Jarkko Hänninen

RISKIENHALLINTA PIENIEN JA KESKISUURIEN KUNTIEN DIGITAALISESSA TURVALLISUUDESSA - TAPAUSTUTKIMUS

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2020

TIIVISTELMÄ

Hänninen, Jarkko
Riskienhallinta pienien ja keskisuurien kuntien digitaalisessa turvallisuudessa - tapaustutkimus
Jyväskylä: Jyväskylän yliopisto, 2020, 102 s.
Kyberturvallisuus, pro gradu -tutkielma
Ohjaaja: Seppänen, Ville

Tutkimuksen tavoitteena oli selvittää pienien ja keskisuurien kuntien digitaaliseen turvallisuuteen ja siihen liittyvään riskienhallintaan liittyviä käytänteitä. Julkisen hallinnon, mukaan lukien kuntien, digitaalista turvallisuutta ja riskienhallintaa ohjataan muun muassa lainsäädännöllä. Laki julkisen hallinnon tiedonhallinnasta (906/2019) asettaa kuntien tietoturvallisuudelle vaatimuksia, jonka takia tutkimuksen tavoitteena oli selvittää myös pienien ja keskisuurien kuntien valmiuksia lainsäädännön tietoturvallisuudelle asettamien vaatimuksien noudattamiseen. Laki julkisen hallinnon tiedonhallinnasta astuu kuntien osalta pääosin voimaan vuoden 2023 alusta, jolloin lain määrittämä siirtymäkausi päättyy ja kuntien tietoturvallisuuden pitäisi olla lain asettamien vaatimuksien tasalla. Tutkimuksessa hyödynnettiin laadullista tutkimusmenetelmää. Tutkimusaineisto koostui yhteensä neljän pienen ja keskisuuren kunnan kunnanjohtajan ja tietoturvasta vastaavan tai kunnan tietohallinnosta vastaavan henkilön teemahaastatteluista. Tutkimustuloksien mukaan pienien ja keskisuurien kuntien digitaalisen turvallisuuden ja siihen liittyvän riskienhallinnan käytänteet vaihtelivat kuntakohtaisesti suuresti ja niissä oli vielä kehitettävää. Tiedonhallintalain kunnille asettamien tietoturvallisuusvaatimuksien toteuttamisessa oli niin ikään vielä kehitettävää suurimmassa osassa tutkimukseen osallistuneista kunnista. Digitaalisen turvallisuuden takaamiseksi ja tiedonhallintalain tietoturvallisuudelle asettamien vaatimuksien toteuttamiseksi oli pienissä ja keskisuurissa kunnissa tarvetta digitaaliseen turvallisuuteen suunnattaville lisäresursseille. Seudullisella yhteistyöllä pystyttiin tutkimustuloksien mukaan jakamaan digitaalisen turvallisuuden kehittämiseen vaadittavia resursseja ja parantamaan pienien ja keskisuurien kuntien digitaalisen turvallisuuden käytänteitä.

Asiasanat: digitaalinen turvallisuus, riskienhallinta, tietoturvallisuus, kyberturvallisuus, toiminnan jatkuvuus ja varautuminen, tietosuoja

ABSTRACT

Hänninen, Jarkko
Risk management in digital security in small and medium-sized municipalities – Case study
Jyväskylä: University of Jyväskylä, 2020, 102 pp.
Cyber Security, Master's Thesis
Supervisor: Seppänen, Ville

The aim of the study was to find out the management practices related to digital security and risk management in small and medium-sized municipalities. Digital security and risk management in public sector, including municipalities, are governed by legislation, among other things. The act on Information Management in Public Administration (906/2019) sets requirements for the information security of municipalities, which is why the aim of the study was also to find out the capacity of small and medium-sized municipalities to comply with the information security requirements set by legislation. The act on Information Management in Public Administration will enter into force for municipalities mainly from the beginning of 2023, when the transition period determined by law will end and the information security of municipalities should be up to date with the requirements set by the law. The study utilized a qualitative research method. The research material consisted of semi-structured interviews from a total of four different municipalities: municipal managers and a person responsible for information security or the person responsible for information management in the municipality. According to the research results, the digital security and related risk management practices of small and medium-sized municipalities varied greatly from municipality to municipality and there was still need for improvement. The implementation of the information security requirements set for municipalities by the Information Management Act also still needed to be developed in most of the municipalities participating in the study. In order to guarantee digital security and to implement the requirements set by the Information Management Act for information security, small and medium-sized municipalities needed additional resources for digital security. According to the research results, regional co-operation was able to share the resources required for the development of digital security and to improve the digital security practices of small and medium-sized municipalities.

Keywords: Digital Security, Risk Management, Cyber Security, Continuity Management, Information Security, Data Protection

KUVIOT

TAULUKOT

SISÄLLYS

1 JOHDANTO

Kuntasektori on joutunut kyberhyökkäysten kohteeksi. Kesällä 2019 Lahden kaupunkiin kohdistui kyberhyökkäys, jonka välittömät kustannukset nousivat useisiin satoihin tuhansiin euroihin. Kyberhyökkäys ei ollut ensimmäinen Lahden kaupungin palveluihin kohdistunut hyökkäys, ja kaupunginjohtajan mukaan kaupungin tietoturvan taso ei ollut riittävällä tasolla (Yleisradio, 2019). Kyberhyökkäyksien kohteeksi ovat viime vuosien aikana kuntasektorilla joutuneet Lahden lisäksi useat muutkin kunnat. Miten digitaalisen turvallisuuden riskienhallintaan suhtaudutaan pienissä ja keskisuurissa kunnissa? Millainen digitaalisen turvallisuuden taso on yleisesti pienissä ja keskisuurissa kunnissa? Millaiset valmiudet pienillä ja keskisuurilla kunnilla on vastata lain julkisen hallinnon tiedonhallinnasta (906/2019) tietoturvallisuudelle asettamiin vaatimuksiin?

Tämän pro gradu –työn aiheena on ”Riskienhallinta pienien ja keskisuurien kuntien digitaalisessa turvallisuudessa - tapaustutkimus”. Työn tavoitteena on selvittää pienien ja keskisuurien kuntien digitaalisen turvallisuuden tilaa sekä siihen liittyviä riskienhallinnan käytänteitä. Työn tavoitteena on lisäksi selvittää pienien ja keskisuurien kuntien valmiuksia laki julkisen hallinnon tiedonhallinnasta (906/2019) asettamien tietoturvallisuusvaatimuksien toteuttamiseen. Laki julkisen hallinnon tiedonhallinnasta astui voimaan vuoden 2020 alusta alkaen. Kuntasektorin osalta lain vaatimukset astuvat voimaan vuoden 2023 alusta lain siirtymäkauden loputtua, jolloin kuntien pitäisi pystyä täyttämään lain kuntasektorille asettamat vaatimukset.

Kuntien digitaalisen turvallisuuden tilaan kohdistuvia tutkimuksia on tehty vähän. Olemassa olevat tutkimukset käsittelevät digitaalista turvallisuutta tietyn osa-alueen näkökulmasta eivätkä kohdistu varsinaisesti pieniin ja keskisuuriin kuntiin (esim. VAHTI Digiturvakyselyt). Tutkimusta pienien ja keskisuurien kuntien valmiuksista laki julkisen hallinnon tiedonhallinnasta tietoturvallisuusvaatimuksien täyttämiseen ei ole tehty. Tutkimuksen tulokset tuovatkin kaivattua lisätietoa pienien ja keskisuurien kuntien digitaalisen turvallisuuden käytänteistä ja tilasta sekä valmiuksista laki julkisen hallinnon tiedonhallinnasta tietoturvallisuus vaatimuksien toteuttamiseen.

1.1 Tutkielman keskeiset käsitteet

Tutkielman keskeisiä käsitteitä ovat digitaalinen turvallisuus, riskienhallinta, riskiarviointi, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus, tietosuoja ja kyberturvallisuus. Digitaalinen turvallisuus käsitteenä sisältää viisi osa-aluetta, jotka ovat riskienhallinta, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus, kyberturvallisuus ja tietosuoja (Valtiovarainministeriö, 2020c). Kyberturvallisuuden käsitteellä tarkoitetaan digitaalisen turvallisuuden viitekehyksessä toimintaympäristöä, jossa tietoa säilytetään, käsitellään ja siirretään. Kyberturvallisuudella tarkoitetaan sanastokeskuksen (2018) mukaan tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Toiminnan jatkuvuuden hallinnan ja varautumisen käsite sisältää suunnitelmia ja toimenpiteitä, joiden tavoitteena on varmistaa organisaation ydintoiminnan häiriötön toiminta eri tilanteissa (Wan & Chan, 2008). Tietoturvallisuudella tarkoitetaan järjestelyjä, joiden avulla tiedon saatavuus, eheys ja luottamuksellisuus pyritään varmistamaan (Sanastokeskus TSK, 2018). Tietosuojalla tarkoitetaan digitaalisen turvallisuuden viitekehyksessä henkilötietosuojaa. Henkilötietosuoja määritellään sanastokeskuksen (2020) mukaan järjestelyiksi, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen. Digitaalisen turvallisuuden osa-alueiden lisäksi tutkielman keskeisiin käsitteisiin lukeutuu laki julkisen hallinnon tiedonhallinnasta (906/2019), jonka osuus tutkielmassa rajoittuu kuntien tietoturvallisuudelle asetettuihin vaatimuksiin.

1.2 Tutkimusmenetelmä, tutkimuskysymykset ja tutkimuksen rakenne

Tutkimus toteutettiin laadullista tutkimusmenetelmää hyödyntäen. Tutkimustehtävänä oli selvittää pienien ja keskisuurien kuntien digitaaliseen turvallisuuteen liittyviä käytänteitä erityisesti riskienhallinnan näkökulmasta. Tutkimustehtävänä oli myös selvittää pienien ja keskisuurien kuntien valmiutta laki julkisen hallinnon tiedonhallinnasta tietoturvallisuudelle asettamien vaatimuksien täyttämiseen. Tutkimustehtävien selvittämiseksi pyritään tutkimuksessa hakemaan vastausta tutkimuskysymyksiin:

- Millainen digitaalisen turvallisuuden tilanne on pienissä ja keskisuurissa kunnissa?
- Miten digitaalisen turvallisuuden riskienhallinta on organisoitu, ja millaisia käytänteitä siihen liittyy pienissä ja keskisuurissa kunnissa?

- Millaiset valmiudet pienissä ja keskisuurissa kunnissa on laki julkisen hallinnon tiedonhallinnasta (906/2019) tietoturvallisuudella asettamien vaatimusten suhteen?

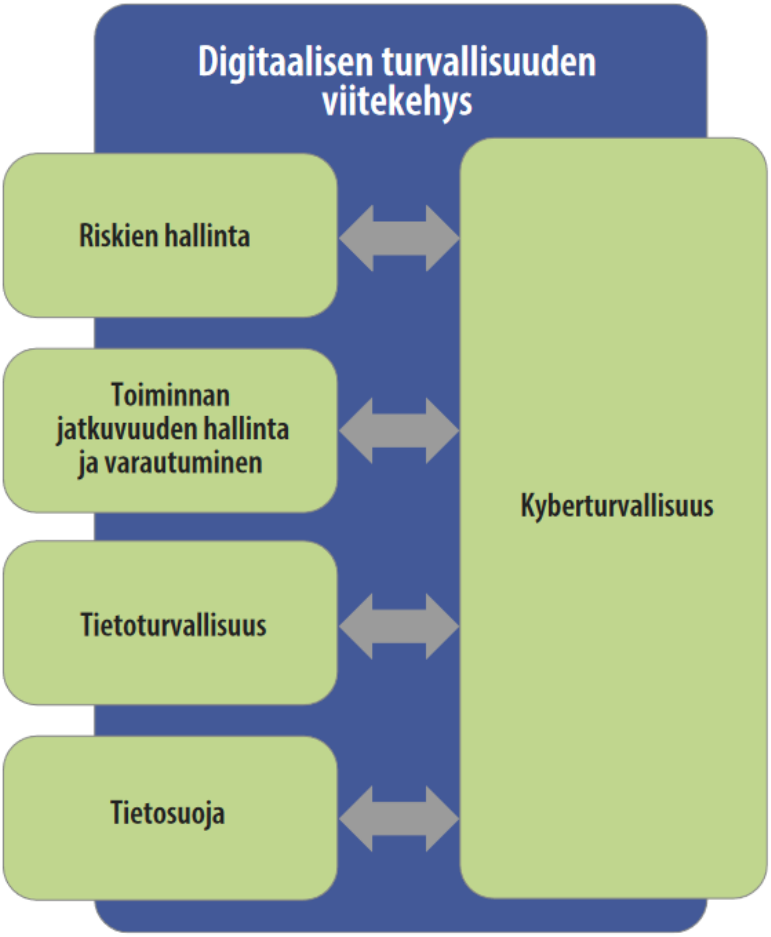
Tutkimuksen empiirinen materiaali kerättiin haastattelemalla neljästä eri kunnasta kunnanjohtajaa ja tietoturvasta vastaavaa henkilöä tai kunnan tietohallinnosta vastaavaa henkilöä. Tutkimusaineisto käsiteltiin kirjalliseen muotoon, minkä jälkeen aineisto analysoitiin hyödyntämällä sisällönanalyysia. Sisällönanalyysilla tuotetusta tiedosta muodostettiin tutkimuksen lopulliset tulokset, joita käsiteltiin vielä tarkemmin tutkimuksen pohdinnoissa ja johtopäätöksissä.

Tämän pro gradu tutkimuksen johdannossa käsitellään työn tavoitteet, keskeiset käsitteet, tutkimusmenetelmä ja tutkimuskysymykset sekä tutkimuksen rakenne. Luvuissa kaksi – viisi käsitellään tutkimuksen keskeiset määritelmät kirjallisuuteen perustuen, jotka muodostavat tutkimuksen teoreettisen viitekehyksen. Tutkimuksen kuudennessa luvussa käsitellään tarkemmin tutkimuksessa hyödynnettyä laadullista tutkimusmenetelmää, tutkimuksen varsinaista tutkimusprosessia sekä arvioidaan tutkimuksen laadukkuutta. Tutkimuksen luvussa seitsemän esitellään tutkimuksen tulokset tutkimuskysymyksittäin. Kahdeksannessa luvussa pohditaan tutkimustuloksia teoriaan nähden ja kootaan johtopäätökset tutkimuksesta.

2 Digitaalinen turvallisuus

Digitaalisen turvallisuuden kokonaisuus muodostuu riskien hallinnan, toiminnan jatkuvuuden hallinnan ja varautumisen, tietoturvallisuuden, tietosuojan ja kyberturvallisuuden osa-alueista. Tässä luvussa käsitellään digitaalisen turvallisuuden osa-alueet, pois lukien riskien hallinnan osa-alue, jota käsitellään tarkemmin luvussa 3.

Digitaalisen turvallisuuden viitekehys (kuvio 1) sisältää digitaaliseen turvallisuuteen liittyvät osa-alueet. Näitä osa-alueita ovat riskien hallinta, toiminnan jatkuvuuden hallinta ja varautuminen, tietoturvallisuus, tietosuoja ja kyberturvallisuus (Valtiovarainministeriö, 2020c).



Kuvio 1 Digitaalisen turvallisuuden viitekehys (Valtiovarainministeriö, 2020a, s. 16)

Digitaalisen turvallisuuden kokonaisuuden muodostavat vahvasti toisiinsa sidoksissa olevat, osittain myös päällekkäiset osa-alueet. Tässä tutkimuksessa digitaalisen turvallisuuden osa-alueiden määrittämisessä hyödynnetään sanastokeskuksen julkaisemaa kyberturvallisuuden sanastoa, jonka

käsitekaavioiden perusteella eri osa-alueet voidaan erottaa omiksi kokonaisuuksiksi.

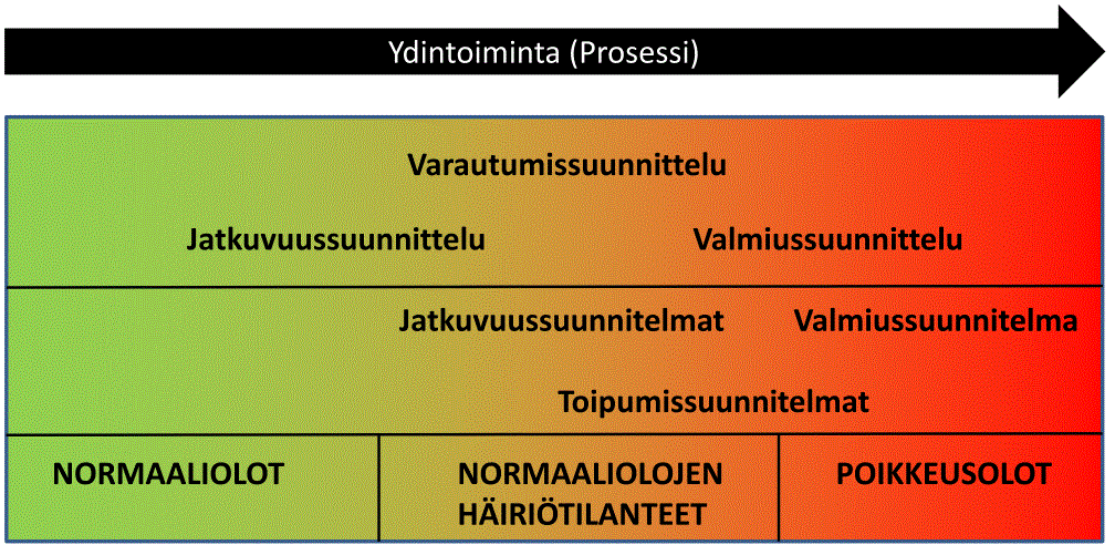
Digitaalisen turvallisuuden keskeisenä tavoitteena on suojata kansalaisia, yhteisöjä ja yhteiskuntaa digitaaliseen toimintaympäristöön kohdistuvilta riskeiltä ja lisätä luottamusta yhteiskunnassa eri toimijoiden välillä, varmistamalla turvallinen digitaalinen toimintaympäristö kansalaisten, yritysten ja yhteisöjen yhteistyöhön (Valtiovarainministeriö, 2020a).

2.1 Toiminnan jatkuvuus ja varautuminen

Digitaalisen turvallisuuden toiminnan jatkuvuus ja varautuminen -osa-alueen tavoitteena on varmistaa organisaation ydintoiminnan häiriötön toiminta eri tilanteissa. Toiminnan jatkuvuuden ja varautumisen kokonaisuus sisältää hallinnollisia prosesseja sekä suunnitelmia, joilla pyritään varautumaan organisaation ydintoimintaa uhkaaviin häiriötilanteisiin ja varmistamaan ydintoimintojen jatkuvuus mahdollisimman vähäisin ja vaikutuksiltaan pienin keskeytyksin (Wan & Chan, 2008; Valtionvarainministeriö, 2016). Toiminnan jatkuvuuden varmistamisesta ja varautumisesta onkin tullut olennainen osa organisaation hallintoa ja hyvää hallintotapaa (European Union Agency for Cybersecurity, 2019).

2.1.1 **Toiminnan jatkuvuuden ja varautumisen suunnittelu**

Toiminnan jatkuvuuden ja varautumisen suunnitteluun sisältyvät suunnitelmat, joilla pyritään varmistamaan organisaation ydintoiminnan mahdollisimman korkea resilienssi ja toiminnantaso. Toiminnan jatkuvuuden ja varautumisen suunnitelmiin lukeutuvat (kuvio 2) mm. jatkuvuussuunnitelmat, varautumis-suunnittelu, toipumissuunnitelmat sekä valmiussuunnitelmat (Valtionvarainministeriö, 2016).



Kuvio 2 Toiminnan jatkuvuus ja varautuminen (Iivari & Laaksonen, 2009)

Toiminnan jatkuvuussuunnitelmiin sisältyvät suunnitelmat toimenpiteistä, joilla pyritään takaamaan organisaation ydintoiminnan prosessien jatkuvuus häiriötilanteiden aikana ja niiden jälkeen (Swanson, Bowen, Phillips, Gallup, & Lynes, 2010). Toiminnan jatkuvuussuunnitelmissa kuvataan sekä normaaliolojen että normaaliolojen häiriötilanteiden toimenpiteet, vastuut ja johtaminen. Kuvausten mukaisesti tapahtuvalla toiminnalla pyritään organisaation ydintoimintoja jatkamaan häiriötapahtumien aikana sekä vähentämään häiriötapahtumien kestoa ja vaikutusta (Niemimaa & Järveläinen, 2013; Valtionvarainministeriö, 2016).

Toipumissuunnitelmat ovat tärkeä osa jatkuvuussuunnittelua. Toipumissuunnitelmat sisältävät yleensä selkeän ja yksityiskohtaisen suunnitelman tietojärjestelmien toipumiseen häiriötilanteesta. Toipumissuunnitelmissa määritellään jatkuvuussuunnitelman piirissä oleville tietojärjestelmille käytännön toimenpiteet sekä vastuut ja roolit häiriötilanteista palautumiseen (Wan & Chan, 2008). Toipumissuunnittelussa huomioidaan myös riittävä ja oikeanlainen viestintä tarvittaville kohderyhmille. Toipumissuunnitelmien ajantasaisuus ja ylläpito tulee huomioida organisaation tuottamien palveluiden lisäksi myös ostettujen palveluiden osalta (Valtionvarainministeriö, 2016).

Valmiussuunnittelu sisältää poikkeusolojen varalle suunnitelmat, joilla pyritään varmistamaan elintärkeiden toimintojen jatkuminen poikkeusoloissa. Valmiussuunnittelulla pyritään turvaamaan yhteiskunnan toiminta, kansallinen turvallisuus sekä väestön perusoikeudet ja turvallisuus poikkeusolojen aikana. Valmiussuunnittelua ohjaa valmiuslaki, joka velvoittaa valtion viranomaisten, valtion liikelaitosten sekä kuntien ja kuntayhtymien valmiussuunnitelmin ja etukäteisvalmisteluin varautumaan tehtäviensä hoitamiseen poikkeusolojen aikana (Oikeusministeriö, 2011).

2.1.2 **Toiminnan jatkuvuuden ja varautumisen toteuttaminen**

Toiminnan jatkuvuuden ja varautumisen toteuttamiseen on julkaistu useita toisiaan muistuttavia viitekehyksiä. Viitekehyksille yhteisiä toiminnan jatkuvuuden ja varautumisen toteuttamisen toimenpiteitä ovat mm. toiminnan suunnitelmallisuus ja tavoitteiden määrittäminen (politiikka), toimintaympäristön analyysi ja riskianalyysi, toiminnan vaikutusanalyysi, toimintojen priorisointi ja järjestelmien luokittelu vaikutusanalyysin mukaisesti, palautumiseen liityvien tavoitteiden määrittely, jatkuvuus- ja toipumissuunnitelmien dokumentointi sekä toiminnan jatkuvuuden ja varautumisen suunnitelmien testaus, harjoittelu ja koulutus (Niemimaa & Järveläinen, 2013; Valtionvarainministeriö, 2016; Swanson ym., 2010; International Organization for Standardization, 2011).

