden arviointia ja siihen liittyviä toimintamalleja voisi valmiusyksikössä kehittää.

Kriittisten tietojärjestelmien kuten toimintojen ja prosessienkin määrittely on jatkuvuuden hallinnan perustana osa organisaation sisäisen toimintaympäristön tunnistamista. Ilman tätä vaihetta jatkuvuus- ja varautumissuunnittelua ei voida kohdentaa tärkeisiin toimintoihin eikä häiriötilanteista toipumisen toimenpiteitä ole mahdollista toteuttaa oikeassa järjestyksessä. Opinnäytetyön viitekehys kytkeytyi jatkuvuuden hallinnan lisäksi tietoturvallisuuteen, tietojärjestelmissä käsiteltävän tiedon ollessa yksi organisaation arvokkaimmista pääomista.

Tietojärjestelmien kriittisyyden arvioinnin prosessin nykytilaa tutkittiin haastattelemalla valmiusyksikössä työskenteleviä tietoturvallisuuden asiantuntijoita sekä tutustumalla prosessiin liittyvään julkiseen dokumentaatioon. Nykytilan hahmottamista varten menetelmänä käytettiin prosessianalyysia ja kehittämisratkaisuja pyrittiin löytämään teoriaan nojaavalla esikuva-arvioinnilla, joka edellytti kattavaa perehtymistä teoreettiseen viitekehykseen.

Tulokset osoittivat, että tietojärjestelmien kriittisyyden arvioinnin sijaan kehittämisessä on ensisijaisesti tarkasteltava jatkuvuuden hallinnan prosessia kokonaisuutena. Kriittisten tietojärjestelmien tunnistaminen perustuukin strategisen tason jatkuvuussuunnitteluun, jonka osana valtioneuvoston kanslian toimintojen ja prosessien kriittisyys tulisi arvioida. Tietojärjestelmien kriittisyyden arvioinnin menetelmissä ja työkaluissa on huomioitava järjestelmien riippuvuussuhteet toimintoihin ja prosesseihin sen sijaan, että tietojärjestelmiä arvioitaisiin niistä erillisinä kokonaisuuksina. Keskeytymisvaikutusten lisäksi yksittäisen järjestelmän kriittisyyden muodostumisessa on huomioitava järjestelmän merkitys strategisten tehtävien kannalta ja järjestelmän sisältämän tiedon arvo.

Asiasanat: Arviointi, Jatkuvuus, Kriittisyys, Tietojärjestelmät, Varautuminen

Laurea University of Applied Sciences
Degree Programme in Security Management
Bachelor's Degree

Abstract

Eero Vento

Case Study: Criticality Evaluation of IT-systems in the Prime Minister's Office

Year 2017 Pages 60

Being prepared requires high-quality measures in the Prime Minister's Office considering its key role in Finland's governmental leadership and societal preparedness. Therefore preparedness must be in compliance with the best practices in accordance with continuity management. In the Prime Minister's Office information and communications technology (ICT) preparedness is managed by the Preparedness Unit. The unit conducts the guidance and coordination of preparedness activities such as contingency and recovery planning by offering shared methods and expertise in the field of information security. As a result of recent changes in the Preparedness Unit's organizational structure the existing code of conduct for ICT-preparedness has been reviewed critically. The review highlights some shortcomings in the process of criticality evaluation of the information systems.

The purpose of this Bachelor's Thesis was to research how the criticality evaluation process is carried out and how it should be carried out in the Prime Minister's Office. The thesis approach is a Case Study where the process is compared with the theoretical framework. The framework focuses on literature, legislation, guidelines and standards. The objective was to construct an understanding of the implementation of a successful evaluation process and what is required of the Prime Minister's Office to implement one successfully. A suggestion of what areas and actions in the process should be developed by the Preparedness Unit was also drawn up.

The theoretical framework consists of theory on information security and continuity management. Information systems process information, which is one of the organization's most important assets. That makes critical information systems a prerequisite for an organization to function.

The case process at the Prime Minister's Office was researched by interviewing specialists and analyzing the process-related documentation. The data gathered with these methods was blueprinted in a process map to determine individual steps, activities and roles in the criticality evaluation of information systems. The blueprinted process was compared against case studies accessible in theory to draw up development solutions.

The conducted study revealed that the organization's continuity management should be viewed at a strategic level before developing the case process. Defining organizational roles, responsibilities, priorities and objectives of the criticality evaluation is important for implementing a successful process. The instruments and methods used in the evaluation should meet the needs of preparedness operations in the Prime Minister's Office. It is crucial to consider information system dependencies on functions and processes instead of evaluating information systems as independent entities.

Keywords: Continuity, Criticality, Evaluation, Information, Preparedness, System

Sisällys

1 Johdanto

Julkisen hallinnon toimijoiden jatkuvuuden hallinnassa keskeistä on poikkeusoloihin varautuminen. Varautumissuunnittelua toteutetaan monella eri tasolla, jotka ovat lähes kaikki riippuvaisia tietoteknisestä ulottuvuudesta. ICT (Information and Communications Technology) -varautumisella pyritäänkin varmistamaan muun muassa toiminnalle kriittisten tietojärjestelmien toiminta kaikissa olosuhteissa. Organisaatiot yksityisellä sektorilla sekä julkisessa hallinnossa toteuttavat ICT-varautumista osana jatkuvuuden hallintaa jatkuvana sekä hallittuna prosessina, jossa pyritään jatkuvalla kehittämisellä vastaamaan toimintaympäristössä tapahtuviin muutoksiin.

Valtioneuvoston kanslian sekä muiden julkishallinnon organisaatioiden toimintaa varautumisen osalta määrittää Suomen lainsäädäntö, mutta siinä huomioidaan myös valtionhallintoa ohjaavat asiakirjat, kuten VAHTI:n eli julkisen hallinnon digitaalisen turvallisuuden johtoryhmän julkaisemat VAHTI-ohjeet, joiden tarkoituksena on ohjata ja yhteen sovittaa julkishallinnon tietoturvallisuutta ja sen kehittämistä. Lainsäädäntö sekä ohjeet asettavat yleisen tason minimivaatimukset varautumiselle, jota kunkin organisaation on muokattava ja kehitettävä edelleen omaan rakenteeseen, toimintastrategiaan sekä -ympäristöön soveltuvaksi.

Tietojärjestelmien kriittisyyden arviointi on osa organisaation sisäisen toimintaympäristön määrittelyä ja tietoturvallisuuden sekä jatkuvuuden hallintaan liittyvän suunnittelun perusta. Valtioneuvoston kansliassa sisäisen toimintaympäristön muutokset kuten hallinnollisen tietoturvallisuuden vastuuorganisaation rakenteelliset muutokset vuoden 2017 aikana ja muutokset tietojärjestelmäkentässä sekä ulkoisen toimintaympäristön muutokset kuten Euroopan Unioni (EU) –tasoisen tietosuojalainsäädännön soveltaminen kansallisessa lainsäädännössä keväästä 2018 alkaen asettavat tarpeen tutkia kriittisyyden arvioinnin prosessia ja arvioida tarvetta sen kehittämiseksi.

Opinnäytetyöhön ryhtymisen taustalla vaikuttaa viiden kuukauden pituinen korkeakouluharjoittelujakso valtioneuvoston kanslian valmiusyksikössä, jossa ajatus kriittisyyden arviointia koskevasta opinnäytetyöstä syntyi. Tavoitteena oli vastata tutkimustarpeeseen tutkimalla kriittisyyden arvioinnin prosessia ja siihen liittyvää teoriaa hallinnollisesta näkökulmasta, sekä selvittää onko kyseistä prosessia, sen menetelmiä ja toimintatapoja tarpeen kehittää toimivaa ICT-varautumisen kokonaisuutta ajatellen. Työn tarkoituksena oli tarjota lopputuotoksessa kehittämisehdotuksia ja ideoita, joita voitaisiin hyödyntää valtioneuvoston kanslian valmiusyksikössä.

Opinnäytetyö on muodoltaan tutkimuksellinen kehittämistyö, jonka tutkimusstrategiana eli menetelmällisten ratkaisujen kokonaisuutena käytettiin tapaustutkimusta (Case Study). Tutkimuksessa tapaus keskittyy valtioneuvoston kanslian jatkuvuuden hallinnan ja hallinnollisen tietoturvallisuuden osana tapahtuvaan tietojärjestelmien kriittisyyden arviointiin valmiusyksikön näkökulmasta. Työstä on rajattu pois tekninen näkökulma, ICT-varautumista koskevien osaprosessien tutkiminen sekä organisaation ulkopuolelle ulottuvia tietojärjestelmiä koskeva kriittisyyden arviointi.

Tutkimusote työssä oli kvalitatiivinen eli laadullinen, sillä tiedon hankinta oli luonteeltaan kokonaisvaltaista ja tiedonkeruun kohdejoukko muodostui muun muassa henkilöistä, jotka valittiin tarkoituksenmukaisesti (Hirsjärvi, Remes & Sajavaara 2009, 164). Tutkimusongelma oli laadultaan tapaustutkimukseen sopiva, sillä tutkimusstrategian valinnalla pyrittiin löytämään vastaus kysymykseen ”miten?” (Ojasalo, Moilanen & Ritalahti 2014, 53). Opinnäytetyössä tutkimuskysymyksiä olivat:

- Miten tietojärjestelmien kriittisyyden arviointi valtioneuvoston kansliassa tehdään?
- Miten tietojärjestelmien kriittisyyden arviointi tulisi tehdä valtioneuvoston kansliassa?

Ensimmäisellä tutkimuskysymyksellä pyrittiin selvittämään, kuinka tietojärjestelmien kriittisyyden arvioinnin prosessi nykytilanteessa toteutuu ja mitä ulottuvuuksia siihen sisältyy. Ulottuvuudet käsittävät muun muassa arviointiin osallistuvat tahot ja tahojen roolit, arvioinnissa noudatettavat toimintamallit kuten käytettävät menetelmät ja työkalut sekä arviointiprosessiin keskeisesti vaikuttavat muut mahdolliset tekijät, kuten strategisen tason ohjaus organisaatiossa.

Toisella tutkimuskysymyksellä tavoiteltiin opinnäytetyön tuotoksena syntyvää perusteltua mallia tai kehitysehdotuksia ja -ideoita siitä, kuinka tietojärjestelmien kriittisyyden arviointia tulisi valtioneuvoston kansliassa toteuttaa. Kehitysnäkökulman tarkastelussa otettiin huomioon prosessi kokonaisuutena sekä siihen vaikuttavat ylemmän tason osatekijät organisaatiokohtaisen jatkuvuussuunnittelun viitekehyksessä.

Työn raportti noudattaa rakenteeltaan Laurea-ammattikorkeakoulun (2016) opinnäytetyöohjeen mukaista rakennetta. Työssä lähdetään liikkeelle toimeksiantajaorganisaation sekä sen sisäisten opinnäytetyön kannalta merkittävien toimijoiden esittelystä. Tämän jälkeen käsitellään tietojärjestelmien kriittisyyden arviointiin liittyvää tietoperustaa eli teoreettista viitekehystä käsittäen jatkuvuuden- sekä tietoturvallisuuden hallinnan yleisen teorian sekä näkökulman julkisen hallinnon varautumiseen.

Tietoperustan jälkeen työssä käsitellään tutkimusmenetelmiä sekä vaiheita ja perustellaan menetelmävalintoja tutkimuksen strategisesta näkökulmasta. Tutkimusvaiheet esitellään käytettyjen menetelmien mukaisessa järjestyksessä. Tutkimustulokset esitellään tämän jälkeen analysoituna tutkimusvaiheita mukailevassa järjestyksessä. Lopussa keskitytään tutkimuksen johtopäätöksiin sekä toimeksiantajalle osoitettuihin kehitysehdotuksiin ja-ideoihin, joiden lisäksi työssä esitellään tutkimustyön pohjalta määriteltyjä jatkotutkimusehdotuksia sekä arvioidaan työn tavoitteiden saavuttamista.

2 Opinnäytetyön toimeksiantaja

Kuten johdannosta käy ilmi, opinnäytetyön toimeksiantaja on valtioneuvoston kanslia, jossa työ toteutettiin valtioneuvoston kanslian valmiusyksikölle. Tämä osio sisältää ministeriön yleisen esittelyn lisäksi valtioneuvoston hallintoyksikön sekä sen osana toimivan valmiusyksikön esittelyt. Esittelyn tavoitteena on, että lukijan on mahdollista hahmottaa pääpiirteittäin opinnäytetyölle olennainen valmiusyksikön toimintaympäristö merkittävän valtionhallinnon organisaation sisällä.

2.1 Valtioneuvoston kanslia

Valtioneuvoston kanslia on pääministerin ministeriönä yksi Suomen kahdestatoista ministeriöstä, jonka toiminta perustuu valtioneuvoston asetukseen valtioneuvoston kansliasta (393/2007). Valtioneuvoston kansliassa työskentelee noin 550 henkilöä (Valtioneuvoston kanslia 2017c) ja sen päätoimipisteet sijaitsevat Helsingissä Valtioneuvoston linnassa sekä Arppeanumissa Senaatintorin laidalla.

Valtioneuvoston kanslian toimintaa johtaa valtioneuvoston päällikkönä toimivan pääministerin toimikaudeksi nimetty valtiosihteeri alivaltiosihteerin avustuksella. Alivaltiosihteerin tehtävänä on johtaa, valvoa ja kehittää ministeriön osastojen, yksikköjen sekä virkamiesten toimintaa. (Valtioneuvoston kanslia 2017b.)

Valtioneuvoston kanslia avustaa pääministeriä valtioneuvoston johtamisessa ja vastaa pääministerin johdolla hallitusohjelman toimeenpanon valvonnasta. Keskeisiä valtioneuvoston kanslian tehtäviä ovat myös Suomen EU-politiikan yhteensovittaminen, valtion omistajapolitiikka, ministeriön alaisten valtio-omisteisten yhtiöiden omistajaohjaus sekä hallituksen toimintaedellytysten turvaaminen kaikissa olosuhteissa. (Valtioneuvoston kanslia 2017a.)

Ministeriön rooli koko valtioneuvoston turvallisuustoiminnassa on merkittävä, sillä valtioneuvoston kanslian vastuulla on valtioneuvoston asetuksen valtioneuvoston kansliasta (393/2007, 1 §) mukaan valtioneuvoston ja sen ministeriöiden yhteisen turvallisuuden ja tietoturvallisuuden ohjaus ja yhteensovittaminen sekä valtioneuvoston turvallisuuspalvelut, yhteisen tieto- ja

viestintätekniikan ja yhteiset tietojärjestelmät kattava tietoturvallisuuden hallinta sekä valtioneuvoston yhteisten ICT-palvelujen ja tietojärjestelmien hallinta ja kehittäminen.

Yhteiskunnallisen varautumisen kannalta merkittäviä vastuualueita ovat Yhteiskunnan turvallisuusstrategian (2017, 30) mukaisesti - - valtioneuvoston yhteisen tilannekuvan kokoaminen ja häiriötilanteiden hallinnan yleinen yhteensovittaminen, valtioneuvoston yhteinen poikkeusoloihin sekä häiriötilanteisiin varautuminen sekä valmiuslaissa tarkoitettujen poikkeusolojen toteaminen ja käyttöönottoasetuksen antaminen yleisestä yhteensovittamisesta.

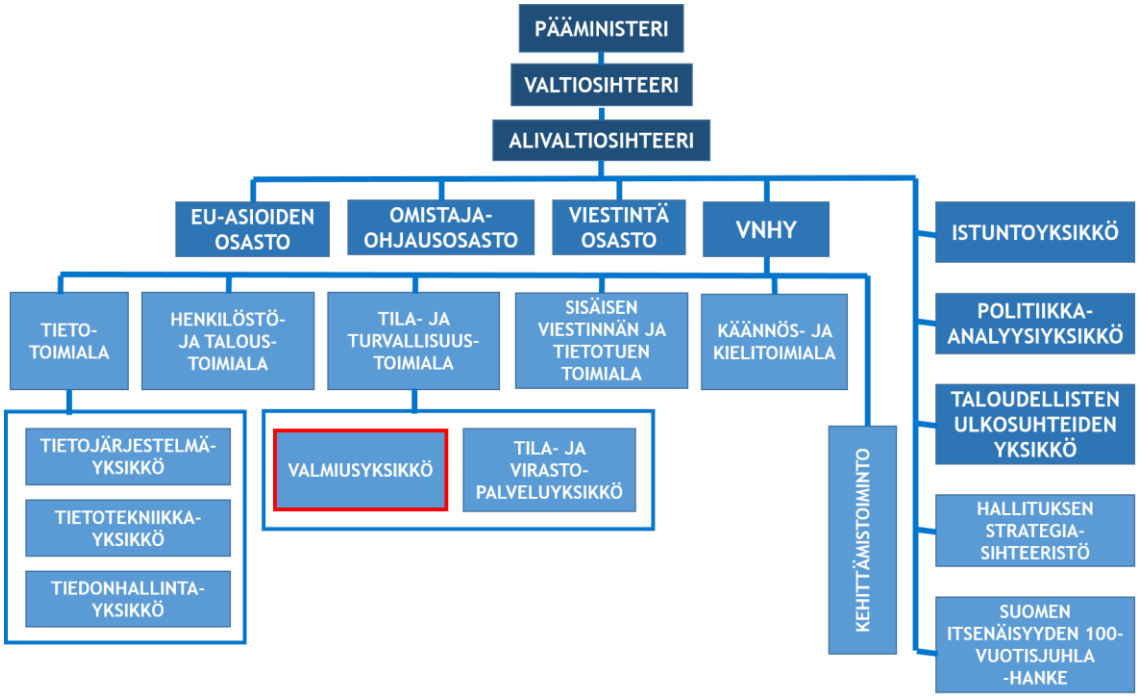
2.2 Valtioneuvoston hallintoyksikkö

Valtioneuvoston kanslia jakautuu organisaationa osastoihin sekä osastoista erillisiin yksiköihin, valtioneuvoston hallintoyksikön (VNHY) ollessa yksi neljästä osastosta. Kuten organisaatiokaaviosta voi havaita (Kuvio 1), valtioneuvoston hallintoyksikkö kattaa huomattavan osan ministeriön organisaatiorakenteesta. Valtioneuvoston hallintoyksikköä johtaa osastopäällikkö ja se jakautuu edelleen toimialoihin, joita johtavat toimialajohtajat. VNHY:n toimialojen alaisuudessa toimii kaiken kaikkiaan 12 yksikköä. (Valtioneuvoston kanslia 2017b.)

VNHY:n toiminta koskettaa kaikkia ministeriöitä, sillä sen tehtäviä ovat valtioneuvoston kanslian sisäisen hallinnon lisäksi ministeriöiden yhteiset hallinto- ja palvelutehtävät. Valtioneuvoston hallintoyksikkö vastaa valtioneuvoston ja sen ministeriöiden yhteisen hallinnon, toiminnan sekä toimintakulttuurin johtamisesta, yhteensovittamisesta ja kehittämisestä. (Valtioneuvoston kanslia 2017b.)

2.3 Valmiusyksikkö

Tila- ja virastopalveluyksikön ohella osana VNHY:n tila- ja turvallisuustoimialaa (Kuvio 1) valmiusyksikkö on valtioneuvoston kanslian turvallisuudesta vastaava sekä koko valtioneuvoston turvallisuutta ohjaava toimielin, jonka päällikkönä toimii valtioneuvoston turvallisuusjohtaja.



Kuvio 1: Valmiusyksikkö valtioneuvoston kanslian organisaatiokaaviossa (Valtioneuvoston kanslia 2017d)

Valmiusyksikön tehtävänä ovat valtioneuvoston kanslian sisäisen turvallisuustoiminnan sekä varautumisen toteuttamisen lisäksi koko valtioneuvoston turvallisuustoiminnan ja varautumisen yhteensovittaminen. Toimielin vastaa valtioneuvoston turvallisuusjärjestelyistä kattaen ministereitä koskevat turvallisuusjärjestelyt, ministeriöiden turvallisuusjärjestelmät ja kiinteistöjen turvallisuusvalvontaan liittyvät tehtävät. Edellä mainittujen tehtävien lisäksi valmiusyksikön vastuulla on valtioneuvoston tilannekuvatoiminta, josta säädetään erikseen laissa valtioneuvoston tilannekeskuksesta (300/2017).

Kuten yhteiskunnan turvallisuusstrategiassakin (2017, 31) mainitaan: ”Valtionjohdon tilannekuvan ylläpitäminen on valtioneuvoston kanslian strateginen tehtävä.” Tilannekeskus kokoaa ja analysoi tasavallan presidentin ja valtioneuvoston päätöksenteon ja toiminnan tueksi tietoa turvallisuustilanteesta ja sellaisista häiriöstä sekä niihin liittyvistä uhkista, jotka voivat vaarantaa yhteiskunnan elintärkeitä toimintoja. Tuotettu tilannekuva muodostaa perustan muun muassa kriisitilanteiden johtamiselle.

Valmiusyksikössä työskentelee turvallisuuden eri osa-alueilta asiantuntijoita, jotka osallistuvat sekä kanslian että valtioneuvoston turvallisuuden kehittämiseen. Valmiusyksikössä huolehditaan valtioneuvoston turvallisuus- sekä tietoturvallisuustoiminnan edellytyksistä ohjeistuksella, kouluttamisella sekä tiedottamisella. Valmiusyksikkö vastaa ministeriössä turvallisuuteen liittyvän asiantuntijuuden ja konsultoinnin tarjoamisesta.

3 Opinnäytetyön tietoperusta

Tässä osiossa perehdytään keskeiseen tietoperustaan eli käsitejärjestelmään, jonka tarkoituksena on Ojasalon, Moilasen ja Ritalahden (2014, 25) mukaan määritellä opinnäytetyön keskeiset käsitteet. Tietoperusta toimii myös tutkimuksen teolle keskeisenä tutkittavaan ilmiöön johdattelevana teoreettisena viitekehyksenä, johon nojaudutaan vahvasti tutkimusvaiheissa.

Tietoperusta sisältää tietoturvallisuuden- ja jatkuvuudenhallinnan yleiskäsitteistön läpikäynnin, kuten jatkuvuussuunnittelun, toipumissuunnittelun, normaaliolojen häiriöiden, häiriötilanteiden ja poikkeusolojen sekä siihen liittyvän varautumisen asiakokonaisuuden käsittelyn. Tietoperusta on muodostettu perehtymällä aihetta koskevaan kirjallisuuteen, tutkimusartikkeleihin, ohjeisiin sekä lainsäädäntöön ja muihin soveltuviin lähteisiin.

Jatkuvuuden hallinnan tietoperustan keskeisenä lähteenä on käytetty Mika Iivarin sekä Mika Laaksosen teosta Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen (2009), jonka käsitteistöä on käytetty myös lähteenä toimivan VAHTI:n jatkuvuudenhallintaa koskevassa ohjeistuksessa. Tietoperustassa painotetaan julkisen hallinnon ICT-varautumista ja tietojärjestelmien kriittisyyden arviointia, jotka käsitellään osiossa viimeisenä.

3.1 Jatkuvuuden- ja tietoturvallisuuden hallinta

Yksi keskeisimmistä elementeistä organisaatioiden toiminnassa on jatkuvuuden varmistaminen eli jatkuvuudenhallinta, sillä sen tarkoituksena on taata organisaation toiminnan jatkuvuus. Toiminnan jatkuvuus on välttämätöntä toimialasta riippumatta niin yrityksille kuin julkisen- tai valtionhallinnon organisaatioillekin. Jatkuvuuden edellytyksenä voidaan ajatella, että organisaation toiminnan on oltava laadukasta ja siinä on huomioitava sekä sisäisen että ulkoisen toimintaympäristön muutokset. Muutosten taustalla voivat vaikuttaa mitkä tahansa syyt, jotka voivat johtua esimerkiksi taloudellisista tai poliittisista lähtökohdista tai asetelmista maailmalla, valtion sisällä tai yksittäisellä toimialalla.

Muutokset voivat aiheuttaa sekä mahdollisuuksia että uhkia. Menestyäkseen organisaatiot pyrkivätkin usein hyödyntämään mahdollisuuksia ja kehittämään omaa toimintaansa tavoitteena suurempi hyöty. Etenkin voittoa tavoitteleville yrityksille toimintaympäristön muutosten luomien mahdollisuuksien hyödyntäminen liiketoiminnassa on keskeistä.

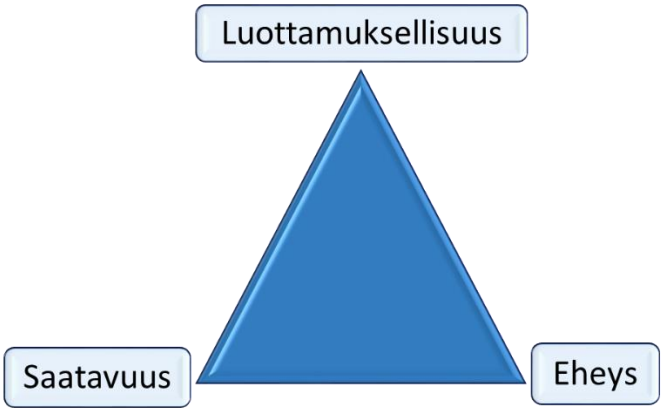
Muuttuva toimintaympäristö voi olla vaaraksi organisaation toiminnalle, mikäli organisaation toimintatavat eivät enää vastaa toimintaympäristön muutosten asettamiin haasteisiin, kuten teknologian kehittymiseen ja sen mukana tulleisiin uudenlaisiin uhkiin. ICT:n eli tieto- ja viestintäteknologian näkökulmasta muutokset, kuten järjestelmien automatisointi sekä monimut-

kaistuminen, tietojen yhteiskäytön lisääntyminen ja laajeneminen, palveluiden riippuvuus toimittajien palveluverkostoista, palveluiden omistus- ja sopimussuhteiden muutokset sekä kansainvälisen yhteistoiminnan ja ohjauksen merkityksen kasvaminen lisäävät uhkia samalla, kun uhat muuttuvat entistä yllätyksellisemmiksi ja ammattimaisemmiksi, niiden vaikutusten ollessa entistä vakavampia (VAHTI 2012, 14).

Toiminnan jatkuvuuden varmistaminen edellyttääkin muutosten aiheuttamien uhkien sekä ongelmatilanteiden ennakoimista ja niihin varautumista. ICT:n näkökulmasta etenkin tietoturvariskien hallinta onkin siksi keskeinen osa myös jatkuvuuden hallintaa.

Nykypäivänä organisaatioiden yksi arvokkaimmista pääomista on tieto, joka pyritään tietoturvallisuustoiminnalla pitämään luotettavana sekä nopeasti ja ainoastaan siihen oikeutettujen henkilöiden saatavilla. Tietoturvallisuuden määritelmät ovat ajan saatossa laajentuneet käsittämään pelkän tiedon lisäksi myös sen käsittelyyn tarkoitetut laitteistot ja ohjelmistot kattavat kokonaisuudet eli tietojärjestelmät. (Hakala, Vainio & Vuorinen 2006, 4.)

Perinteisesti tietoturvallisuus ymmärretään luottamuksellisuuden, eheyden sekä saatavuuden tai käytettävyyden muodostamana kokonaisuutena ja visuaalisesti se kuvataankin usein näiden arvojen muodostamana kolmiona (Kuvio 2). Luottamuksellisuus tarkoittaa sitä, että esimerkiksi tietojärjestelmän sisältämiin tietoihin on pääsy vain niihin oikeutetuilla henkilöillä. Eheydellä tarkoitetaan järjestelmän tietojen paikkaansa pitävyyttä sekä virheettömyyttä ja saatavuus toteutuu kun tietojärjestelmä on käytettävissä riittävän nopeasti ja sen sisältämät tiedot ovat saatavilla oikeassa muodossa. (Hakala ym. 2006, 4.)



Kuvio 2: Tietoturvallisuuden perinteiset osa-alueet

Tietoturvallisuustoiminta kattaa näinollen esimerkiksi tietojärjestelmien suojausmenetelmät luottamuksellisuuden varmistamiseksi, järjestelmien automatisoinnin, tietojen käsittelyyn riittävän ohjelmistojen tehokkuuden ja soveltuvuuden varmistamisen saatavuuden tai käytettävyyden takaamiseksi, tarkistus- ja varmennusmenetelmät sekä virheen tunnistus- ja korjausmenetelmillä varustetut protokollat ja laitteet eheyden varmistamiseksi. (Hakala ym. 2006, 4-5.)

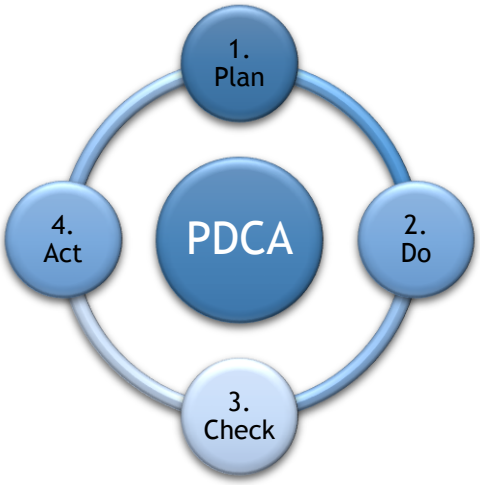
Perinteisten tietoturvallisuuden osa-alueiden lisäksi muun muassa Hakala, Vainio ja Vuorinen (2006, 5) ovat esitelleet kiistämättömyyden ja pääsynvalvonnan osa-alueet kattavan tietoturvallisuuden laajennetun määritelmän. Kiistämättömyydellä tarkoitetaan tässä määritelmässä esimerkiksi tietojärjestelmien kykyä tunnistaa käyttäjäntunnistusmenetelmin sitä käyttävien henkilöiden tiedot ja tallentaa ne esimerkiksi käyttörekisteriin tai –lokiin. Kiistämättömyydellä on mahdollista todentaa tietojärjestelmän luvaton käyttö esimerkiksi tapauksissa, joissa luvatonta tietojärjestelmän käyttäjää vastaan harkitaan oikeudellisia toimia.

Vaikka tiedon luottamuksellisuuden ylläpito kattaakin varsinaisiin tietoihin pääsyn valvonnan, tietoturvallisuuden ylläpito vaatii myös tietojenkäsittelyyn kuuluvan infrastruktuurin käytön rajoittamista. Pääsynvalvonnalla tarkoitetaan laitteiden tai tietoliikenneyhteyksien kuten organisaation langattomien verkkojen tarkoituksenmukaisen käytön valvontaa, jolla pyritään takaamaan laitteiden sekä verkkojen hyvä käytettävyyden taso, estämällä niitä kuormittava ylimääräinen tai luvaton käyttö. Luvaton käyttö on myös yksi keskeisin syy tietoturvallisuuden vaarantumiselle, kuten haittaohjelmien leviämiselle tietojärjestelmissä. (Hakala ym. 2006, 5-6.)

Organisaation tietoturvatoiminta vaatii strategisten linjausten mukaista hallinnointia ja kehittämistä kaikissa organisaation toimintaprosesseissa. Tietoturvallisuutta ohjataankin usein tietoturvallisuuspolitiikalla, jonka tarkoituksena on toimia keskipitkän aikavälin ohjeena tietoturvallisuuden suunnittelusta ja kehittämisestä vastaaville tahoille (Hakala ym. 2006, 7).

Organisaation tietoturvallisuutta koskevien strategisten linjausten toteuttamisen kokonaisuutta, joka kattaa politiikan, organisoinnin, suunnittelun, vastuut, käytänteet, prosessit sekä toiminnan resurssit, kutsutaan tietoturvallisuuden hallintajärjestelmäksi (Information Security Management System, ISMS). Hallintajärjestelmä vaatii jatkuvaa kehittämistä, jotta se vastaa organisaation toimintaympäristön ja toiminnan muutosten asettamiin tarpeisiin. Jatkuva kehittäminen vaatii myös tietoturvatoiminnan seurantaa sekä sen tarkoituksenmukaisuuden ja tehokkuuden arviointia. Tämä jatkuvan kehittämisen malli kuvataan usein ISO/IEC 27001 – tietoturvastandardissa esitetyn PDCA (Plan-Do-Check-Act) -mallin mukaisesti, jossa jatkuvan parantamisen perustan muodostavat suunnittelu, toteutus, tarkistus ja kehitys –vaiheet (Kuvio

3). Jatkuvalla kehittämisellä tavoitellaan organisaation valmiuksia tietoturva-asioiden systemaattiseen hallintaan. (VAHTI 2007, 38–40; Hakala ym. 2006, 106.)



Kuvio 3: Jatkuvan parantamisen PDCA–malli

Vaikka tietoturvallisuuden ja jatkuvuuden hallinta kytkeytyvät vahvasti toisiinsa, on jatkuvuuden hallinnan kokonaisuudessa huomioitava muutkin ulottuvuudet kuin tieto. Siksi se on integroitava osaksi organisaation kaikkea riskienhallintaa ja johtamisjärjestelmiä niin, ettei se ole vain ICT- tai tietoturva-asiantuntijoiden vastuulla oleva erillinen prosessi. Kuten tietoturvallisuustoiminta myös jatkuvuuden hallinta pitäisi saada kiinteäksi osaksi organisaation muuta toimintaa, prosesseja ja palveluita. Silloin jatkuvuuden hallinta olisi lähellä myös ylintä johtoa ja jatkuvuuden hallintaan liittyvät toimet olisivat osa organisaation strategisen suunnittelun prosesseja. (Iivari & Laaksonen 2009, 15–16; VAHTI 2016, 65.) Jatkuvuussuunnittelua sen tasoja sekä vastuita käsitellään seuraavassa osiossa.

3.2 Jatkuvuus- ja toipumissuunnittelu

Organisaatiot kohtaavat uhkia, jotka voivat johtua Iivarin ja Laaksosen (2009, 18) mukaan vaikkapa inhimillisistä virheistä, väärinkäytöksistä, avainhenkilön menetyksestä, sähkö- tai tietoliikennekatkoksista, tulipaloista, vesivahingoista tai esimerkiksi toimitilojen vaurioitumisesta. Jatkuvuuden hallinta edellyttää organisaatiotasolla uhkien huomioimista ja niihin varautumisen suunnittelua, jota kutsutaan jatkuvuussuunnitteluksi.

Jatkuvuussuunnittelulla ylläpidetään organisaation toiminnan laatua ja toteutetaan toiminnan jatkuvuutta vaarantavien riskien hallintaa. Jatkuvuussuunnittelu ei siis ole kertaluontoinen suunnitelma vaan jatkuva ja hallittu prosessi, joka sekin noudattelee jo esiteltyä jatkuvan

parantamisen PDCA–mallia (Kuvio 3; Iivari & Laaksonen 2009, 22-23). Organisaation jatkuvuussuunnittelua hallinnoivaa systemaattista kokonaisuutta kutsutaankin jatkuvuudenhallintajärjestelmäksi (Business Continuity Management System, BCMS).

Organisaation toimintaan normaalioloissa kohdistuvat uhat ovat erilaisia ja vaativat jatkuvuussuunnittelun näkökulmasta vaihtelevan määrän resursseja. Uhkien karkea jako tapahtuu yleensä ongelmiin tai häiriöihin sekä häiriötilanteisiin. Normaalioloissa organisaatiot voivat kohdata ongelmia tai häiriöitä, kuten laitteiden vikaantumista tai lyhyitä sähkökatkoksia, jotka voivat muodostaa hetkellisesti toiminnallisia haasteita. Häiriöistä toipuminen ei kuitenkaan vaadi organisaatiolta suuria resursseja ja toipuminen on yleensä nopeaa. Jatkuvuussuunnittelussa huomioidaan normaaliolojen häiriöt esimerkiksi normaalein varmistusprosessein, huoltotoimenpitein sekä järjestelmien ja toimintatapojen dokumentoinnilla. (Iivari & Laaksonen 2009, 95.)

Toiminnan vaikutusanalyysiä (Business Impact Analysis, BIA) käytetään usein jatkuvuussuunnittelun menetelmänä ja sen tulokset muodostavat keskeisen osan jatkuvuussuunnitelmista (Iivari & Laaksonen 2009, 154). Analyysin avulla voidaan arvioida haitallisten tekijöiden vaikutuksia tarkasteltavaan toimintoon, toimintojen keskeytymisen vaikutuksia organisaatiolle, priorisoida toimintoja ja asettaa yksittäisille tärkeille toiminnoille palautumistavoitteita, jotka ilmaistaan toipumisaikana (Recovery Time Objective, RTO) sekä toipumispisteenä (Recovery Point Objective, RPO). RTO kertoo ajan, jonka kuluessa toiminto tulee saada palautettua toimintaansa häiriötilanteesta ja RPO tarkoittaa tilaa, johon toiminto on palautettava häiriön jälkeen. (VAHTI 2016, 24–25.)

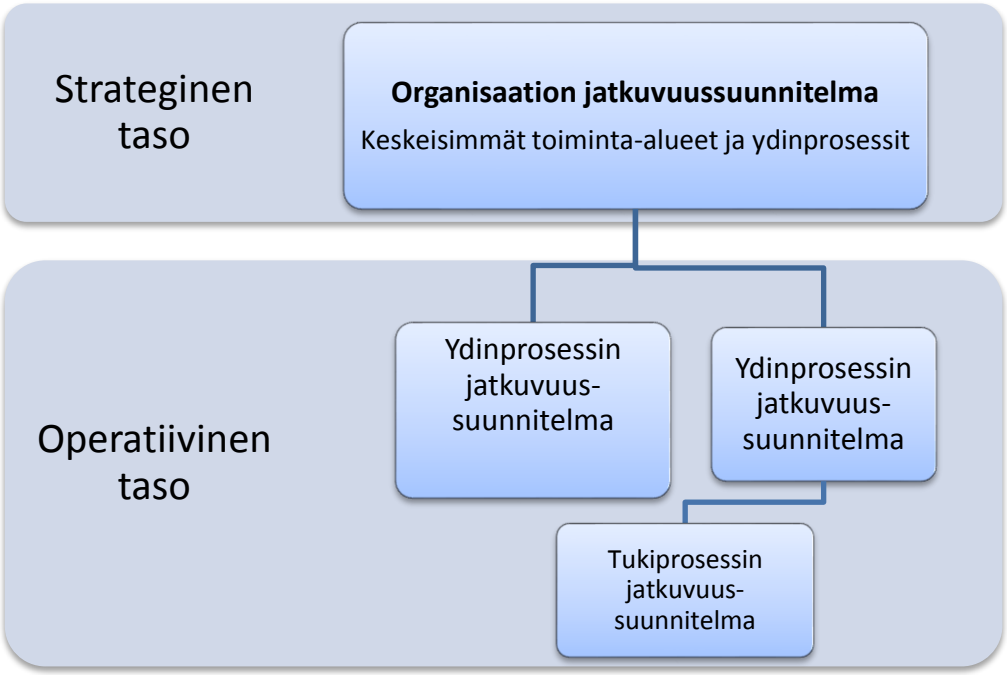
Jatkuvuuden hallinnan näkökulmasta häiriöitä haasteellisempia ovat normaaliolojen häiriötilanteet, joissa voi olla kyse vakavastakin organisaation sisäisestä kriisistä tai onnettomuudesta. Paikallisesti organisaation toimintaa vaikeuttava häiriötilanne vaatiikin jo hieman enemmän resursseja, ja toipuminen häiriötilanteista voi olla hidasta. Sen vuoksi toipumiseen on syytä varautua vaikutusanalyysiin perustuviin toipumistavoitteisiin sekä prioriteetteihin vastaavilla yksityiskohtaisilla toipumissuunnitelmilla. (Iivari & Laaksonen 2009, 96.)

Toipumissuunnittelu on jatkuvuussuunnittelun osaprosessi, joka keskittyy yksittäisestä organisaation kohtaamasta häiriötilanteesta toipumiseen ja organisaation toiminnan palauttamiseen normaaliksi (Iivari & Laaksonen 2009, 19). Toipumissuunnitelmaa tarvitaan vain silloin, kun riski realisoituu jatkuvuussuunnittelussa toteutetuista varotoimista huolimatta. Vakavissa häiriötilanteissa useampien prosessien toiminta voi keskeytyä, joten toipumissuunnitelmat on osattava kohdentaa oikein. Toiminnan jatkuvuuden kannalta keskeiset prosessit onkin kuvattava, jotta voidaan hahmottaa, mitkä prosessit ovat tärkeitä ja palautettava ensimmäisenä

häiriötilanteesta toipumiseksi. On myös selvitettävä, tukevatko prosessit toisiaan ja tarvitsevatko prosessit toisia prosesseja toimiakseen. (Hakala ym. 2006, 24; Iivari & Laaksonen 2009, 105.)

Toipumissuunnitelmat käsittävät jatkuvuussuunnittelussa tärkeiksi määriteltyjen prosessien ja niihin liittyvien tietojärjestelmien varautumisen vaatimukset, toipumisen resurssit sekä vastuut ja toimintaohjeet erilaisissa häiriötilanteissa (Iivari & Laaksonen 2009, 19). Jatkuvuussuunnittelun ja toipumissuunnittelun suhdetta on havainnollistettu myöhemmin kuviossa (Kuvio 5).

Jatkuvuussuunnittelua toteutetaan organisaatioissa monella tasolla. Se jakautuukin hierarkkisesti strategisen tason sekä operatiivisen tason jatkuvuussuunnitteluun (Kuvio 4). Strategisen tason jatkuvuussuunnittelu on organisaation toimintastrategiaan pohjautuvaa jatkuvuussuunnittelua, jossa määritellään jatkuvuuden kannalta tärkeimmät toiminta-alueet sekä prosessit. Strategisen tason suunnitelmat ovatkin ikään kuin organisaation kattavia ohjeistuksia jatkuvuudenhallinnasta, joissa kuvataan toimintojen tärkeysjärjestyksen lisäksi toimintoja uhkaavat riskit sekä niitä koskevat jatkuvuus- ja toipumisvaatimukset. Strategisen tason suunnittelu vastaa organisaation ylin johto, sillä siinä asetetaan tavoitteet sekä painopisteet koko organisaation jatkuvuudenhallinnalle. Menestyksellisen jatkuvuuden hallinnan toteuttaminen ei ole mahdollista ilman johdon täyttä sitoutumista strategisen tason suunnitteluun. (Iivari & Laaksonen 2009, 25; VAHTI 2012, 32.)



Kuvio 4: Jatkuvuussuunnittelun tasot

Toiminnot, prosessit ja tietojärjestelmät omistavat toimielimet vastaavat suunnittelusta operatiivisella tasolla, jossa jatkuvuussuunnittelu noudattaa strategisen tason suunnittelulla asetettuja linjauksia. Operatiivisella tasolla jatkuvuus- sekä toipumissuunnitelmat koskevat yksittäisiä organisaation toimintoja sekä niille tärkeitä prosesseja ja järjestelmiä. Suunnitelmat tehdään koskemaan vähintäänkin niitä toimintoja, jotka on strategisen tason suunnitelmassa määritelty tärkeiksi. (Iivari & Laaksonen 2009, 26.)

Toiminnot omistavien toimielinten rooli suunnittelussa on keskeinen, sillä heillä on paras tuntemus oman alueensa toiminnasta sekä siihen tarvittavista ja suojattavista tiedoista, kohteista sekä järjestelmistä. Omistajien vastuulla on määritellä suojaustarpeet, keskeytymisvaikutukset ja toipumisvaatimukset. Mikäli esimerkiksi järjestelmän tuotannosta vastaa palveluntuottaja, nämä vaatimukset osoitetaan palveluntuottajalle. Omistajat osallistuvat muun muassa tärkeysluokitteluun, tavoitellun toipumisajan sekä -pisteen määrittelyyn ja prosessikuvauksen muodostamiseen, mikäli riittävää prosessikuvausta ei vielä ole olemassa. (Iivari & Laaksonen 2009, 101; VAHTI 2016, 32.)

Palveluntuottajat vastaavat tuottamiensa palveluiden osalta asiakasorganisaation asettamien vaatimusten teknisestä toteuttamisesta sopimuksen mukaisesti. Palveluntuottajilla on päävastuu ylläpitää toipumista tukevia prosesseja, kuten asiakastukea sekä muutos- ja häiriönhallintaa. Tämä edellyttää myös viestinnän sekä tilannekuvan ylläpitämistä asiakasorganisaatiolle. (VAHTI 2016, 33.) Tietojärjestelmien osalta keskeinen julkishallinnon palveluntuottaja on Valtion tieto- ja viestintätekniikkakeskus Valtori.

Vaikka organisaation ylin johto ei itse laadi operatiivisen tason suunnitelmia, se koordinoi ja ohjaa suunnittua. Sillä varmistetaan, että koko organisaatiossa jatkuvuussuunnittelu on yhdenmukaista ja eri toimintoja koskevien suunnitelmien väliset riippuvuussuhteet on mahdollista huomioida. Johdon tulisi nimetä jatkuvuussuunnittelun koordinoinnista vastaavaksi henkilöksi turvallisuusjohtaja tai tietoturvapäällikkö, joka vastaa myös organisaation turvallisuustoiminnan koordinoinnista. (Iivari & Laaksonen 2009, 97.) Suunnittelun vastuutahona eli koordinaattorina organisaatiossa voi näinollen toimia esimerkiksi koko tietoturvatoimielin, joka ei sekään laadi varsinaisia suunnitelmia vaan vain varmistaa, että suunnitelmat laaditaan asianmukaisesti, pidetään ajan tasalla ja harjoitukset toteutetaan suunnitellusti (Iivari & Laaksonen 2009, 99).