Toiminnan jatkuvuuden ja varautumisen toteuttaminen aloitetaan edellä mainittujen viitekehyksien mukaan määrittämällä organisaation toiminnan jatkuvuuden ja varautumisen politiikka. Toiminnan jatkuvuuden ja varautumisen politiikka hyväksytään organisaation johdon toimesta, joka mahdollistaa riittävät valtuudet toiminnan jatkuvuuden ja varautumisen toteuttamiselle (Niemimaa & Järveläinen, 2013). Toiminnan jatkuvuuden ja varautumisen politiikan tulisi sisältää tarvittavat tiedot toiminnan tavoitteista, vastuista, resursseista sekä muista käytännön suunnitelmista organisaatiotasolta operatiiviselle tasolle (Swanson ym., 2010; International Organization for Standardization, 2011).

Organisaation toimintaympäristön tunteminen ja analysointi toimivat perustana riskianalyysin suorittamiselle, jonka perustella organisaation riskienhallintaa suoritetaan. Riskianalyysin avulla selvitetään toimintaympäristöön kohdistuvia sisäisiä ja ulkoisia riskejä, jotka voivat toteutuessaan vaikuttaa organisaation toiminnan jatkuvuuteen. Toimintaympäristön analyysin ja riskianalyysin suorittamisen avulla organisaatio saa riskienhallintaan tarvittavaa tietoa toimintaympäristöstään sekä toimintaympäristöä mahdollisesti uhkaavista riskitekijöistä (Niemimaa & Järveläinen, 2013; International Organization for Standardization, 2013c).

Toiminnan vaikutusanalyysillä tarkoitetaan prosessia, jossa organisaation toimintoihin kohdistuvien riskien vaikutusta ja merkityksellisyyttä arvioidaan organisaation ydintoiminnan kannalta. Toiminnan vaikutusanalyysilla pyritään selvittämään organisaation kannalta kriittiset toiminnot ja niiden keskeytyksestä aiheutuvat vaikutukset organisaation toiminnalle (Botha & Von Solms, 2004 ; Valtionvarainministeriö, 2016; Niemimaa & Järveläinen, 2013). Organisaatioiden ydintoiminnot ovat digitalisaation myötä vahvasti sidoksissa tietojärjestelmiin ja muuhun toimintaa tukevaan tieto- ja viestintätekniikkaan. Toiminnan vaikutusanalyysissa voidaankin hyödyntää organisaation toimintaympäristöön tehdyn riskianalyysin tuloksia kriittisyyden, vaikutusten ja häiriöiden aiheuttamien menetyksien arvioinnissa (Niemimaa & Järveläinen, 2013; Niemimaa, 2017).

Toimintojen priorisoinnilla pyritään varmistamaan organisaation ydintoiminnan kannalta tärkeimpien toimintojen jatkuvuus määritetyn tason mukaisesti. Toimintojen priorisoinnissa huomioidaan toiminnan vaikutusanalyysin tulokset, joiden pohjalta organisaation johto hyväksyy organisaation toiminnan jatkuvuudelle asetetut vaatimukset. Toiminnan jatkuvuudelle asetetut vaatimukset määrittävät toiminnan palautumiselle vähimmäistavoitteet, jonka perusteella järjestelmät luokitellaan kriittisyyden mukaisesti (International Organization for Standardization, 2011).

Palautumiselle asetetut tavoitteet sisällytetään organisaation toipumissuunnitelmiin, joilla pyritään varmistamaan organisaation ydintoiminnan jatkuvuus ennalta määritettyjen tavoitteiden mukaisesti. Toipumissuunnitelmat määritetään kaikille toiminnan vaikutusanalyysissa esiin nousseille, organisaation ydintoiminnalle merkityksellisille järjestelmille ja palveluille. Toipumissuunnitelman tulisi sisältää toipumisaikatavoitteen ja toipumispistetavoitteen määrityksen lisäksi myös tiedot mm. toipumiseen osallistuvista henkilöistä ja toipumiseen liittyvistä vastuista (Botha & Von Solms, 2004 ; Niemimaa & Järveläinen, 2013; International Organization for Standardization, 2011).

Jatkuvuussuunnitelmien dokumentoinnissa tulee huomioida niiden sisällöllinen kattavuus. Jatkuvuussuunnitelman tulisi sisältää riittävät tiedot jatkuvuuden johtamisesta, vastuista ja toiminnasta mahdollisissa häiriötilanteissa (Niemimaa & Järveläinen, 2013; Valtionvarainministeriö, 2016). Jatkuvuussuunnitelmaan liittyvän toipumissuunnitelman pitäisi puolestaan sisältää mahdollisimman helposti ja nopeasti ymmärrettävää tietoa palautukseen liittyvistä toimenpiteistä, jotta palautumisprosessiin liittyvä toiminta olisi mahdollisimman tehokasta (Niemimaa, 2017).

Suunnitelmien testaamisella, harjoittelulla ja koulutuksella pyritään varmentamaan jatkuvuuteen ja varautumiseen liittyvien prosessien toiminta oikeissa häiriötilanteissa. Jatkuvuuden ja varautumisen testaamisella pyritään lisäksi myös muun muassa varmistamaan suunnitelmien kattavuus kaikkien organisaation ydintoimintojen osalta muuttuvassa toimintaympäristössä. Testaamisen ja harjoittelun avulla jatkuvuuden ja varautumisen prosessit saadaan tutuiksi niistä vastaaville ja operoiville tahoille, jolloin toiminta oikeassa jatkuvuuden häiriötilanteessa on tehokkaampaa. Testaamisen ja harjoittelun esiin nostamat epäkohdat ja puutteet tulee korjata, jolloin jatkuvuuden hallinnan prosessit pysyvät ajantasaisina ja toimivina. Jatkuvuussuunnitelmiin liittyvä koulutus tulee olla kohdennettua ja jatkuvaa, jolloin kohderyhmien osaaminen ja toiminta pysyvät jatkuvuudelle asetettujen tavoitteiden tasolla (Botha & Von Solms, 2004; Niemimaa & Järveläinen, 2013; Valtionvarainministeriö, 2016).

2.1.3 **Jatkuvuuden hallinnan seuranta ja arviointi**

Jatkuvuuden hallinnan seurannan, mittaamisen ja arvioinnin keinoilla pyritään varmistamaan jatkuvuuden hallinnan prosessien toimivuus ja jatkuvuuden hallinnalle ennalta asetettujen tavoitteiden toteutuminen.

Jatkuvuuden hallinnan prosessien mittaamisessa hyödynnetään ennalta määritettyjä mittareita, joiden tulisi pohjautua organisaation ydintoimintoihin. Jatkuvuuden hallinnan seurannassa ja mittaamisessa pitäisi huomioida toteutuneiden häiriötilanteiden lisäksi myös muita mitattavia kohteita (Valtionvarainministeriö, 2016; International Organization for Standardization, 2011). Vahti 2/2016 -ohjeen mukaan näitä mitattavia kohteita voivat olla esimerkiksi:

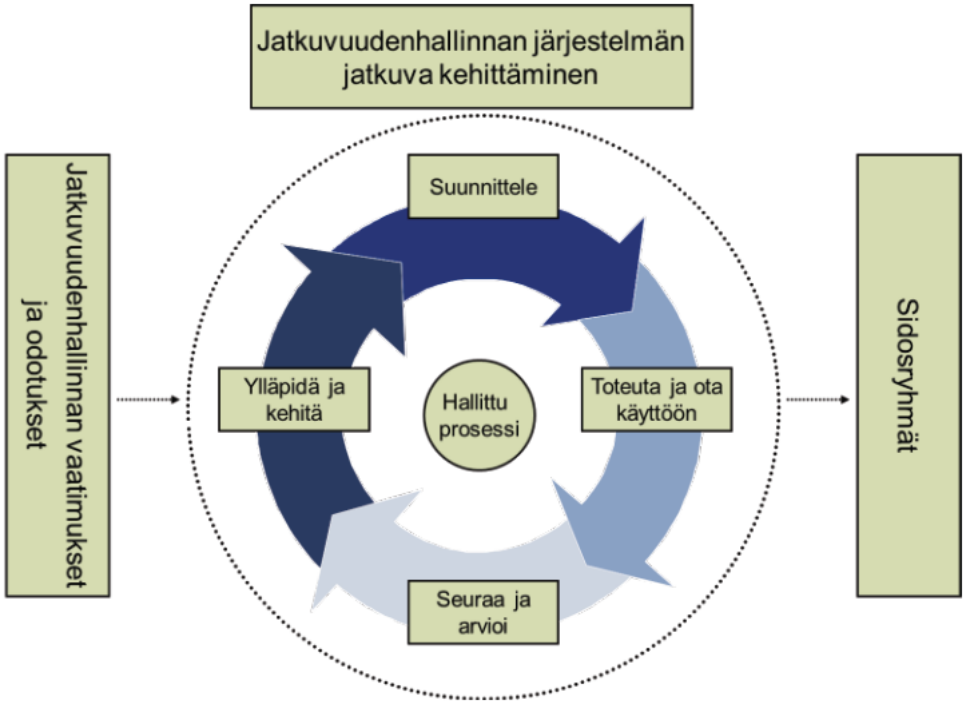
- *Toteutuneet palautusajat ja -pisteet vs. toipumisskenaarioissa arvioidut tavoitteet (RTO ja RPO)*
- *Riskianalyysin onnistuminen (BIA vs. toteutunut vahinko, SLA:n vastaavuus)*
- *Reagointi-, vaste- ja läpimenoajat (oma henkilöstö, palvelutarjoaja jne.) vs. luvatut*
- *Suunnittelemattomien käyttökatkojen pituus*
- *Jatkuvuus- ja toipumissuunnitelmien sisällön ajantasaisuus (vastaavatko suoritetut toipumistoimenpiteet suunniteltuja; vastaavatko toiminnan prosessit kuvattuja?)*
- *Viestinnän onnistuminen (saavatko oikeat tahot oikean tiedon oikeaan aikaan?)*
- *Tapahtuneet merkittävät virhe- ja häiriötilanteet vs. skenaariot joihin on varauduttu*
- *Hallintajärjestelmän vuosikellon mukaisten toimenpiteiden toteutuminen*
- *Dokumenttien ajantasaisuus*
- *Koulutusten järjestäminen ja kohdentaminen*
- *Hallintajärjestelmän auditoinnit ja standardinmukaisuus*
- *Omien seurantajärjestelmien havainnointikyky. (Valtionvarainministeriö, 2016)*

Jatkuvuuden hallinnan jatkuvaan kehittämiseen organisaatioissa voidaan hyödyntää sisäisiä ja ulkoisia auditointeja ja katselmuksia. Auditointien tuloksena syntyvät raportit tarjoavat organisaatiolle tärkeää tietoa jatkuvuuden hallintajärjestelmään liittyvien suunnitelmien parantamiseksi ja toiminnasta löytyvien puutteiden korjaamiseksi (Valtionvarainministeriö, 2016).

Organisaation johdon osallistuminen ja tuki jatkuvuuden hallinnan kehittämiselle ja resursoinnille tulee varmistaa, jotta jatkuvuuden hallinnan resurssit ovat riittävät ja jotta prosessi kohdistuu tarkoituksen mukaisiin asioihin (Valtionvarainministeriö, 2016).

2.1.4 Jatkuvuuden hallinnan kehittäminen

Jatkuvuuden hallinnan suunnittelu ja kehittäminen ovat jatkuva prosessi, joka pitäisi integroida osaksi organisaation toimintaa. Jatkuvuuden hallinnan kehittäminen perustuu jatkuvuuden hallinnan standardeissa PDCA-sykliin (kuvio 3), jossa prosessi etenee jatkuvana suunnittelusta toteutukseen, tarkistukseen ja tarvittaviin muutoksiin ja kehitykseen. Muutoksien jälkeen sykli aloitetaan jälleen alusta, jolloin järjestelmän kehittäminen säilyy jatkuvana prosessina (International Organization for Standardization, 2011; Valtionvarainministeriö, 2016).



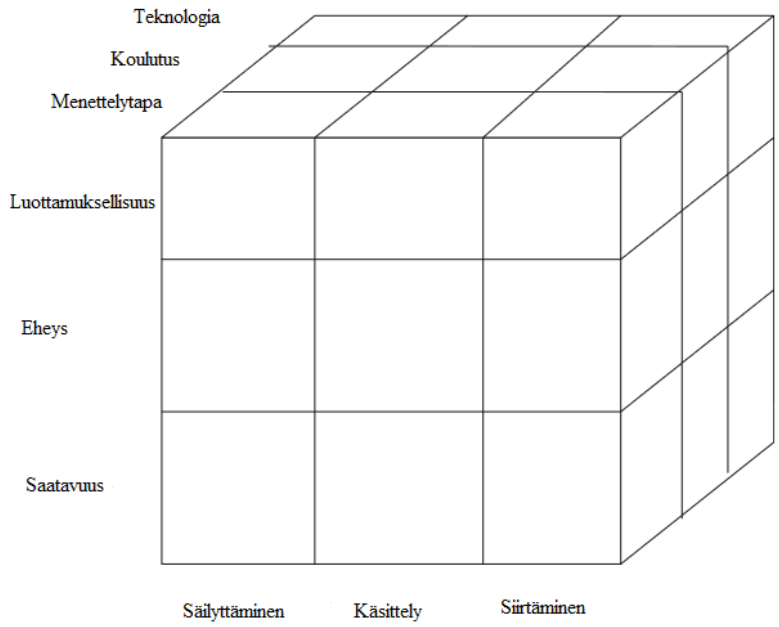
Kuvio 3 PDCA-sykli jatkuvuuden hallinnan kehittäminen (Iivari & Laaksonen, 2009)

Jatkuvuuden hallinnan kehittämisessä tulee huomioida suunnitelmien ajantasaisuus, josta syystä muutokset toimintaympäristössä, riskeissä ja prosesseissa tulisi viedä aina saatavilla oleviin jatkuvuussuunnitelmiin (Botha & Von Solms, 2004; Niemimaa & Järveläinen, 2013). Jatkuvuuden hallintaan liittyvien toimenpiteiden ja suunnitelmien ajantasaisena pitämiseksi organisaatiossa voidaan hyödyntää esimerkiksi ns. vuosikelloa, johon voidaan ajoittaa organisaatiolle sopiviin ajankohtiin jatkuvuuden hallintaan liittyvät ylläpito- ja kehittämistoimenpiteet (Valtionvarainministeriö, 2016).

2.2 Tietoturvallisuus

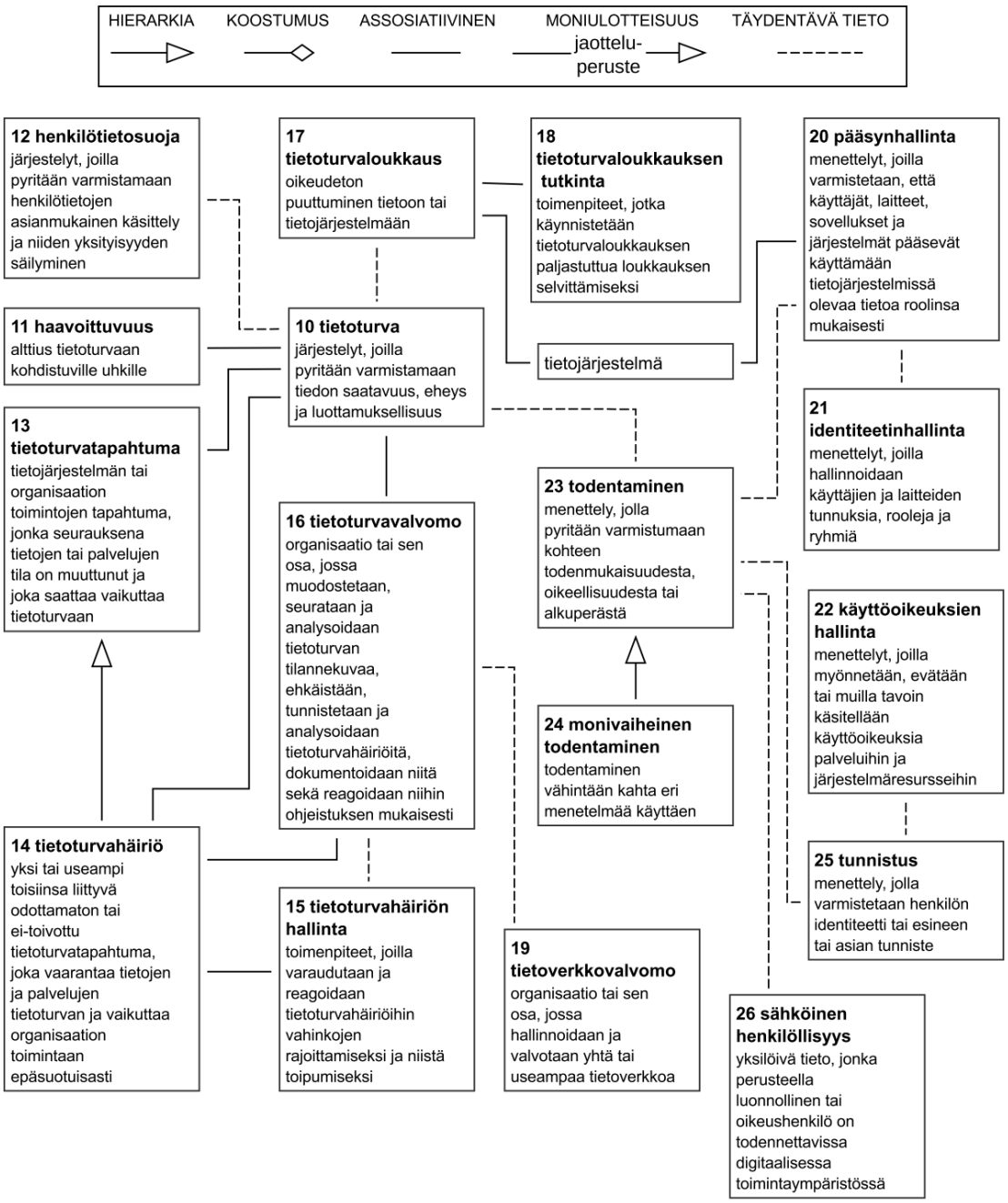
Tässä aliluvussa käsitellään tietoturvallisuutta digitaalisen turvallisuuden osa-alueena. Tietoturvallisuus-käsitteeseen ovat perinteisesti liittyneet kiinteänä osana kyberturvallisuuden ja tietosuojan osa-alueet, jotka käsitellään tässä tutkimuksessa omissa aliluvuissaan.

Jennex ja Zyngier (2007) kuvasivat julkaisussaan kuvion 4 mukaisesti tiedon hallinnan turvallisuuden periaatteet "tietoturvakuutiona". Kuvauksen malli perustuu vuonna 1994 julkaistuun National Security Telecommunications and Information Systems Security Committee -esitykseen. Samat periaatteet soveltuvat tietoturvallisuuden periaatteiden kuvaamiseen vielä nykyäänkin. Tietoturvallisuuden periaatteet muodostuvat tiedon luottamuksellisuudesta, eheydestä ja saatavuudesta. Kuvauksessa on huomioitu myös tietoturvallisuuteen liittyvät hallintakeinot sekä tiedon prosessoinnin eri vaiheet, joissa tiedolle asetetut turvallisuusvaatimukset tulee huomioida (Jennex & Zyngier, 2007).



Kuvio 4 Tiedon hallinnan turvallisuus (Jennex & Zyngier, 2007, s. 498)

Tietoturvalla tarkoitetaan sanastokeskuksen (2018) tietoturvan käsitekaavion (kuvio 5) mukaan: *järjestelyjä, joiden avulla tiedon saatavuus, eheys ja luottamuksellisuus pyritään varmistamaan* (Sanastokeskus TSK, 2018).



Kuvio 5 Tietoturva-käsitekaavio (Sanastokeskus TSK, 2018, s. 20)

2.2.1 **Tietoturvanhallinta**

Tietoturvallisuus ja digitaalinen toimintaympäristö ovat nykyään vahvasti liitoksissa organisaation kaikkiin toimintoihin. Tästä syystä tietoturvanhallinta koskettaakin organisaation kaikkia työntekijöitä ja vastuu siitä pitäisi olla organisaation johdolla (Soomro, Shah, & Ahmed, 2016). Tietoturvan- ja digiturvanhallinnan tulee perustua digitaalisen toimintaympäristön määrittämiseen ja ymmärtämiseen, tietoturvallisuudelle asetettuihin vaatimuksiin sekä riskienhallinnan analyyseihin (kts. luku 3), joiden perusteella

organisaatiolle tärkeimmät resurssit voidaan turvata riittävin hallintakeinoin (Humphreys, 2008; International Organization for Standardization, 2013a; International Organization for Standardization, 2013c).

Tietoturvanhallintaan hyödynnetään organisaatioissa lisääntyvässä määrin tietoturvallisuuden hallintajärjestelmiä. Tietoturvallisuuden hallinta-järjestelmällä pyritään varmistamaan sen sisältämien resurssien tietoturvallisuus hyödyntämällä riskiarviointiin perustuvia riittäviä hallintakeinoja (Humphreys, 2008). Tietoturvallisuuden hallintajärjestelmän käyttöönotossa tulee huomioida muun muassa ylimmän johdon sitoutuminen sen kehittämiseen ja hyödyntämiseen, ylimmän johdon laatimat organisaation toimintaa ja tietoturvallisuuden hallintajärjestelmää tukevat tietoturvapoliitikat sekä tietoturvaan liittyvien roolien, vastuiden ja valtuuksien määrittäminen. Käyttöönotettavan järjestelmän suunnittelun tulee perustua riskienhallinnan prosessin tuottamiin riskianalyysin tuloksiin ja tietoturvallisuudelle asetettuihin tavoitteisiin (International Organization for Standardization, 2013a).

Tietoturvallisuuden hallintajärjestelmä ei yksistään riitä takaamaan organisaation riittävää tietoturvallisuuden tasoa. Teknologisien ratkaisujen lisäksi organisaation tietoturvanhallinnassa täytyisikin huomioida myös organisaatiolliset ja henkilöstöön liittyvät tekijät (Nazareth & Choi, 2015; Soomro ym., 2016).

2.2.2 **Pääsynhallinta**

Pääsynhallinta tarkoittaa sanastokeskuksen (2018) mukaan: *menettelyt, joilla varmistetaan, että käyttäjät, laitteet, sovellukset ja järjestelmät pääsevät käyttämään tietojärjestelmissä olevaa tietoa roolinsa mukaan*. Pääsynhallinnalla pyritään varmistamaan, että digitaalisten resurssien hyödyntäminen tapahtuu määritettyjen oikeuksien ja valtuutuksien mukaisesti. Pääsynhallinta voidaan jakaa tunnistuksen, todentamisen, valtuutuksen varmentamisen ja pääsyn myöntämisen tai estämisen vaiheisiin. Pääsynhallintaan sisältyvät myös pääsynhallinnan seurannan ja kirjautumisyritysten tallentamisen vaiheet. Pääsynhallinnan hallintakeinoiksi lukeutuvat teknisten hallintakeinojen lisäksi myös esimerkiksi fyysiset hallintakeinot. Fyysisillä hallintakeinoilla voidaan mm. rajoittaa tai estää fyysisesti resursseihin pääsyä (Chapple, Steward, & Gibson, 2018). Pääsynhallinnan keinoilla voidaan vaikuttaa myös digitaalisien resurssien luottamuksellisuuden, eheyden ja saatavuuden säilymiseen. Lisäksi pääsynhallinnalla voidaan tukea tietoturvaperiaatteiden, kuten esim. vähimpien oikeuksien periaatetta (Grance, Stevens, & Myers, 2003). Pääsynhallinta tietojärjestelmiin voidaan organisaatiossa toteuttaa usealla eri tavalla. Roolipohjaista pääsynhallintaa hyödynnetään yhä useammissa organisaatioissa näinä päivinä. Rooleihin pohjautuvassa pääsynhallinnassa käyttöoikeudet ja resursseihin pääsy määritetään työtehtävien eli työroolien perusteella. Roolipohjainen pääsynhallinta yksinkertaistaa organisaation käyttöoikeuksien hallintaa, poistamalla tarpeen käyttäjäkohtaisista oikeuksien määrittelyistä (National Institute of Standards and Technology, 2013).

Identiteetinhallinnalla tarkoitetaan sanastokeskuksen (2018) mukaan: *menettelyt, joilla hallinnoidaan käyttäjien ja laitteiden tunnuksia, rooleja ja ryhmiä*. Identiteetinhallinnan periaatteena on, että yhdellä käyttäjällä on yksi identiteetti, johon häneen liittyvät roolit ja ryhmät liitetään. Identiteetinhallinnan menettelyillä pyritään helpottamaan organisaation pääsynhallintaa ja digitaalisiin resursseihin liittyvien käyttäjäoikeuksien hallintaa. Useissa organisaatioissa onkin identiteetinhallinta ja pääsynhallinta yhdistetty identiteetin ja pääsynhallinnan kokonaisuudeksi, jota hallinnoidaan sitä varten käyttöönotetulla hallintajärjestelmällä (Thakur & Gaikwad, 2015).

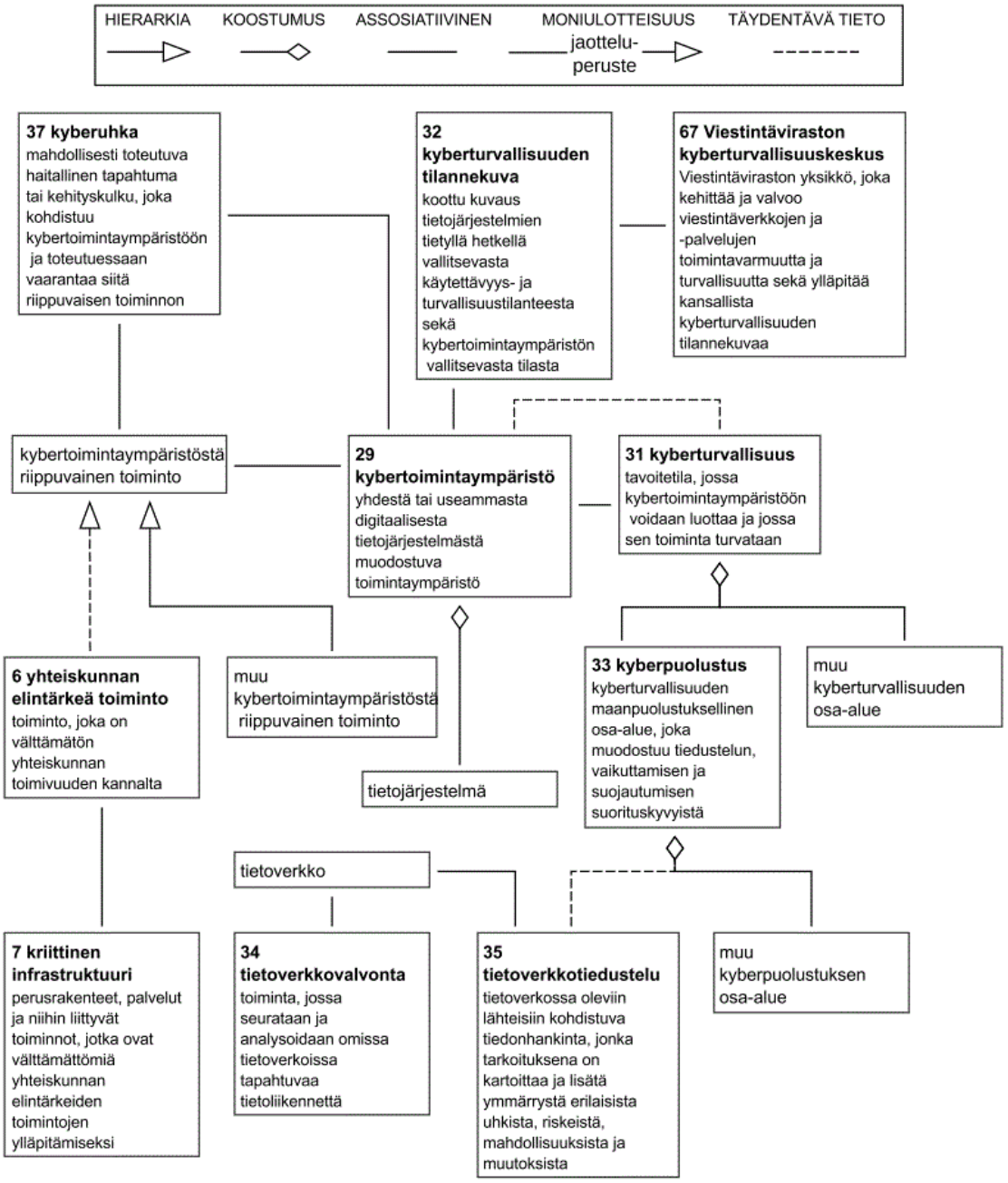
2.2.3 **Tietoturvan valvonta**

Tietoturvan ja kyberturvan valvonnan tavoitteena on organisaation digitaalisen toimintaympäristön turvallisuuden varmistaminen. Toimintaympäristön valvonnalla pyritään tarkkailemaan ja analysoimaan uhkia ja tietoturvahäiriöitä, aktiivisesti suojautumaan uhkia vastaan sekä hallitsemaan ja toipumaan tietoturvahäiriöistä (Kowtha, Nolan, & Daley, 2012). Tietoturvan ja kyberturvan valvontaa varten organisaatioihin on perustettu tietoturvavalvomoita, joissa digitaalisen toimintaympäristön valvontaa voidaan suorittaa keskitetysti asianmukaisin valvontajärjestelmin. Tietoturvavalvomoissa hyödynnetään eri lähteistä kerättyä tietoverkkoon ja tietojärjestelmiin liittyvää sensori- ja lokitietoa, joita analysoimalla pyritään havaitsemaan tietoturvaan liittyviä poikkeamia esim. SIEM-järjestelmien avulla (Bhatt, Manadhata, & Zomlot, 2014). Digitaalisen toimintaympäristön valvonnalla pidetään organisaatioissa yllä myös tietoturvaan liittyvää ajantasaista tilannekuvaa. Tietoturvavalvomoiden välisellä yhteistyöllä ja tilannekuvan koordinaatiolla voidaan uhkatietoa jakaa organisaatioiden kesken sekä helpottaa kansallisen tilannekuvan ylläpitoa (Kowtha ym., 2012).

Tietoturvatapahtuman määritelmä on sanastokeskuksen (2018) mukaan: *tietojärjestelmän tai organisaation toimintojen tapahtuma, jonka seurauksena tietojen tai palvelujen tila on muuttunut ja joka saattaa vaikuttaa tietoturvaan*. Tietoturvatapahtuman määritelmän mukaan tietoturvatapahtuma voi aiheutua organisaation sisäisestä tai ulkoisesta tietoturvahäiriöstä tai muusta organisaation palvelun tilaan vaikuttavasta tekijästä, joka saattaa vaikuttaa tietoturvaan. Tietoturvatapahtuma voi siis olla esimerkiksi tietoturvahäiriö tai jokin muu tapahtuma, jolla voi olla vaikutusta organisaation tietoturvan tilaan. Tietoturvatapahtumat käsitellään organisaatiossa yleensä tietoturvaryhmän tai tietoturvavalvomon toimesta (Gabriel, Hoppe, Pastwa, & Sowa, 2009).

2.3 Kyberturvallisuus

Kyberturvallisuus digitaalisen turvallisuuden osa-alueena tarkoittaa sanastokeskuksen mukaan *tavoitetilaa, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan* (Sanastokeskus TSK, 2018). Kyberturvallisuudella pyritäänkin digitaalisen tietoturvan lisäksi turvaamaan myös kybertoimintaympäristö sekä siihen liittyvät fyysisen maailman toiminnot. Kyberturvallisuuden käsitekaavio (kuvio 6) tarjoaa kattavan kokonaiskuvan kyberturvallisuuden eri osa-alueista, joista kyberturvallisuuden toimintaympäristö muodostuu (Sanastokeskus TSK, 2018).



Kuvio 6 Kyberturvallisuuden käsitekaavio (Sanastokeskus TSK, 2018, s. 24)

Kyberturvallisuuteen liittyvä kybertoimintaympäristö muodostuu toiminnoista, joihin hyödynnetään tietojärjestelmiä ja tiedonsiirron mahdollistavaa tietoverkkoa. Kybertoimintaympäristön turvallisuutta pyritään ylläpitämään seuraamalla sen tilaa aktiivisesti ja tarvittaessa reagoimaan siihen kohdistuviin uhkiin ja haavoittuvuuksiin.

Kriittinen infrastruktuuri ja useat muut yhteiskunnan kannalta tärkeät toiminnot ovat nykyään pääosin yhteydessä tietoverkkoon ja ovat täten riippuvaisia kybertoimintaympäristöstä sekä alttiita kybertoimintaympäristöön kohdistuville riskeille. Kybertoimintaympäristön kannalta onkin tärkeää tiedostaa siihen kohdistuvat uhkatekijät sekä seurata sen tilaa riittävillä toimenpiteillä. Tässä aliluvussa käsitellään kyberturvallisuuteen liittyviä osa-alueita.

2.3.1 **Tietoverkkoturvallisuus**

Tietoverkkoturvallisuus kyberturvallisuuden osana sisältää erilaisia toimenpiteitä, joilla pyritään lisäämään tietoverkkojen luotettavuutta ja toimintavarmuutta. Tietoverkkoturvallisuuden tavoitteina ovat mm. tietoverkon laillisen käytön turvaaminen sekä tietoverkon laittoman hyödyntämisen estäminen (Hoque, Bhuyan, Baishya, Bhattacharyya, & Kalita, 2014).

Tietoverkkoturvallisuuden takaamiseksi tietoverkon suunnittelussa tulisi huomioida turvallisuusperiaatteiden lisäksi tietoverkkoon liittyvien riskianalyysien tulokset. Tietoverkon suunnittelussa huomioitavia turvallisuusperiaatteita ovat mm. syvyyssuuntainen turvallisuussuunnittelu, verkon segmentointi ja resurssien sijoittaminen luottamuksellisuuden mukaisesti, pienimmän valtuuden periaate, verkon vikasietoisuuden varmistaminen, tehtävien eriyttäminen, tunkeutumisen estäminen ja havainnointi sekä muut tietoverkkoarkkitehtuuriin liittyvät turvallisuusperiaatteet. (Stawowski, 2009).

Tietoverkkoturvallisuuden kehittämisessä hyödynnetään muun muassa tietoverkkotiedustelua, jonka avulla kartoitetaan ja analysoidaan suojattavaa tietoverkkoa sekä pyritään lisäämään organisaation tietämystä verkkoa mahdollisesti uhkaavista tekijöistä ja olemassa olevista riskitekijöistä. Tietoverkkotiedustelussa hyödynnetään osittain samoja ohjelmistotyökaluja, joita käytetään myös tietoverkkohyökkäyksien tiedusteluvaiheessa. (Hoque ym., 2014).

Tietoverkkovalvonnalla seurataan ja analysoidaan omissa tietoverkoissa tapahtuvaa tietoliikennettä. Tietoverkkovalvonnan tavoitteena on varmistaa tietoverkon turvallisuus sekä havainnoida mahdolliset tunkeutumisyritykset. Tietoverkon ja –järjestelmien turvallisuuden valvontaan on tarjolla useita erilaisia hallintajärjestelmiä, jotka helpottavat tietoliikenteen ja tunkeutumisyritysten havainnointia ja analysointia. (Bryant & Saiedian, 2020).

2.3.2 **Tietojärjestelmäturvallisuus**

Organisaatioiden ydintoiminnot ovat nykyään voimakkaasti sidoksissa organisaatiossa hyödynnettäviin tietojärjestelmiin. Tästä syystä

tietojärjestelmien turvallisuus ja toimintavarmuus ovat organisaation toiminnan kannalta tärkeitä. Tietojärjestelmien turvallisuuden hallintaan liittyviin käytäntöihin kuuluvat Kankanhalli ym. (2003) mukaan ulkoiset turvallisuustoiminnot, joita ovat fyysinen, henkilöstö- ja hallinnollinen turvallisuus sekä sisäiset turvallisuustoiminnot, joihin kuuluvat laitteisto- ja ohjelmistoturvallisuus. Kyseiset k äytännöt voidaan tietojärjestelmäturvallisuudessa jakaa myös hallintakeinojen mukaisesti hallinnollisiin, teknisiin ja fyysisiin hallintakeinoihin (D'Arcy & Herath, 2011).

Hallinnolliset hallintakeinot tietojärjestelmäturvallisuudessa sisältävät muun muassa tietoturvallisuuspolitiikat, ohjeistukset, opastukset ja henkilöstökoulutukset sekä henkilöstöturvallisuuden. Tietoturvapolitiikoilla määritellään organisaation tietoturvallisuuden tavoitteet ja periaatteet. Niillä ohjataan myös kaikkea organisaation tietoturvallisuuteen liittyvää toimintaa (International Organization for Standardization, 2013b). Tietoturvapolitiikat ovatkin eräänlainen lausunto työntekijöiden velvollisuuksista ja rooleista liittyen tieto- ja teknologiaresurssien turvaamiseen (Bulgurcu, Cavusoglu, & Benbasat, 2010). Tietoturvapoliitiikkoihin ja –sääntöihin voidaan myös pelotteena toimivana hallintakeinona sisällyttää sanktioita kielletynlaisesta toiminnasta (Kankanhalli, Teo, Tan, & Wei, 2003). Tietoturvapolitiikkojen lisäksi ohjeistuksilla ja henkilöstökoulutuksilla voidaan vaikuttaa henkilöstön ja muiden kohderyhmien tietoturvallisuuteen liittyvään käyttäytymiseen ja tietoisuuteen. Henkilöstöturvallisuuteen liittyviä muita toimenpiteitä organisaatiossa ovat mm. henkilöstön luotettavuuden tarkastus sekä tietoturvavastuiden määrittely työhön liittyen (International Organization for Standardization, 2013b).

Tietojärjestelmäturvallisuuteen liittyvät tekniset hallintakeinot voidaan jakaa laitteisto- ja ohjelmistoturvallisuuteen. Laitteisto- ja ohjelmistoturvallisuuden toimenpiteillä pyritään estämään tietojärjestelmien luvaton käyttö ja tietoaineistojen luvaton hyödyntäminen (Kankanhalli ym., 2003). Turvallisen ohjelmiston tai järjestelmän kehittämisessä on huomioitava turvallisuusvaatimukset ohjelmiston määrittelyvaiheesta asti. Ohjelmistolle asetetut turvallisuusvaatimukset perustuvat ohjelmistolle suoritettavaan riskiarviointiin. Riskiarvioinnissa pyritään tunnistamaan ja määrittämään kaikki ohjelmistoon tai järjestelmään mahdollisesti liittyvät uhkat ja haavoittuvuudet. Tunnistamisessa ja määrittämisessä hyödynnetään muun muassa uhkaprofiileja, hyökkäysmallinnuksia ja uhkalähteitä (Islam & Falcarin, 2011). Laitteistoturvallisuus käsittää tietojärjestelmien käytössä hyödynnettävien laitteistojen turvallisuuden. Laitteistoturvallisuuden varmistaminen on vaikeaa, johtuen muun muassa laitteissa hyödynnettävien mikropiirien pitkistä toimitusketjuista. Laitteistoihin kohdistuvia uhkia ovat esimerkiksi laitteistotroijalaiset, mikropiirien suunnitelmien väärinkäyttö ja väärennökset, takaisinmallinnukset ja sivukanava-analyysit (Rostami, Koushanfar, & Karri, 2014).

Fyysinen turvallisuus tietojärjestelmäturvallisuudessa käsittää laitteistojen ja tietojärjestelmien fyysisen suojaamisen tiloihin liittyvin hallintakeinoin.

Fyysisen suojaamisen hallintakeinoihin lukeutuvat muun muassa rakenteelliset suojaratkaisut, turvajärjestelmät ja –laitteet ja turvallisuuteen liittyvät menettelytavat. Fyysisien turvaratkaisujen valinnat perustuvat tietojärjestelmiin suoritettaviin riskiarviointeihin (Puolustusministeriö, 2015).

2.3.3 **Kriittinen infrastruktuuri**

Kriittisellä infrastruktuurilla tarkoitetaan palveluita ja perusrakenteita, jotka ovat yhteiskunnan kannalta välttämättömiä elintärkeiden toimintojen ylläpitämiseksi. Näihin perusrakenteisiin ja palveluihin lukeutuvat mm. energian tuotanto- ja siirtojärjestelmät, tieto- ja viestintäjärjestelmät, liikenne ja logistiikka sekä vesi- ja jätehuolto (Sanastokeskus TSK, 2018).

Kriittisen infrastruktuurin palvelut ovat nykyään pitkälle riippuvaisia toisistaan, ja riskienhallinnassa pitää huomioida luonnonkatastrofien ja muiden perinteisten riskitekijöiden lisäksi myös kyberturvallisuuteen liittyvät tekijät. Kyberhyökkäyksillä on mahdollista vaikuttaa tietoverkossa oleviin kriittisen infrastruktuurin palveluihin. Kyberhyökkäyksien aiheuttamia vaikutuksia kriittiseen infrastruktuuriin tulisi pienentää rakentamalla resilienssiä lisääviä mekanismeja palveluihin (Hayel & Quanyan Zhu, 2015).

Suomessa kyberturvallisuuskeskus tarjoaa kyberturvallisuuteen liittyvää tilannetietoa ja tietoturvaloukkausten havainnointiin liittyvää palvelua huoltovarmuuskriittisille palveluntuottajille toimialakohtaisesti.

2.3.4 **Kyberturvallisuuden tilannekuva**

Kyberturvallisuuden tilannekuvaa tulisi organisaatioissa seurata aktiivisesti. Sen luomisessa hyödynnetään kaikkea saatavilla olevaa olennaista tietoa, jota havainnoimalla, tulkitsemalla ja yhdistelemällä muodostetaan ajantasainen tilannekuva organisaation kyberturvallisuudesta (Franke & Brynielsson, 2014).

Suomessa kyberturvallisuuden tilannekuvaa ylläpitää kansallisella tasolla Liikenne- ja viestintäviraston kyberturvallisuuskeskus. Kyberturvallisuuskeskus tarjoaa ajantasaista tilannekuvaa kyberturvallisuuteen vaikuttavista tapahtumista ja ilmiöistä sitä tarvitseville (Franke & Brynielsson, 2014) ja siitä kiinnostuneille organisaatioille ja kansalaisille. Kyberturvallisuuskeskuksen lisäksi useat julkiseen hallintoon kuuluvat organisaatiot ylläpitävät tilannekuvaa oman organisaationsa tarpeista lähtien (Valtiovarainministeriö, 2020c).

2.3.5 **Kyberpuolustus**

Kyberpuolustuksen kokonaisuudesta Suomessa vastaa puolustusvoimat. Kyberpuolustuksella tarkoitetaan valtiovarainministeriön julkaisuja 2020:23 (2020) mukaan: *kansallisen kyberturvallisuuden maanpuolustuksellista osa-aluetta, joka muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä.*

Kyberpuolustus tuottaa myös tarvittavaa tilannetietoa puolustusvoimien ja valtionjohdon päätöksenteon tueksi (Valtiovarainministeriö, 2020c).

2.3.6 **Kyberturvallisuuden hallinta**

Kyberturvallisuuden hallinnassa tulee huomioida organisaation digitaaliseen toimintaympäristöön kohdistuvat riskit ja toimintaympäristölle asetetut vaatimukset. Kyberturvallisuuden kypsyysasteen arvioimiseen ja kehittämiseen on National Institute of Standards and Technology (2018) julkaissut viitekehyksen, jota organisaatiot voivat hyödyntää kyberturvallisuuden kypsyysasteen arvioinnissa ja kehittämisessä. Viitekehys koostuu viidestä ydintoiminnosta, jotka ovat toimintaympäristön tunnistaminen ja suojaaminen ja havainnointi-, toiminta- ja palautumiskyky kybertapahtumien yhteydessä. Viitekehykseen sisällytettyjen tasojen perusteella voidaan organisaatioissa myös arvioida kyberturvallisuuden riskienhallinnan kypsyysastetta. Kyberturvallisuuden riskienhallinnan kypsyysaste viitekehyksessä muodostuu riskienhallintaan liittyvien prosessien, riskienhallinnan ohjelman ja riskienhallinnan ulkoisten osallistujien huomioimisen kypsyyden mukaan (National Institute of Standards and Technology, 2018a).