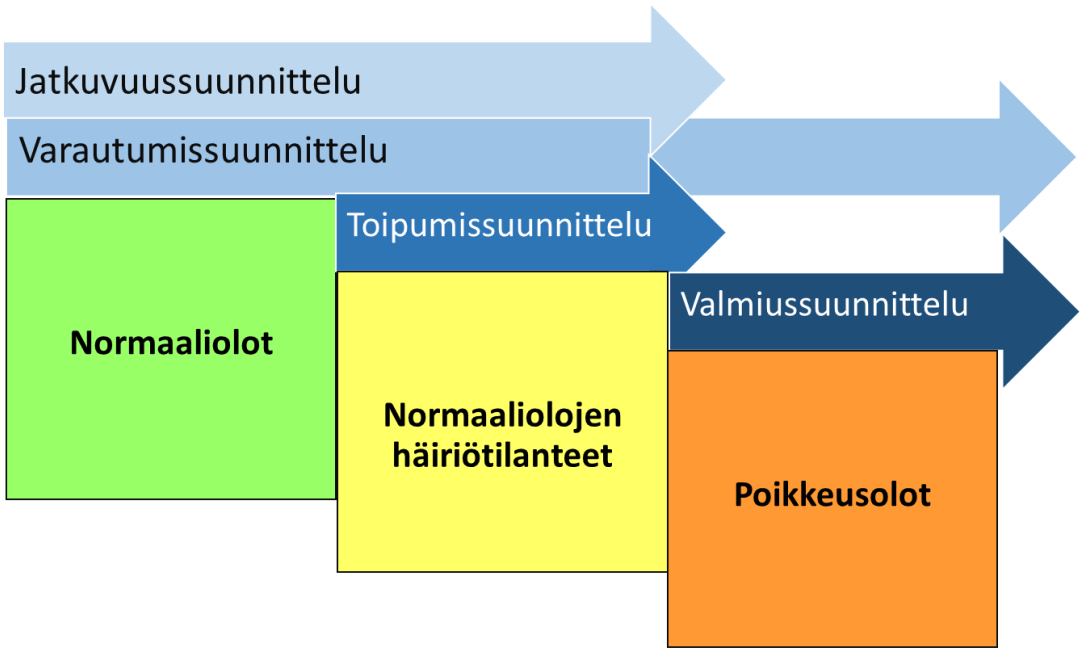
3.3 Varautumis- ja valmiussuunnittelu

Yhteiskunnan toimivuuden kannalta elintärkeiksi toiminnoiksi on valtioneuvoston periaatepäätöksenä 2.11.2017 julkaistussa valtioneuvoston hallinnonalojen varautumista ohjaavassa Yhteiskunnan turvallisuusstrategiassa (14) määritelty johtaminen, kansainvälinen ja EU-toiminta, puolustuskyky, sisäinen turvallisuus, talous, infrastruktuuri ja huoltovarmuus, väestön

toimintakyky ja palvelut sekä henkinen kriisinkestävyys. Nämä toimintokokonaisuudet ovat yhteiskunnan toimivuuden kannalta välttämättömiä ja niitä on ylläpidettävä kaikissa olosuhteissa, myös valmiuslain (1552/2011) tarkoittamat poikkeusolot mukaan lukien.

Poikkeusoloilla tarkoitetaan yhteiskunnassa esiintyvää häiriötekijää, jolla on laajat yhteiskunnalliset vaikutukset ja joka hankaloittaa organisaatioiden toimintaa huomattavasti (Iivari & Laaksonen 2009, 96). Valmiuslaissa (1552/2011, 3§), jonka tarkoituksena on turvata viranomaisille riittävät toimivaltuudet poikkeusoloissa, poikkeusoloiksi katsotaan yhteiskuntaan kohdistuva aseellinen tai siihen rinnastettava hyökkäys tai sen huomattava uhka, erityisen vakava suuronnettomuus sekä edellä mainittuja koskevat välittömät jälkitilat, vakava väestön toimeentuloon tai talouselämään kohdistuva tapahtuma tai sen uhka ja erityisen vakavan suuronnettomuuden vaikutuksia vastaava laajalle levinnyt vaarallinen tartuntatauti.

Poikkeusolot voivat tuhota yritysten liiketoimintamahdollisuudet kokonaan, eikä toimintaa käytännössä ole mahdollista jatkaa normaalisti. Normaaliolojen häiriötilanteiden lisäksi poikkeusolot kattavaa jatkuvuuden hallintaa kutsutaan varautumissuunnitteluksi, jossa poikkeusoloihin varaudutaan täsmällisemmin häiriötilanteista poikkeusoloihin laajennetulla toipumissuunnittelulla eli valmiussuunnittelulla (Iivari & Laaksonen 2009, 20–21). Jatkuvuus-, toipumis, varautumis- ja valmiussuunnittelun suhde on havainnollistettu alla kuviossa (Kuvio 5).



Kuvio 5: Jatkuvuus- ja toipumissuunnittelun sekä varautumis- ja valmiussuunnittelun välinen suhde (Iivari & Laaksonen 2009, 19)

Yhteiskunnan elintärkeiden toimintojen turvaamiseksi tarkoitetun varautumissuunnittelun taustalla vaikuttaa julkishallinnon organisaatioita sekä huoltovarmuuskriittisiä organisaatioita koskevan varautumisvelvollisuuden täyttäminen. Valmiuslain (1552/2011, 12 §) varautumisvelvollisuuden mukaan ”- - valtioneuvoston, valtion hallintoviranomaisten, valtion itsenäisten julkisoikeudellisten laitosten, muiden valtion viranomaisten ja valtion liikelaitosten sekä kuntien, kuntayhtymien ja muiden kuntien yhteenliittymien tulee valmiussuunnitelmin ja poikkeusoloissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä varmistaa tehtäviensä mahdollisimman hyvä hoitaminen myös poikkeusoloissa.”

Varautuminen käsittää myös huoltovarmuuskriittiset organisaatiot, jotka ylläpitävät huoltovarmuutta eli yhteiskunnan taloudellisia perustoimintoja, jotka ovat vakavien häiriöitilanteiden tai poikkeusolojen aikaan välttämättömiä yhteiskunnan toimivuuden, väestön turvallisuuden ja elinmahdollisuuksien sekä maanpuolustuksen materiaalisten edellytysten turvaamiseksi (Huoltovarmuuskeskus 2017b). Elinkeinoelämän asema yhteiskunnallisessa varautumisessa on tärkeä ja yritykset vastaavat jatkossakin keskeisessä asemassa talouden ja infrastruktuurin toimivuuden varmistamisesta. Tämä korostaa edelleen yritysten toiminnan jatkuvuuden turvaamisen merkitystä. (Yhteiskunnan turvallisuusstrategia 2017, 8.)

Valtioneuvoston kanslian sovittaessa yhteen EU:ssa päätettävien asioiden valmistelua ja käsittelyä sekä turvatessa valtion ylimmän johdon toimintaedellytyksiä kaikissa tilanteissa, on sillä keskeinen asema yhteiskunnan elintärkeiden toimintojen turvaamisessa. Nopean ja joustavan päätöksentekovalmiuden mahdollistaminen edellyttää muun muassa toimitilojen ja teknisten järjestelmien toiminnasta sekä kehittämisestä huolehtimista. (Yhteiskunnan turvallisuusstrategia 2017, 30.)

Johtamisen edellytyksenä on toiminnan jatkuvuuden hallinta, yhteistoiminta ja tilannekuvan muodostaminen. Tilannekuvan tuottaminen on valtioneuvoston kanslian varautumistoiminnassa keskeistä, sillä pääministerin rooli valtioneuvoston johtajana korostuu häiriötilanteissa, joissa on toimittava reaaliaikaiseen tietoon perustuen (Yhteiskunnan turvallisuusstrategia 2017, 15–16).

Valtioneuvoston kansliassa toimiva tilannekeskus tuottaa ennakoivaa, reaaliaikaista ja analysoitua tilannekuvaa valtion ylimmän johdon päätöksenteon tueksi kaikissa olosuhteissa. Tilannekuvatoiminnassa ja häiriötilanteiden hallinnassa korostuu yhteistyö, sillä siinä hyödynnetään myös muiden turvallisuustoimijoiden tukea. (Yhteiskunnan turvallisuusstrategia 2017, 30.) Myös kansainvälisen ja EU-toiminnan näkökulmasta tilannekeskus on keskeisessä asemassa, sen toimiessa Suomen yhteyspisteenä EU:n poliittisen kriisitoiminnan integroitujen jär-

jestelyjen (The EU Integrated Political Crisis Response, IPCR) yhteyspisteenä. IPCR:n tavoitteena on luoda Euroopan Unionille kyky tukea tehokkaasti jäsenvaltioitaan kriisitilanteiden hallinnassa. (Yhteiskunnan turvallisuusstrategia 2017, 34.)

3.4 Tietojärjestelmät ja ICT-varautuminen

San Franciscon yliopiston emeritusprofessori Steven Alter (2008, 6) on kuvaillut tietojärjestelmiä ihmisten sekä laitteiden toimintaan perustuviksi informatiivisia palveluita tai tuotteita tuottaviksi, tietoa sekä tekniikkaa hyödyntäviksi työjärjestelmiksi, joiden prosessit ja toiminnot keskittyvät tiedon käsittelyyn kattaen tiedon keräämisen, hakemisen, tallentamisen, muokkaamisen, siirtämisen, lähettämisen sekä esittämisen. Ihmisten ja laitteiden yhteistoimintaan perustuen tietojärjestelmä muodostaakin sosio-teknisen kokonaisuuden (Sjöroos 2017).

Koska tiedon käsittelyä tapahtuu nykypäivänä organisaatioiden kaikissa toiminnoissa, myös tietojärjestelmät ovat keskeinen osa organisaation toimintoja ja monet organisaatioiden kriittisistä prosesseista ovat riippuvaisia tietojärjestelmien toimivuudesta. Niiden sisältämä tieto on välttämätöntä esimerkiksi organisaation ydintoiminnoille, henkilöstölle sekä ulkoisille sidosryhmille, lakiin sekä sopimuksiin perustuvien vaatimusten täyttämiseksi sekä johdon päätöksenteolle (Ransome & Rittinghouse 2011, 87). Organisaation välttämättömiä tietojärjestelmiä ovat esimerkiksi henkilöstö-, talous- ja toimitilahallinnon sekä turvallisuuteen liittyvät järjestelmät.

ICT-varautumisella tarkoitetaan organisaation tietojärjestelmät kattavan tieto- ja viestintäteknisen ulottuvuuden jatkuvuudenhallintaa. ICT-varautumista käsitellään usein strategisella tasolla osana tietoturvallisuuspolitiikka, joka kuvaa eri liiketoimintaprosessien tietojen turvaamistason ja sen ylläpitoon tarvittavat menetelmät sekä keinot organisaation tietoturvallisuuden hallinnointiin ja kehittämiseen (Hakala ym. 2006, 7). Julkisen hallinnon organisaatioille suunnatussa ICT-varautumisen vaatimukset -ohjeessa (VAHTI 2012, 11) se määritellään riskienhallintaan pohjautuvaksi ICT-toiminnan jatkuvuuden hallinnaksi sekä tietojen turvaamiseksi niin normaaliolojen häiriötilanteissa kuin poikkeusoloissa. ICT-varautuminen voidaankin ymmärtää opinnäytetyön kontekstissa ennemmin tieto- ja viestintäteknologiaa koskevana varautumissuunnitteluna kuin jatkuvuussuunnitteluna.

Koko yhteiskunnan ollessa entistä riippuvaisempi ICT-palveluista, Suomen kyberturvallisuus –strategiassakin (2013, 39) kuvatussa sähköisen tiedon käsittelyyn tarkoitettujen tietoverkkojen ja –järjestelmien muodostamassa keskinäisriippuvassa ympäristössä eli kybertoimintaympäristössä ilmenevien uhkien ja niihin varautumisen merkitys kasvaa. ICT-varautumisen kannalta haasteita luovat uhkien realisoitumisen, sekä niiden aiheuttamien häiriöiden vaikutusten

äkillisyys ja ennalta arvaamattomuus. Häiriöt voivat saada alkunsa esimerkiksi tahallisesta vahingonteosta, väärinymmärryksestä, onnettomuudesta, sähkö- tai tietoliikennekatkosta, järjestelmän toiminta- tai käyttövirheestä, laiteviasta tai vaikkapa luonnonilmiöstä. (VAHTI 2012, 15.)

Uhkien monimuotoisuus ja arvaamattomuus aiheuttaa haasteita koko yhteiskunnalle, sillä myös yhteiskunnan elintärkeitä toimintoja tukevat palvelut ovat riippuvaisia ICT-infrastruktuurin toimivuudesta. ICT-palveluilla tarkoitetaan esimerkiksi tietoliikenne- ja käyttöpalveluita, tietoteknisten laitteiden huoltopalveluita sekä tietojärjestelmien kehitys- ja muutostenhallintaan liittyviä palveluita (VAHTI 2012, 57). Suomessa julkisen hallinnon ICT-palveluihin kuuluvat kaikki valtion yhteiset ICT-palvelut, hallinnon turvallisuusverkko (TUVE), jonka toiminta perustuu lakiin julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015), ja siihen liittyvät palvelut sekä yhteiset sähköisen asioinnin tukipalvelut (Yhteiskunnan turvallisuusstrategia 2017, 60).

ICT-palveluiden jatkuvuus pyritään varmistamaan viranomaisten, palveluntuottajien sekä asiakasorganisaatioiden yhteisillä toimintaperiaatteilla sekä menettelytavoilla, joiden tarkoituksena on taata yhtenäinen tietoturvallisuuden taso sekä kyky toiminnan jatkamiseen normaaliolojen häiriötilanteissa ja poikkeusoloissa (VAHTI 2012, 12–13). Hyvä esimerkki viranomaisten ICT-varautumisen yhtenäisestä toteuttamisesta on jo edellä mainittu hallinnon turvallisuusverkko, sillä se muodostaa yhtenäisen turvallisuuden ja varautumisen vaatimukset täyttävän tietoliikenneinfrastruktuurin, joka on useiden eri turvallisuusviranomaisten sekä valtion johdon käytettävissä kaikissa tilanteissa. Sen verkko- ja infrapalvelut tuottaa valtion omistaman Suomen Erillisverkot Oy:n (ERVE) tytäryhtiö Suomen Turvallisuusverkko Oy (STUVE) ja ICT- sekä integraatiopalveluita tuottava valtion tieto- ja viestintätekniikkakeskus Valtorin TUVE-yksikkö (Saastamoinen 2017).

Valtiovarainministeriön ohjatessa ICT-palveluita koskevaa varautumista ja turvallisuutta, keskeisimpiä ohjeita ovat valtiovarainministeriön alaisuudessa toimivan julkisen hallinnon digitaalisen turvallisuuden johtoryhmän julkaisemat ohjeet, jotka ohjeistavat ICT-infrastruktuurin, palveluiden ja turvallisuuden vähimmäisvaatimukset. (Yhteiskunnan turvallisuusstrategia 2917, 60.) ICT-varautumisen vaatimuksen ohjetta käsitellään myöhemmin kohdassa 3.6.1. Yhteiset toimintamallit antavat perustan tietojärjestelmiä koskevalle jatkuvuus- ja toipumissuunnittelulle sekä poikkeusolot huomioivalle varautumis- ja valmiussuunnittelulle.

3.5 Tietojärjestelmien kriittisyyden arviointi ja tiedon luokittelu

Tietojärjestelmien kriittisyyden arviointia käsiteltäessä on syytä ymmärtää, mitä kriittisyydellä opinnäytetyön kontekstissa tarkoitetaan. Kriittisyyttä voidaan tarkastella esimerkiksi suoraan turvallisuuden tai talouden näkökulmasta, jolloin järjestelmiin kohdistuvat häiriöt

vaarantavat turvallisuuden tai vahingoittavat taloutta (Tanhuamäki 2006, 12). Kriittinen järjestelmä voidaan ymmärtää myös yhteiskunnalle välttämättömien rakenteiden ja toimintojen eli kriittisen infrastruktuurin (Critical Infrastructure, CI) osana, jonka lamautuminen voi vaarantaa kansallista turvallisuutta, taloutta, yleistä terveyttä sekä valtionhallinnon toimintaa (Pullinen 2012, 13; Huoltovarmuuskeskus 2017a).

Julkisen hallinnon ICT-varautumisen yhteydessä tietojärjestelmien kriittisyyden arvioinnissa huomioidaankin yleensä yhteen liittyvien organisaation ydintoimintojen ja yhteiskunnan elintärkeiden toimintojen toimivuuden kannalta keskeisiä järjestelmäpiirteitä sekä niiden käyttötarkoituksia riippuen siitä, onko varautumisessa kyse normaaliolojen häiriötilanteisiin vai poikkeusoloihin varautumisesta. Mikäli kysymyksessä on yhteiskunnan elintärkeiden toimintojen kannalta kriittinen järjestelmä, se voidaan katsoa joissakin asiayhteyksissä myös osaksi kriittistä infrastruktuuria.

Kuten jo kohdassa 3.2 esitettiin, toiminnan jatkuvuuden hallinta vaatii tärkeiden prosessien tunnistamista. Sama ajatus pätee myös yksittäisiin tietojärjestelmiin. Ilman tietoresurssien kuten järjestelmien kriittisyyden arviointia, ei organisaatiossa ole mahdollista kehittää toimivaa riskienhallintaohjelmaa, jolla saavutettaisiin tarvittava suojauksen ja varautumisen taso. Jokaisen organisaation tulisi siis määritellä toimintokriittiset tietojärjestelmät. Suuremmissa organisaatioissa tietoteknisen infrastruktuurin ollessa monimutkaista, tietojärjestelmädokumentaatio on erillään jatkuvuussuunnitelmista, jotka kuitenkin laaditaan tietojärjestelmiä koskevan määrittelyn pohjalta. Dokumentaatiota on tärkeää päivittää aina kun tietojärjestelmiin tehdään muutoksia. (CISM 2012, 115; Ransome & Rittinghouse 2011, 89.)

Toiminnalle välttämättömien eli kriittisten tietojärjestelmien tunnistaminen sekä niiden kriittisyyden arviointi, joka johtaa tietojärjestelmien kriittisyys- tai tärkeysluokitteluun, on keskeinen osa jatkuvuuden hallintaa toimialasta riippumatta. Luokiteltavien järjestelmien tunnistaminen perustuu ylimmän johdon suorittamaan strategisen tason määrittelyyn, jossa organisaatiorakenne pilkotaan toimintoperusteisesti toimielimiin kuten yksiköihin. Yksiköiden tärkeys koko organisaation toiminnan kannalta määritellään ja niiden hyödyntämät tietojärjestelmät tunnistetaan. (CISM 2012, 116.)

Tunnistetut ICT-palvelut ja -järjestelmät on luokiteltava niiden kriittisyyden mukaan, jotta korjaavat toimenpiteet osataan priorisoida ja kohdentaa tehokkaasti häiriötilanteissa (VAHTI 2012, 34). Tietojärjestelmien kriittisyyden arvioinnissa määritelläänkin järjestelmiä koskeva toiminnan palautusjärjestys (Iivari & Laaksonen 2009, 205). On muistettava, että tietojärjestelmät eivät ole itseisarvo, vaan ne tukevat tärkeiden prosessien toimintaa. Jatkuvuussuunnittelusta kirjoittaneet Kliem ja Richie (2016, 181) ovat korostaneet, että varautumissuunnitte-

lulla pyritään ensisijaisesti turvaamaan tietojärjestelmien sijaan tärkeiden prosessien toimivuus ja toipuminen häiriötilanteista. Liiallinen keskittyminen tietojärjestelmiin on heidän mukaansa jatkuvuuden hallinnassa yksi yleisimmistä virheistä.

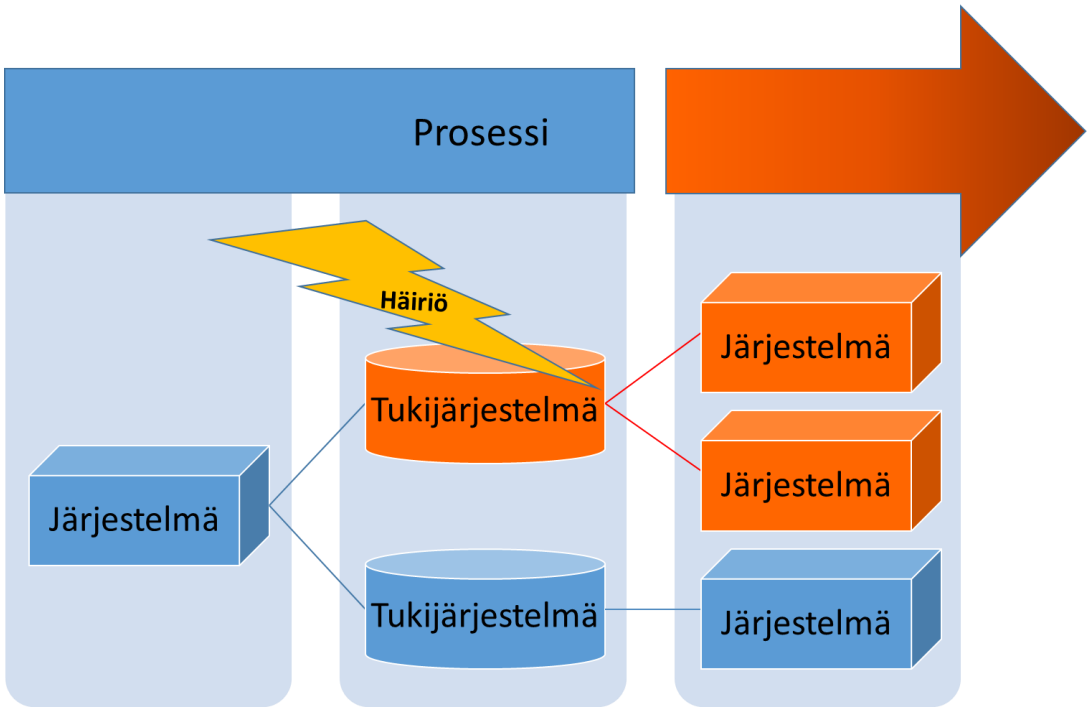
Kriittisyyden arviointi paitsi määrittää tietojärjestelmän tärkeyden organisaatiolle toimii myös kaikkien järjestelmien palvelutasovaatimukset esittävien palvelutasosopimusten (Service Level Agreement, SLA) ja edelleen jatkuvuuden hallintaan liittyvien toimenpiteiden kuten esimerkiksi toipumissuunnitelmien laatimisen sekä niiden pohjalta tietojärjestelmille toteutettavien suojaus-ja varautumistoimenpiteiden perustana (Iivari & Laaksonen 2009, 160). Julkisen hallinnon osalta SLA-palvelutasot on määritelty muun muassa julkisen hallinnon tietohallinnon neuvottelukunnan eli JUHTA:n (2012) julkaisemassa JHS 174 –suosituksessa ICT-palvelujen palvelutasoluokituksesta palvelun laadun mukaisesti.

Tietojärjestelmien kriittisyyden arviointiin liittyy yleensä vaikutusanalyysi, sillä tietojärjestelmien arvioinnissa on otettava huomioon käyttökatkojen vaikutukset organisaation toimintaan. Vaikutusanalyysi onkin yleisesti vaatimuksena toimivan kriittisyyden arvioinnin toteuttamiseksi ja sen tulokset tarjoavat myös perustan tiedon luokittelulle sekä varautumistoimenpiteiden kohdistamiselle (CISM 2012, 64).