2.4 Tietosuoja

Tietosuojan käsite on vuosien varrella muuttunut. Tietosuoja käsitteenä sisältyy yksityisyyden suojan käsitteen osa-alueeksi, joka useimmiten tulkitaan ihmisoikeudeksi. Tietosuojan tärkeys ja merkitys ovat kasvaneet kommunikoinnin ja tietojen digitalisoituessa kiihtyvällä tahdilla (Bélanger & Crossler, 2011). Tässä aliluvussa tietosuojaa käsitellään digitaalisen turvallisuuden osa-alueena. Digitaalisen turvallisuuden osana tietosuojalla tarkoitetaan henkilötietosuojaa. Henkilötietosuoja määritetään sanastokeskuksen (liite 1) mukaan: *järjestelyiksi, joilla pyritään varmistamaan henkilötietojen asianmukainen käsittely ja niiden yksityisyyden säilyminen* (Sanastokeskus TSK, 2020).

2.4.1 Henkilötieto

Henkilötieto on sanastokeskuksen määrityksen mukaan: *tieto, joka kuvaa luonnollista henkilöä, hänen ominaisuuksiaan tai elinolosuhteitaan ja joka voidaan yhdistää häntä, hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskevaksi* (Sanastokeskus TSK, 2020). Henkilötieto muodostuu siis tiedosta, joka liittyy suoraan luonnollisen henkilön ominaisuuksiin, käyttäytymiseen, kommunikointiin ja muuhun henkilökohtaiseen tietoon. Näihin henkilökohtaisiin tietoihin lukeutuvat mm. terveystieto, biometrinen tieto, geneettinen tieto, arkaluonteiset henkilötiedot ja muut henkilötiedot (Sanastokeskus TSK, 2020; Bélanger & Crossler, 2011). Henkilötieto on lähtökohtaisesti salassa pidettävää tietoa.

2.4.2 Henkilörekisterit ja henkilötietojen käsittely

Henkilörekisterien muodostumista, ylläpitoa ja henkilötietojen käsittelyä sekä niihin liittyviä velvollisuuksia säätelee Euroopan laajuisesti EU:n tietosuoja-asetus (Euroopan parlamentti ja neuvosto, 2016). Lisäksi Suomessa on säädetty tietosuojalaki, jolla täsmennetään tietosuoja-asetuksen kansallista soveltamista (Oikeusministeriö, 2018).

Henkilörekistereillä tarkoitetaan tietojoukkoa, johon on koottu ja järjestetty henkilötietoja määritettyä käyttötarkoitusta varten. Henkilörekisterin pitäjän täytyy laatia henkilörekisteriin liittyvä rekisteriseloste, joka sisältää tiedot rekisterinpitäjästä, rekisteröidyistä ja siitä, mitä henkilötietoja rekisterissä on sekä mihin niitä käytetään ja minne tietoja luovutetaan. Rekisteriselosteesta täytyy myös ilmetä, miten rekisterin tiedot on suojattu (Sanastokeskus TSK, 2020).

Henkilötietojen käsittelylle on EU:n tietosuoja-asetuksessa asetettu lainmukaisuuden, asianmukaisuuden ja läpinäkyvyyden vaatimukset. Tiedot on kerättävä tiettyä, laillista tarkoitusta varten, ja niiden on oltava asianmukaisia, olennaisia ja rajoitettuja tiedon tarpeellisuuteen rajautuen. Lisäksi kerättyjen henkilötietojen on oltava täsmällisiä ja niitä on säilytettävä ainoastaan välttämätön aika

muodossa, josta rekisteröidyn tunnistaa. Henkilötietojen käsittelyssä on varmistettava tiedon turvallisuuden säilyminen asianmukaisin hallintakeinoin (Euroopan parlamentti ja neuvosto, 2016).

Henkilötietojen käsittelyyn on rekisteröidyltä saatava suostumus, johon rekisterinpitäjällä on osoitusvelvollisuus. Rekisteröidyllä on myös oikeus peruuttaa suostumuksensa yhtä helpolla tavalla, kuin suostumuksen antaminen on ollut. Tietosuoja-asetuksessa on huomioitu erikseen, tarkemmin säännöin mm. lapsien ja erityisien henkilötietoryhmien esim. geneettisiin ja biometrisiin henkilötietoihin kohdistuva käsittely (Euroopan parlamentti ja neuvosto, 2016).

2.4.3 **Henkilötietosuoja**

Henkilötietoihin liittyvät rekisteröidyn oikeudet ja organisaatioiden halu hyödyntää tietoja ovat usein ristiriidassa. Esimerkiksi elektronisessa kaupankäynnissä kuluttaja toivoo tietoja hyödynnettävän ainoastaan ostotapahtumassa, kun myyntiyritys haluaisi hyödyntää asiakastietoja lisäarvon tuottamiseen (Bélanger & Crossler, 2011). Henkilötietosuojaan liittyvä lainsäädäntö ja sen noudattamisen valvominen ovat tärkeitä asioita rekisteröidyn oikeuksien takaamiseksi. Tietosuoja-asetuksen voimaan astuessa julkishallinnon organisaatioilta sekä organisaatioilta, joissa käsitellään laajamittaisesti henkilötietoja, on vaadittu tietosuojavastaavan nimittämistä. Tietosuojavastaavan tehtävänä organisaatiossa on huolehtia tietosuojan alaisten henkilötietojen käsittelyn asianmukaisuudesta ja lainmukaisuudesta (Euroopan parlamentti ja neuvosto, 2016). Tietosuojaa kansallisella tasolla EU:ssa valvoo tietosuojaviranomainen, joka Suomessa on tietosuojavaltuutettu. Tietosuojavaltuutetun toimisto tarjoaa valvonnan lisäksi myös muita tietosuojaan liittyviä ohjeistuksia ja ohjausta Suomessa asuville henkilöille ja organisaatioille (Tietosuojavaltuutetun toimisto, 2010).

3 RISKIENHALLINTA DIGITAALISESSA TURVALLISUUDESSA

Tässä luvussa käsitellään riskienhallintaa digitaalisen turvallisuuden viitekehyksessä. Digitaalisen turvallisuuden riskien hallinnan teoreettista kokonaisuutta lähestytään tässä tutkimuksessa yhdistämällä digitaalisen turvallisuuden näkökulma organisaation riskien hallintaan sekä muihin digitaalisen turvallisuuden riskien hallinnan osa-alueisiin. Julkisen hallinnon, johon myös kuntasektori lukeutuu, digitaalista turvallisuutta ohjataan muun muassa lainsäädännöllä. Digitaalisen turvallisuuden riskienhallinnan teoreettisen viitekehyksen muodostamisessa hyödynnetään tässä tutkimuksessa tutkimusartikkeleiden lisäksi International Organization for Standardization standardeja, National Institute of Standards and Technology:n riskienhallintaan liittyviä ohjeistuksia sekä muuta kirjallisuuden tarjoamaa tietoa.

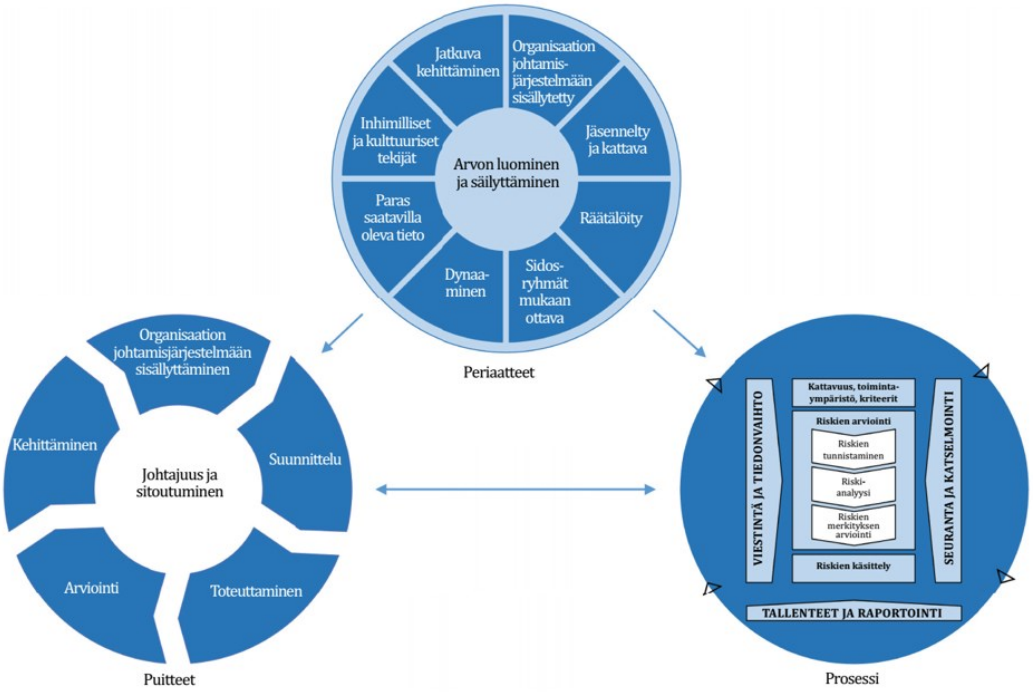
3.1 Organisaation riskienhallinta

Riski-sanan alkuperästä ei ole kielitieteessä toistaiseksi päästy yksimielisyyteen. Sanan alkuperänä on joko arabiankielinen sana risq tai latinankielinen sana riscum, joilla on varsin erilaiset merkitykset. Arabiankielinen sana risq viittaa annettuun mahdollisuuteen tehdä voittoa, kun taas latinankielisen sanan riscum alkuperä viittaa vaaraan. Eurooppalaisessa kulttuurissa riski-sanaan yhdistetäänkin sekä positiivisia että negatiivisia merkitysvivahteita. Riski-sanan määritelmään liitetään niin taloudellisessa kuin myös tieteellisessä yhteisössä käsitteet todennäköisyys sekä vaikutus lopputulokseen. Riskin kaavana käytetäänkin yleisesti *Riski = todennäköisyys x vaikutus lopputulokseen* (Walker, 2013).

Nykyaikaisen organisaation riskienhallinnan katsotaan alkaneen vuoden 1955 jälkeen. Riskienhallinnan painopisteet organisaatioissa ja yrityksissä ovat muuttuneet vuosien kuluessa huomattavasti kehittyessään kohti tämänhetkistä riskienhallintaa. Nykyisen riskienhallinnan tavoitteena organisaatiossa on luoda viitekehys, joka mahdollistaa organisaation käsitellä siihen kohdistuvia riskejä ja epävarmuuksia (Dionne, 2013).

Organisaatioiden tietojen sekä toiminnan prosessien muuttuessa digitaalisiksi on digitaalisesta turvallisuudesta tullut organisaatioille entistä tärkeämpää. Digitaaliseen turvallisuuteen kohdistuvien riskitekijöiden lisääntyminen ja vaikutusten voimistuminen organisaatioiden toimintaa kohtaan on lisännyt digitaalisen turvallisuuden tärkeyttä myös organisaatioiden hallinnon ja yleisen riskienhallinnan sisällä. Digitaaliseen turvallisuuteen pitäisikin kiinnittää enemmän huomiota myös organisaation johdon tasolta, eikä sitä pitäisi käsitellä ainoastaan teknologisena asiana (Fazlida & Said, 2015).

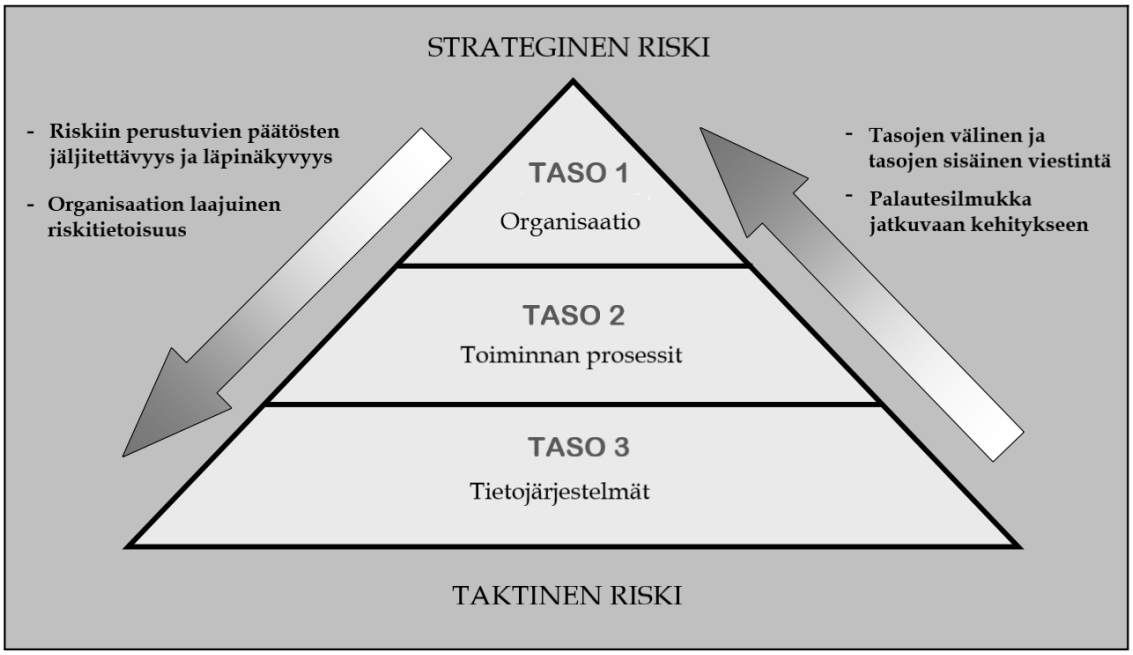
Organisaation digitaalisen turvallisuuden riskienhallinnan on oltava linjassa organisaation yleisen riskienhallinnan (kuvio 7) kanssa. Digitaalisen turvallisuuden riskienhallinnassa ja sen johtamisessa pitäisikin huomioida ISO/IEC 31000 -standardin mukaiset periaatteet ja puitteet, varsinaisen riskienhallinan prosessin lisäksi. Riskienhallinnan toimintamallia olisi sovellettava organisaation toimintamalliin sopivaksi, jolloin riskeihin voidaan reagoida nopeasti ja riittävällä tavalla. Systemaattista riskienhallintaa hyödynnetään digitaalisessa turvallisuudessa myös esimerkiksi tietoturvallisuuden hallintajärjestelmää luotaessa mm. tarpeiden tunnistamiseen. (International Organization for Standardization, 2013c).



Kuvio 7 Organisaation riskienhallinta: Periaatteet, puitteet ja prosessi (International Organization for Standardization, 2018)

Organisaation kattava digitaalisen turvallisuuden riskienhallinta vaatii koko organisaation (kuvio 8) laajuista osallistumista. Organisaation ylin johto määrittää strategisen näkemyksen ja riskienhallinnan ylätason tavoitteet organisaatiolle. Organisaation ylin johto myös vastaa riskienhallinnan kokonaisuudesta ja tekee päätökset mm. riskienhallinnan resursseista ja hyväksyttävistä riskitasoista. Organisaation keskijohto puolestaan suunnittelee ja johtaa riskienhallintaan liittyviä projekteja ja prosesseja. Keskijohto tekee riskienhallintaan liittyviä päätöksiä esim. organisaation kokonais- ja turvallisuusarkkitehtuureista, palveluiden toimittajista jne. Työntekijä ja asiantuntija –tason riskienhallintaan liittyvät vastuut ja toimenpiteet kohdistuvat pääasiallisesti järjestelmä- ja toiminnantasolle sekä organisaation turvallisuussääntöjen noudattamiseen. Organisaation riskienhallinta vaatii myös

aktiivista viestintää ja palautteen antoa organisaation eri tasojen sisällä sekä organisaation tasojen välillä (National Institute of Standards and Technology, 2012; National Institute of Standards and Technology, 2018).



Kuvio 8 Monitasoinen organisaation laajuinen riskienhallinta (National Institute of Standards and Technology, 2011)

3.2 Riskienhallinnan strategia

Organisaation riskienhallinnan strategia on suunnitelma, jolla pyritään takaamaan organisaation ydintoiminnan ja tavoitteiden saavuttaminen. Riskienhallinnan strategian laajuuteen vaikuttavat yleensä organisaation koko ja toimintaympäristö (Andress & Leary, 2017, 24).

Riskienhallinnan strategia ja strateginen toimintasuunnitelma kehitetään samalla tavalla kuin mikä tahansa muu organisaation toimintaan liittyvä prosessi. Riskienhallinnan strategian ja strategisen toimintasuunnitelman ohjaamana organisaation johto ja turvallisuudesta vastaavat henkilöt määrittävät organisaation riskienhallinnan tavoitteet ja suunnitelmat sekä vastuut niiden saavuttamiseksi. Riskienhallinnalle asetetut tavoitteet ja suunnitelmat ohjaavat organisaation henkilöstöä ja toimintaa asetettuja tavoitteita kohti (Andress & Leary, 2017, 25).

Riskienhallinnan strategisen toimintasuunnitelman kehittämisessä hyödynnetään organisaatioissa erilaisia metodeja. Yleisimmin käytettäviä metodeja ovat uhkaan perustuva ja kyvykkyyteen perustuva suunnittelu (Andress & Leary, 2017). Uhkaan perustuva suunnittelu pohjautuu puolustuksellisiin vastatoimenpiteisiin, joilla mahdollisiin ihmisen aiheuttamiin tai luonnollisiin uhkakyvykkyyksiin pyritään vastaamaan. Uhkaan perustuva suunnittelu pohjautuu

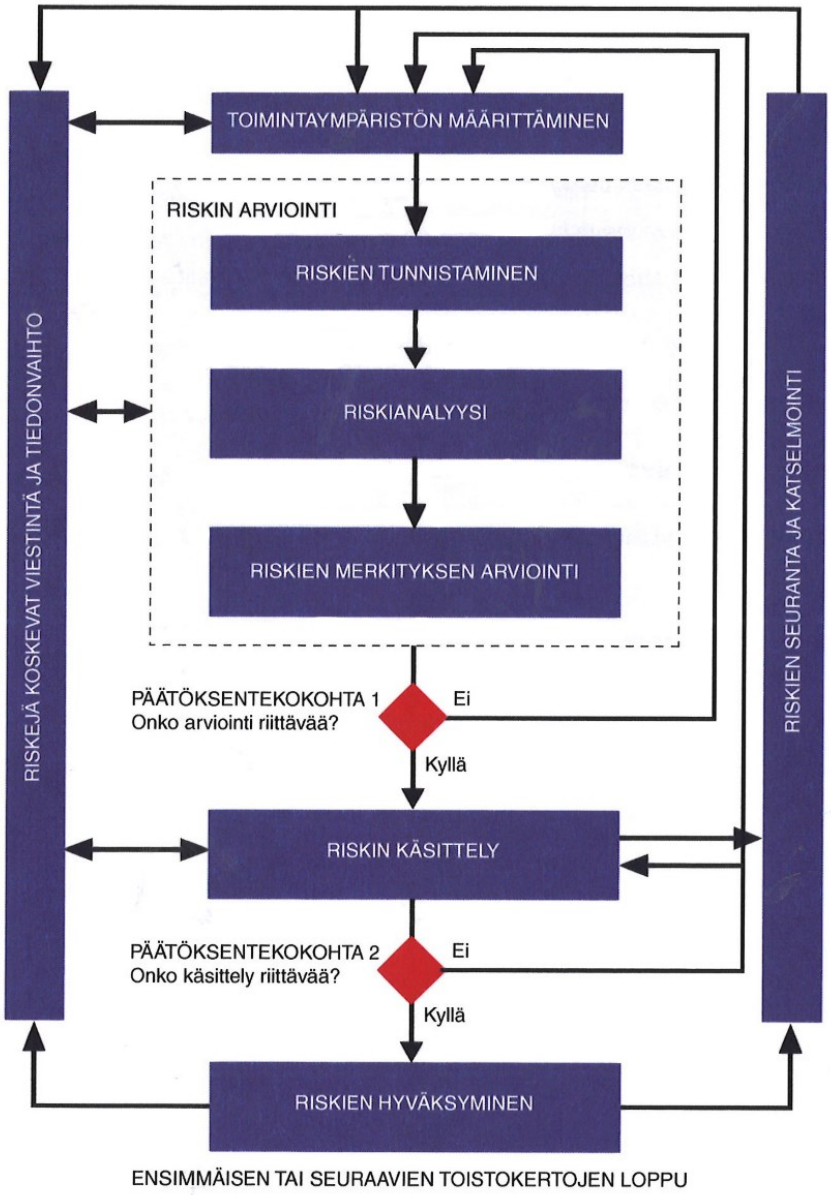
tietoturvallisuuteen liittyvässä suunnittelussa vahvasti Yhdysvaltain puolustusvoimien strategisen suunnittelun prosesseihin kylmän sodan jälkeiseltä ajalta (Andress & Leary, 2017). Tätä suunnittelumetodia on hyödynnetty myös esimerkiksi NIST:n sekä ISO/IEC:n standardeissa.

Digitaalisen turvallisuuden riskienhallinnan strategiasta päättää organisaation ylin johto. Digitaalisen turvallisuuden riskienhallinnan strategiaan kuuluvia päätöksiä ovat mm. linjaukset riskienhallinnan laajuudesta, tavoitteista, budjetista jne. ISO/IEC-standardit eivät varsinaisesti ota kantaa digitaalisen riskienhallinnan strategiaan, vaikka riskienhallinnan prosessi käsittääkin strategian määrittämiseen liittyvät elementit. NIST:n standardin mukaan digitaalisen riskienhallinnan strategia muodostetaan organisaatiotason valmisteluvaiheessa.

3.3 Riskienhallinnan prosessi

Riskienhallinnan prosessi (kuvio 9) on jatkuva, iteratiivinen prosessi, jossa organisaatioon kohdistuvia riskejä pyritään tunnistamaan, arvioimaan ja käsittelemään prosessissa määritellyssä sisäisessä ja ulkoisessa toimintaympäristössä. Riskejä käsitellään riskinkäsittelysuunnitelman mukaisesti niin, että riskit saadaan kustannustehokkaasti organisaation määrittämälle, hyväksyttävälle tasolle (International Organization for Standardization, 2013c).

Riskienhallinnan prosessin vaiheita ovat ISO/IEC-standardin mukaan toimintaympäristön määrittäminen, riskienarviointi, riskien käsittely, riskien hyväksyminen, riskien seuranta sekä viestintä ja tiedonvaihto riskeistä. Organisaation riskienhallinnan prosessi perustuu aina parhaaseen saatavilla olevaan tietoon sekä organisaation riskienhallinnalle asettamiin tavoitteisiin (International Organization for Standardization, 2013c).



Kuvio 9 Riskienhallinnan prosessi (International Organization for Standardization, 2013c, s. 22)

3.3.1 **Toimintaympäristön määrittäminen**

Riskienhallinnan toimintaympäristön määrittämisellä pyritään organisoimaan riskienhallinnan prosessia sekä määrittämään riskienhallinnan peruskriteerit ja riskienhallinnan rajat ja laajuus (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016). Riskienhallinnan toimintaympäristön määrityksessä huomioidaan sekä organisaation sisäinen että ulkoinen toimintaympäristö. Riskienhallinnan toimintaympäristön määrittämisen päämääränä organisaatiolla voi olla esimerkiksi turvallisuuden hallintajärjestelmän tukeminen, häiriöiden käsittelysuunnitelman tekeminen tai toiminnan jatkuvuussuunnitelman muodostaminen (International Organization for Standardization, 2013c).

Riskienhallinnan organisointiin kuuluvia toimia ovat mm. riskienhallintaan liittyvien vastuiden ja roolien määrittäminen, organisaation sidosryhmien tunnistaminen, analysointi ja tarvittavien suhteiden muodostaminen sekä riskienhallinnan prosessin kehittäminen. Riskienhallintaan liittyvien vastuiden ja roolien määrittämisessä on hyvä huomioida myös organisaation sidosryhmien ja ulkopuolisten tahojen vastuut ja roolit organisaatiolle sekä organisaatiota koskevat vaatimukset sidosryhmiä kohtaan (International Organization for Standardization, 2013c; International Organization for Standardization, 2013a). Organisaation rakenne, toiminta ja tehtävät vaikuttavat osaltaan riskienhallintaan liittyvien tehtävien ja roolien määrittämiseen. Mikäli yhdellä henkilöllä on useita riskienhallintaan liittyviä rooleja, täytyy huomioida, ettei roolien ja niihin liittyvien tehtävien välille muodostu eturistiriitoja (National Institute of Standards and Technology, 2018b).

Riskienhallinnan peruskriteerit muodostuvat ISO/IEC 27005-standardin mukaan riskien merkityksen arviointikriteereistä, vaikutuskriteereistä sekä riskien hyväksymiskriteereistä. Riskienhallinnan peruskriteereiden määrittämisellä organisaatio muodostaa itselleen soveltuvan toimintamallin riskienhallintaan.

Riskien merkityksen arviointikriteereillä arvioidaan riskien merkitystä organisaation ydintoiminnalle. Riskien merkityksen arviointikriteereitä laadittaessa tulisikin huomioida mm. ydintoimintaan liittyvien prosessien strateginen arvo, suojattavien kohteiden kriittisyys organisaatiolle, normien ja sopimusten vaatimukset ja velvoitteet sekä maineeseen mahdollisesti vaikuttavat negatiiviset seuraukset. Riskien merkityksen arviointikriteereitä voidaan hyödyntää myös riskien käsittelyn tärkeysjärjestyksen muodostamisessa (Shameli-Sendi ym., 2016).

Vaikutuskriteereitä laadittaessa organisaatiossa pyritään arvioimaan riskin toteutumisen vaikutuksia kustannuksien ja vahingon näkökulmasta. Vaikutukset voivat aiheuttaa joko suoraa rahallista arvon menetystä tai epäsuoraa arvon menetystä. Suoraa rahallista menetystä aiheuttavia vaikutuksia ovat esimerkiksi toimintaan liittyvät tappiot ja vahingoittuneet prosessit. Epäsuoraa menetystä organisaatiolle aiheuttaa esimerkiksi organisaation maineen vahingoittuminen tapahtuman seurauksesta (Shameli-Sendi ym., 2016).

Riskien hyväksymiskriteerit määrittävät merkittävältä osalta organisaation riskinottokykyä ja –halua. Riskien hyväksymiskriteerien muodostamisessa huomioidaan yleensä organisaation toiminta, tavoitteet ja periaatteet. Tietyillä toimialoilla riskien hyväksymiskriteerit ovat korkeammat, johtuen esimerkiksi lakien ja viranomaismääräysten vaikutuksesta. Riskien hyväksymiskriteereissä huomioidaankin yleensä mm. organisaation toiminnankriteerit, sosiaaliset ja inhimilliset tekijät, organisaation toiminnot jne. Riskien hyväksymiskriteereihin voidaan hyväksyä poikkeuksia organisaation johdon toimesta. Tällöin organisaatio voi hyväksyä normaalia korkeamman riskin tietyissä tilanteissa. Tällaisia tilanteita voivat olla esimerkiksi tilanteet, joissa riskin elinkaari on lyhyt tai joissa organisaatio hyötyy riskinotosta taloudellisesti (International Organization for Standardization, 2013c).

Riskienhallinnan laajuus ja rajat määritetään toimintaympäristön määrityksen yhteydessä. Organisaation täytyy huomioida useita eri tekijöitä riskienhallinnan laajuutta ja rajoja määritettäessä. Huomioitavia tekijöitä ovat mm. organisaation tehtävä ja rakenne, tietoturvapolitiikka, suojattavat kohteet, liiketoimintaprosessit, lakien ja muiden velvoitteiden vaatimukset organisaatiolle jne. Organisaatiosta täytyykin kerätä tarvittava tieto, jonka perusteella riskienhallinnan laajuus ja rajat voidaan määrittää. Riskienhallinnan laajuus voidaan myös rajata käsittämään osa organisaatiosta, kuten esimerkiksi organisaation tietotekninen infrastruktuuri. Rajausta tehtäessä organisaation on kuitenkin perusteltava rajauksen ulkopuolelle jätetyt asiat. (Fenz, Heurix, Neubauer, & Pechstein, 2014; International Organization for Standardization, 2013c.)

3.3.2 **Riskien arviointi**

Riskien arviointiin kuuluvia toimintoja ovat mm. riskien tunnistus, riskien määritys määrällisesti sekä riskien laadullinen kuvaus. Edellä mainittujen toimenpiteiden jälkeen riskien arvioinnissa asetetaan riskit tärkeysjärjestykseen organisaation tavoitteisiin perustuen, hyödyntäen riskien merkityksen arviointikriteerejä (International Organization for Standardization, 2013c). Riskiarviointi suoritetaan koko organisaation laajuudessa, ja arvioinnissa huomioidaan digitaalisen turvallisuuden kaikki osa-alueet (Fenz ym., 2014; National Institute of Standards and Technology, 2018b).

Riskien tunnistamisen tavoitteena on tunnistaa kaikki mahdolliset tapahtumat, jotka voivat aiheuttaa organisaatiolle haittaa tai tappiota. Määrityksen yhteydessä kerätään tietoa siitä, miten, missä ja miksi tapahtuma voisi aiheuttaa organisaatiolle haittaa tai tappiota. Riskien tunnistamisella pyritään kattamaan kaikki riskit, myös sellaiset, joita organisaatio ei hallitse tai joiden lähde on tuntematon (Shameli-Sendi ym., 2016; Fenz ym., 2014; International Organization for Standardization, 2013c). Riskien tunnistamiseen kuuluvat suojattavien kohteiden, uhkien, käytössä olevien hallintakeinojen, haavoittuvuuksien ja seurausten tunnistamisen osa-alueet.

Suojattavien kohteiden tunnistamisella pyritään määrittämään kaikki organisaation tavoitteita ja toimintaa tukevat kohteet, olivatpa ne aineellisia tai aineettomia. Aineellisiin kohteisiin kuuluvat mm. toimitilat, laitteet ja henkilökunta. Aineettomia kohteita ovat esimerkiksi digitaalisessa muodossa oleva tieto sekä yrityksen maine (Shameli-Sendi ym., 2016; Fenz ym., 2014; National Institute of Standards and Technology, 2018). Suojattavat kohteet on tunnistettava sillä tarkkuudella, että niihin kohdistuvia riskejä pystytään arvioimaan kerättyyn tietoon perustuen. Suojattaville kohteille kuuluisi määrittää myös omistajat, jotka osaltaan ovat vastuussa kohteen turvallisuudesta (International Organization for Standardization, 2013c).

Uhkien tunnistamisella pyritään kartoittamaan suojattavia kohteita mahdollisesti vahingoittavia tekijöitä. Uhkat voivat kohdistua niin aineellisiin kuin myös aineettomiin suojattaviin kohteisiin, kuten esimerkiksi tietoon,

prosessiin tai toimitilaan. Uhkan aiheuttajana voi olla ihminen, joko tahattomasti tai tahallisesti, tai uhka voi olla luonnollinen. Uhkat pyritään tunnistamaan yleisellä tasolla, ja ne luokitellaan tyypeittäin esimerkiksi tekniset viat ja luvattomat teot. Uhkien tunnistamisella kartoitetaan myös tarvittaessa kaikki yksittäiset uhkat, jolloin odottamattomia uhkia ei jää huomiotta. Uhkien tunnistamisessa kannattaa hyödyntää organisaation omaa henkilökuntaa, yhteistyöorganisaatioita sekä muita toimijoita, jotka voivat tarjota ajankohtaista uhkatietoa uhkien tunnistamiseen (Shameli-Sendi ym., 2016; International Organization for Standardization, 2013c).

Käytössä olevien hallintakeinojen tunnistuksella pyritään tunnistamaan organisaatiolla jo käytössä olevat hallintakeinot. Hallintakeinojen tunnistuksen yhteydessä olemassa olevien hallintakeinojen toimivuus tulisi testata, jolloin toimimattomat hallintakeinot voidaan poistaa käytöstä ja korvata toimivilla hallintakeinoilla. Hallintakeinojen tunnistuksella organisaation on mahdollista välttää moninkertaisten hallintakeinojen luomisesta aiheutuvaa turhaa työtä ja kustannuksia (Fenz ym., 2014). Tunnistettavat hallintakeinot voivat organisaatiosta riippuen olla esimerkiksi identiteetin hallintakeinoja, fyysiseen tai tilaturvallisuuteen liittyviä hallintakeinoja tai tietoturvallisuuteen liittyviä toimintaperiaatteita. Käytössä olevien hallintakeinojen tunnistuksessa kannattaa hyödyntää mm. organisaation jo dokumentoituja turvallisuuden hallintaprosesseja sekä muuta jo olemassa olevaa dokumentaatiota. Käytössä ja suunnitteilla olevat hallintakeinot tulisi dokumentoida omaksi luetteloksi, jolloin niiden uudelleen hyödyntäminen helpottuu (International Organization for Standardization, 2013c; National Institute of Standards and Technology, 2018).

Haavoittuvuuksien tunnistamisen päätarkoitus on kartoittaa organisaation toimintaympäristöön liittyviä haavoittuvuuksia, joita uhkat voisivat käyttää hyväkseen ja vahingoittaa suojattavia kohteita ja organisaatiota (Fenz ym., 2014; National Institute of Standards and Technology, 2012). Haavoittuvuuksia voidaan havaita organisaation eri riskienhallinnan tasoilta, ja ne voivat koskea esimerkiksi fyysistä ympäristöä, tietojärjestelmäkonfiguraatiota, prosessia tai riippuvuutta ulkoisista tahoista (Shameli-Sendi ym., 2016; International Organization for Standardization, 2013c). Haavoittuvuus itsessään ei aiheutta vahinkoa suojattavalle kohteelle, vaan vaatii aina haavoittuvuutta hyödyntävän uhkan toteutumisen vahingon aiheuttamiseen. Haavoittuvuus, johon uhkaa ei kohdistu, ei myöskään edellytä hallintakeinon käyttöä.

Seurausten tunnistamisessa arvioidaan mahdollisen tietoturvapoikkeaman aiheuttamia seurauksia, jotka kohdistuvat suojattavaan kohteeseen ja organisaatioon. Seuraukset aiheutuvat suojattavan kohteen käytettävyyden, eheyden tai luottamuksellisuuden menettämisestä ja voivat olla joko pysyviä tai tilapäisiä. Seurausten tunnistamisessa suojattaville kohteille pyritään määrittämään arvo, joka kuvaa kohteen taloudellista arvoa sekä toimintaan aiheutuvia seuraamuksia (Shameli-Sendi ym., 2016; Fenz ym., 2014). Seurausten tunnistamisen tarkastelussa hyödynnetään ennalta määritettyjä vaikutuskriteereitä, jotka määritetään toimintaympäristön määritys vaiheessa (International Organization for Standardization, 2013c).

3.3.3 **Riskianalyysi**

Riskianalyysin avulla pyritään määrittämään riskin toteutumisen todennäköisyyttä, riskin toteutuessa sen seurausten vakavuutta sekä turvakontrolleja lieventämään seurauksia (Syalim, Hori, & Sakurai, 2009). Riskianalyysissa hyödynnetään riskien tunnistamisvaiheen tuloksia tarkempien analyysien tekoon. Riskianalyysin yksityiskohtaisuus voi vaihdella esimerkiksi suojattavan kohteen kriittisyyden tai häiriöalttiuden mukaan. Riskianalyysin tekoon voidaan hyödyntää laadullista analyysia, määrällistä analyysia tai laadullisen ja määrällisen analyysin yhdistelmää.

Laadullisessa riskianalyysissa riskin todennäköisyyttä ja seurausten vakavuutta arvioidaan hyödyntämällä laatumääritteisiä, ei numeraalisia asteikkoja. Laatumääritteinen asteikko voi muodostua esimerkiksi arvoista erittäin matala, matala, keskitasoinen, korkea ja erittäin korkea. Laadullisen riskianalyysin hyviä puolia ovat mm. sen helppo ymmärrettävyys ja muokattavuus olosuhteiden mukaisiksi. Laadullinen riskianalyysi soveltuu nykyaikaisten monimutkaisten järjestelmärakenteiden riskianalyysiin, josta on vaikea muodostaa tarkkoja laskennallisia malleja. Laadullisen riskianalyysien tulokset sopivat hyvin myös riskien viestintään päättävälle portaalle helpon ymmärrettävyyden ja hahmotettavuuden ansiosta. Laadullisen riskianalyysin huonona ominaisuutena voidaan pitää sen tulosten voimakasta riippuvuutta riskianalyysin tekijöiden käsityksistä (Karabacak & Sogukpinar, 2005; National Institute of Standards and Technology, 2012).

Määrällisessä riskianalyysissa todennäköisyyttä ja seurauksia kuvataan numeerisilla arvoilla. Yleisesti ja laajalti käytetty määrällisen riskanalyysin metodi on ns. ALE-malli (kuvio 10) (Tekijän käännös: Annual Loss Expected=Vuosittainen odotettu menetys) (Rot, 2008). Määrällinen riskianalyysi tarvitsee yleensä enemmän täsmällistä tietoa kuin laadullinen riskianalyysi. Määrällisessä riskianalyysissa hyödynnetäänkin normaalisti tietoa useammasta lähteestä. Useissa määrällisen riskianalyysin tapauksissa hyödynnetään organisaation aiempia häiriötietoja (International Organization for Standardization, 2013c). Määrällisen riskianalyysin hyvänä puolena on turvakontrolleista saadun hyödyn laskeminen mallilla. Kyseisen analyysimallin huonoihin puoliin lukeutuvat puolestaan useiden turvakontrollien yhteisen vaikutuksen laskemiseen liittyvät puutteet (Ekelhart, Fenz, Klemen, & Weippl, 2007).

$$ALE = \text{(Tapahtuman todennäköisyys) x (menetetty arvo)}$$

$$ALE = \sum_{i=1}^{n} I(O_i)F_i$$

missä:

$\{O_1, O_2, \ldots, O_n\}$ – tapahtuman negatiivisten vaikutusten sarja;
$I(O_i)$ – tapahtuman aiheuttamat arvon menetykset,
F_i – tapahtuman i toistumistiheys.

Kuvio 10 Määrällisen riskianalyysin ALE-malli (Rot, 2008)

Riskianalyysissa, jossa yhdistetään laadullisen ja määrällisen analyysin menetelmiä, hyödynnetään molempien analyysien vahvuuksia. Tyypillisesti **puoli-määrällisessä riskianalyysissä** käytetään joko asteikkoa (esim. 1 - 10) tai vaihtoehtoisesti arvokoreja (esim. 0 - 10, 11 - 30, 31 - 70, 71 - 90, 91 - 100). Puoli-määrällisellä riskianalyysilla päästään laadullista riskianalyysia tarkempaan erottelukykyyn riskien arvioinnissa, mikä osaltaan helpottaa myös riskien suhteellista priorisointia. Puoli-määrällistä riskiarviointia kannattaa hyödyntää myös analyyseissa, joissa tapahtuman aiheuttama arvon menetys on vaikeaa tai epävarmaa arvioida (National Institute of Standards and Technology, 2012).

Seurausten arvioinnissa organisaatio pyrkii arvioimaan turvallisuushäiriöiden vaikutukset organisaation toimintaan. Turvallisuushäiriön aiheuttamien seurausten arvioinnissa huomioidaan seuraukset suojattavien kohteiden käytettävyydelle, eheydelle ja luottamuksellisuudelle. Turvallisuushäiriöiden aiheuttamien seurausten arvioinnissa organisaatiossa luokitellaan suojattavat kohteet niiden kriittisyyden perusteella järjestykseen. Suojattavien kohteiden kriittisyys määräytyy niiden tärkeydestä organisaation toimintatavoitteiden saavuttamisen kannalta. Suojattavien kohteiden arvon määrityksessä voidaan hyödyntää liiketoiminnan vaikutusanalyysia, jossa huomioidaan suojattavan kohteen aiheuttamat vaikutukset organisaation toimintaan sekä muut turvallisuushäiriöstä aiheutuvat seuraamukset (Shameli-Sendi ym., 2016; International Organization for Standardization, 2013c).

Turvallisuushäiriön vaikutukset voivat aiheuttaa aineellisia tai aineettomia vaikutuksia. Vaikutukset voivat kohdistua useampaan suojattavaan kohteeseen samanaikaisesti, tai vaikutukset voivat kohdistua ainoastaan osaan suojattavaa kohdetta. Turvallisuushäiriön vaikutukset voivat aiheuttaa seurauksia organisaation eri (kuvio 8) tasoille joko samanaikaisesti tai erikseen. Organisaation tasolle 1 aiheutuvia seuraamuksia ovat esimerkiksi oikeudelliset

ja organisaation maineeseen vaikuttavat seuraukset. Organisaation tasolle 2 eli toiminnanprosessitasolle vaikutukset kohdistuvat organisaation toimintoihin, kuten esimerkiksi tuotantoprosesseihin. Organisaation tason 3 vaikutukset puolestaan vaikuttavat järjestelmätasolle ja koskevat tietojärjestelmiä (National Institute of Standards and Technology, 2011).

Suojattavaan kohteeseen ja organisaatioon kohdistuvien seurauksien ilmaisemisessa voidaan käyttää organisaation määrittämiä vaikutuskriteereitä. Käytettävät vaikutuskriteerit voivat olla esimerkiksi teknisiä, inhimillisiä tai taloudellisia. Seurausten arvioinnin määrittämisen lähtötietona voidaan hyödyntää riskinhallinnan prosessin edeltävien vaiheiden jo tuottamaa tietoa (Shameli-Sendi ym., 2016; International Organization for Standardization, 2013c).

Häiriön todennäköisyyden arviointia varten täytyy organisaation suojattavien kohteiden mahdolliset häiriötapahtumat olla tunnistettu. Häiriön todennäköisyyden arviointi perustuu haavoittuvuutta hyödyntävän uhkatapahtuman ja siihen liittyvän vaikutuksen yhteisarviointiin, joko laadullisilla tai määrällisillä menetelmillä. Arvioinnissa organisaation kannattaa hyödyntää kaikkea käytettävissä olevaa tietoa ja seikkoja, jotka helpottavat arvioinnin tekemistä. Hyödynnettäviä tietoja ovat mm. tilastot ja kokemus uhkien todennäköisyydestä, tahattomat uhkat kuten sääolot ja luonnonilmiöt, tahalliset uhkat kuten hyökkääjien kyvykkyys ja suojattavan kohteen houkuttelevuus sekä käytettävien hallintakeinojen vaikuttavuus. (National Institute of Standards and Technology, 2012; International Organization for Standardization, 2013c.)

Häiriön todennäköisyyden arviointi käyttäen haavoittuvuus- ja uhkapareja saattaa olla haastavaa erityisesti toiminnanprosessitasolla. Toiminnan prosesseihin vaikuttavat uhkatapahtumat saattaavat hyödyntää useita haavoittuvuuksia, joihin ei välttämättä ole olemassa toimivia hallintakeinoja. Tietyissä tapauksissa häiriön todennäköisyyden arviointi voikin johtaa toimintojen tai prosessien uudelleen suunnitteluun, joka mahdollistaa toiminnan jatkuvuuden, vaikka tietojärjestelmät olisivat vaarantuneet (National Institute of Standards and Technology, 2012).

Häiriön todennäköisyys saattaa muuttua nopeasti esimerkiksi uusien haavoittuvuuksien löytymisen johdosta. Organisaation kannattaakin pitää aktivisesti yllä oman toimintaympäristönsä haavoittuvuuksiin ja uhkiin liittyvää tilannekuvaa, jotta mahdollisiin muutoksiin voidaan reagoida riittävän nopeasti.

Riskitason määrittämisessä kaikki organisaation toimintaympäristöä uhkaavat riskit analysoidaan ja riskien seurauksille ja todennäköisyyksille määritetään arvot, joko laadullisesti tai määrällisesti. Riskitason määrittämisessä organisaatiossa täytyy huomioida myös toiminnot, joiden haavoittuvuuksille ja uhkatekijöille ei ole olemassa olevia hallintakeinoja (Shameli-Sendi ym., 2016; National Institute of Standards and Technology, 2011; International Organization for Standardization, 2013c).

Riskitason määrittämiseen liittyy paljon epävarmuuksia, minkä takia edeltävien vaiheiden analyysit täytyy suorittaa mahdollisimman tarkasti ja luotettavasti. Riskitason määrittämisen epävarmuudet korostuvat erityisesti

kohdistettujen hyökkäyksien riskitason määrittämisessä, joissa hyödynnettävien haavoittuvuuksien ja uhkatekijöiden käyttäytymistä on erityisen vaikea arvioida. Riskitason määrittämisen tarkkuuteen ja luotettavuuteen vaikuttavat osaltaan arviointia tekevien henkilöiden tietämyksen ja kokemuksen lisäksi myös organisaation kulttuuri. Usean eri henkilön tekemät arvioinnit saattavatkin erota toisistaan ja tuoda organisaatioon monipuolisempaa näkemystä riskitason määrittämiseen (National Institute of Standards and Technology, 2011).