Organisaatioon kohdistuvien vaikutusten lisäksi kriittisyyden arvioinnissa tulisi Iivarin ja Laaksosen (2009, 169) mukaan huomioida tietojärjestelmien käyttötarkoitus, tietosisältö sekä niiden välisen tietoliikenteen sisältö. Kriittisyyden taso eli tärkeysluokka määräytyy käytettävän luokituksen mukaan, jossa jokaisella luokalla on määritellyt kriteerit. Tietojärjestelmän tärkeysluokka muodostetaan aina sen sisältämien korkeimman luokan ominaisuuksien mukaan, mikäli tietojärjestelmä vastaa useiden eri luokkien mukaisia kriteereitä (Iivari & Laaksonen 2009, 160).

Kuten kriittisten prosessien tunnistamisessa myös tietojärjestelmien arvioinnissa on huomioitava niiden väliset riippuvuussuhteet. Mikäli riippuvuussuhteita ei huomioida, voi yksittäisessä ei kriittiseksi järjestelmäksi arvioidussa tukijärjestelmässä tapahtuva häiriö ja sen aiheuttama toimintakatkos lamauttaa kriittiseksi arvioidun järjestelmän toiminnan (Kuvio 6). Organisaation kriittiseksi luokitellulla järjestelmällä tai prosessilla voi siis ollakin tukijärjestelmiä, jotka ovat sen toiminnalle välttämättömiä. (Iivari & Laaksonen 2009, 114.)

Riippuvuussuhteet huomioidaan kriittisyyden arvioinnissa samalla korkeamman tason periaatteella kuin tietojärjestelmien ominaisuudet. Tämä tapahtuu niin, että tietojärjestelmä joka tukee muita toimintoja, luokitellaan aina kriittisimmän toiminnon mukaan. Silloin esimerkiksi tukijärjestelmät sijoitetaan kriittisimpien pääjärjestelmien kanssa samaan kriittisyysluokkaan (Iivari & Laaksonen 2009, 160–161).



Kuvio 6: Tukijärjestelmän toimintahäiriö voi lamauttaa useita järjestelmiä ja pysäyttää järjestelmistä riippuvaisen toimintaprosessin

Iivari ja Laaksonen (2009, 161) ovat todenneet, että tietojärjestelmien kriittisyyden arviointiin ei ole olemassa kaikille sopivaa toimintamallia, vaan jokaisen organisaation on huomioitava arvioinnissa omat tarpeensa ja määriteltävä kriittisyysluokkien kriteerit sekä määrän.

Suomessa julkisen hallinnon tietojärjestelmien luokitteluun vaikuttaa keskeisenä tekijänä tiedon luokittelua koskeva kansallinen sekä EU -lainsäädäntö, joka velvoittaa julkishallinnon organisaatioita tältä osin. Tiedon luokitteluun on käytettävä tietoturvallisuusasetuksen eli valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) mukaisia turvallisuus- sekä suojaustasoja. Asetuksessa (681/2010, 8-9 §) säädetään, että salassa pidettävät asiakirjat tai tiedot on luokiteltava suojaustasoluokitusten I-IV mukaan sen perusteella, mitä suojattavan edun kannalta välttämättömiä tietoturvallisuusvaatimuksia niiden sisällön käsittelyssä tulee noudattaa.

Salassa pidettävien tietojen suojaustasojen lisäksi asetuksessa säädetään myös tietojen turvallisuusluokituksesta, jota voi käyttää vain, mikäli ”- - asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle - -” (681/2010, 11 §). Turvallisuusluokituksen suojaustasoja sekä salassa pidettävän tiedon suojaustasoja on käytössä molempia yhteensä 4 (Taulukko 1) ja niitä voidaan käyttää rinnakkain tai toisensa korvaten.

Suojaustasot	Turvallisuusluokat
SALASSA PIDETTÄVÄ, Suojaustaso I	ERITTÄIN SALAINEN, Suojaustaso I
SALASSA PIDETTÄVÄ, Suojaustaso II	SALAINEN, Suojaustaso II
SALASSA , Suojaustaso III	LUOTTAMUKSELLINEN, Suojaustaso III
SALASSA PIDETTÄVÄ, Suojaustaso IV	KÄYTTÖ RAJOITETTU, Suojaustaso IV

Taulukko 1: Tietoturvallisuusasetuksen (681/2010) mukaiset tiedon suojaustasot ja turvallisuusluokat

Mikäli tietoa vaihdetaan kansainvälisesti, julkisessa hallinnossa on huomioitava myös kansainvälisten tiedon turvallisuusluokitusjärjestelmien kuten NATO:n (North Atlantic Treaty Organization) tai EU:n luokitusjärjestelmät. Kansallinen luokitusjärjestelmä vastaa ainakin edellä mainittujen luokittelujärjestelmien malleja. Tietojen kuuluessa luokittelusta tehdyn molemminpuolisen sopimuksen piiriin tai tietoturvallisuusvelvoitteista annetun lain piiriin, niihin tehdään Suomen turvallisuusluokitusta vastaava merkintä (VAHTI 2010, 58).

On muistettava, että vaikka tiedon luokittelumallit ovat velvoittavia, kriittisyyttä arvioidaan monesta eri näkökulmasta, ensisijaisesti organisaation strategiset toimintatavoitteet huomioiden. Valtioneuvoston kansliassa toteutuvaa kriittisyyden arviointia on käsitelty tutkimuksen tuloksissa kohdassa 5.1. Kriittisyyden arviointiin liittyen on olemassa lähinnä jatkuvuuden hallintaa käsitteleviä sekä kansallisia että kansainvälisesti yleisesti hyödynnettäviä malleja, joita on mahdollista käyttää apuna arvioinneissa. Kansalliset julkiselle hallinnolle tarkoitetut ohjeet ovat luonnollisesti tietoturvallisuuslainsäädäntöä noudattelevia. Toimintamalleja käsitteleviä ohjaavia dokumentteja esitellään tietojärjestelmien kriittisyyden arvioinnin näkökulmasta seuraavassa osiossa.

3.6 Tietojärjestelmien kriittisyyden arviointi ohjaavissa dokumenteissa

Vaikka jatkuvuuden sekä tietoturvallisuuden hallintaa koskevia standardeja, ohjeita ja työkaluja on useita, ne sisältävät yksityiskohtaisten menetelmäohjeiden sijaan lähinnä suuntaviivoja ja yleispäteviä toimintamalleja tietojärjestelmien kriittisyyden arviointia varten.

Tässä osiossa käsitellään joidenkin tunnetuimpien standardien, ohjeiden ja työkalujen yhtymäkohtia tietojärjestelmien kriittisyyden arviointiin. Käsiteltävänä ovat ICT-varautumista koskevat VAHTI-ohjeet, kansainväliset ISO-standardit, VAHTI-ohjeiden tapaan Yhdysvaltojen julkisen hallinnon tietoturvallisuuden jatkuvuussuunnittelun ohjeena toimiva NIST 800-34 sekä Katakri, joka on kansallinen tietoturvallisuuden auditointityökalu viranomaisille.

3.6.1 ICT-varautumisen vaatimukset

Julkisen hallinnon ICT-varautumista ohjaava keskeinen dokumentti on julkisen hallinnon digitaalisen turvallisuuden johtoryhmän julkaisema ICT-varautumisen vaatimukset. Julkaisu on ohje, jonka tavoitteena on tehostaa sekä yhdenmukaistaa ministeriöiden ja hallinnonalojen organisaatioiden ICT-varautumista. Ohje asettaa varautumisen yhtenäistämisen kannalta keskeiset vaatimukset julkisen hallinnon toimijoille sekä näihin palvelusopimussuhteessa oleville yrityksille. Vaatimusten tarkoituksena on parantaa verkostomaisesti toimivien palveluiden jatkuvuutta, häiriönsietokykyä sekä toipumista häiriötilanteista. Ohje keskittyy parantamaan organisaatioiden kykyä varautua tietoturva- sekä kyberuhkiin. (VAHTI 2012, 5.)

Ohje edellyttää valtionhallinnon organisaatioita ottamaan toiminnassaan huomioon siinä kuvatut vaatimukset, jotka on ulotettava koskemaan sekä valtionhallinnon sisäisiä että ulkoisia palveluntuottajia (VAHTI 2012, 5). Keskeisenä vaatimuksena on, että organisaatioiden on määriteltävä kullekin palvelulle ja järjestelmälle niitä edellyttävä varautumisen taso ja tason mukainen palveluiden toteuttamisen aikataulu sekä resursoida toteutus osana normaalia talouden ja muun toiminnan suunnittelua (VAHTI 2012, 11).

Julkishallinnon organisaatioiden on arvioitava järjestelmien kriittisyys ja luokiteltava ne ensisijaisesti elinkaaren luonnollisessa vaiheessa kuten päivityksen tai kilpailutuksen yhteydessä joko perustasolle, korotetulle tai korkealle tasolle varautumisen vaatimusten mukaan (VAHTI 2012, 25). Arvioinnissa on otettava huomioon järjestelmien merkitys niin organisaation omalle toiminnalle kuin yhteiskunnan elintärkeille toiminnoille ja arvioitava erilaisten uhkien vaikutus niiden toimintakykyyn (VAHTI 2012, 34).

VAHTI-ohjeessa (2012, 21–23) kuvataan järjestelmien tunnuspiirteitä varautumisen vaatimustasojen mukaisesti. Avoimelle tasolle luokitellaan tyypillisesti järjestelmä, jonka luokittelu on kesken tai järjestelmä ei täytä ICT-varautumisen vaatimuksia. Avoimessa luokassa olevat järjestelmät voivat olla esimerkiksi lisäarvoa tuottavia järjestelmiä, joiden sijaan voidaan käyttää toista käytössä olevaa järjestelmää ja joiden toimimattomuus ei lamauta organisaation perustoimintoja.

Perustasolla järjestelmät ovat osana organisaation normaaleja toimintoja, mutta niiden hetkelliset häiriöt eivät vaikuta organisaation ydintoimintoihin. Tyypillisen perustason järjestelmän hyödyntäminen tapahtuu virka-aikana, joten ilmaantuneen häiriön korjaustoimenpiteet voidaan aloittaa havaintoa seuraavana arkipäivänä, joka on myös järjestelmän tavoitteellinen toipumisaika häiriöstä. (VAHTI 2012, 21–22.)

Korotettu taso on organisaatioiden toiminnan jatkuvuuden kannalta kriittisten toimintojen minimitaso. Tasolle luokitellaan yhteiskunnan elintärkeitä toimintoja tukevat sekä häiriötilanteissa tarpeelliset järjestelmät, kuten kriisiviestintään tarkoitetut järjestelmät. Korotetun tason luokittelu vaatii organisaatiolta häiriöihin varautumisen toimenpiteitä, joiden todentamiseen suositellaan ulkopuolista tahoa. (VAHTI 2012, 21–22.)

Korkealle tasolle luokitellut järjestelmät kytkeytyvät yhteiskunnan elintärkeiden toimintojen toimivuuteen kuten turvallisuusviranomaisten toimintaan. Järjestelmissä esiintyvät häiriöt ja toimintakatkot johtavat vakaviin toiminnallisiin häiriöihin sekä taloudellisiin vaikutuksiin, joten niiltä edellytetään ympärivuorokautista toimintaa, valvontaa, hallintaa sekä viankorjausta. Korkean tason järjestelmien on myös toimittava vaikka tietoliikenneyhteydet ulkomaille olisivat poikki tai yksi sen konesaleista vaurioituisi. Luokitus vaatii kansallisen tietoturvaviranomaisen (National Communications Security Authority, NCSA) eli Viestintäviraston tai sen hyväksymän toimijan suorittaman todentamisen. (VAHTI 2012, 22–23.)

Korkean tason luokituksen lisäksi järjestelmät voidaan luokitella erityistasolle, jos järjestelmän toiminta edellyttää korotetun ja korkean tason vaatimusten soveltamista ja yhteisistä menetelmistä poikkeavien erityisten varautumisratkaisujen käyttöönottoa. Luokituksesta päätetään hallinnonaloilla ministeriötasolla ja sen hyväksyy valtiovarainministeriö. Luokituksen mukaiset menettelyt vaativat myös Viestintäviraston tai sen hyväksymän toimijan suorittaman todentamisen. (VAHTI 2012, 23.)

3.6.2 ISO –standardit

Kansainvälisen standardoimisjärjestö ISO (International Organization for Standardization) on maailmalla arvostettu standardeita julkaiseva järjestö. Järjestön jäseniä ovat kansalliset standardoimisjärjestöt kuten Suomen Standardoimisliitto SFS ry, joka vastaa ISO–standardien kansallisesta julkaisusta. Standardeja käytetään yleisesti niin liiketoimintaympäristössä kuin julkisessa hallinnossakin ja osa niistä soveltuu sertifiointikäyttöön. Standardit ovat luonteeltaan suosituksia, vaikka niitä käytetäänkin usein velvoittavina vaatimuksina organisaatioiden välisissä sopimussuhteissa.

Järjestö on julkaissut muun muassa jatkuvuuden hallinnan suunnitteluun käytettäviä standardeja. SFS-EN ISO 22313:2014 Yhteiskunnan turvallisuus –standardissa (Suomen Standardoimisliitto SFS 2014, 13) opastetaan jatkuvuuden hallintajärjestelmän käyttöön ja kriittisten tietojärjestelmien tunnistaminen esitetään osana jatkuvuuden hallinnan suunnitteluvaihetta sekä sisäisen toimintaympäristön arviointia. Sama malli esitetään myös SFS-ISO 31000:2011 Riskienhallinta –standardissa (Suomen Standardoimisliitto SFS 2011a, 22), jossa tietojärjestelmien, tiedonkulun ja päätöksentekoprosessien arvioinnit ovat sisäisen toimintaympäristön arvioinnin osana välttämättömiä riskien hallinnan toteuttamiseksi.

ISO/IEC 27000 –standardisarja sisältää yleisesti tietoturvallisuuden hallintaan käytettyjä suosituksia, joissa esitetään muun muassa malli tietoturvallisuuden hallintajärjestelmälle. Koska jatkuvuudenhallinnalla pyritään myös tiedon turvaamiseen, on standardeissa useita yhtymäkohtia tietojärjestelmiä koskevaan toipumissuunnitteluun.

Tietojärjestelmien kriittisyyden arviointi voidaan katsoa osaksi organisaation tietoturvallisuuden hallintajärjestelmää tukevien tietoturvavaatimusten määrittelyä (Suomen Standardoimisliitto SFS 2011b, 48). Informaatioteknologiaa koskevaa turvallisuutta ja tietoturvariskien hallintaa käsittelevässä standardissa SFS-ISO/IEC 27005 (Suomen Standardoimisliitto SFS 2013, 34) on käytetty suojattavien kohteiden käsitettä, joka määritellään siinä seuraavasti: ”Suojattava kohde on mikä tahansa asia, jolla on arvoa organisaatiolle ja joka sen vuoksi edellyttää suojaamista.”

Suojattavaksi kohteeksi voidaan katsoa esimerkiksi tietojärjestelmä. Standardin mukaan jokaiselle suojattavalle kohteelle on määriteltävä omistaja vastuiden määrittämiseksi. Omistajalla voi olla omistusoikeuden sijaan esimerkiksi vastuu tietojärjestelmän tuottamisesta, ylläpidosta, kehittämisestä, turvallisuudesta tai käytöstä ja se on usein sopivin taho määrittämään tietojärjestelmän kriittisyys organisaatiolle. (Suomen Standardoimisliitto SFS 2013, 34.)

Standardissa esitetään yleispätevä malli organisaation suojattavien kohteiden arvon määrittämiseksi. Suojattavan kohteen ollessa tietojärjestelmä, arviointimallia voidaan soveltaa esimerkiksi tietojärjestelmien kriittisyyden arviointiin. Mallissa lähdetään liikkeelle arviointiin käytettävien kriteerien määrittelystä. Esimerkkinä arvon muodostaviksi kriteereiksi siinä on esitelty häiriön aiheuttaman luottamuksellisuuden, eheyden tai käytettävyyden menetykseen liittyvät kustannukset. Standardissa suositellaankin sellaisten kriteerien käyttämistä, jotka perustuisivat häiriön korvauskustannuksen lisäksi sen aiheuttamiin organisaation toimintaan kohdistuviin haitallisiin vaikutuksiin. (Suomen Standardoimisliitto SFS 2013, 78.)

Organisaation on valittava arvon määrittelemiseksi kriteerit, jotka ovat sen toiminnan ja turvallisuusvaatimusten kannalta olennaisia. Mallin seuraavassa vaiheessa määritelläänkin, mitä osa-alueita suojattavien kohteiden luottamuksellisuuden, eheyden, käytettävyyden, kiistämättömyyden, vastuullisuuden tai aitouden ja luotettavuuden menetyksen aiheuttamien seurauksien vaikutuksista otetaan arvioinnissa huomioon. (Suomen Standardoimisliitto SFS 2013, 78.)

Vaikutusten esimerkkeinä standardissa on lueteltu lainsäädännön tai määräysten rikkominen, haitallinen vaikutus organisaation suorituskykyyn tai maineeseen, henkilötietojen vuotaminen

tai muu tietovuoto, ihmisten tai ympäristön turvallisuuden vaarantuminen, haitalliset vaikutukset lakien täytäntöönpanoon ja julkisen järjestyksen rikkominen. (Suomen Standardoimisliitto SFS 2013, 78.)

Kriteerien määrittelyvaihetta seuraa standardissa käytettävän arviointiasteikon määrittäminen, jossa valitaan käytettävien kriittisyysluokkien määrä. Tähän ei ole standardin mukaan yleispätevää sääntöä, mutta tasojen määrä parantaa erottelukykyä. Toisaalta tasojen määrä vaikuttaa myös arviointien yhdenmukaisuuteen. Tasoja voi olla kolmesta kymmeneen, mutta niiden määrässä on noudatettava organisaation riskienarviointiprosessin kanssa yhtenäistä toimintamallia. (Suomen Standardoimisliitto SFS 2013, 78.)

Standardin mukaan arvioinnissa on syytä huomioida myös arvioinnin kohteisiin liittyvät riippuvuussuhteet. Tämä tarkoittaa sitä, että arvoon vaikuttavat myös tietojärjestelmien tukemien liiketoimintaprosessien olennaisuus sekä määrä. Tietojärjestelmien sekä prosessien väliset sekä tietojärjestelmien väliset riippuvuussuhteet olisi siis tunnistettava ennen arviointia. (Suomen Standardoimisliitto SFS 2013, 78.)

3.6.3 NIST 800-34

National Institute of Standards and Technology (NIST) ohjaa Yhdysvaltain hallinnon tietoturvallisuustoimintaa ja on julkaisemassaan liittovaltion tietojärjestelmien jatkuvuussuunnittelua koskevassa ohjeessa käsitellyt muun muassa tietojärjestelmiä koskevaa jatkuvuussuunnittelun prosessia. Ohjeessa kriittisten tietojärjestelmien arviointi toteutetaan osana vaikutusanalyysia, joka esitellään kolmivaiheisena prosessina. Siinä vaikutusanalyysi kattaa toimintaprosessien ja toipumisen kriittisyyden määrittelyn, vaadittavien resurssien tunnistamisen sekä järjestelmäresurssien toipumisprioriteettien tunnistamisen. (Bowen, Gallup, Lynes, Swanson & Wohl Phillips 2010, 15–16.)

Ohjeen mukaisessa mallissa kriittisyyden tarkasteluun on useita näkökulmia, sillä tietojärjestelmät kuvataan monimutkaisina kokonaisuuksina, jotka tukevat usein monia organisaation toimintaprosesseja. Siinä edellytetäänkin tietojärjestelmiä koskevasta jatkuvuussuunnittelusta vastaavalta taholta tiivistä työskentelyä sekä johdon että sisäisten ja ulkoisten toimintojen edustajien kanssa, jotta riippuvuussuhteet tietojärjestelmien ja prosessien välillä voidaan selvittää. (Bowen ym. 2010, 16.)

Riippuvuussuhteiden tunnistamisen jälkeen on analysoitava järjestelmille merkittävien prosessien vaikutusta niiden sisältämän tiedon saatavuuteen, eheyteen sekä luottamuksellisuuteen, joiden avulla muodostetaan vaikutustasot arvioitavalle tietojärjestelmälle. (Bowen ym. 2010, 16.) Vaikutustasot on jaettu Yhdysvaltain hallinnon tiedon ja tietojärjestelmien turvalli-

suusluokittelustandardin (Standards for Security Categorization of Federal Information and Information Systems 2004, 6) mukaisiin kategorioihin, jotka ovat alhainen (Low), kohtalainen (Moderate) ja korkea (High).

3.6.4 Katakri 2015

Tietoturvallisuuden auditointityökalussa (Katakri 2015) kootaan yhteen viranomaisten salassa pidettävän tiedon suojaamiseksi tarkoitetut vähimmäisvaatimukset. Työkalun vaatimusten sisältö perustuu voimassaolevaan lainsäädäntöön, josta keskeisimpänä vaatimusperustana on käytetty valtioneuvoston asetusta tietoturvallisuudesta valtionhallinnossa (681/2010).

Katakri on tarkoitettu lähinnä yritysten turvallisuusjärjestelyjen toteutumisen sekä viranomaisten tietojärjestelmien turvallisuuden arviointiin, mutta siinä on joitakin yhtymäkohtia tietojärjestelmien kriittisyyden arviointiin osana jatkuvuuden hallintaa. Työkalu koostuu kolmesta tietoturvallisuuden hallintaan liittyvästä osa-alueesta, joita ovat turvallisuusjohtaminen, fyysinen turvallisuus sekä tekninen tietoturvallisuus. Teknisen tietoturvallisuuden osa-alueessa on kuvattu yksityiskohtaisia vaatimuksia tietojen käsittelyn vaiheisiin liittyen. (Katakri 2015, 3.)

Turvallisuusjohtamisen osa-alueessa vaatimuksena jatkuvuudenhallinnasta esitetään, että toipuminen sekä toiminnan jatkuvuuden varmistaminen on huomioitu jatkuvuussuunnittelussa ja suunnittelu sisältää sekä ennaltaehkäiseviä että korjaavia toimenpiteitä (Katakri 2015, 10). Tietojen luokittelun vaatimuksena on yksiselitteisesti se, että tiedot on luokiteltu lakisääteisten vaatimusten perusteella (Katakri 2015, 12). Tämä koskee myös tietojärjestelmien kriittisyyden arvioinnissa huomioitavaa luokittelua järjestelmän käsittämän tiedon osalta.

Fyysisen turvallisuuden osa-alueessa tietojärjestelmien kriittisyyden arviointiin yhtymäkohtana on jatkuvuudenhallinnan vaatimus siitä, että tietojärjestelmien komponentteina toimivat kriittiset palvelimet ja laitteet on tunnistettu ja varmennettu toimintavaatimusten mukaisesti (Katakri 2015, 28). Kriittisten palvelinten ja laitteiden tunnistaminen ei käytännössä ole mahdollista, mikäli tietojärjestelmiä koskevaa kriittisyyden arviointia ei ole organisaatiossa tehty.