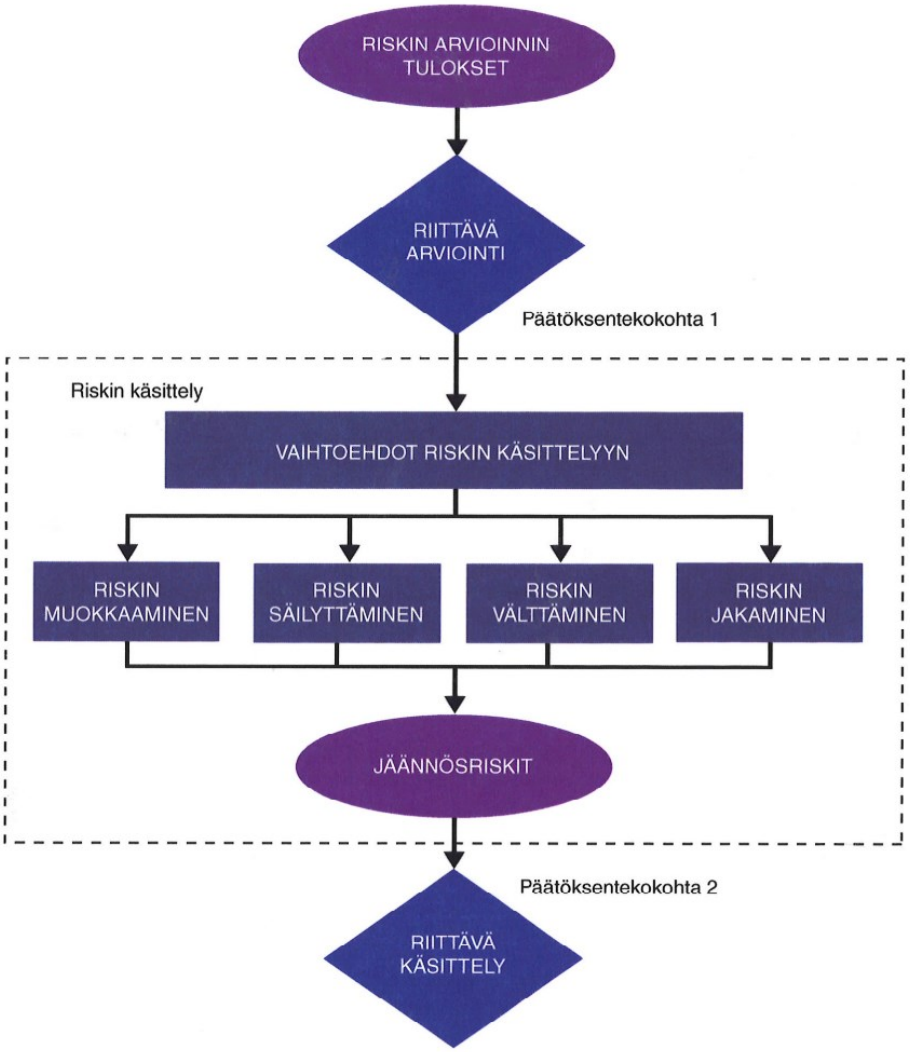
3.3.4 **Riskien merkityksen arviointi**

Riskien merkityksen arvioinnissa organisaatio määrittää riskit tärkeysjärjestykseen, ympäristön määrittämisvaiheessa luotujen riskien merkityksen arviointikriteereihin pohjautuen. Riskien merkityksen arviointikriteereiden lisäksi arvioinnissa olisi huomioitava organisaatiota sitovat sopimukset, lakien ja viranomaisten vaatimukset, sidosryhmien ja organisaation näkemykset kriteereistä sekä tehtyjen riskitason arviointien luotettavuus. Riskien merkityksen arvioinnissa täytyy myös huomioida useamman riskin yhteisvaikutukset organisaation ydintoiminnoille sekä toimintaympäristön suojattaville kohteille. Useampi tasoltaan vähäinen riski saattaa muodostaa organisaation toiminnolle tai suojattavalle kohteelle korkeamman tason riskin, joka täytyy asettaa tärkeysjärjestyksessä korkeammalle (Shameli-Sendi ym., 2016; National Institute of Standards and Technology, 2012; International Organization for Standardization, 2013c).

Riskien arviointiin liittyvät epävarmuustekijät vaikuttavat myös riskien merkityksen arviointiin. Riskien merkityksen arvioinnissa huomioitavia epävarmuustekijöitä ovat mm. uhkatekijöiden tunnistamiseen liittyvät epävarmuudet, teknologioihin liittyvät tuntemattomat haavoittuvuudet, tunnistamattomat riippuvuudet ja tietämättömyys tulevaisuuden aiheuttamista muutoksista (National Institute of Standards and Technology, 2012).

3.3.5 **Riskien käsittely**

Riskien käsittelyyn (kuvio 11) ryhdytään riskien arviointikriteereiden perusteella määritetyn tärkeysjärjestyksen muodostamisen jälkeen. Riskien käsittelyä varten luodaan riskinkäsittelysuunnitelma, joka sisältää tärkeysjärjestyksen mukaisen suunnitelman riskien minimoimiseksi hallintakeinojen avulla. Riskien hallintakeinojen avulla riskit pyritään käsittelemään tasolle, joka täyttää riskien hyväksymiskriteerit ja jonka organisaatio pystyy hyväksymään. Riskien hallintakeinoina organisaatio voi hyödyntää riskin muokkaamista, säilyttämistä, välttämistä tai jakamista (Shameli-Sendi ym., 2016; International Organization for Standardization, 2013c; Matulevičius, Mayer, & Heymans, 2008).



Kuvio 11 ISO/IEC 27005:2013 -mukainen riskin käsittelytoiminto (International Organization for Standardization, 2013c, s. 48)

Riskien käsittelyssä organisaation tulee huomioida toimintaympäristön määrittelyn yhteydessä esille tulleet rajoitukset sekä lakien ja viranomaisten asettamat vaatimukset. Riskien käsittelyssä organisaatio pyrkii yleensä mahdollisimman kustannustehokkaaseen toimintaan, joka ohjaa osaltaan myös hallintakeinojen valintaa (Shameli-Sendi ym., 2016). Tietyissä tilanteissa, kuten esimerkiksi organisaation toiminnan jatkuvuuden varmistamiseksi, hallintakeinojen kustannuksia ei voida perustella pelkästään taloudellisilla perusteilla. Tällaisissa tilanteissa, kuten muutenkin riskien käsittelyn hallintakeinojen kustannusten hyväksymisestä ja budjetoinnista, päättää organisaation johto (International Organization for Standardization, 2013c).

Riskien käsittelyssä organisaation tulee huomioida digitaalisen turvallisuuden kaikki osa-alueet. Hallintakeinojen valinnassa tulee huomioida niin tietosuojan, tietoturvan kuin kyberturvallisuudenkin osa-alueet. Mikäli organisaatiolla jo käytössä olevat hallintakeinot eivät riitä tarjoamaan

vaatimusten mukaista suojaa, voidaan hallintakeinoja täydentää järjestelmäkohtaisilla hallintakeinoilla (National Institute of Standards and Technology, 2018b).

Riskin muokkaamisella pyritään varmistamaan organisaation strategisten tavoitteiden, toiminnan vaatimusten ja organisaation prioriteettien toteutuminen. Riskin muokkaamisen hallintakeinoilla pyritään varmistamaan organisaation toimintaympäristössä käsiteltävän, tallennettavan ja siirrettävän tiedon riittävä suojaaminen siihen kohdistuvia haavoittuvuuksien ja uhkien muodostamia riskejä vastaan (National Institute of Standards and Technology, 2011). Riskin muokkaamisen hallintakeinoilla pyritään riskin toteutumisen todennäköisyyttä tai riskin aiheuttamien seurausten vaikutusta pienentämään. Parhaimmissa tapauksissa hallintakeinoilla pystytään riskin toteutumisen todennäköisyys poistamaan täysin, jolloin kyseiseen riskiin ei kohdistu jäännösriskiä (Blakley, McDermott, & Geer, 2001).

Riskin muokkaamisen hallintakeinoja voidaan hyödyntää organisaation kaikilta tasoilta. Organisaation (kuvio 8) tasolta 1 hyödynnettäviä riskin muokkaamisen hallintakeinoja ovat esimerkiksi hallinnolliset hallintakeinot, kuten turvallisuuspolitiikat ja -strategiat. Organisaation tasolta 2 hyödynnettäviä riskin muokkaamisen hallintakeinoja ovat esimerkiksi toiminnan prosessien ja yritysarkkitehtuurin suunnitteleminen vastaamaan tietosuojan ja tietoturvallisuuden vaatimuksia. Organisaation tasolta 3 hyödynnettäviä riskin muokkaamisen hallintakeinoja ovat puolestaan esimerkiksi tekniset hallintakeinot, kuten järjestelmäkovennukset ja palomuurit (National Institute of Standards and Technology, 2011).

Riskin muokkaamisen hallintakeinot voidaan jakaa kolmeen kategoriaan: estäviin hallintakeinoihin, havaitseviin hallintakeinoihin ja korjaaviin hallintakeinoihin. Estävät hallintakeinot suojaavat suojattavan kohteen haavoittuvuuksia, estäen hyökkäyksien onnistumisen tai vähentäen hyökkäyksen vaikutuksia. Havaitsevilla hallintakeinoilla pyritään havaitsemaan hyökkäykset, jolloin estävät ja korjaavat hallintakeinot käynnistyvät suojaamaan kohdetta. Korjaavilla hallintakeinoilla pyritään puolestaan vähentämään hyökkäyksen vaikutusta tai helpottamaan hyökkäyksestä toipumista normaaliin tilaan (Galder & Watkins, 2010).

Riskin muokkaamisen hallintakeinojen valintaan vaikuttavia rajoituksia on useita. Hallintakeinojen valinnassa pitäisikin huomioida toimintaympäristön lisäksi myös organisaatioon liittyvät muut tekijät. Hallintakeinojen valinnassa tarkasteltavia rajoituksia ovat mm. tekniset rajoitukset, taloudelliset rajoitukset ja helppokäyttöisyys. (International Organization for Standardization, 2013c).

Riskin säilyttämiseen sellaisenaan voidaan organisaatiossa päätyä, mikäli riskiin liittyvä riskitaso on riskien hyväksymiskriteereiden sisällä. Riskin säilyttämisen päätös perustuu riskien merkityksen arviointiin. Riskin säilyttäminen on järkevä ratkaisu, kun riskin käsittelyyn liittyvät kustannukset ylittävät riskistä aiheutuvat mahdolliset menetykset (Bojanc & Jerman-Blažič, 2008; International Organization for Standardization, 2013c).

Riskin välttämiseen organisaatiossa päädytään, mikäli riskin aiheuttama vaikutus suojattavaan kohteeseen ylittää suojattavasta kohteesta saadun hyödyn. Riski voidaan välttää luopumalla riskin aiheuttamasta toiminnosta tai muuttamalla toimintojen suoritusolosuhteita suotuisammiksi esimerkiksi siirtämällä toiminnan tuotantopaikka turvallisempaan sijaintiin (Shameli-Sendi ym., 2016; Bojanc & Jerman-Blažič, 2008; International Organization for Standardization, 2013c).

Riskin jakamisella ja riskin siirtämisellä organisaatio pyrkii pienentämään riskiä, osittain siirtämällä riskin vaikutusta organisaation ulkopuolelle tai toiselle organisaation sisäiselle tekijälle. Riskin jakamisella tai siirtämisellä pyritään riskin vaikutusta organisaation sisäiseen toimintaympäristöön vähentämään tasolle, jonka organisaatio voi hyväksyä. Riskin jakamisessa tulee huomioida organisaation kulttuuristen ja hallinnollisten tekijöiden lisäksi myös organisaation ulkopuoliset velvoitteet ja vastuut. Riskiä voidaan jakaa esimerkiksi kumppanille, joka kykenee tarkkailemaan ja vastaamaan välittömästi riskin toteutumisen uhkaan. Riskiä voidaan jakaa tai siirtää myös esimerkiksi ottamalla vakuutus riskiä vastaan. Riskin jakamisessa ja siirtämisessä organisaation täytyy kuitenkin muistaa, ettei kokonaisvastuuta voida täysin ulkoistaa. Riskin jakamisessa ja siirtämisessä täytyy myös huomioida, ettei siitä aiheudu muutoksia organisaatiossa tunnistetuille riskeille tai ettei uusia riskejä muodostu (Bojanc & Jerman-Blažič, 2008; National Institute of Standards and Technology, 2011; International Organization for Standardization, 2013c).

3.3.6 **Riskien hyväksyminen**

Riskien hyväksyminen organisaatiossa perustuu pääasiallisesti ennalta määritettyihin riskien hyväksymiskriteereihin. Riskien hyväksymiskriteereissä on huomioitu organisaation ydintoiminnan lisäksi organisaatiota velvoittavat normit ja sopimukset, jotka ohjaavat organisaation riskinottoa ja riskien hyväksymistä. Riskien hyväksymiskriteereissä on määritetty, millainen jäännösriski on organisaation kannalta hyväksyttävää (Shameli-Sendi ym., 2016; International Organization for Standardization, 2013c).

Riskien hyväksymisessä organisaation täytyy huomioida toimintojen ja prosessien riippuvuudet toisistaan. Toimintoihin ja prosesseihin hyväksytyt riskit saattavat vaikuttaa organisaation muihin toimintoihin tai prosesseihin odottamattomalla tavalla, mikäli riippuvuudet jäävät huomioimatta (National Institute of Standards and Technology, 2011).

Tietyissä tapauksissa jäännösriski saattaa poiketa määritetyistä riskien hyväksymiskriteereistä. Tällaisissa tapauksissa riskit voivat tarjota organisaatiolle huomattavia hyötyjä tai jäännösriskin muokkaamisesta aiheutuvat kustannukset voivat olla liian korkeat suhteessa jäännösriskin vaikutuksiin. Riskien hyväksymiskriteereiden mukaiset ja niistä poikkeavat riskit organisaatiossa hyväksyy organisaation johto, ja päätökset hyväksytyistä riskeistä olisi hyvä tehdä perusteluineen kirjallisesti (Galder & Watkins, 2010; International Organization for Standardization, 2013c). Riskien

hyväksymiskriteereistä poikkeavien jäännösriskien hyväksynnän seurauksena organisaation on syytä tarkistaa riskien hyväksymiskriteerien ajantasaisuus (International Organization for Standardization, 2013c).

3.3.7 **Riskejä koskeva viestintä ja tiedonvaihto**

Riskejä koskeva tiedonvaihto ja viestintä ovat tärkeä osa riskienhallinnan prosessia, ja ne koskettavat koko organisaation henkilöstöä. Riskeihin liittyvällä viestinnällä voidaan kasvattaa organisaation henkilöstön tietoturvatietoisuutta, joka parantaa organisaation sisäistä tietoturvakäyttäytymistä ja tietoturvasääntöjen noudattamista (Bulgurcu ym., 2010).

Riskejä koskevalla viestinnällä voidaan yhtenäistää riskeihin liittyviä näkemyksiä ja käsityksiä organisaation riskienhallinnasta vastaavien tahojen ja muiden sidosryhmien välillä. Näkemyksien ja käsityksien ollessa yhtenevät helpottuvat riskeihin liittyvien päätöksien tekeminen sekä ymmärrys päätöksien hyödyistä ja taustalla olevista syistä. Riskejä koskeva viestintä perustuu kahden suuntaiseen viestintään (kuvio 8), joka mahdollistaa muun muassa riskejä koskevan tiedon keräämisen, päätöksen teon tukemisen ja riskienhallinan jatkuvan kehityksen. (National Institute of Standards and Technology, 2011; International Organization for Standardization, 2013c.)

Riskejä koskeva viestintä ja tiedonvaihto ovat organisaatiossa jatkuva käytäntö, ja sitä suoritetaan riskienhallinnan prosessin kaikkien vaiheitten aikana. Tehokkaalla riskeihin liittyvällä viestinnällä varmistetaan ajantasainen tieto ja käsitys organisaation riskienhallinnan prosessista ja sen tuomista hyödyistä ja tuloksista. Tästä syystä organisaation kannattaa laatia riskejä koskevat viestintäsuunnitelmat, jotka käsittävät hätätilanneviestinnän sekä normaalin riskejä koskevan viestinnän. Riskeihin liittyvän viestinnän tehtävät ja vastuut organisaatiossa on määritettävä selkeästi. Riskejä koskevassa viestinnässä kannattaa hyödyntää organisaation viestintäyksikköä tai viestintäasiantuntijoita tehokkaan viestinnän takaamiseksi (International Organization for Standardization, 2013c).

3.3.8 **Riskien seuranta ja katselmointi**

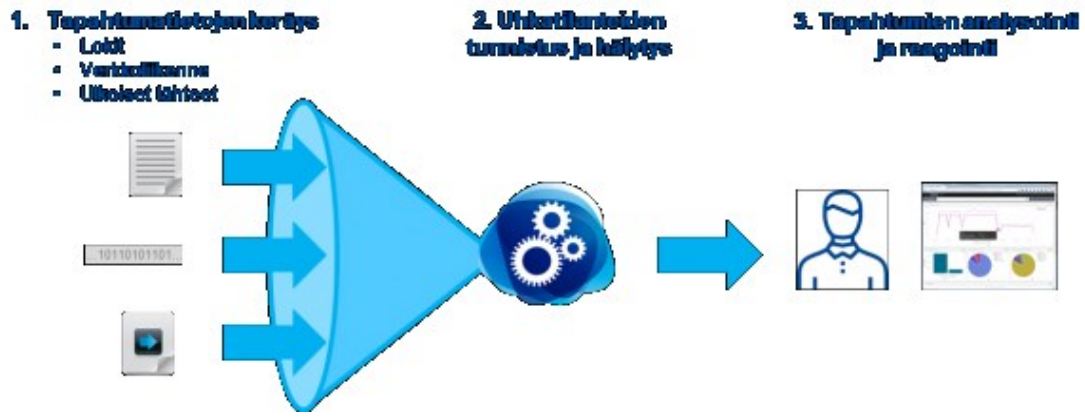
Riskien seurannan ja katselmoinnin tavoitteena on varmistaa, että tarvittavat riskinhallinnan toimenpiteet on otettu käyttöön ja ne vastaavat organisaation toiminnan ja ulkopuolisten velvoitteiden ja vastuiden (lait ja sopimukset) vaatimuksiin. Riskien seurannalla pyritään myös varmistamaan riskienhallintaan liittyvien toimenpiteiden tehokkuus ja ajantasaisuus sekä tunnistamaan toimintaympäristöön ja järjestelmiin vaikuttavat muutokset. Toimintaympäristöön ja järjestelmiin vaikuttavien muutoksien havainnoinnissa pyritään haavoittuvuuksien ja uhkien lisäksi havainnoimaan myös riskien seurauksissa ja todennäköisyyksissä tapahtuvia muutoksia. Riskeissä tapahtuvissa muutoksissa tulee huomioida myös usean muutoksen yhdessä aiheuttamat mahdolliset kertymävaikutukset (Shameli-Sendi ym., 2016; National

Institute of Standards and Technology, 2011; International Organization for Standardization, 2013c).

Riskien seurannassa täytyy huomioida organisaation ulkopuolelta tulevien muutosten lisäksi myös organisaation omassa toiminnassa tapahtuvat muutokset. Riskienhallintaan vaikuttavia, organisaation sisäisiä muutoksia ovat esimerkiksi ydintoimintavaatimusten muutokset ja organisaation prosesseissa tapahtuvat muutokset. Riskien seurannassa tai katselmoinnissa havaitut toimintaympäristön muutokset toimivat syötteenä riskienhallinnan prosessiin. Toimintaympäristössä havaituilla muutoksilla voi olla vaikutusta organisaation riskienhallintaan, jolloin organisaation kannattaa suorittaa riskien arviointi tai koko riskienhallinnan prosessi uudelleen varmistuakseen riskienhallinnan toimenpiteiden tehokkuudesta ja ajantasaisuudesta (International Organization for Standardization, 2013c).

Riskien seurannassa voidaan hyödyntää ulkoisia palveluja, jotka helpottavat tiedonsaantia uusista haavoittuvuuksista ja uhkista. Kotimaassa tietoa haavoittuvuuksista ja ajankohtaisista uhkista tarjoaa Traficomin Kyberturvallisuuskeskus (Traficom, 2020). Ulkomailla toimivia uhkista ja haavoittuvuuksista tietoa tarjoavia organisaatioita ovat mm. National Vulnerability Database (NVD, 2020) sekä Exploit Database (Offensive Security, 2020).

Riskien seurantaan ja katselmointiin liittyvää tapahtumatietoa voidaan organisaatiossa kerätä myös automatisoidusti. Tiedonkeruuseen ja analysointiin on tarjolla useita erilaisia työkaluja ja järjestelmiä, jotka helpottavat tietoliikenteen ja järjestelmien turvallisuustapahtumien havainnointia ja analysointia. Tehokasta tiedonkeruuta ja analysointia voidaan suorittaa esimerkiksi (kuvio 12) SIEM-järjestelmillä (Tutkijan käännös : Security Information and Event Management = Turvallisuus tiedon ja tapahtumien hallinta).



Kuvio 12 SIEM-järjestelmän toiminta (Insta Group, 2017)

Riskien seurantaan ja katselmointiin liittyvä viestintä tapahtuu (kuvio 8), kuten muukin riskeihin liittyvä viestintä, organisaation tasojen sisällä ja organisaation tasojen välillä. Riskeissä tapahtuvien muutosten koskettaessa yhteistyötahoja on

viestintää kohdennettava myös niille. Organisaation sisäisellä viestinnällä pyritään tietoturvatietoisuuden kasvattamisen lisäksi myös tukemaan riskienhallintaan liittyvien hallinnollisten päätösten tekoa sekä varmistamaan tarvittavien riskienhallintaan liittyvien resurssien ja työkalujen saatavuus toiminnanprosessi- ja tietojärjestelmätasoille (Dempsey ym., 2011).

3.4 Yhteenveto riskienhallinnasta

Digitaalisen turvallisuuden riskienhallinnan osa-alueita käsittelevää kirjallisuutta ja akateemisia tutkimusjulkaisuja on runsaasti saatavilla. Digitaalinen turvallisuus sateenvarjokäsitteenä, joka sisältää digitaalisen turvallisuuden johtamisen ja riskienhallinnan, jatkuvuuden hallinnan ja varautumisen, tietoturvallisuuden, kyberturvallisuuden ja tietosuojan osa-alueet, on vielä uusi, ja sitä kokonaisuutena käsitteleviä tutkimusjulkaisuja ei vielä ole saatavilla. Digitaalisen turvallisuuden riskienhallinnan osa-alueita käsittelevä kirjallisuus ja tutkimusjulkaisut painottuvat vahvasti tietoturvallisuuden riskienhallintaan, käsittäen osittain myös kyberturvallisuuden ja tietosuojan osa-alueet. Jatkuvuuden hallinnan ja varautumisen osa-alueesta löytyy myös runsaasti julkaisuja, mutta aihetta käsitellään useasti liiketoiminnan näkökulmasta.