4 Tutkimusasetelma, -vaiheet ja -menetelmät

Tapaustutkimus valittiin opinnäytetyön tutkimusstrategiaksi, sillä sen avulla oli mahdollista tarkastella perusteellisesti toimeksiantajaorganisaation sisäistä kriittisyyden arvioinnin prosessia. Tavoitteena oli muodostaa tapauksen käsittämästä prosessista ja siihen liittyvästä teoreettisesta viitekehyksestä mahdollisimman syvällinen ja kokonaisvaltainen kuva sekä tuottaa

tutkimuksen keinoin kehittämisehdotuksia ja -ideoita. Tapaustutkimus oli luonnollinen valinta, sillä se mahdollisti tavoitteeseen pääsemiseksi intensiivisen sekä yksityiskohtaisen tiedon keräämisen useita eri menetelmiä käyttäen. (Hirsjärvi ym. 2009, 132–135; Ojasalo ym. 2014, 37.)

Tapaustutkimuksen ollessa yksi kvalitatiivisen eli laadullisen tutkimuksen lajeista (Hirsjärvi ym. 2009, 162), myös opinnäytetyön painopiste oli laadullisessa tutkimusotteessa. Laadulliselle tutkimusotteelle ominaisesti opinnäytetyö vaati kokonaisvaltaista tiedonkeruuta ja siinä keskityttiin tulkintaan, joka näkyy myös laadullisen lähestymistavan menetelmävalinnoissa. Menetelmissä tapausta koskevan tiedonkeruun kohdejoukko oli valittu tarkoituksenmukaisesti käsittäen vain tutkittavaan tapaukseen liittyvät henkilöt sekä dokumentit. (Hirsjärvi ym. 2009, 164.)

Tapaustutkimuksessa lähdettiin johdannossa esiteltyjen tutkimuskysymysten mukaisesti liikkeelle prosessin nykyisen tilan selvittämisestä eli siitä, miten tietojärjestelmien kriittisyyden arviointi valtioneuvoston kansliassa toteutetaan. Tiedon keräämiseen käytettiin arviointiprosessiin osallistuvien asiantuntijoiden haastattelua teemahaastattelulla kasvotusten sekä puhelimitse. Keskeisenä menetelmänä prosessiin perehtymiseen käytettiin haastattelujen lisäksi dokumenttianalyysiä, jossa keskityttiin tietojärjestelmien kriittisyyden arviointia koskevaan julkiseen dokumentaatioon.

Haastattelujen ja dokumenttianalyysin avulla kerätyn tiedon pohjalta prosessin kuvaamiseksi käytettiin menetelmänä prosessianalyysia eli blueprinting'iä, jossa prosessin vaiheita tarkasteltiin kuvaamalla ja mallintamalla ne prosessikaavioon. Prosessikaavion tavoitteena olikin arviointiprosessin kehittämiskohteiden hahmottaminen. Kehittämisratkaisujen löytämiseksi käytettiin menetelmänä benchmarking'ia eli esikuva-arviointia, jossa pyrittiin etsimään prosessiin sopivia vaihtoehtoisia toimintatapoja teoreettisesta viitekehyksestä sekä muista tarkoitukseen soveltuvista lähteistä.

Tämän osion tarkoituksena on perustella ja esitellä opinnäytetyössä käytetyt menetelmät lähteenä käytettyihin tutkimusoppaisiin pohjautuvan teorian avulla sekä käsitellä menetelmien työvaiheet. Varsinaiset tulokset sekä niiden analysointi käydään läpi kohdassa 5 ja menetelmien työdokumentaatio kuten haastattelurungot ja vertailutaulukko ovat dokumentin liitteenä (Liitteet 1, 2 ja 3).

4.1 Haastattelu

Haastattelu on tapaustutkimuksille keskeinen tiedonlähde ja haastateltavat henkilöt voivat muodostua tutkimuksen onnistumisen kannalta ratkaiseviksi tiedonlähteiksi (Yin 2009, 106–

107). Haastattelu toimii varsinkin kvalitatiivisten tutkimusten päämenetelmänä, ja tämän ollessa myös opinnäytetyön tutkimusote, haastattelut olivat luonnollinen valinta tiedonkeruumenetelmäksi. Valintaa tuki myös se, että tutkittava aihe oli haastattelijalle ennestään tuntematon. (Hirsjärvi ym. 2009, 205.)

Yin (2009, 106) on todennut, että tapaustutkimuksessa menetelmänä käytettävien haastatteluiden tulisi olla enemmän jouhevan keskustelun muotoisia kuin jäykkiä haastattelutilanteita tiukasti rajattuine kysymyksineen. Tähän perustuen haastattelulajina käytettiin teemahaastattelua eli puolistrukturoitua haastattelua, joka on strukturoidun eli lomakehaastattelun ja avoimen eli keskusteluluonteisen haastattelun välimuoto (Hirsjärvi ym. 2009, 208).

Teemahaastattelussa aiheet olivat selvillä ja alustavat kysymykset oli laadittu ennakkoon, mutta kysymysten tarkkaa muotoa, niiden lukumäärää tai järjestystä ei ollut ennalta määritelty (Hirsjärvi ym. 2009, 208). Menetelmä mahdollisti sen, että ennalta laaditut haastattelutilanteeseen soveltumattomiksi havaitut kysymykset voitiin jättää kysymättä ja tarpeen vaatiessa haastateltaville voitiin esittää vasta haastattelutilanteessa mieleen tulleita kysymyksiä (Ojasalo ym. 2014, 108).

Työn tiiviin aikataulun vuoksi teemahaastattelu toteutettiin ryhmähaastatteluna, jonka avulla tiedonkeruu oli tehokkaampaa kuin yksilöhaastattelussa, sillä tietoa oli mahdollista kerätä nopeasti ja samanaikaisesti usealta vastaajalta (Hirsjärvi ym. 2009, 210; Hirsjärvi & Hurme 2008, 63). Useamman haastateltavan läsnäolo auttoi aktivoimaan keskustelua käsitellyistä teemoista ja toi esille erilaisia näkökulmia. Taustalla vaikutti myös opinnäytetyön suunnitteluvaiheen riskienarviointi, jossa työn eteneminen pyrittiin ryhmähaastattelulla varmistamaan, mikäli joku haastateltavista henkilöistä esimerkiksi sairastumisen tai muun tapahtuman vuoksi olisi estynyt osallistumaan haastattelutilaisuuteen sovittuna ajankohtana. Haastattelun runko laadittiin ennalta haastattelutilannetta varten ja se sisälsi käsiteltävät aiheet sekä alustavia kysymyksiä. Ryhmähaastattelun teemarunko on esitelty liitteenä (Liite 1).

Haastattelulla pyrittiin selvittämään tietojärjestelmien kriittisyyden arvioinnin nykytilan lisäksi jatkuvuuden hallinnan organisaatiokohtaisia puitteita ja tutkittavan arviointiprosessin edellytyksiä. Haastattelun teemarunko muodostettiin teoreettisen viitekehyksen rakennetta mukaillen siten, että ensimmäiseksi käsiteltävät aiheet liittyivät jatkuvuuden hallinnan käsitteistöön, rooleihin sekä suunnittelun vastuisiin. Jatkuvuuden hallinnan käsitteistön läpikäymisen tarkoituksena oli varmistaa, että osapuolet ymmärtävät haastattelutilanteessa käytettävien käsitteiden merkityksen samalla tavalla. Haastattelussa ei syvennytty välittömästi tarkastelemaan kriittisyyden arviointia myös sen vuoksi, että tarkoituksena oli muodostaa prosessin toimintaympäristöstä objektiivinen kuva ja huomata seikkoja, jotka voisivat vaikuttaa välillisesti tai suoraan tutkittavaan prosessiin.

Yhtenä teemana oli vastuiden ja roolien lisäksi tietojärjestelmien kriittisyyden arvioinnin perusteiden sekä prosessissa sovellettavien ja hyödynnettävien ohjeiden, menetelmien sekä työkalujen käsitteleminen. Teeman tarkoituksena oli selvittää, kuinka kriittisyyden arviointi valtioneuvoston kansliassa tapahtuu ja ketkä siihen osallistuvat.

Ensimmäinen haastattelutilaisuus pidettiin valtioneuvoston kanslian tiloissa Helsingissä 20.10.2017. Haastatteluun oli varattu aikaa 2 tuntia. Ryhmähaastatteluun osallistuivat neuvotteleva virkamies Petri Puhakainen sekä erityisasiantuntijat Marko Sjöroos ja Mika-Jan Pullinen valtioneuvoston kansliasta.

Ensimmäisen teemahaastattelun lisäksi pidettiin toinen teemahaastattelu puhelimitse 6.11.2017, jossa haastateltavana oli tietoturvallisuuden erityisasiantuntija Marko Sjöroos valtioneuvoston kansliasta. Haastattelussa keskityttiin niin ikään teemarunkoon (Liite 2) ennalta laadittujen aiheiden ja alustavien kysymysten avulla viimeaikaisiin tietojärjestelmien kriittisyyden arviointia koskeviin tapahtumiin, prosessin vaiheiden selvittämiseen sekä siihen, mitä tietojärjestelmien kriittisyysarvion muodostaminen valtioneuvoston kanslian tarpeet huomioiden edellyttää.

Haastatteluista kerätty laadullinen tieto kirjoitettiin puhtaaksi eli litteroitiin laadullista analyysia varten. Haastattelutiedon perusteella muodostettu valtioneuvoston kanslian kriittisyyden arvioinnin nykytila on kuvattu tulokset –osiossa kohdassa 5.1.

4.2 Dokumenttianalyysi

Haastatteluiden tukena kriittisyyden arvioinnin prosessiin perehtymiseksi käytettiin tutkimusmenetelmänä dokumenttianalyysia, jota käytetäänkin yleensä yhdistettynä muihin tiedonkeruumenetelmiin. Dokumenttianalyysi kattoi kaikki tutkimusaineistoksi kelpaavat dokumentit, jotka sisälsivät käyttökelpoista tietoa tietojärjestelmien kriittisyydestä ja sen arvioinnista. Tarkasteltavaan dokumenttiin suhtauduttiin analyysissä kriittisesti, huomioimalla erityisesti mihin tarkoitukseen dokumentti on tuotettu, ja kuka sen on tuottanut. (Ojasalo ym. 2014, 43.) Dokumenttianalyysillä keskityttiin tutkittavana olleiden tietojärjestelmien kriittisyyden arvioinnin prosessia koskevaan dokumentaatioon sisällön analyysillä eli sanallisella kuvauksella (Ojasalo ym. 2014, 137) siitä, mitä kyseiset dokumentit käsittelevät ja mikä on niiden tarkoitus prosessissa.

Dokumenttianalyysissä ei käsitelty järjestelmiä koskevia arviointeja tai tietojärjestelmäkuvauksia. Näiden dokumenttien sisällöllä ei ollut merkitystä tutkimustavoitteiden saavuttamiseksi, sillä tutkittava oli arviointitietojen sijaan toimintatapa ja käytettävät menetelmät

sekä työkalut. Tämän lisäksi kyseisten dokumenttien käsittely ei ollut mahdollista niiden sisältämien tietojen salassapidon vuoksi.

Osa menetelmän tuloksista on esitelty osana teoriapohjaa, sillä keskeisenä aineistona menetelmässä toimivat valtioneuvoston kansliaa varautumisessa velvoittava lainsäädäntö, josta keskeisimpänä dokumenttina käytettiin valmiuslakia (1552/2010) sekä julkista hallintoa ohjaavat Yhteiskunnan turvallisuusstrategia (2017) ja ICT-varautumisen vaatimukset –ohje (VAHTI 2012), joihin valtioneuvoston kansliassa toteutettava ICT-varautuminen perustuu. Keskeisimpänä dokumenttina kriittisyyden arvioinnin prosessin tutkimiseen käytettiin valtiovarainministeriön (2017) julkaisemaa vaikutusanalyysityökalua, joka käsitellään kohdassa 5.2.

4.3 Prosessianalyysi

Prosessianalyysi eli blueprinting valittiin menetelmäksi, sillä sen avulla oli mahdollista ymmärtää kokonaisuutta yksittäisiä vaiheita tarkastelemalla ja selvittää, miten vaiheet vaikuttavat arviointiprosessin kokonaisuuteen. Menetelmän tarkoituksena oli luoda prosessin eri vaiheita havainnollistava yksityiskohtainen prosessin etenemiskartta eli prosessikaavio. (Ojasalo ym. 2014, 44.)

Yksityiskohtaisen prosessikartan laatiminen ei haastatteluissa sekä dokumenttianalyysillä kerättyjen tietojen perusteella suunnitellulla tarkkuudella onnistunut, sillä tietojärjestelmien kriittisyyden arvioinnista ei ollut nykytilassa olemassa yksiselitteistä prosessia, jossa yksityiskohtaiset vaiheet olisi mallinnettu tai mallinnettavissa visuaaliseen prosessikarttaan.

Yksityiskohtaisen prosessikartan sijaan menetelmällä kuvattiin tietojärjestelmien kriittisyydenarvioinnin prosessi osallistuvien tahojen roolien, vastuiden sekä tehtävien tarkkuudella vaiheittain niin tarkasti kuin nykytilan mallintaminen yhdeksi prosessiksi oli haastatteluilla kerätyn tiedon perusteella mahdollista. Prosessin nykytila on kuvattu työn tuloksissa kohdassa 5.1, jossa kuvauksen perusteella mallinnettu prosessi toimii nykytilan hahmottamista tukevana visuaalisena kuviona (Kuvio 7).

4.4 Benchmarking

Vaihtoehtoisia toimintatapoja etsittiin useisiin ulkopuolisiin teorialähteisiin tutustumalla. Päämenetelmänä kehittämisratkaisujen etsimiseen käytettiin tietoperustassa esitellyn sekä menetelmän aineistoksi kerätyn tiedon analyysiin perustuvaa bencmarking'ia eli esikuva-arviointia. Esikuva-arvioinnin tavoitteena oli muodostaa vertailukohtia ja kerätä niistä valtioneuvoston kanslian toimintaympäristöön sekä prosessiin soveltuvia parhaita käytäntöjä, joita oli mahdollista hyödyntää arviointiprosessia koskevien kehitysratkaisujen muodostamisessa. (Ojasalo ym. 2014, 44.)

Vertailukohtia etsittiin kirjallisuuslähteistä sekä sähköisistä tiedonhakupalveluista, kuten Google Scholar'ista sekä EBSCOhost -yhdistelmähausta, joka kohdistuu kaikkiin Laurea-ammattikorkeakoululle myönnettyihin EBSCO –tietokantoihin. Hakusanoina toimivat opinnäytetyön keskeiset käsitteet sekä yhdessä että erikseen. Hakusanoina käytettyjä käsitteitä olivat muun muassa ”business continuity planning”, ”continuity management”, ”ICT”, ”preparedness”, ”ICT-system”, ”IT-system”, ”criticality”, ”importance”, ”business impact analysis”, ”assessment” ja ”evaluation”. Etsimisestä ja hakusanoilla löydettyjen dokumenttien tarkastelusta huolimatta vertailuun soveltuvia kriittisyyden arvioinnista kuvattuja työtapoja tai yksityiskohtaisia malleja ei löytynyt. Sen sijaan tietojärjestelmien luokittelemiseksi löytyi tietoperustasta esimerkkejä, joten menetelmä rajattiin valtioneuvoston kansliassa käytettävän vaikutusanalyysityökalun sisältämän luokittelumallin sekä lähdemateriaalista löydettyjen luokittelumallien vertailuun.

Käytössä olevan luokittelumallin vertailukohtia olivat tietoperustassakin esitetyt VAHTI-ohjeen (2012, 21–23) ICT-varautumisen vaatimustasojen mukaiset luokitukset, Laaksosen ja Iivarin (2009, 162) esittelemä IT-järjestelmien luokittelumalli, Riman ja Snedakerin (2013, 232–234) kriittisyyden arviointimalli, SFS-ISO/IEC 27005 informaatioteknologiastandardin (Suomen Standardoimisliitto SFS 2013, 78) malli järjestelmien luokittelusta sekä NIST 800–34 –ohjeessa (Bowen ym. 2010, 15–16) käytetty järjestelmien vaikutustasoluokittelu. Vertailu toteutettiin taulukossa (Liite 3) ja sen keskeisimpiä tuloksia on avattu kohdassa 5.3.

5 Tutkimuksen tulokset

Menetelmillä kerätty tieto analysoitiin laadullisella analyysilla, joka on Hirsjärven, Remeksen ja Sajavaaran (2009, 224) mukaan ymmärtämiseen pyrkivälle lähestymistavalle ominainen analyysimuoto. Analyysissä sekä haastatteluilla että dokumenttianalyysillä kerättyä tietoa tarkasteltiin menetelmäoppaan (Ojasalo ym. 2014, 110) mukaisesti useaan kertaan ja siitä etsittiin yhtymäkohtia teoreettiseen viitekehykseen.

Tutkimustyön tulokset esitellään tässä osiossa. Tulokset käydään menetelmien ja tutkimusvaiheiden mukaisessa järjestyksessä siten, että ensimmäisenä tuloksista käsitellään kriittisyyden arvioinnin nykytilaa, vastuita ja menetelmiä. Nykytilaa havainnollistetaan kuvauksen lisäksi blueprinting –menetelmällä laaditulla prosessikaaviolla (Kuvio 7), jonka vaiheet esitellään rooli- ja vastuujaon mukaan. Nykytilan kuvaus sekä dokumenttianalyysin tulokset vastaavat tutkimuskysymykseen: ”Miten tietojärjestelmien kriittisyyden arviointi valtioneuvoston kansliassa tehdään?”.

Nykytilan esittelyn jälkeen tuloksissa pureudutaan teorialähteistä löydettyihin keskeisimpiin vertailukohtiin. Vertailun kohteena olivat järjestelmien luokittelumallit, joista etsittiin valtioneuvoston kansliassa käytettävään kriittisyysluokitteluun sopivia malleja kuten luokittelukriteereitä. Vertailulla pohjustetaan kodan 6 johtopäätöksiä sekä kehitysehdotuksia, joilla vastataan tutkimuskysymykseen: ”Miten tietojärjestelmien kriittisyyden arviointi tulisi tehdä valtioneuvoston kansliassa?”.

5.1 Tietojärjestelmien kriittisyyden arvioinnin nykytila

Valtioneuvoston kanslian valmiusyksikkö vastaa valtioneuvoston kanslian varautumisen kokonaisuudesta tehtäviensä mukaisesti. Valmiusyksikössä tapahtuvan valmiussuunnittelu kattaa Sjöroosin (2017) mukaan seitsemän P:n sääntöä noudattaen hallintajärjestelmän eli ohjelman (programme), sidosryhmät (providers), toimintakyvyn (performance), henkilöstön (people), toimitilat (premises), prosessit (processes) sekä organisaation profiilin (profile). Suunnittelussa huomioidaan myös osittain erillisenä osa-alueena tietojärjestelmät kattava ICT-ulottuvuus ja suunnittelun kokonaisuuden painopiste on poikkeusoloihin varautumisessa (Puhakainen, Pullinen & Sjöroos 2017).

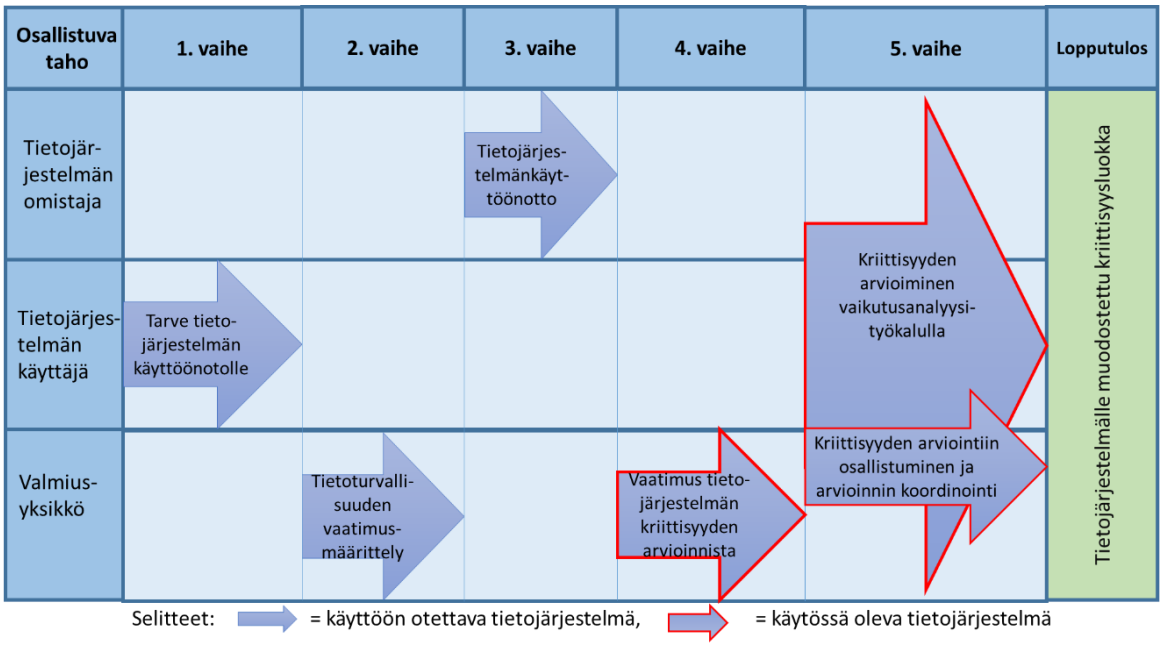
Valtioneuvoston kanslian vastuut yhteiskunnallisessa varautumisessa määritellään Yhteiskunnan turvallisuusstrategiassa, ja niiden osalta suunnittelusta vastaa valmiusyksikkö. Yksikkökohtaisia vastuita organisaation normaaliolojen jatkuvuudenhallinnassa ei kuitenkaan ole strategisella tasolla määritelty. (Puhakainen ym. 2017.)

Viimeksi vuoden 2016 aikana valmiusyksikkö on ICT-varautumista koordinoivana tahona edellyttänyt organisaation muilta toimielimiltä eli yksiköiltä tietojärjestelmien kriittisyyden arviointia, sillä vastuu kriittisyysarvion laatimisesta kuuluu järjestelmän omistajalle. Arvioinnit toteutettiin toisistaan erillisinä ja vain toimielinten omat lähtökohdat huomioiden, joka johti siihen, että suurin osa järjestelmistä arvioitiin korkeimpaan kriittisyysluokkaan. Arviointien näkökulmat olivat olleet puutteellisia, sillä arvioissa ei ollut esimerkiksi otettu huomioon eroa normaaliolojen ja poikkeusolojen välillä. (Sjöroos 2017.)

Viimeisimmissä käyttöönotettavien uusien tietojärjestelmien kriittisyyden arvioinneissa on valtioneuvoston kansliassa käytetty valtiovarainministeriön (2017) julkaisemaa tietojärjestelmien vaikutusanalyysityökalua, sillä sen käyttö vastaa VAHTI:n suosituksia, eikä käyttöä tarvitse erikseen perustella (Puhakainen ym. 2017). ICT-varautumisen vaatimukset –ohjeessa (VAHTI 2012, 30) suositellaankin järjestelmien varautumistoimenpiteiden kohdentamisen perustaksi vaikutusanalyysin tuloksia. Työkalua tai sen perusteella muodostuvaa tietojärjestelmän luokittelua ei ole Puhakaisen, Pullisen ja Sjöroosin (2017) mukaan tarkasteltu kriittisesti, eikä sitä ole kehitetty organisaation toimintaan parhaiten soveltuvaksi.