Digitaaliseen turvallisuuteen liittyvään riskienhallintaan on kehitetty useita eri standardeja. Riskienhallinnan standardeista yleisimmin käytetty on ISO/IEC-standardi, jota hyödynnetään myös tämän tutkimuksen riskienhallintaosuuden teoreettisena päälähteenä. NIST eli National Institute of Standards and Technology on yhdysvaltalainen organisaatio, joka julkaisee mm. digitaaliseen turvallisuuteen liittyviä standardeja, joita hyödynnetään Yhdysvalloissa ja useissa muissa maissa. Tässä tutkimuksessa NIST:n standardeja on käytetty muun kirjallisuuden ja tutkimustiedon ohella täydentämään riskienhallinnan teoriaa.

Digitaaliseen turvallisuuteen liittyvillä riskienhallinnan toimenpiteillä pyritään varmistamaan organisaation ydintoiminnan jatkuvuus sekä organisaation toimintaympäristössä prosessoitavan tiedon luottamuksellisuus, saatavuus ja eheys. Digitaalisen turvallisuuden riskienhallinnan tulee tukea ja olla linjassa organisaation strategian ja asetettujen tavoitteiden kanssa.

Digitaalisen turvallisuuden riskienhallinnan strategialla ja siihen liittyvällä toimintasuunnitelmalla organisaation ylinjohto määrittää mm. riskienhallinnan tavoitteet, laajuuden sekä budjetin. Riskienhallinnan strategia ohjaa riskienhallinnan prosessin toimintaympäristön määritystä, asettamalla sille tavoitteet ja laajuuden.

Toimintaympäristön määrityksessä organisaation tulee huomioida riskienhallinnan organisoimisen, laajuuden ja peruskriteerien luomisen lisäksi myös sitä velvoittavat sopimukset ja lainsäädäntö. Toimintaympäristön määrittämisen jälkeen riskienhallinnan prosessissa suoritetaan riskien arviointi.

Riskien arvioinnissa riskit tunnistetaan ja analysoidaan sekä riskien merkitykset arvioidaan organisaatiolle ja määritetylle toimintaympäristölle. Riskien tunnistamisessa organisaatio pyrkii tunnistamaan siihen kohdistuvat uhkatekijät, haavoittuvuudet, suojattavat kohteet, käytössä olevat hallintakeinot sekä mahdollisten tietoturvapoikkeamien aiheuttamat seuraukset.

Riskien analysoinnissa organisaatiossa voidaan käyttää laadullista, määrällistä tai laadullista ja määrällistä yhdistävää riskianalyysia. Laadullisessa riskianalyysissa riskejä arvoidaan laadullisin määrittein, kuten esimerkiksi arvioimalla riskin todennäköisyyttä ja seurausten vakavuutta asteikolla matala, keskitasoinen ja korkea. Määrällisessä riskianalyysissa puolestaan hyödynnetään numeerisia arvoja kuten arvoja, yhdestä sataan, tai lasketaan vuosittainen odotettu menetys riskeille. Laadullista ja määrällistä yhdistävässä riskianalyysissa hyödynnetään numeerisia arvoja esim. yhdestä sataan, jotka on jaoteltu riskitasoa kuvaaviin tasoihin.

Riskien merkityksen arvioinnissa organisaatio määrittää tunnistetut ja analysoidut riskit tärkeysjärjestykseen, ympäristön määrittämisvaiheessa luotujen riskien merkityksen arviointikriteereihin pohjautuen. Riskien merkityksen arvioinnissa huomioidaan arviointikriteereiden lisäksi myös organisaation sopimukset ja muut velvoitteet, jotka vaikuttavat osaltaan riskien tärkeysjärjestyksen määritykseen.

Riskien tärkeysjärjestyksen määrityksen jälkeen organisaatiossa määritetään riskien käsittelyä varten riskinkäsittelysuunnitelma. Suunnitelma sisältää organisaation ydintoimintaan ja toimintaympäristöön kohdistuvien riskien käsittelyn tasolle, jonka organisaatio on valmis hyväksymään, ennalta määritettyjen kriteereihin perustuen. Riskinkäsittelyssä voidaan riskejä muokata, jakaa, välttää tai säilyttää. Riskienkäsittely pyritään suorittamaan organisaatiossa mahdollisimman kustannustehokkaasti.

Riskien hyväksyminen organisaatiossa perustuu riskien hyväksymiskriteereihin, jotka määritetään ympäristön määrittämisen yhteydessä. Riskien hyväksymiskriteerit määrittävät organisaation riskinottohalukkuutta, jota ohjaavat osaltaan myös organisaatiota velvoittavat sopimukset ja lainsäädäntö.

Riskejä koskevaa viestintää ja tiedonvaihtoa suoritetaan organisaatiossa jatkuvana prosessina. Riskejä koskeva viestintää suoritetaan organisaation tasojen sisäisesti sekä tasojen välisesti. Organisaatio viestii riskeistä myös organisaation ulkopuolelle tarvittaessa. Riskejä koskevalla viestinnällä edesautetaan organisaation riskienhallinnan onnistumista sekä lisätään organisaation tietoturvatietoisuutta.

Riskien seurantaa ja katselmointia suoritetaan organisaatiossa jatkuvasti. Riskien seurannan avulla riskienhallinnan prosessia pyritään kehittämään aktiivisesti ja riskeihin pyritään reagoimaan riittävällä nopeudella. Riskien seurannassa organisaatio voi hyödyntää asiantuntevaa organisaation sisäistä tai ulkoista toimijaa. Riskien seurannassa organisaation kannattaa myös hyödyntää kaikkea saatavilla olevaa tietoa.

4 Laki julkisen hallinnon tiedonhallinnasta

Lailla julkisen hallinnon tiedonhallinnasta pyritään varmistamaan julkisen hallinnon tiedonhallinnan ja tietoaineistojen yhdenmukaisuus sekä tietoaineistojen tietoturvallinen ja laadukas hyödyntäminen. Lailla pyritään lisäksi edistämään tietojärjestelmien ja tietovarantojen yhteentoimivuutta julkisen hallinnon viranomaisten välillä (Oikeusministeriö, 2020).

Tässä luvussa käsitellään tiedonhallintalain vaikutuksia kuntasektorin näkökulmasta julkisen hallinnon digitaaliseen turvallisuuteen, digitaalisen turvallisuuden riskienhallintaan ja lain toimeenpanoon. Tiedonhallintalain käsittely rajataan tässä tutkimuksessa lain lukuun 4 – tietoturvallisuus.

4.1 Tiedonhallintalain vaikutukset kuntien digitaalisen turvallisuuden hallintaan

Lailla julkisen hallinnon tiedonhallinnasta tavoitellaan julkisen hallinnon tiedonhallinnan yhteentoimivuuden, tehokkuuden ja turvallisuuden lisäämistä. Tässä aliluvussa käsitellään lain vaikutuksia kuntien digitaalisen turvallisuuden hallintaan.

Tiedonhallintalaissa digitaaliseen turvallisuuteen liittyvät asiat käsitellään luvussa 4 – tietoturvallisuus. Luku sisältää lain pykälät 12-18, joissa määritellään seuraavaa:

12 § Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen
13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
14 § Tietojen siirtäminen tietoverkossa
15 § Tietoaineistojen turvallisuuden varmistaminen
16 § Tietojärjestelmien käyttöoikeuksien hallinta
17 § Lokitietojen kerääminen
18 § Turvallisuusluokiteltavat asiakirjat valtionhallinnosta
(Oikeusministeriö, 2020)

Lain 12 §:n mukaan tiedonhallintayksikön on tunnistettava luotettavuutta edellyttävät tehtävät ja varmistettava niissä toimivien henkilöiden luotettavuus henkilöturvallisuusselvityksien kautta (Oikeusministeriö, 2020). Luotettavuutta edellyttäviin tehtäviin lukeutuvat muun muassa salassa pidettävän materiaalin käsittelyyn osallistuvat tehtävät. Näitä tehtäviä kunnissa ovat esimerkiksi henkilötietojen käsittelyyn osallistuvien henkilöiden tehtävät. Kuntien tietoaineistot voivat sisältää myös muuta salassa pidettävää materiaalia, jotka täytyy huomioida lain asettamien vaatimuksien noudattamisessa.

Lain 13 § sisältää useita vaatimuksia tiedonhallintayksikölle. Vaatimuksia ovat lain mukaan:

1. Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava sen tietoturvallisuus elinkaaren ajalta.
2. Toimintaympäristöön kohdistuvat olennaiset riskit on tunnistettava, ja tietoturvallisuustoimenpiteet on mitoitettava riskiarvioinnin mukaisesti.
3. Viranomaisen tehtävien hoitamiseen liittyvien olennaisien tietojärjestelmien vikasietoisuus ja käytettävyys on varmistettava säännöllisellä testauksella.
4. Tietojärjestelmien ja tietovarantojen tietorakenteet on suunniteltava siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa viranomaisten asiakirjojen julkisuuden osalta.
5. Viranomaisen on varmistettava hankittaville tietojärjestelmille toteutetut asianmukaiset tietoturvallisuustoimenpiteet.
   (Oikeusministeriö, 2020)

Lain 13 §:n 1. kohdan mukaan kuntien on seurattava digitaalisen toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava toiminta-ympäristön tietoturvallisuus koko sen elinkaaren ajalta. Kuntien täytyy lain mukaan valvoa digitaalisen toimintaympäristönsä tietoturvallisuuden tilaa. Valvonnan täytyy kohdistua kaikkiin kunnan toiminnan kannalta olennaisiin tietoaineistoihin, tietojärjestelmiin ja tiedonsiirrossa hyödennettävään tietoverkkoon.

Lain 13 §:n 2. kohdan mukaan digitaalisen toiminta-ympäristön tietoturvallisuustoimenpiteet on mitoitettava riskiarviointiin perustuen. Kuntien riskienhallinnan täytyy käsittää digitaalinen toimintaympäristö kokonaisuudessaan. Tietoturvallisuustoimenpiteet täytyy kohdistaa ja mitoittaa riskiarvionnin perusteella olennaisiin tietojen-käsittelynympäristöihin.

Lain 13 §:n 3. kohdan mukaan kuntien viranomaistehtävissä hyödynnettävien olennaisten tietojärjestelmien täytyy olla vikasietoisia ja käytettävissä tarpeen mukaan. Tietojärjestelmien vikasietoisuutta ja käytettävyyttä on myös testattava säännöllisesti. Kyseessä olevien palveluiden osalta kuntien täytyy varmistaa, ettei niissä ole yksittäistä pistettä, jonka toimintahäiriö keskeyttäisi koko palvelun.

Lain 13 §:n 4. kohdan mukaan kuntien tietojärjestelmien ja tietovarantojen tietorakenteet on suunniteltava viranomaisten asiakirjojen julkisuus ja vaivaton julkaisu huomioiden. Kuntien täytyy huomioida asiakirjojen julkisuus ja mahdollisuus niiden julkaisuun järjestelmissä, joissa viranomaisten julkisia asioita käsitellään, esim. asianhallintajärjestelmissä.

Lain 13 §:n 5. kohdan mukaan kuntien on varmistettava tietojärjestelmien hankinnan yhteydessä, että niihin on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Kuntien täytyy varmistaa tietojärjestelmien asianmukaiset tietoturvallisuusominaisuudet hankinnan yhteydessä. Tietoturvallisuusvaatimukset ja niiden toteutus ja testaus täytyy huomioida riittävällä tavalla myös hankintasopimuksissa.

Lain 14 §:n mukaan viranomaisen on toteutettava salassa pidettävien tietojen tiedonsiirto salattua tai muuten suojattua tiedonsiirtoyhteyttä

käyttämällä. Lisäksi tiedon vastaanottaja on varmistettava tai tunnistettava riittävän tietoturvallisella tavalla ennen salassa pidettäviin tietoihin pääsyä. Lain 14 §:n mukaan kuntien on hyödynnettävä salassa pidettävien tietojen tiedonsiirtoon salattua tai suojattua tiedonsiirtoyhteyttä. Salatussa tiedonsiirrossa voidaan hyödyntää salattuja tiedonsiirtoprotokollia kuten esim. TLS/SSL- tai IPSec–protokollia. Tiedon vastaanottajan varmistamisessa ja tunnistamisessa voidaan hyödyntää pääsynhallintaan liittyviä hallintakeinoja.

Lain 15 §:n mukaan tietoaineistojen turvallisuus täytyy varmistaa tarpeellisin tietoturvallisuustoimenpitein. Tietoaineistojen muuttumattomuus, saatavuus, käyttökelpoisuus, alkuperäisyys, ajantasaisuus ja virheettömyys täytyy varmistaa tietoturvallisuustoimenpitein. Lisäksi tietoaineistot täytyy suojata teknisiltä ja fyysisiltä vahingoilta ja käsittelyyn ja säilytykseen käytettävien toimitilojen pitää olla riittävän tietoturvallisia. Lain 15 §:n vaatimuksien toteuttamissa täytyy kunnissa hyödyntää tietoturvallisuuteen ja jatkuvuuden hallintaan liittyviä hallintakeinoja. Tietoaineistojen käsittelyssä ja säilytyksessä täytyy huomioida tekniseen ja fyysiseen tietoturvallisuuteen liittyvät riittävät hallintakeinot.

Lain 16 §:n mukaan vastuussa olevan viranomaisen on määritettävä tietojärjestelmän käyttöoikeudet käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan ja käyttöoikeudet on pidettävä ajantasaisina. Lain 16 §:n vaatimuksien toteuttamiseksi kuntien pääsynhallintaan liittyvät hallintakeinot täytyy suunnitella siten, että tietojärjestelmien käyttöoikeudet ovat hallittavissa työtehtävien mukaan ja että käyttöoikeudet pysyvät ajantasaisina. Käyttöoikeuksien määrittämisessä ja pääsynhallinnassa voidaan hyödyntää esimerkiksi roolipohjaista pääsynhallintaa.

Lain 17 §:n mukaan viranomaisen on huolehdittava tietojärjestelmien lokitietojen tarpeellisesta keräämisestä. Lokitietoja kerätään tietojärjestelmien käyttöön ja tietojen luovutuksiin liittyen tietojärjestelmistä, joiden käyttö edellyttää tunnistautumista tai kirjautumista.

Lain 18 §:n vaatimukset eivät kohdistu kuntien toimintaan, mistä syystä sen käsittely rajautuu pois tästä tutkimuksesta.

4.2 Tiedonhallintalain tietoturvallisuusvaikutuksien voimaantulo ja täytäntöönpano kuntasektorilla

Tiedonhallintalaki astui voimaan 1. tammikuuta 2020. Lakiin määritettyjen siirtymäsäännöksien johdosta lain 12—16 §:ssä säädetyt vaatimukset on toteutettava kunnissa 36 kuukauden kuluessa lain voimaantulosta. Lain 17 §:n mukaisia vaatimuksia lokitietojen keräämisestä sovelletaan lain voimaantulon jälkeen hankittaviin tietojärjestelmiin. Pykälän asettamia vaatimuksia sovelletaan myös ennen lain voimaantuloa hankittuihin tietojärjestelmiin 24 kuukauden kuluttua lain voimaantulosta (Oikeusministeriö, 2020).

Tiedonhallintalain täytäntöönpanoa Suomessa ohjaa valtiovarainministeriö. Täytäntöönpanon keskeisessä roolissa on tiedonhallintalautakunta, joka asetettiin lain voimaantulon jälkeen tammikuussa 2020. Valtiovarainministeriö järjestää eri puolille Suomea tiedonhallintalain koulutuskierroksia, jotka on suunnattu erityisesti kunnille, kuntayhtymille ja muille valtionhallintoon kuulumattomille julkisen hallinnon toimijoille (Valtiovarainministeriö, 2020d).

Tiedonhallintalain vaatimuksien täytäntöönpano kunnissa on viime kädessä kuntien omalla vastuulla. Lain vaatimusten toteuttamisessa ja täytäntöönpanossa on kunnissa huomioitava muutoksien tekoon vaadittava aika. Tarvittavien muutostoimenpiteiden suorittaminen kannattaisikin aloittaa hyvissä ajoin ennen siirtymäsäännöksien päättymistä.

5 Kunnat

Suomessa on vuonna 2020 kuntaliiton mukaan yhteensä 310 kunta. Kunnista 203 käyttää kunta-nimitystä ja loput 107 kaupunki–nimitystä kunnastaan. Suomen kuntien mediaani asukasluku oli 6 081 vuonna 2018. Keskimääräinen asukasluku oli samana vuonna puolestaan 17 743 (Kuntaliitto, 2019a). Suomessa on, kunnille lainsäädännön määrittämiin tehtäviin ja asukasmääräänsä nähden, paljon kuntia, ja ne ovat kooltaan melko pieniä. Tässä tutkimuksessa pienien kuntien asukasmäärän ylärajaksi määritetään 10 000 henkilöä ja keskisuurien kuntien asukasmäärän ylärajaksi 50 000 henkilöä, virallisen määrityksen puuttuessa.

5.1 Kuntaorganisaatiot

Kuntaorganisaation mallit vaihtelevat kuntien välillä. Kuntalain määrittämiä pakollisia toimielimiä kunnassa ovat kunnanvaltuusto, kunnanhallitus, keskusvaalilautakunta ja tarkastuslautakunta (Oikeusministeriö, 2015). Kuntalain mukaisien toimielimien lisäksi kunnanvaltuusto voi asettaa tarvittavia johtokuntia ja lautakuntia täydentämään kuntaorganisaation johtamisjärjestelmää.

Kuntaorganisaation johtamisjärjestelmät voidaan jakaa kuntaliiton mukaan viiteen eri malliin. Kuntaliitto nimeää nämä johtamisjärjestelmämallit perinteiseksi malliksi, valtuusto—kunnanhallitus–malliksi, valiokuntamalliksi, puheenjohtajamalliksi ja elämänkaarimalliksi (Kuntaliitto, 2019b).

Perinteisessä mallissa kunnanvaltuusto käyttää ylintä päätösvaltaa ja tekee kunnan strategisen tason päätökset. Kunnanhallituksen tehtävänä perinteisessä mallissa on johtaa kunnan hallintoa sekä valmistella ja toimeenpanna kunnanvaltuuston päätökset. Lautakunnat puolestaan toimivat kunnanvaltuuston ja kunnanhallituksen asioiden valmistelussa ja päätösten toimeenpanossa sekä vastaavat hallinnonalansa päätöksenteosta (Kuntaliitto, 2019b).

Valtuusto—kunnanhallitus –malli on perinteisestä johtamisjärjestelmä-mallista karsitumpi malli, jossa kunnanhallitus hoitaa lain määrittämissä puitteissa myös lautakuntien tehtäviä. Valtuusto—kunnanhallitus–mallissa on kunnassa säilytettävä kuitenkin lainsäädännön edellyttämät lautakunnat (Kuntaliitto, 2019b).

Valiokuntamallisessa johjamisjärjestelmässä lautakuntien tilalla toimivat valiokunnat. Valiokunnat muodostuvat kunnanvaltuuston jäsenistä, jolloin poliittisesti valitut valtuutetut pääsevät vaikuttamaan kunnan asioihin jo varhaisessa vaiheessa. Valiokuntamallissa voidaan painottaa joko kunnanhallituksen tai kunnanvaltuuston asemaa. Kunnanhallitusta painottavassa mallissa valiokunnat toimivat ainoastaan valmistelevina toimieliminä (Kuntaliitto, 2019b).

Puheenjohtajamalli voi noudattaa joko valiokuntamallia tai perinteistä johtamisjärjestelmämallia. Puheenjohtajamallissa kunnan lautakuntien puheenjohtajat valitaan kunnanhallituksen jäsenistä, jotka ovat yleensä myös kunnanvaltuutettuja (Kuntaliitto, 2019b).

Elämänkaarimallissa pyritään kuntalaisille tarjoamaan palveluita väestöryhmittäin. Palvelutoiminta ja sen johtaminen on järjestetty väestöryhmien tarpeiden mukaisiin kokonaisuuksiin. Lautakuntien organisointiin liittyvät kokonaisuudet voivat koostua esimerkiksi lasten ja lapsiperheiden asioista, työikäisten asioista ja ikääntyvien asioista (Kuntaliitto, 2019b).

5.2 Kuntien tehtävät ja palvelut

Kunnille on määritetty laissa useita palveluita, joita niiden täytyy järjestää asukkailleen. Kuntien lakisääteisiin tehtäviin liittyvät palvelut ovat valtiovarainministeriön mukaan:

- *koulutus ja päiväkoti*
- *kulttuuri-, nuoriso- ja kirjastopalvelut*
- *kaupunkisuunnittelu, maankäyttö*
- *veden- ja energiantuotanto*
- *jätehuolto*
- *ympäristöpalvelut*
- *sosiaali- ja terveyspalvelut*
- *palo- ja pelastustoimi*
  (Valtionvarainministeriö, 2020*)*

Kuntien talouden helpottamiseksi on niille asetettuja lakisääteisiä tehtäviä yritetty vähentää edeltävän, vuosien 2015-2019, hallituskauden aikana. Kuntien tehtävien vähentäminen havaittiin kuitenkin valtiovarainministeriön tilaaman selvityksen mukaan haastavaksi, tehtävien ja palveluiden vakiintuneiden käytäntöjen ja niihin liittyvien rakenteiden johdosta. Kunnilla on myös oikeus päättää tarjota lakisääteisien tehtävien lisäksi muita palvelutasoa nostavia palveluita (Valtiovarainministeriö, 2019).

Kunnat voivat perustaa kuntayhtymän hoitamaan jotain kunnan tehtävää niiden puolesta. Kuntayhtymälle määritellään jäsenkuntien valtuustojen hyväksymässä perussopimuksessa toimiala sekä toimintaan liittyvät toimielimet ja henkilöstö. Kuntayhtymiä oli vuonna 2016 yhteensä 138, edustaen useaa kunnan toimialaa (Kuntaliitto, 2020).

5.3 Kuntien tietohallinto

Kuntien tietohallinnon järjestäminen kuuluu kuntien itsehallinnon piiriin. Kuntien tietohallintoon liittyvät tehtävät sisältyvät osaksi kuntien järjestämis- ja tuotantovastuista säädettyjä tehtäviä. Kunnat voivat organisoida oman tietohallintonsa perustuslain 124 §:n julkisten hallintotehtävien hoitamiselle asettamien vaatimuksien ja rajoitteiden puitteissa (Voutilainen & Kurvinen, 2015).