Vaikutusanalyysityökalussa kriittisyyden arviointi ja tärkeysluokan määrittely on keskeisin osa-alue, mutta sen perusteella arvioidaan tietojärjestelmän kriittisyyden lisäksi muun muassa riippuvuussuhteita muihin tietojärjestelmiin ja palveluihin sekä toiminnan keskeytymisen ajallisia ja Yhteiskunnan turvallisuusstrategiassa (2010, 15–16) kuvattujen uhkamallien vaikutuksia tietojärjestelmälle. Analyysi sisältää myös tietojärjestelmän kannalta Yhteiskunnan turvallisuusstrategian (2017) mukaisten yhteiskunnan elintärkeiden toimintojen merkityksen arvioinnin. Työkalu on esitelty dokumenttianalyysiin perustuen kohdassa 5.2.

Tietojärjestelmien kriittisyyden arviointi toteutuu valmiusyksikön vaatimuksesta ja uuden järjestelmän osalta sen jälkeen kun tietojärjestelmän tietoturvallisuusvaatimukset on valmiusyksikössä määritelty ja järjestelmä on otettu käyttöön. Vaikutusanalyysityökalua hyödynnetään erikseen arviointia varten järjestettävässä arviointitilaisuudessa. Viimeisimmissä arviointitilaisuuksissa on arvioitu käyttöönotettavia tietojärjestelmiä ja niihin ovat osallistuneet järjestelmän omistajan asemassa toimivan tietojärjestelmäyksikön tai muun yksikön tai hankkeen johtoryhmän edustaja, järjestelmän käyttäjää edustava tietohallintoyksikön asiantuntija sekä tapahtumaa ohjaava valmiusyksikön tietoturvallisuuden asiantuntija. Arvioinnissa käytettävän menetelmän antaa valmiusyksikön edustaja, joka ohjaa tilaisuutta, mutta ei osallistu varsinaiseen arviointiin. Arvioinnin lopputuotoksena ovat vaikutusanalyysin tulokset, jotka sisältävät tietojärjestelmälle määritellyn kriittisyysluokituksen. (Puhakainen ym. 2017.) Nykyinen valtioneuvoston kansliassa tapahtuva tietojärjestelmien kriittisyysluokittelun prosessi on prosessianalyysiin perustuen mallinnettu alle prosessikaavioon (Kuvio 7).



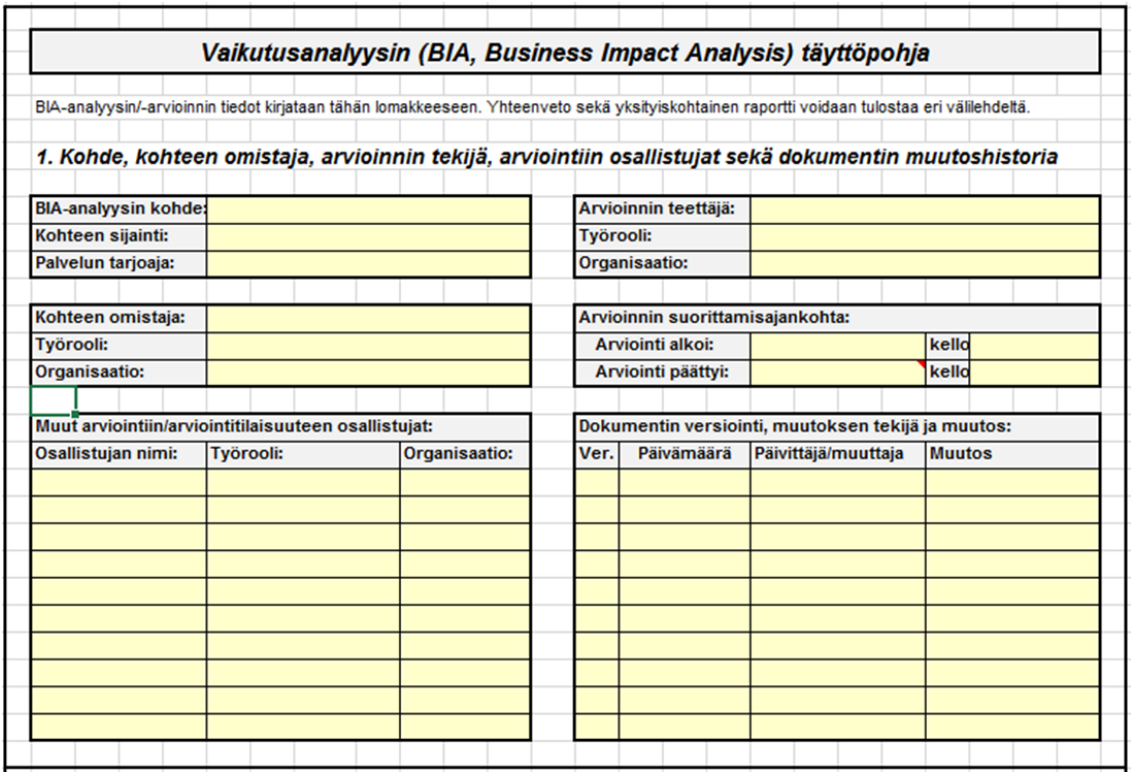
Kuvio 7: Tietojärjestelmien kriittisyyden arvioinnin prosessi valtioneuvoston kansliassa

Sjöroosin (2017) mukaan tietojärjestelmien kriittisyyden muodostumisen on valtioneuvoston kansliassa perustuttava etenkin tietojärjestelmän merkitykseen strategien tehtävien hoitamisen kannalta, joita ovat organisaation ydintoiminnot kuten henkilöstöhallinto, lakisääteiset tehtävät sekä varautumisen osalta Yhteiskunnan turvallisuusstrategiassa (2017) valtioneuvoston kanslialle määritellyt vastuualueet.

5.2 Vaikutusanalyysityökalu

Valtioneuvoston kansliassa käytettävä analyysityökalu on laadittu täytettävään Microsoft Excel –pohjaan. Dokumenttianalyysin tulosten havainnollistamiseksi työkalua on tässä osiossa havainnollistettu ottamalla näyttökuvia (Kuviot 8, 9, 10, 11, 12, 13 ja 14) sen osista tekstin yhteyteen. Työkalulla tehtävän analyysin tuloksina saadaan arvioitavasta tietojärjestelmästä muodostettua sen sisältämien tietojen suojaustaso, vaadittava tietoturvallisuuden taso, palvelutaso, kriittisyysarvio, riippuvuussuhteet sekä merkitys yhteiskunnan elintärkeiden toimintojen näkökulmasta ja mahdollisten uhkakuvien vaikutukset.

Pohja sisältää sekä täyttöpohjan että tulostussivut, joissa keskeisessä asemassa on vaikutusanalyysin yhteenveto (Kuvio 15). Täyttöpohjan ensimmäiseen kohtaan (Kuvio 8) merkitään arvioitavan kohteen tiedot, joita ovat kohteen nimi, sijainti ja mahdollinen palvelun tarjoaja sekä omistajan nimi, organisaatio sekä työrooli. Kohteen ja omistajan tietojen lisäksi kohtaan merkitään arvioinnin teettäjän tiedot, arviointiin osallistuneet henkilöt ja arvioinnin toteutusajankohta. Ensimmäinen osio antaa mahdollisuuden myös versioida dokumentin.



Vaikutusanalyysin (BIA, Business Impact Analysis) täyttöpohja

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

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

BIA-analyysin kohde:		Arvioinnin teettäjä:	
Kohteen sijainti:		Työrooli:	
Palvelun tarjoaja:		Organisaatio:	

Kohteen omistaja:		Arvioinnin suorittamisajankohta:			
Työrooli:		Arviointi alkoi:		kello	
Organisaatio:		Arviointi päättyi:		kello	

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

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

Kuvio 8: Työkalun täyttöpohjan kohta 1

Varsinaiseen analysointivaiheeseen käytettävissä osioissa tuotetaan arvoja osa-alueille, joita ovat:

- Tietojärjestelmän tietojen, tietoturvatason ja ICT-varautumisen luokitukset
- Tietojärjestelmän tietoturvallisuuden (luottamuksellisuus, eheys, saatavuus) tärkeys ja palvelutasotavoitteet tietojärjestelmälle
- Tietojärjestelmässä ilmenevän odottamattoman käyttökatkon ja sen sisältämien tietojen menetyksen tai vanhenemisen vaikutukset (pieni ja suuri vaikutusraja)
- Keskeiset riippuvuudet: tietojärjestelmän riippuvuudet ja riippuvuudet tietojärjestelmästä
- YTS 2010 -uhkakuvien vaikutukset tietojärjestelmään

Arvioitavan tietojärjestelmän sekä arviointitapahtuman tietojen jälkeen täyttöpohjan toisessa kohdassa (Kuvio 9) määritellään tietojärjestelmässä käsiteltävien tietojen sekä tietojärjestelmän tietoturva- ja ICT-varautumisen luokitukset. Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa (681/2010) mukaisten tiedon suojaustaso- sekä turvallisuusluokitusten perusteella työkalu muodostaa kohdetta koskevan tietoturvatason korkeamman taulukkoon syötetyn luokan perusteella. Esimerkiksi tietojen suojaustason ollessa arvoltaan 1 ja turvallisuusluokituksen ollessa arvoltaan 3, työkalu määrittelee kohteen tietoturvatasoksi arvon 3 (Kuvio 9). Työkalu jättää ICT-varautumisen tason määrittelyn arviointia suorittavien henkilöiden tehtäväksi, mutta ohjeistaa noudattamaan esimerkiksi ICT-varautumisen vaatimukset (VAHTI 2012, 20–23) -ohjeen mukaisia tasoja, joita on käsitelty jo aiemmin kohdassa 3.5.1.

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

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

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

Täyttövinkkinä seuraavaa:
- useimmiten järjestelmässä tai palvelussa on käytössä vain jompi kumpi eli suojaustaso tai turvallisuusluokitus
- tietoturvaluokkaan tulee arvo automaattisesti tietojen tason

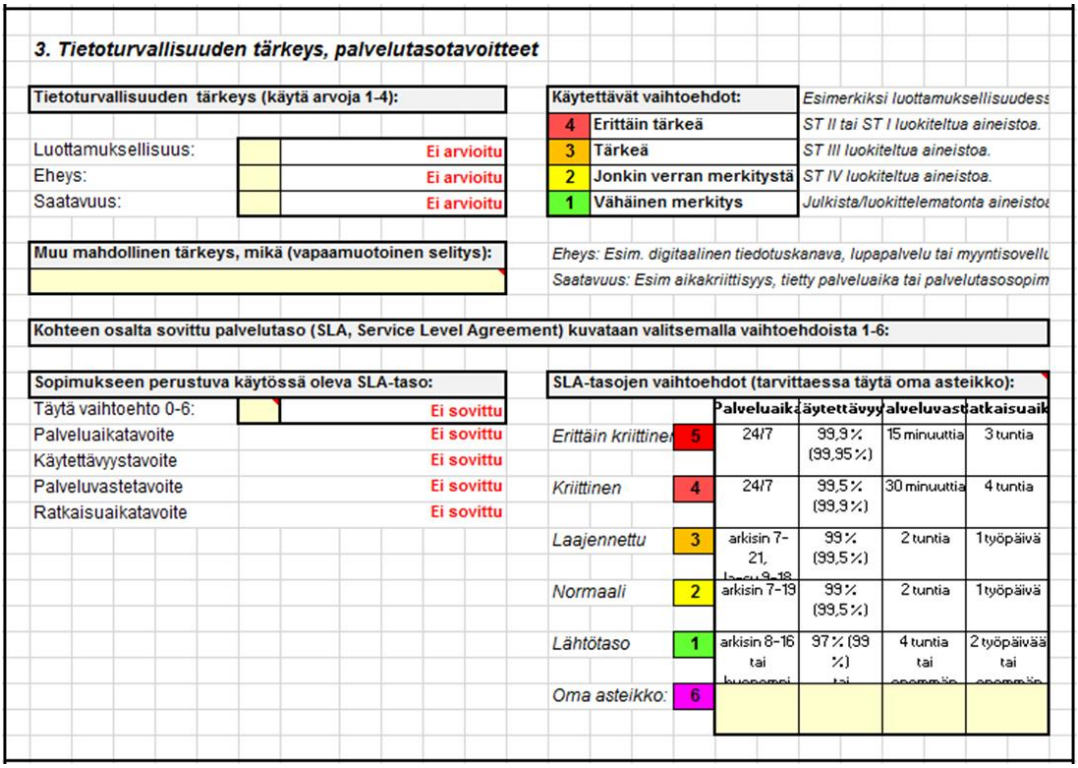
Kohteen tietoturvataso ja/tai ICT-varautumistaso vaihtoehdot:	
4	Korkea taso
3	Korotettu taso
2	Perustaso
1	Ei tasoluokittelua

Korkein kohteen sisältämien tietojen luokitus(merkintä) /1-5):		
Suojaustaso (ST...):		Ei arvioitu
Turvallisuusluokitus:		Ei arvioitu

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

Kuvio 9: Työkalun täyttöpohjan kohta 2

Työkalun täyttöpohjan kolmannessa kohdassa (Kuvio 10) arvioidaan tietojärjestelmässä toteutuvan tietoturvallisuuden tärkeyttä 4-portaisella asteikolla luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta sekä palvelusopimukseen perustuvaa palvelutasoa 5-portaisen asteikon mukaisesti, jossa huomioidaan palveluaika, palvelun käytettävyys, aikavaste sekä ratkaisuaika. Työkalun SLA-tasot noudattelevat JUHTA:n (2012, 18) tietoliikenteen peruspalveluiden palvelutasoluokkia, mutta palvelutasolle on mahdollista asettaa palvelusopimuksen mukaiset kriteerit kohtaan 6. Valtioneuvoston kansliassa taso määritellään valtioneuvoston kanslian sekä palveluntuottajan välisessä sopimuksessa (Sjöroos 2017). Valittu palvelutaso sekä tietoturvallisuuden tärkeyden arviointi näkyvät sellaisenaan työkalun tulostussivuilla.



3. Tietoturvallisuuden tärkeys, palvelutasotavoitteet

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

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

Muu mahdollinen tärkeys, mikä (vapaamuotoinen selitys):

Eheys: Esim. digitaalinen tiedotuskanava, lupapalvelu tai myyntisovellu
Saatavuus: Esim aikakriittisyys, tietty palveluaika tai palvelutasosopim

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

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

SLA-tasojen vaihtoehdot (tarvittaessa täytä oma asteikko):		Palveluaik	äytettävyy	alveluvast	atkaisuaik
Erittäin kriittinen	5	24/7	99,9 % (99,95 %)	15 minuuttia	3 tuntia
Kriittinen	4	24/7	99,5 % (99,9 %)	30 minuuttia	4 tuntia
Laajennettu	3	arkisin 7–21,	99 % (99,5 %)	2 tuntia	1 työpäivä
Normaali	2	arkisin 7–19	99 % (99,5 %)	2 tuntia	1 työpäivä
Lähtötaso	1	arkisin 8–16 tai	97 % (99 %)	4 tuntia tai	2 työpäivää tai
Oma asteikko:	6				

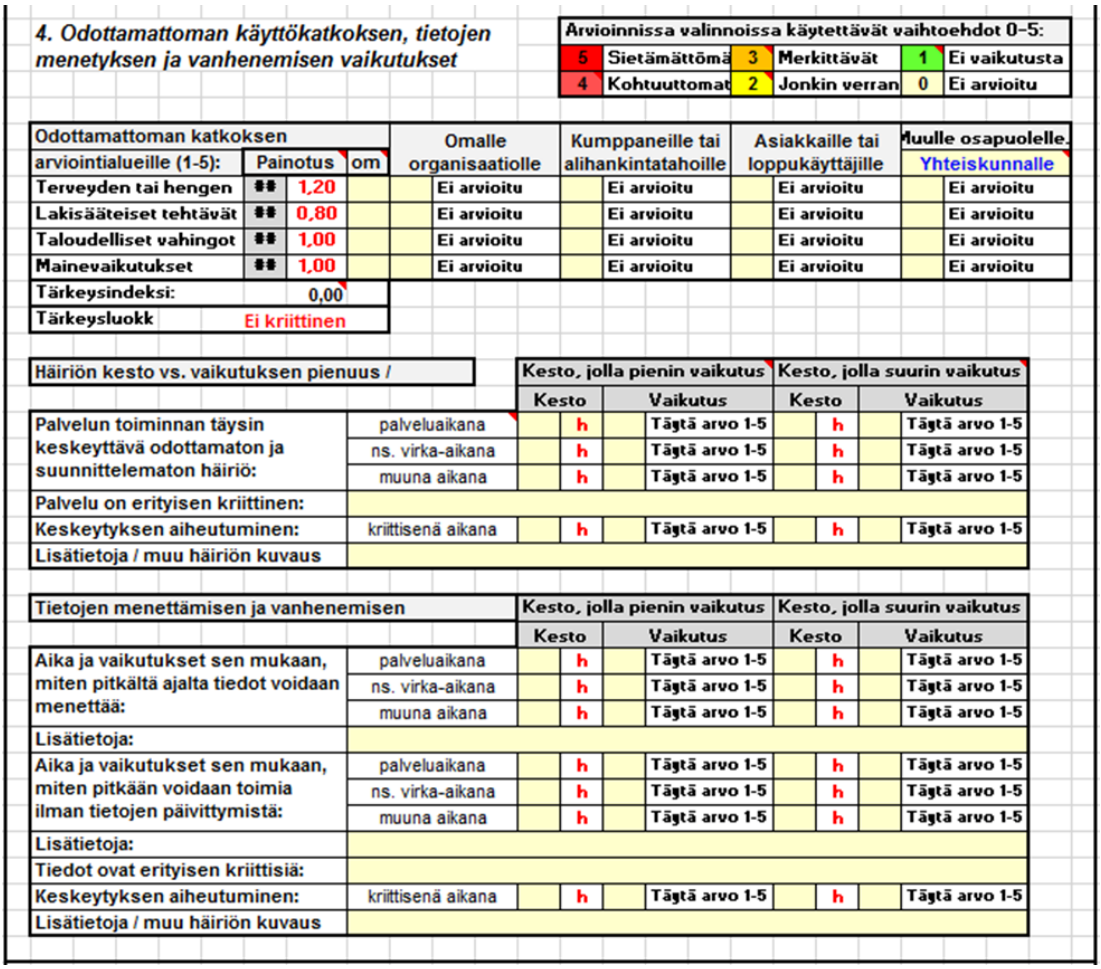
Kuvio 10: Työkalun täyttöpohjan kohta 3

Neljännessä kohdassa (Kuvio 11) tapahtuu arvioitavan tietojärjestelmän tärkeyden eli kriittisyyden arviointi. Täyttöpohjassa kriittisyys ilmaistaan tärkeysindeksin lukuarvona sekä sanallisessa muodossa tärkeysluokkana joko ei kriittisenä, normaalina tärkeytenä, merkittävänä, tärkeänä, erittäin tärkeänä tai kriittisenä/elintärkeänä. Tärkeyttä arvioidaan terveyteen tai henkeen, lakisääteisiin tehtäviin, taloudellisiin vahinkoihin tai maineeseen liittyvien joko omaan organisaatioon, kumppaneille tai alihankkijoille, asiakkaille tai loppukäyttäjille sekä yhteiskunnalle kohdistuvien vaikutusten perusteella. Työkalussa on asetettu oletuspainotukset vaikutusten laadusta riippuen.

Tärkeysindeksi muodostetaan työkalussa kaavalla, jossa omaan organisaatioon kohdistuvien vaikutusten arvo kerrottuna kahdella vähennetään asiakkaisiin tai loppukäyttäjiin kohdistuvien vaikutusten yhteisarvosta (Kuvio 12). Tärkeysindeksin määräytymisperiaatteeksi on ilmoitettu vaikutukset omalle organisaatiolle sekä vaikutukset asiakkaille sekä kumppaneille, mikäli ne ovat merkittävimpiä kuin vaikutukset omalle organisaatiolle. Kumppaneiden ja alihankkijoiden merkitystä ei painoteta laskukaavassa, koska ne huomioidaan sopimusteknisin keinoin. (Kangas 2016, 12.)

Neljäs kohta (Kuvio 11) sisältää myös häiriön pituuden vaikutuksia toiminnan keskeytymiseen sekä tietojen menettämisen ja vanhenemiseen palveluaikana, virka-aikana, muuna aikana

sekä kriittisenä aikana. Häiriöiden kestojen arvioinneilla ei ole vaikutusta kriittisyysluokan muodostamiseen, vaan ne näkyvät sellaisenaan tulostussivuilla.



4. Odottamattoman käyttökatkoksen, tietojen menetyksen ja vanhenemisen vaikutukset

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

Odottamattoman katkoksen arviointialueille (1-5):		Painotus	om	Omalle organisaatiolle	Kumppaneille tai alihankintatahoille	Asiakkaille tai loppukäyttäjille	Muulle osapuolelle. Yhteiskunnalle
Terveyden tai hengen	##	1,20		Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Lakisääteiset tehtävät	##	0,80		Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Taloudelliset vahingot	##	1,00		Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Mainevaikutukset	##	1,00		Ei arvioitu	Ei arvioitu	Ei arvioitu	Ei arvioitu
Tärkeysindeksi:		0,00					
Tärkeysluokk		Ei kriittinen					

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

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

Kuvio 11: Työkalun täyttöpohjan kohta 4

Älä muuta näitä kaavoja

Tärkeysluokan apulaskukaava

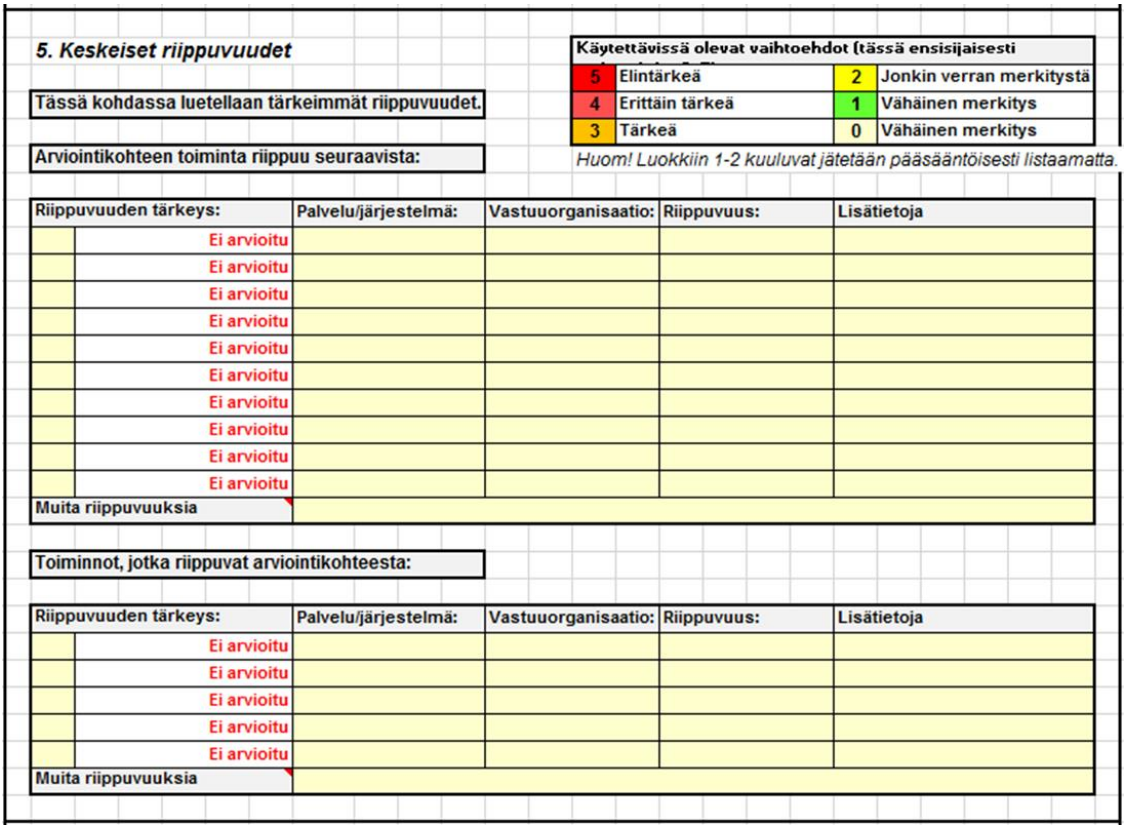
jos asiakas + yhteiskunta - 2 x oma > 3, nousua 2 tai >2, nousua 1

O	K	A	Y	(A+Y) -2xO	Ero > / = kuin		O+>=	O+ >=3/>=2	
Oma	Kum	Asia	Yht		>=3	>=2			
0	0	0	0	0	0	0	0	1,20	0,0
0	0	0	0	0	0	0	0	0,80	0,0
0	0	0	0	0	0	0	0	1,00	0,0
0	0	0	0	0	0	0	0	1,00	0,0
								Tärk.indeksi	0,00

Kuvio 12: Tärkeysindeksin muodostuminen työkalussa

Työkalun viidennessä kohdassa (Kuvio 13) määritellään tietojärjestelmän riippuvuuksia ja arvioidaan niiden merkityksiä 5-portaisella asteikolla. Työkaluun syötetään muut järjestelmät tai palvelut, joista arvioitavan tietojärjestelmän toiminta riippuu, sekä toiminnot jotka ovat

riippuvaisia arvioinnin kohteesta. Riippuvuuksista ilmoitetaan palvelun tai järjestelmän nimen ja tärkeyden lisäksi siitä vastaava organisaatio, riippuvuuden kuvaus sekä muut mahdolliset lisätiedot. Riippuvuustiedot näkyvät syötetyssä muodossa työkalun tulostussivuilla.



5. Keskeiset riippuvuudet

Tässä kohdassa luetellaan tärkeimmät riippuvuudet.

Arviointikohteen toiminta riippuu seuraavista:

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

Huom! Luokkiin 1-2 kuuluvat jätetään pääsääntöisesti listaamatta.

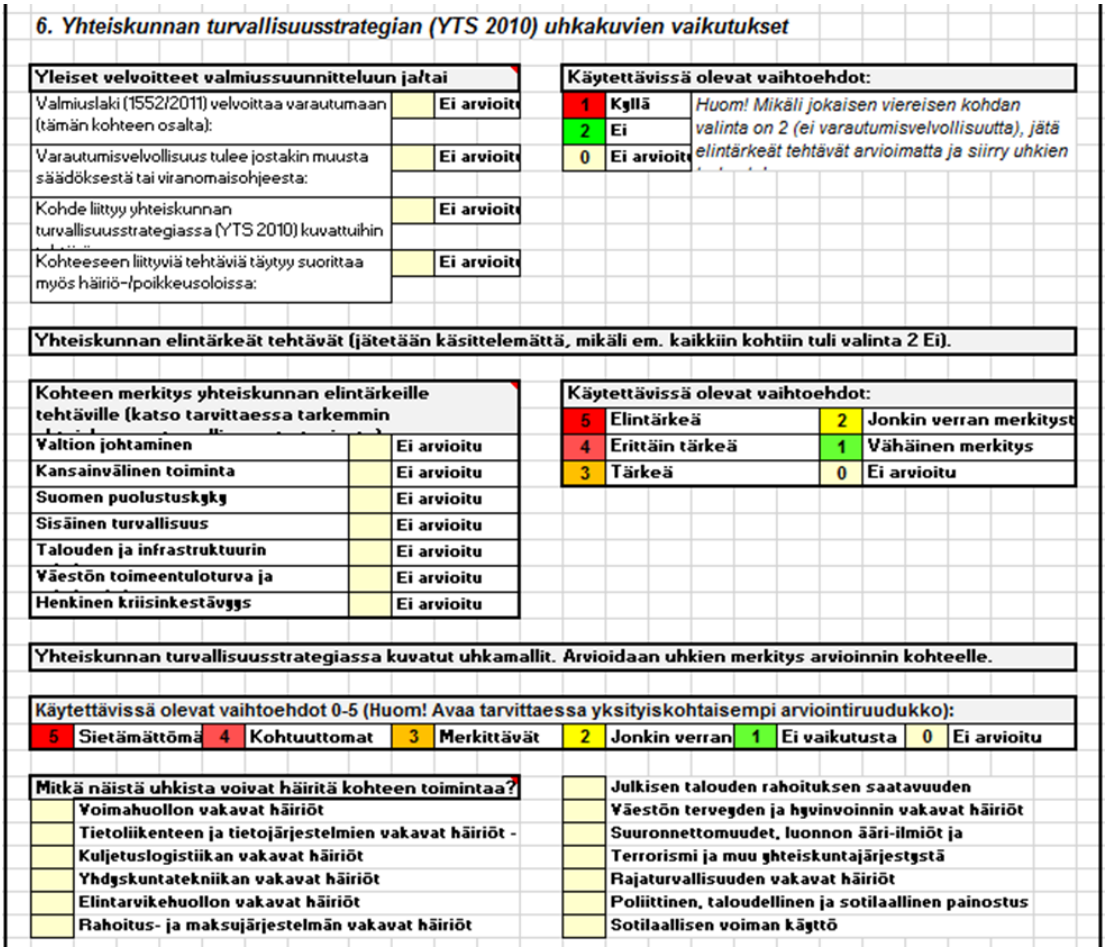
Riippuvuuden tärkeys:		Palvelu/järjestelmä:	Vastuuorganisaatio:	Riippuvuus:	Lisätietoja
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
	Ei arvioitu				
Muita riippuvuuksia					

Toiminnot, jotka riippuvat arviointikohteesta:

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

Kuvio 13: Työkalun täyttöpohjan kohta 5

Työkalun täyttöpohjan viimeinen kohta (Kuvio 14) käsittää Yhteiskunnan turvallisuusstrategian (2010) mukaisten uhkamallien vaikutusten arvioinnin. Ensimmäisenä merkitään täyttääkö arvioitava kohde valmiuslain (1552/2011), muun säädöksen tai viranomaisohjeen mukaista varautumisvelvollisuutta, liittyykö kohde Yhteiskunnan turvallisuusstrategiassa (2010) kuvattuihin tehtäviin myös poikkeusoloissa ja täytyykö kohteeseen liittyviä tehtäviä suorittaa myös poikkeusoloissa. Mikäli jokin näistä kriteereistä täyttyy eli kun yhteenkin edellä luetelluista vaihtoehdoista vastataan täyttöpohjaan ”Kyllä”, arvioidaan 5-portaisella asteikolla kohteen merkitys kaikkien seitsemän yhteiskunnan elintärkeän toiminnon näkökulmasta sekä Yhteiskunnan turvallisuusstrategiassa (2010) esiteltyjen uhkien vaikutukset kohteeseen.



6. Yhteiskunnan turvallisuusstrategian (YTS 2010) uhkakuvien vaikutukset

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

Käytettävissä olevat vaihtoehdot:		
1	Kyllä	*Huom! Mikäli jokaisen viereisen kohdan valinta on 2 (ei varautumisvelvollisuutta), jätä elintärkeät tehtävät arvioimatta ja siirry uhkien*
2	Ei	
0	Ei arvioit	

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

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

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

Yhteiskunnan turvallisuusstrategiassa kuvatut uhkamallit. Arvioidaan uhkien merkitys arvioinnin kohteelle.

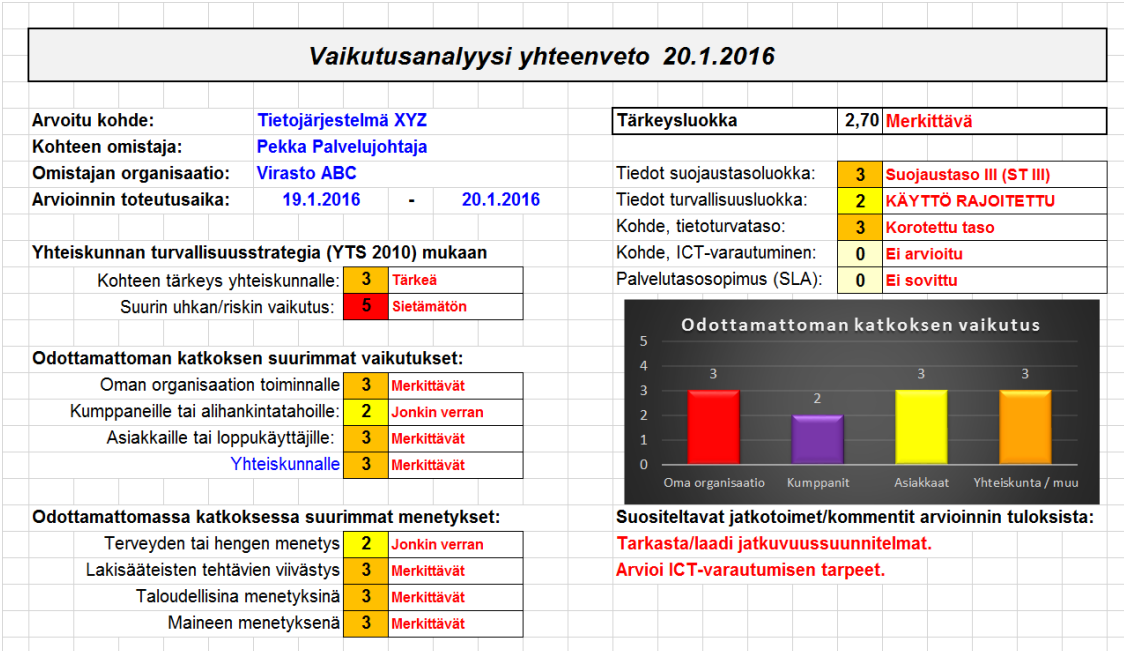
Käytettävissä olevat vaihtoehdot 0-5 (Huom! Avaa tarvittaessa yksityiskohtaisempi arviointiruudukko):									
5	Sietämättömä	4	Kohtuuttomat	3	Merkittävät	2	Jonkin verran	1	Ei vaikutusta	0	Ei arvioitu

Mitkä näistä uhkista voivat häiritä kohteen toimintaa?			
	Voimahuollon vakavat häiriöt		Julkisen talouden rahoituksen saatavuuden
	Tietoliikenteen ja tietojärjestelmien vakavat häiriöt -		Väestön terveyden ja hyvinvoinnin vakavat häiriöt
	Kuljetuslogistiikan vakavat häiriöt		Suuronnettomuudet, luonnon ääri-ilmiöt ja
	Yhdyskuntatekniikan vakavat häiriöt		Terrorismi ja muu yhteiskuntajärjestyst
	Elintarvikehuollon vakavat häiriöt		Rajaturvallisuuden vakavat häiriöt
	Rahoitus- ja maksujärjestelmän vakavat häiriöt		Poliittinen, taloudellinen ja sotilaallinen painostus
			Sotilaallisen voiman käyttö

Kuvio 14: Työkalun täyttöpohjan kohta 6

Tarkasteltaessa teorian näkökulmasta työkalu muodostaa kokonaisuudessaan kattavan analyysin yksittäisestä tietojärjestelmästä huomioiden varautumiselle keskeiset osa-alueet kuten odottamattomien katkosten vaikutukset järjestelmään, järjestelmän riippuvuussuhteet, tietoturvallisuus-, palveluvaatimus- ja varautumistason sekä yhteiskunnan elintärkeät toiminnot ja uhkakuvat järjestelmän näkökulmasta.

Keskeinen ongelma on kuitenkin tulostussivun yhteenvedossa (Kuvio 15) keskeisessä asemassa oleva kriittisyysarviota ilmentävä tärkeysluokka, jonka muodostumisessa ei oteta huomioon edellisessä kappaleessa lueteltuja osa-alueita. Kun puhutaan kriittisyyden arvioinnista, kaikilla arvioitavana olevilla osa-alueilla on oltava vaikutus arvioinnin tulokseen. Osa-alueita jotka eivät ole merkityksellisiä arvioinnin kannalta, ei pidä ottaa huomioon, mutta kriittisyyteen vaikuttavat osa-alueet on työkalusta poiketen aina huomioitava kriittisyyden arvon eli työkalun tapauksessa tärkeysindeksin muodostamisessa.



Vaikutusanalyysi yhteenveto 20.1.2016

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

Tärkeysluokka	2,70	Merkittävä
Tiedot suojaustasoluokka:	3	Suojaustaso III (ST III)
Tiedot turvallisuusluokka:	2	KÄYTTÖ RAJOITETTU
Kohde, tietoturvataso:	3	Korotettu taso
Kohde, ICT-varautuminen:	0	Ei arvioitu
Palvelutasosopimus (SLA):	0	Ei sovittu

Yhteiskunnan turvallisuusstrategia (YTS 2010) mukaan

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

Odottamattoman katkoksen suurimmat vaikutukset:

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

Odottamattomassa katkoksessa suurimmat menetykset:

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

Suositeltavat jatkotoimet/kommentit arvioinnin tuloksista:

Tarkasta/laadi jatkuvuussuunnitelmat.

Arvioi ICT-varautumisen tarpeet.

Kuvio 15: Vaikutusanalyysin tulostussivun yhteenveto (Kangas 2016, 17)

5.3 Vaihtoehtoiset tietojärjestelmien kriittisyyden arvioinnin toimintamallit

Organisaationa valtioneuvoston kanslia eroaa perinteisistä liike-elämän organisaatioista huomattavasti ja tämä seikka on huomioitava myös jatkuvuussuunnittelun tavoitteissa. Julkista hallintoa velvoittaa Suomessa lainsäädäntö, joka asettaa joitakin velvoitteita sekä myös rajoitteita jatkuvuussuunnitteluun. Vaikka jatkuvuuden hallinta on tietoperustassa kuvatuilta pääperiaatteiltaan samanlaista kaikissa organisaatioissa toimialasta riippumatta, oli syvälle jatkuvuuden hallintaan sijoittuvan yksittäisen tietojärjestelmien kriittisyyden arvioinnin prosessiin haastavaa löytää tutkimusteorioista soveltuvia malleja.

Kuten menetelmät osion kohdassa 4.4 kävi ilmi, ei tiedonhaku tuottanut tältä osin toivottua tulosta. Lisäksi opinnäytetyössä käytetyt teorialähteet osoittivat VAHTI-ohjeiden tarjoavan valtioneuvoston kanslian toimintaympäristöön parhaiten soveltuvan käytännön tietojärjestelmien kriittisyyden arviointiin, niiden perustuessa kansalliseen lainsäädäntöön ja ollessa vähintäänkin yhtä perusteellisia kuin aihetta käsittelevät teokset, standardit ja muut ohjeet.

Vertailu kuitenkin toteutettiin tietojärjestelmien luokitteluun soveltuvien tietoperustasta sekä muista lähteistä löydettyjen mallien kesken. Vertailutulokset perustuvat vertailutaulukon (Liite 3) sisältämiin tietoihin, jotka on kerätty menetelmäosiossa kuvatuista lähteistä ja osin teoriapohjan sisällöstä. Taulukko (Liite 3) sisältää luokitusmallin lähdetiedon, luokitusmallin mukaiset luokat sekä tiedon siitä, mihin kriteereihin luokittelu perustuu. On huomattava, että erilaisista lähtökohdista ja soveltamistarkoituksista johtuen luokittelumallit eivät

olleet suoraan vertailukelpoisia. Esimerkiksi varautumisen vaatimustasot (VAHTI 2012, 21–23) ovat kriittisyyden luokittelusta erillinen malli, joka on huomioitu aiemmin käsitellyssä vaikutusanalyysityökalussa tulostussivun yhteenvedossa omana kohtanaan. Mallien valitsemiseen vaikutti kuitenkin se, että ne liittyvät kaikki keskeisesti järjestelmien kriittisyyden määrittelemiseen.

Vertailtavista malleissa luokkien määrä vaihteli kolmesta kuuteen. Huomionarvoinen seikka oli se, että NIST 800-34 -ohjeen (Bowen ym. 2010, 15–16) luokkien määrä vastasi VAHTI-ohjeen (2012, 21–23) varautumistasojen määrää, joita oli molempia 3. Luokkien määrä pysyi kaikissa vertailumalleissa SFS-ISO/IEC 27005 -standardin (Suomen Standardoimisliitto SFS 2013, 78) suositusten mukaisesti kolmen ja kymmenen luokan välissä.

Vaikutusanalyysityökalun tärkeysluokittelu mukaan lukien kaikissa vertailtavissa malleissa luokitus perustuu tietojärjestelmän toiminnan keskeytymisestä organisaatiolle aiheutuviin vaikutuksiin. Käytössä olevassa vaikutusanalyysityökalussa on myös huomioitu eriteltyinä kustannus, terveys, maine- ja suorituskykyvaikutukset lakisääteisten tehtävien hoitamisen muodossa, kuten SFS-ISO/IEC 27005 -standardissa (Suomen Standardoimisliitto SFS 2013, 78), joka on malleista ainoa, jossa vaikutusten ilmenemismuotoa on avattu tarkemmin. Luokituksen määräytymisen perusteiden yhtäläisyydet vertailumalleihin jäävät kuitenkin siihen.

Vaikutuksia yksilöivä SFS-ISO/IEC 27005 –standardi (Suomen Standardoimisliitto SFS 2013, 78) ottaa edellä mainittujen lisäksi huomioon myös tietojen- sekä henkilötietojen vuotamisen. Tietojen arvoa korostaa myös Iivarin ja Laaksosen (2009, 162) IT-järjestelmien luokitteluesimerkki, jossa luokitusperusteena on suoraan järjestelmän tietosisältö sekä tietoliikenteen sisältö sen sijaan, että tiedon arvo huomioitaisiin vain keskeytymisvaikutusten näkökulmasta. Toisaalta SFS-ISO/IEC 27005 -standardi (Suomen Standardoimisliitto SFS 2013, 78) huomioi tietoturvallisuuden osa-alueiden vaarantumisen useiden eri vaikutusten, kuten yleisen järjestyksen rikkomisen taustalla.

Kaikissa vertailumalleissa käytettävä luokittelun perusteena ovat järjestelmän riippuvuudet, joita valtioneuvoston kansliassa käytettävä tärkeysluokittelu ei huomioi. Keskeisenä käytössä olevasta mallista puuttuvana luokituksen määräytymisen osatekijänä on vertailun perusteella myös tavoitteellinen toipumisaika, jota on käytetty VAHTI-ohjeen (2012, 21–23) mallissa sekä Iivarin ja Laaksosen (2009, 162) luokitteluesimerkissä.

Teoriapohjaan nojaten kansainvälisistä ohjeista ja standardeista on havaittavissa, etteivät ne käsittele jatkuvuuden hallinnan prosesseja yksityiskohtaistesti, vaan ohjeet on kuvattu yleisellä tasolla, jossa ne jättävät varaa kansallisen lainsäädännön soveltamiseen. Kuten Suo-

messa myös muualla kansalliset ohjeet huomioivat isäntävaltionsa voimassaolevan lainsäädännön, eivätkä ne lainsäädännöllisten eroavaisuuksien osalta sovellu käytettäväksi Suomen julkisessa hallinnossa. Vertailtavina olevista malleista voidaan havaita, että niissä keskeisiä tietojärjestelmien luokittelun perusteita olivat tieto, toiminnan keskeytymisen vaikutukset organisaatiolle, toipumisvaatimukset sekä riippuvuussuhteet.

6 Johtopäätökset ja kehitysehdotukset

Tietojärjestelmien kriittisyyden arviointi on pieni mutta keskeinen osa valtioneuvoston kanslian jatkuvuuden hallintaa, jossa se muodostaa vaikutusanalyysin osana perustan ICT-varautumiselle sekä tietojärjestelmiä koskevalle yksityiskohtaiselle toipumis- tai valmiussuunnittelulle. Jotta tietojärjestelmien kriittisyyden arviointia voitaisiin kehittää organisaation varautumisen tarpeet täyttäväksi prosessiksi, tulisi koko jatkuvuuden hallinnan puitteet varmistaa parhaiden käytänteiden mukaisiksi.

Tietojärjestelmien kriittisyyden arvioinnin toteutuminen edellyttää valtioneuvoston kansliassa strategisen tason määräyksiä tai ohjeita, joilla ylin johto ohjaa kaikkea jatkuvuussuunnittelua, asettaen sille painopisteitä sekä tavoitteita. Strategisen tason ohjauksesta vastaa ylin johto ja sitä koordinoi turvallisuudesta- ja varautumisesta vastaavana toimielimenä valmiusyksikkö. Operatiivisen tason suunnittelua ohjaavan dokumentaation tuottaminen voi tapahtua valmiusyksikössä edellyttäen johdon sitoutumista strategisen tason suunnitteluprosessiin.

Keskeisimpänä kehitystoimenpiteistä ovat toimintojen ja prosessien arvioiminen strategisten tehtävien hoitamisen näkökulmasta sekä toimielinkohtaisten jatkuvuuden hallinnan vastuiden määritteleminen. Vastuiden selkeyttämiseksi tulisi organisaatiotason määräyksiä tai ohjeita kehittää siten, että niissä olisi määritelty yksikkötasolle ulottuvat ICT-varautumisen vastuut.

Kehitysehdotuksena on, että tietojärjestelmien kriittisyyden arvioinnin osalta vastuiden määrittelemiseen sovellettaisiin alla olevaa tutkimuksen tietoperustaan pohjautuvaa vastuunjakotaulukkoa (Taulukko 2).

Vastuutaho	Vastuualue/tehtävä

Ylin johto (tai valmiusyksikkö ylimmän johdon tukemana)	• Jatkuvuuden hallinnan strateginen ohjaus
	  ○ Strategisten tehtävien kannalta kriittisten toimintojen ja prosessien määritteleminen
	  ○ Vastuiden määrittäminen
	• Operatiivisen tason jatkuvuussuunnitelmien hyväksyminen
	• Tietojärjestelmien kriittisyysarvioiden hyväksyminen

Toimielimet (Osastot/yksiköt)	• Omistamiensa tietojärjestelmien toipumissuunnittelu
	  ○ Tietojärjestelmien kriittisyyden arviointi
	  ○ Suojaustarpeiden määritteleminen
	  ○ Toipumisvaatimusten määritteleminen
	  ○ Palvelutasovaatimusten määritteleminen

Turvallisuustoimielin (Valmiusyksikkö)	• ICT-varautumisen koordinointi ja toteutumisen valvonta • Arvioinnin koordinointi ja asiantuntija-avun tarjoaminen • Suunnitelmien tarkastaminen • Tietojärjestelmien tietoturvallisuuden vaatimusmäärittely • Valmiusharjoitusten järjestäminen
Palveluntuottaja	• Vaatimusten mukainen tekninen toteutus ○ Palvelutason varmistaminen

Taulukko 2: Vastuunjakotaulukko

Jokaisen osaston ja yksikön olisi tiedostettava oma roolinsa valtioneuvoston kanslian jatkuvuussuunnittelussa ja mitä tämä rooli heiltä edellyttää. Tietojärjestelmää käyttöönotettaessa tietojärjestelmille tulisi ISO-standardien mukaisesti strategisella tasolla määritellä omistaja, jolle on oltava selvää, että uuden järjestelmän kriittisyyden arviointi on yksi ensimmäisistä toimenpiteistä tietojärjestelmän käyttöönoton jälkeen. Tämä perustuu siihen, että tietojärjestelmien kriittisyyden arviointi esitetään riskienhallintaa sekä yhteiskunnan turvallisuutta käsittelevissä ISO-standardeissa osana organisaation sisäisen toimintaympäristön arviointia, johon standardien mukaiset riskien- ja jatkuvuuden hallinnan toimenpiteet kuten tietojärjestelmiä koskeva toipumissuunnittelu perustuu.

Kuten kuvatusta nykyisestä prosessista (Kuvio 7) voi havaita, tietojärjestelmien arviointia koordinoivalla valmiusyksiköllä on valmiuksiin nähden suuri vastuu varsinaisen kriittisyysarvion muodostamisessa. Asiantuntijaresursseja käytetään ohjaustoimenpiteisiin, jotka eivät olisi tarpeellisia, mikäli organisaatiokohtaiset roolit ja vastuut olisivat kaikkien osalta määritelty.

Valmiusyksikkö huolehtii viimekädessä toimenpiteistä, jotka kuuluisivat tietojärjestelmien omistajille. Varautumisesta vastaavana toimielimenä valmiusyksikön on kuitenkin välttämätöntä laatia järjestelmiä koskevat arvioinnit ICT-varautumisen ja siihen liittyvän valmiussuunnittelun perustaksi.

Strategisen tason ohjauksessa tietojärjestelmien omistajien vastuuta arvion muodostamisesta tulisi korostaa, sillä heillä on tietoperustaankin nojaten paras mahdollinen tuntemus järjestelmän merkityksestä osana toimintoa ja siksi eniten valmiuksia kriittisyysarvion muodostamiseen. Haastatteluiden perusteella tietojärjestelmien kriittisyyden arviointia on valmiusyksikön toimesta edellytetty järjestelmien omistajilta, mutta tulokset eivät olleet vertailukelpoisia. Arviointien heikko laatu saattoi johtua riittävän ohjaamisen puuttumisesta sekä siitä, että haastattelut osoittivat tietojärjestelmien kriittisyyden arvioinnin sekä tietojärjestelmiä koskevan valmiussuunnittelun tapahtuvan osin erillisenä organisaation varsinaisia toimintoja koskevasta suunnittelusta. Opinnäytetyön teoreettisessa viitekehyksessä nämä poikkeuksetta kytkeytyvät toisiinsa.

Toimielimet voivat suorittaa organisaation varautumisen tarpeet täyttävää kriittisyyden arviointia omille tietojärjestelmilleen vain, jos arviointiin käytettävät menetelmät ja työkalut ovat yhdenmukaisia ja ne huomioivat toimielinkohtaisten tarpeiden sijaan organisaatiokohtaiset tarpeet. Tämä edellyttää etenkin sitä, että valtioneuvoston kanslian sisäisten toimintojen ja prosessien kriittisyys on arvioitu ja dokumentoitu siten, että se on kaikkea jatkuvuussuunnittelua operatiivisella tasolla toteuttavien toimielinten saatavilla. Jatkuvuussuunnittelua koskevat käytänteet ja ohjeet poikkeuksetta osoittavat, että myös yksittäisiä tietojärjestelmiä tulee arvioida riippuvuussuhteet kriittisiin prosesseihin ja toimintoihin huomioiden.

Vertailukelpoisuuden kannalta välttämätöntä, että tietojärjestelmien kriittisyyden arvioinnissa hyödynnetään organisaatiossa samaa menetelmää. Viimeisimmät tietojärjestelmien kriittisyysarviot ovatkin muodostettu valmiusyksikön edustajan ohjaamana samalla vaikutusanalyysityökalulla, jonka käyttöä suositellaan valtionhallinnossa. Vertailu kuitenkin osoitti, että työkalun kriittisyysarvon eli tärkeysindeksin muodostumisen perusteet ovat puutteelliset. Lisäksi tietoperustan mukaan tietojärjestelmien kriittisyyden arviointiin ei voi laatia yleispätevää ja kaikille organisaatioille sopivaa työkalua tai menetelmää. Tämä pätee myös julkiseen hallintoon, jossa valtioneuvoston kanslia on organisaationa varsin poikkeuksellinen. Ministeriö on valtionhallinnon varautumisessa keskeisessä asemassa esimerkiksi valtion johtamisen näkökulmasta, sen turvatessa valtioneuvoston toiminta kaikissa olosuhteissa ja valtioneuvoston johtajana toimivan pääministerin aseman korostuessa edelleen yhteiskunnallisissa häiriö- ja kriisitilanteissa.

Vaikka vertailukelpoisuus täyttyykin organisaatiossa käytettäväksi valitun työkalun myötä, valmiin työkalun soveltuvuutta tulisi tarkastella kriittisesti organisaation varautumistarpeet huomioiden. Käytössä olevalla vaikutusanalyysityökalulla on mahdollista määrittää tietojärjestelmäkohtainen varautumisen taso, arvioida sen merkitystä yhteiskunnan elintärkeiden toimintojen näkökulmasta ja erilaisten uhkien vaikutusta tietojärjestelmään VAHTI:n (2012) ICT-varautumisen vaatimukset -ohjeen mukaisesti. Tähän perustuen kyseisen vaikutusanalyysityökalun käyttö vaikutusanalyysin muodostamiseksi on organisaation edun mukaista. Dokumenttianalyysillä selvisi, että työkalulla on mahdollista selvittää myös tietojärjestelmää koskeva tietoturvallisuustaso, tiedon suojaamisen taso sekä palvelutaso.

Tämä kaikki tieto on toipumis- sekä valmiussuunnittelun näkökulmasta hyödyllistä, mutta ei dokumenttianalyysin perusteella vaikuta työkalun muodostamaan kriittisyysluokkaan. Puute on keskeinen, sillä kriittisyysluokituksen perusteet eivät vastaa valtioneuvoston kanslian tarpeita huomioivaa kriittisyyden määritelmää. Kehitysehdotuksena on, että valmiusyksikössä kehitettäisiin tietojärjestelmien kriittisyyden arviointiin soveltuva menetelmä, joka olisi erillään vaikutusanalyysistä tai nykyistä menetelmää kehitettäisiin siten, että arvio muodostettaisiin pelkkien omaan organisaatioon kohdistuvien vaikutusten sijaan koko vaikutusanalyysin tulosten kokonaisuus huomioiden.

Mikäli kriittisyyden arvioinnin menetelmää kehitetään, se tulisi ottaa käyttöön kaikkien uusien tietojärjestelmien kriittisyyden arvioinneissa ja kaikki jo käytössä olevat järjestelmät olisi arvioitava kyseisellä menetelmällä arviointien vertailukelpoisuuden varmistamiseksi. Uutta menetelmää käytettäessä on tutkittava myös tietojärjestelmien toipumissuunnitelmien ja palvelutasojen vastaavuutta päivitettyihin kriittisyysarvioihin.

Tietojärjestelmien kriittisyyden arvioinnin mallien, työkalujen ja menetelmien löytymättömyys vertailukohteiksi viittaa siihen, että aihe edellyttää yleisesti lisätutkimusta, sillä tietojärjestelmien kriittisyyden arviointi on tietoperustaan nojaten keskeinen toimenpide ICT-varautumisessa toimialasta ja organisaatiosta riippumatta. Kriittisyyden arviointia koskevien parhaiden käytäntöjen julkaiseminen olisi keino jakaa malleja ja vertailukohtia organisaatioiden toimintaan ja auttaisi kaikkia organisaatiota kehittämään omia toimintamallejaan tältä osin.

Julkisen hallinnon osalta ehdotuksena on, että toimintamallien kehittämiseksi toteutettaisiin kansainvälistä vertailututkimusta eri valtioiden vastaavien julkisen hallinnon organisaatioiden toimintatapojen kesken, sillä yksittäisen valtion sisällä julkisen hallinnon organisaatiot omaavat lähes poikkeuksetta merkittäviä eroavaisuuksia toisiinsa nähden. Vertailututkimuksen tulokset auttaisivat kehittämään tietojärjestelmän kriittisyyden arviointia ja siihen liittyviä toimialakohtaisia käytänteitä kansainvälisesti.

Kaiken kaikkiaan opinnäytetyön tuotos vastasi asetettuihin tavoitteisiin. Opinnäytetyöllä löydettiin vastaukset asetettuihin tutkimuskysymyksiin, sillä muodostettu nykytilan kuvaus tietojärjestelmien kriittisyyden arvioinnista sekä teoreettiseen viitekehykseen nojaavan tutkimustyön avulla esille nostetut puutteet ja niihin ratkaisuja tarjoavat kehitysehdotukset sekä -ideat vastaavat toimeksiantajan tarpeisiin.

Valmiusyksikössä on mahdollista hyödyntää opinnäytetyön tuloksia valtioneuvoston kansliassa toteutettavan tietojärjestelmien kriittisyyden arvioinnin prosessin kehittämistoimenpiteissä ja niiden suunnittelussa. Vaikka keskeisin tuotos oli ehdotus arviointimenetelmän kehittämisestä, opinnäytetyö painottaa teoreettiseen viitekehykseen nojaten organisaation sisäisen vastuun jakamisen ja roolien selkiyttämisen merkitystä edellytyksenä onnistuneelle tietojärjestelmien arviointityölle.

Lähteet

Painetut lähteet

CISM. 2012. CISM Review Manual 2012. Rolling Meadows, IL: ISACA.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Hirsjärvi, S. & Hurme, H. 2008. Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö. Helsinki: Gaudeamus.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15., uudistettu painos. Helsinki: Tammi.

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Helsinki: Tietosanoma.

Katakri. 2015. Tietoturvallisuuden auditointityökalu viranomaisille. Helsinki: Puolustusministeriö.

Kliem, R. L. & Richie G. D. 2016. Business continuity planning: a project management approach. Boca Raton, FL: CRC Press.

Ojasalo, K., Moilanen T. & Ritalahti, J. 2014. Kehittämistyön menetelmät: Uudenlaista osaamista liiketoimintaan. 3., uudistettu painos. Helsinki: Sanoma Pro.

Yin, R. K. Case Study Reserch. 2009. 4th edition. Thousand Oaks, CA: Sage.

Sähköiset lähteet

Alter, S. 2008. Defining Information Systems as Work Systems: Implications for the IS Field. Viitattu 17.9.2017. http://repository.usfca.edu/cgi/viewcontent.cgi?article=1021&context=at

Bowen, P., Gallup, D., Lynes, D., Swanson, M. & Wohl Phillips, A. 2010. NIST Special Publication 800-34 Rev. 1: Contingency Planning Guide for Federal Information Systems. National Institute of Standards and Technology. Viitattu 27.10.2017.
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Huoltovarmuuskeskus. 2017a. CIIP-käsite. Viitattu 17.10.2017.
https://www.huoltovarmuuskeskus.fi/toimialat/tietoyhteiskunta/ciip-kasite/

Huoltovarmuuskeskus. 2017b. Mitä on huoltovarmuus?. Viitattu 16.10.2017.
https://www.huoltovarmuuskeskus.fi/tietoa-huoltovarmuudesta/mita-on-huoltovarmuus/

JUHTA. 2012. JHS 174: ICT-palvelujen palvelutasoluokitus. Viitattu 29.10.2017.
http://docs.jhs-suositukset.fi/jhs-suositukset/JHS174/JHS174.pdf

Kangas, A. 2016. Vaikutusanalyysi (BIA, Business Impact Analysis) käyttäjän ohje. Lausuntopalvelu.fi. Viitattu 30.10.2017.
https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?attachmentId=911

Laki valtioneuvoston tilannekeskuksesta 300/2017. Annettu Helsingissä 24.5.2017. Viitattu 16.9.2017. http://www.finlex.fi/fi/laki/alkup/2017/20170300

Pullinen, M. 2012. Kriittisten tietojärjestelmien suojaaminen kyberuhilta. Laurea-ammattikorkeakoulu. Tietojenkäsittelyn koulutusohjelma. Opinnäytetyö YAMK. Viitattu 17.10.2017. https://www.theseus.fi/bitstream/handle/10024/46341/Pullinen_Mika.pdf?sequence=1&isAllowed=y

Ransome, J.F. & Rittinghouse, J.W. 2011. Business Continuity and Disaster Recovery for InfoSec Managers. Amsterdam: Elsevier Science. E-kirja. Viitattu 18.10.2017. ProQuest Ebook Central.

Rima, C. & Snedaker, S. 2013. Business Continuity and Disaster Recovery Planning for IT Professionals. 2nd edition. Amsterdam: Elsevier Science. E-kirja. Viitattu 18.10.2017. ProQuest Ebook Central.

Saastamoinen, T. 2017. Julkisen hallinnon turvallisuusverkkotoiminta (TUVE-toiminta). Valtiovarainministeriö. Viitattu 27.10.2017. http://vm.fi/turvallisuusverkkotoiminta

Standards for Security Categorization of Federal Information and Information Systems. 2004. FIPS PUB 199. Viitattu 27.10.2017. http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf

Suomen kyberturvallisuus –strategia. 2013. Valtioneuvoston periaatepäätös. Turvallisuuskomitea. Viitattu 16.10.2017.
https://www.turvallisuuskomitea.fi/index.php/fi/mcdc/14-suomen-kyberturvallisuusstrategia

Suomen Standardoimisliitto SFS. 2011a. SFS-ISO 31000:2011 Riskienhallinta. Periaatteet ja ohjeet. Viitattu 27.10.2017. SFS Online.

Suomen Standardoimisliitto SFS. 2011b. SFS-ISO/IEC 27003 Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmän toteuttamisohjeita. Viitattu 27.10.2017. SFS Online.

Suomen Standardoimisliitto SFS. 2013. SFS-ISO/IEC 27005 Informaatioteknologia. Turvallisuus. Tietoturvariskien hallinta. 2. painos. Viitattu 27.10.2017. SFS Online.

Suomen Standardoimisliitto SFS. 2014. SFS-EN ISO 22313:2014 Yhteiskunnan turvallisuus. Liiketoiminnan jatkuvuuden hallintajärjestelmät. Opastusta käyttöön. Viitattu 27.10.2017. SFS Online.

Tanhuamäki, H. 2006. Kriittisten tietojärjestelmien muutoksen hallinta. Tampereen yliopisto. Tietojenkäsittelytieteiden laitos. Pro gradu -tutkielma. Viitattu 17.10.2017.
http://tampub.uta.fi/bitstream/handle/10024/93207/gradu00904.pdf?sequence=1

Valmiuslaki 1552/2011. Annettu Helsingissä 29.12.2011. Viitattu 16.9.2017.
http://www.finlex.fi/fi/laki/ajantasa/2011/20111552

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 681/2010. Annettu Helsingissä 1.7.2010. Viitattu 27.10.2017.
http://www.finlex.fi/fi/laki/alkup/2010/20100681#Pidp450012832

Valtioneuvoston asetus valtioneuvoston kansliasta 393/2007. Annettu Helsingissä 4.4.2007. Viitattu 21.9.2017. http://finlex.fi/fi/laki/ajantasa/2007/20070393

Valtioneuvoston kanslia. 2017a. Ministeriö. Viitattu 21.9.2017.
http://vnk.fi/ministerio

Valtioneuvoston kanslia. 2017b. Johto- ja organisaatio. Viitattu 21.9.2017.
http://vnk.fi/ministerio/johto-ja-organisaatio

Valtioneuvoston kanslia. 2017c. Työskentely VNK:ssa. Viitattu 21.9.2017. http://vnk.fi/rekry/tyoskentely-kansliassa

Valtiovarainministeriö. 2017. Vaikutuanalyysin (BIA, Business Impact Analysis) täyttöpohja. Viitattu 20.10.2017. http://vm.fi/documents/10623/307681/Vaikutusanalyysi/7463adc9-eced-42ac-a83b-ac2aedc007f5

VAHTI. 2007. Tietoturvallisuudella tuloksia: Yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 30.10.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229

VAHTI. 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Viitattu 30.10.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=b4a90e50-7307-4004-ac8e-b9103220db6a&groupId=10128&groupId=10229

VAHTI. 2012. ICT-varautumisen vaatimukset. Viitattu 16.10.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c99a95f5-c150-49b6-aa5c-a90a821da13e&groupId=10229

VAHTI. 2016. Toiminnan jatkuvuuden hallinta. Viitattu 30.10.2017. https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229

Yhteiskunnan turvallisuusstrategia. 2010. Valtioneuvoston periaatepäätös. Puolustusministeriö. Viitattu 15.10.2017. https://www.defmin.fi/files/1696/Yhteiskunnan_turvallisuusstrategia_2010.pdf

Yhteiskunnan turvallisuusstrategia. 2017. Valtioneuvoston periaatepäätös. Turvallisuuskomitea. Viitattu 3.11.2017. https://www.turvallisuuskomitea.fi/index.php/fi/yhteiskunnan-turvallisuusstrategia-2017

Julkaisemattomat lähteet

Laurea-ammattikorkeakoulu. 2016. Opinnäytetyöohje. Viitattu 16.9.2017. Opiskelijoiden intranet LINK.

Puhakainen, P., Pullinen, M. & Sjöroos, M. 2017. Valmiusyksikön tietoturvallisuusasiantuntijoiden ryhmähaastattelu 20.10.2017. Valtioneuvoston kanslia. Helsinki

Sjöroos, M. 2017. Tietoturvallisuuden erityisasiantuntijan puhelinhaastattelu 6.11.2017. Espoo.

Valtioneuvoston kanslia. 2017d. Valtioneuvoston kanslia. Tulostettu 6.10.2017. Organisaatiota esittelevä PowerPoint –esitys.

Kuviot

Taulukot

Liitteet

Liite 1: Haastattelun 20.10.2017 teemarunko

Teema 1: Käsitteet ja roolit

1. Mitkä ovat organisaatiossa käytettävät jatkuvuudenhallinnan käsitteet?
   Miten koetaan a) jatkuvuussuunnittelu, b) varautuminen ja c) valmiussuunnittelu?

2. Yksiköiden roolit ICT-varautumisessa

Teema 2: Suunnittelu ja vastuut

3. Toteutetaanko tietojärjestelmiä koskeva suunnittelu osana prosessien tai toimintojen jatkuvuussuunnittelua?

4. Miten suunnittelun vastuunjako on toteutettu?

Teema 3: Kriittisyyden arvioinnin prosessi

5. Mihin organisaation tietojärjestelmien kriittisyyden arviointi ja sen kehittäminen perustuu?

6. Tietojärjestelmien kriittisyyden arvioinnissa sovellettavat ohjeet, työkalut ja menetelmät

7. Tietojärjestelmien kriittisyyden arviointiin osallistuvat tahot

8. Tietojärjestelmien kriittisyyden arvioinnin vaiheet

Liite 2: Haastattelun 6.11.2017 teemarunko

1. **Tietojärjestelmien kriittisyyden arvioinnin hallinnoinnin ja seurannan työkalut**

- Onko työkaluja kuten vuosikello käytössä?

- Jos ei, onko suunniteltu käyttöönotettavaksi?

2. **Viimeisimmät toimenpiteet organisaatiossa tietojärjestelmien kriittisyyden arvioinnin osalta**

- Miten prosessi on toteutunut?

- Miten prosessi on ohjattu?

- Mitä on saatu aikaan?

3. **Organisaation tarpeet tietojärjestelmien kriittisyyden arvioinnissa**

- Miten tietojärjestelmien kriittisyys ymmärretään?

- Mistä tekijöistä kriittisyysarvo tulisi organisaation näkökulmasta muodostua?

Liite 3: Luokittelumallien vertailu

Luokittelumallin lähde	Luokittelu	Luokittelun peruste (kriteerit)
Vaikutusanalyysi-työkalun tärkeys-luokittelu	1. Ei Kriittinen 2. Normaali tärkeys 3. Merkittävä 4. Tärkeä 5. Erittäin tärkeä 6. Kriittinen/elintärkeä	Odottamattoman katkoksen, tietojen menetyksen ja vanhenemisen vaikutukset: • Terveyden tai hengen vaara • Lakisääteiset tehtävät • Taloudelliset vahingot • Mainevaikutukset, jotka kohdistuvat omaan organisaatioon, asiakkaisiin ja loppukäyttäjiin tai yhteiskuntaan asteikolla 1-5: 0. Ei arvioitu 1. Ei vaikutusta 2. Jonkin verran 3. Merkittävät 4. Kohtuuttomat 5. Sietämättömät
VAHTI 2/2012: Järjestelmien varautumistasot	1. Perustaso 2. Korotettu taso 3. Korkea taso	• Toiminnan keskeytymisen vaikutukset • Tavoitteellinen toipumisaika • Merkitys elintärkeiden toimintojen kannalta • Toimintavaatimus häiriötilanteissa ja poikkeusoloissa
Iivari & Laaksonen: IT-järjestelmien luokittelun esimerkki	Luokka I Luokka II Luokka III Luokka IV	• Toiminnan keskeytymisen vaikutukset • Tavoitteellinen toipumisaika • Käyttötarkoitus • Tietosisältö • Tietoliikenteen sisältö (esim. raha ja määrä) • Riippuvuussuhteet ja niiden määrä
Rima & Snedaker: Kriittisyyden arviointijärjestelmän esimerkki	1. Critical functions 2. Essential functions 3. Necessary functions 4. Desirable functions	• Riippuvuus organisaation ydintoimintoihin • Toimintahäiriön vaikutukset organisaatiolle o Vakavuus ja välittömyys
SFS-ISO/IEC 27005	3-10 luokkaa, jotka vastaavat organisaatiossa käytössä olevaa riskienarviointimallia	• Toimintahäiriön seurauksena järjestelmän sisältämän tiedon luottamuksellisuuden, eheyden ja käytettävyyden menetyksen organisaatiolle aiheuttama o kustannus o vaikutus suorituskykyyn o vaikutus maineeseen o henkilötietojen tai muun tiedon vuotaminen o ihmisten tai ympäristön turvallisuuden vaarantuminen o vaikutus lakien täytäntöönpanoon o järjestyksen rikkomiseen • Järjestelmän riippuvuuksien olennaisuus ja määrä
NIST 800-34 -vaikutustason luokittelumalli	1. Low 2. Moderate 3. High	Keskeytymisvaikutukset riippuvuuksien mukaan