Kuntien tietohallinnon kuten myös koko julkisen hallinnon tietohallinnon ohjauksesta vastaa valtiovarainministeriön JulkICT-osasto. Julkisen hallinnon ICT:n ohjauskeinoina (liite 2) hyödynnetään mm. normiohjausta, informaatio-ohjausta sekä hanketoimintaa. JulkICT-osaston pyrkimyksenä on kehittää kuntien ja valtion välistä tietohallintoon liittyvää yhteistyötä sekä tukea kuntien digitalisaation kehitystä ja sen hyödyntämistä kuntien palveluissa, hallinnossa ja johtamisessa (Valtiovarainministeriö, 2020e).

Julkisen hallinnon tietohallinnon neuvottelukunta JUHTA toimii kuntien ja ministeriöiden pysyvänä neuvottelu- ja yhteistyöelimenä. Neuvottelukunnan tavoitteena on julkisen hallinnon tietohallinnon strategisen ohjaamisen ja koordinoinnin tukeminen sekä julkisten palveluiden tasokkuuden edistäminen Suomessa (Valtiovarainministeriö, 2020e).

5.4 Kuntien digitaalinen turvallisuus

Kunnat vastaavat tiedonhallintayksikkönä palvelujensa digitaalisesta turvallisuudesta itsenäisesti. Kuntien ja muun julkisen hallinnon digitaalisen turvallisuuden lähtökohtina ovat valtiovarainministeriön mukaan: *Suomen Kyberturvallisuusstrategia ja sen toimeenpano sekä säädöksissä julkisen hallinnon toimijoille määritellyt tietoturvallisuutta ja kyberturvallisuutta koskevat vaatimukset* (Valtiovarainministeriö, 2020a).

Kuntien digiturvallisuuden tulee perustua tietoriskien hallinnan mukaiseen riskiarviointiin, ja sen tulee täyttää lainsäädännön tietoturvallisuudelle ja kyberturvallisuudelle asetetut vähimmäisvaatimukset (Valtiovarainministeriö, 2020a).

Julkisen hallinnon digitaalisen turvallisuuden strategisesta ohjauksesta vastaa valtiovarainministeriön asettama julkisen hallinnon digitaalisen turvallisuuden strateginen johtoryhmä. Digitaalisen turvallisuuden strategisen johtoryhmän tehtävät ovat valtiovarainministeriön mukaan:

1) *Koordinoi julkisen hallinnon digitaalisen turvallisuuden strategista riskiarviota.*
2) *Luo ja koordinoi toiminnan ja osaamisen kehittämisen kattavan kansallisen strategisen tason digitaalisen turvallisuuden yhteistoimintamallin.*
    - *Valtion, kuntien ja kuntayhtymien toiminta ja vastuut*

- *Julkisen hallinnon ja yksityisen sektorin välinen yhteistyö*
- *Julkisen hallinnon ja tutkimuksen yhteistyö*
- *Kansainvälinen yhteistyö*

3) *Arvioi julkisen hallinnon strategista digitaalisen turvallisuuden tilannetta.*
   - *Asettaa ja seuraa tavoitteita*
   - *Viestii turvallisuuden tilasta ja sen kehittymisestä*
4) *Arvioi, ohjaa, koordinoi ja valvoo keskeisiä kehitettäviä digitaalisen turvallisuuden palveluja.*
5) *Valvoo digitaalisen turvallisuuden toimeenpanosuunnitelman ja kuntien digitaalisen turvallisuuden tiekartan toteutumista.*
   (Valtiovarainministeriö, 2020b)

Julkisen hallinnon digitaalisen turvallisuuden operatiivisen tason ohjausryhmänä toimii digi- ja väestötietoviraston Vahti–johtoryhmä. Digi- ja väestötietovirasto tarjoaa myös kunnille ajantasaista ohjeistusta, harjoituksia ja muuta tukea digitaalisen turvallisuuden kehittämiseen (Digi- ja väestötietovirasto, 2020).

6 TUTKIMUKSEN TOTEUTUS

Tässä luvussa esitellään tutkimuksen toteutusta. Tutkimuksen toteutuksen esittelyssä edetään tieteentraditioista tutkimusmetodologian kautta tutkimuksessa hyödynnettyihin tutkimusmetodeihin. Tässä luvussa esitellään myös tutkimukseen liittyvä tutkimusprosessi, jossa lukijalle esitellääään tutkimuksen etenemistä ja siihen liittyvien valintojen tekoa. Tutkimuksen varsinaiset tulokset käsitellään luvussa 7.

6.1 Tutkimusmenetelmä

Tieteentraditiot voidaan erottaa kahteen aatehistorialliseen perinteeseen, aristoteeliseen ja galileiseen perinteeseen. Näiden perinteiden tieteellisien selityksien vastakohtaisia määrityksiä on kuvattu teleologiseksi ja kausaaliseksi selityksiksi. Tieteenfilosofiset traditiot voidaan jaotella edellä mainittujen aatehistoriallisten perinteiden alle lukuisiin eri traditioihin (Tuomi & Sarajärvi, 2018).

Tieteelliset tutkimusmenetelmät voidaan kategorisoida laadullisiin ja määrällisiin tutkimusmenetelmiin (Myers, 1997). Määrällisissä tutkimuksissa hyödynnetään numeerisia menetelmiä, ja tutkimusmenetelmässä pyritään mahdollisimman suureen objektiivisuuteen. Laadullisessa tutkimuksessa puolestaan pyritään ymmärtämään ilmiötä osallistujan ja hänen institutionaalisen toimintaympäristönsä näkökulmasta, hyödyntäen laadullisia menetelmiä (Myers, 1997). Laadullisien ja määrällisien tutkimusmenetelmien metodit eroavat toisistaan tutkimuksessa kerättävien ja hyödynnettävien tutkimusaineistojen sekä käytettävien tutkimusanalyysimenetelmien osalta (Myers, 1997).

Laadullisella tutkimuksella on määrällisestä tutkimuksesta eroavat ominaispiirteensä. Laadullisen tutkimuksen tyypillisiksi piirteiksi Hirsjärvi ym. (2010) nimeää:

1. *Tutkimus on luonteeltaan kokonaisvaltaista tiedon hankintaa ja aineisto kootaan luonnollisissa, todellisissa tilanteissa.*
2. *Suositaan ihmistä tiedon keruun instrumenttina.*
3. *Käytetään induktiivista analyysia.*
4. *Laadullisien metodien käyttö aineiston hankinnassa*
5. *Valitaan kohdejoukko tarkoituksenmukaisesti, ei satunnaisotoksen menetelmää käyttäen.*
6. *Tutkimussuunnitelma muotoutuu tutkimuksen edetessä.*
7. *Käsitellään tapauksia ainutlaatuisina ja tulkitaan aineistoa sen mukaisesti.* (Hirsjärvi, Remes, & Sajavaara, 2010, 164)

Laadullinen tutkimus voidaan ryhmitellä myös tutkimustyypeittäin neljän eri mielenkiinnon kohteen mukaan. Näitä mielenkiinnon kohteita ovat kielen piirteet, säännönmukaisuuksien etsiminen, tekstin ja toiminnan merkityksen ymmärtäminen ja reflektio. Jokaiseen tutkimustyyppiin liittyy myös useita tutkimuslajeja, joten laadullisen tutkimuksen kenttä on metodologisesti varsin laaja (Hirsjärvi ym., 2010).

Laadullisessa tutkimuksessa voidaan hyödyntää tutkimusaineiston analysointiin useita erilaisia analyysimenetelmiä. Opinnäytetöissä usein käytetyssä sisällönanalyysissa tutkimusaineisto pyritään tiivistämään ja luokittelemaan tai järjestämään kategorioihin (Tuomi & Sarajärvi, 2018). Sisällönanalyysia voidaan käyttää esimerkiksi fenomenologisessa tutkimuksessa, etnografisessa tutkimuksessa ja ankkuroidun teorian tutkimuksessa (Tuomi & Sarajärvi, 2018). Analyysimenetelmät voidaan jakaa myös empiiriseen ja teoreettiseen analyysiin. Empiirisessä analyysissa korostetaan analyysi- ja aineiston keräämismetodeja, kun teoreettisessa analyysissa analyysirungon muodostavat problematisointi, eksplikointi ja argumentointi (Tuomi & Sarajärvi, 2018).

Laadullinen analyysi voidaan Alasuutarin (2011) mukaan jakaa kahteen eri vaiheeseen: havaintojen pelkistämiseen ja arvoituksen ratkaisemiseen. Havaintojen pelkistämisessä tutkimusaineistoa tarkastellaan tietystä teoreettismetodologisesta näkökulmasta, jolloin tutkimusaineistosta saadaan kulloinkin käytetyn kysymyksenasettelun kannalta relevanttia tietoa. Havaintoja pyritään tarkastelun jälkeen yhdistämään yhteisen piirteen, nimittäjän tai säännön mukaan, jolloin havainnot saadaan karsittua tutkimuksen kannalta oleellisiksi (Alasuutari, 2011).

Arvoituksen ratkaiseminen eli tulosten tulkinta on laadullisen analyysin toinen vaihe. Tuloksien tulkinnassa tehdään merkitystulkintaa tutkivasta ilmiöstä. Merkitystulkintaa tehdään tuotettujen havaintojen muodostamien johtolankojen ja teoreettisen ydinkäsitteen suhteen. Merkitystulkinnalla pyritään muodostamaan yhtenäisiä rakennekokonaisuuksia, jotka muodostavat tutkimuksen varsinaiset tulokset (Alasuutari, 2011).

6.2 Tutkimuksen aineisto

Tutkimusaineistona voidaan laadullisessa tutkimuksessa hyödyntää useita erilaisia aineistoja. Aineistot voivat koostua esimerkiksi dokumenteista ja teksteistä, haastatteluista, kyselyistä, osallistujien havainnoinnista (Myers, 1997; Conboy ym., 2012). Tutkimusaineisto ja sen keruumenetelmä määräytyvät pääsääntöisesti tutkimustehtävän ja valitun tutkimustyypin ohjaamana. Tutkimusaineisto ja sen keruumenetelmä kannattaakin suunnitella tarkkaan, että ne tukisivat tutkimustehtävän ratkaisua parhaalla mahdollisella tavalla.

Kaikissa aineiston keruumenetelmissä on omat vahvuudet ja heikkoudet. Kyselyn eduiksi Hirsjärvi ym. (2010) mainitsee mm. laajan tutkimusaineiston keruun helppouden ja vaivattomuuden tutkijan kannalta. Kyselyiden

heikkoudeksi sama teos mainitsee mm. epävarmuudet vastausvaihtoehtojen sopivuudesta tutkittavan kannalta sekä vastaajan yleisen suhtautumisen tutkimusta kohtaan. Haastattelu tiedonkeruumenetelmänä on ainutlaatuinen kielellisen vuorovaikutuksen vuoksi. Haastatteluun tiedonkeruumenetelmänä sisältyvät myös omat edut ja heikkoudet. Haastattelun etuihin lukeutuvat mm. sen joustavuus aineistoa kerätessä sekä syvällisemmän tiedon saanti haastatteluiden kautta. Haastattelun heikkouksiin lukeutuvat mm. haastattelun vaatima aika sekä tilanteen mahdollinen haastavuus haastateltavan kannalta (Hirsjärvi ym., 2010).

Haastattelu tiedonkeruumenetelmänä voidaan jakaa kolmeen eri tyyppiin. Haastattelutyypit muodostuvat strukturoidusta haastattelusta, teemahaastattelusta ja avoimesta haastattelusta. Strukturoidussa haastattelussa kysymysten esitysjärjestys ja kysymysten muoto on ennalta määrätty ja siten helposti toteutettava. Teemahaastattelussa ovat haastattelun teema-alueet tiedossa, mutta kysymykset ja niiden järjestys muodostuvat haastattelun edetessä. Avoimesta haastattelusta käytetään myös nimitystä syvähaastattelu. Avoimessa haastattelussa ei ole mitään varsinaista runkoa, vaan haastattelu jää täysin haastateltavan ohjailtavaksi (Hirsjärvi ym., 2010).

Haastattelut voidaan toteuttaa yksilöhaastatteluna, parihaastatteluna tai ryhmähaastatteluna. Haastattelumuotoja voidaan myös käyttää täydentämään toisiaan yhdistämällä niitä. Pari- ja ryhmähaastattelumuotoja hyödynnetään erityisesti esimerkiksi lapsia haastateltaessa epävarmuuksien pienentämiseksi (Hirsjärvi ym., 2010).

6.3 Tutkimusprosessi

Tässä aliluvussa esitellään tutkimuksen eteneminen sekä tutkimuksessa tehdyt valinnat. Tutkimuksen eteneminen ja varsinaisen tutkimustehtävän muotoutuminen kuvataan suoraan kronologisesti etenevänä, vaikka prosessissa oli myös jonkin verran iteraatiota.

6.3.1 **Tutkimustehtävä**

Tutkimustehtävän muotoutumiseen vaikuttivat vuoden 2020 alusta voimaan astunut laki julkisen hallinnon tiedonhallinnasta sekä pienien ja keskisuurien kuntien digitaalisen turvallisuuden tilasta olevan tutkimustiedon vähäisyys. Tutkimustehtävän valintaa edesauttoi myös tutkijan henkilökohtainen mielenkiinto digitaalista turvallisuutta ja sen nykytilaa kohtaan. Tutkimustehtäväksi muodostui selvittää pienien ja keskisuurien kuntien digitaalisen turvallisuuden tila, erityisesti riskienhallinnan näkökulmasta. Tutkimuksessa pyrittiin selvittämään myös pienien ja keskisuurien kuntien valmius tiedonhallintalain asettamien tietoturvavaatimuksien suhteen.

6.3.2 **Tutkimusstrategia**

Tutkimustehtävän valinnan jälkeen alkoi pohdinta tutkimustehtävän ratkaisemiseksi hyödynnettävästä tutkimusstrategiasta eli tutkimusotteesta. Tutkimusstrategian valintaan vaikuttivat tutkittavan ilmiön luonne sekä tutkimustehtävän selvittämiseen tarvittavan tutkimusaineiston laatu. Tutkimuksessa oli tarvetta tutkimusaineistolle, joka tarjoaisi mahdollisimman syvällistä sekä uutta tietoa tutkittavasta aiheesta. Tutkimusstrategiaksi valikoitui edellä mainittujen asioiden ohjaamana laadullinen tutkimus, joka mahdollistaa muun muassa syvällisen tiedonhankinnan ja kerätyn tutkimusaineiston analysointiin sopivat analyysimenetelmät.

6.3.3 **Käsitteellisteoreettinen osio**

Tutkimuksessa hyödynnettiin käsitteellisteoreettisen osion tiedonhaussa pääasiassa Google Scholar –palvelua, tietojärjestelmätieteen tieteellisiä julkaisuja, ohjelmistotuotannon tieteellisiä julkaisuja sekä digitaalisen turvallisuuden osa-alueista julkaistuja standardeja. Käsitteellisteoreettista osiota täydennettiin hyödyntämällä ministeriöiden julkaisuja, kuntaliiton julkaisemia tietoja sekä voimassa olevaa digitaaliseen turvallisuuteen liittyvää lainsäädäntöä.

Digitaalinen turvallisuus on käsitteenä kohtalaisen uusi. Tutkimusjulkaisuissa ja standardeissa käsiteltävät digitaalisen turvallisuuden osa-alueet eivät välttämättä rajaa käsiteltäviä asioita samalla tavalla, kuin valtionhallinnossa nykyään rajataan kyseiset osa-alueet. Erityisesti tietoturvallisuuden ja kyberturvallisuuden käsitteiden rajaukset eivät tutkimusjulkaisuissa ja standardeissa vastaa suoraan digitaalisen turvallisuuden osa-alueiden rajausta. Digitaalisen turvallisuuden osa-alueiden rajauksien selventämiseksi tutkimuksessa käytettiin, myös valtiovarainministeriön käyttämiä, sanastokeskuksen julkaisemia käsitekaavioita kyberturvallisuuden, tietoturvallisuuden ja tietosuojan sisältämistä käsitteistä.

Käsitteellisteoreettinen osio käsittelee digitaalisen turvallisuuden osa-alueita, kuntien toimintaa sekä lakia julkisen hallinnon tiedonhallinnasta, jotka ovat tutkimustehtävän kannalta merkityksellisiä asiakokonaisuuksia. Lakia julkisen hallinnon tiedonhallinnasta rajattiin tutkimuksessa käsiteltäväksi tutkimuksen kannalta merkitykselliseen tietoturvaa käsittelevään lukuun. Digitaalisen turvallisuuden osa-alueista pyrittiin käsitteellisteoreettisessa osuudessa painottamaan riskienhallinnan osuutta, sen tutkimuksen kannalta merkityksellisyyden vuoksi.

6.3.4 **Tutkimusaineisto**

Tutkimusaineiston hankintaan päätettiin tutkimuksessa hyödyntää puolistrukturoitua teemahaastattelua. Puolistrukturoidun teemahaastattelun valintaan päädyttiin, koska se mahdollistaa tutkimusteemoihin liittyvien valmiiden kysy-

mysten hyödyntämisen sekä jatkokysymyksien käytön kerätyn tiedon syventämiseksi. Tutkimusaineiston keräämisessä pyrkimyksenä olikin saada haastattelukysymyksien vastauksien lisäksi myös teemaan liittyvää muuta tietoa.

Haastateltavaksi kohderyhmäksi kunnista valikoituivat ensisijaisesti riskienhallinnasta vastaava ylin operatiivinen johto eli kunnanjohtajat. Koska haastattelukysymykset sisälsivät pääasiassa digitaaliseen turvallisuuteen liittyviä kysymyksiä, annettiin haastatteluun mahdollisuus osallistua myös kunnan digitaalisesta turvallisuudesta vastaavalle asiantuntijalle, joilla on syvällisempi substanssiosaaminen teemasta.

Haastattelupyyntö toimitettiin sähköpostitse yhteensä kahdeksaantoista kuntaan. Haastattelupyyntö toimitettiin pääsääntöisesti kunnanjohtajalle. Tutkija oli myös sähköpostin lähetyksen jälkeen yhteydessä useaan kuntaan puhelimitse, motivoidakseen kuntia osallistumaan tutkimukseen. Haastateltavien saaminen tutkimukseen osoittautui vaikeaksi, johtuen koronapandemian aiheuttamista kiireistä. Tutkijalle välittyi myös tunne, että pienien ja keskisuurien kuntien digitaalisen turvallisuuden nykytilanne vaikutti tutkimukseen osallistumishalukkuuteen vähentävästi.

Haastattelut järjestettiin vuoden 2020 huhti- ja toukokuun aikana. Haastatteluihin osallistui (taulukko 1) yhteensä neljä kuntaa. Haastateltavista kunnista kahdesta haastatteluun osallistuivat sekä kunnanjohtaja että asiantuntija. Yhdestä kunnasta osallistui digiturvallisuudesta vastaava asiantuntija ja yhdestä kunnasta kunnanjohtaja, joka myös vastaa kuntansa digitaalisen turvallisuuden koordinoinnista.

TAULUKKO 1 Haastateltavat

Haastateltava(t)		**Hyödynnetty tekniikka**
Haastateltava 1	Kunnanjohtaja + tietohallintopäällikkö	Skype
Haastateltava 2	Kunnanjohtaja + atk-suunnittelija	Skype
Haastateltava 3	Tietohallintojohtaja	Teams
Haastateltava 4	Kunnanjohtaja	Skype

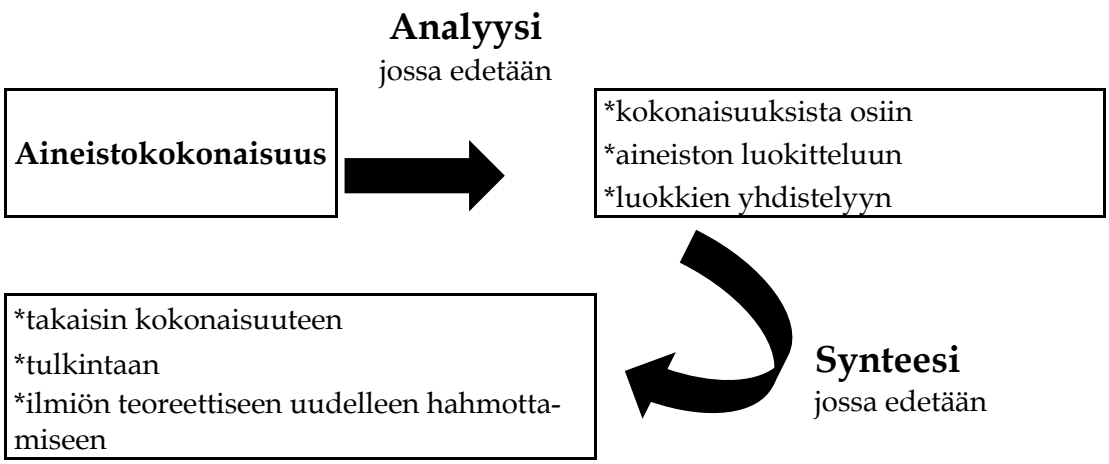
Haastattelut olivat pituudeltaan keskimäärin noin tunnin mittaisia. Haastettelut tallennettiin digitaaliseen muotoon puhelimen äänitallenninta hyödyntäen jatkokäsittelyä varten. Kaikilta tiedonantajilta pyydettiin lupa haastatteluiden tallentamiseen ennen tallentamisen aloittamista. Haastattelujen aluksi tutkija varmisti, että haastateltavat tuntevat digitaalisen turvallisuuden käsitteen sekä kertasi digitaalisen turvallisuuden viitekehyksen osa-alueet varmistaakseen asian. Haastattelut etenivät pääasiallisesti tutkimuskysymyksien teemojen mukaisesti, ja tiedonantajien vastaukset liittyivät digitaalisen turvallisuuden viitekehykseksen teemoihin joko suoraan tai epäsuorasti. Tutkija pyysi haastattelujen aikana haastatteluteemaan liittyviä tarkennuksia ja ohjasi haastattelua jatkokysymyksien avulla saadakseen mahdollisimman syvällistä tietoa haastatteluteemaan liittyen. Haastattelun lopuksi tutkija asianmukaisesti kiitti osallistujia vaivannäöstä ja osallistumisesta tutkimukseen.

Haastatteluiden päättymisen jälkeen tutkija litteroi haastattelut kirjalliseen muotoon sisällön analysointia varten. Litteroinnin tarkkuudessa huomioitiin sen soveltuvuus suoraan tutkimusaineiston analysointia varten, siten että kaikki yksityiskohdat säilyivät muuttumattomina.

6.3.5 **Sisällönanalyysi**

Tutkimuksen sisällönanalyysissa analysoitiin (kuvio 13) tutkimuksen aineistokokonaisuus pilkkomalla, luokittelemalla ja yhdistelemällä luokkia tutkimuksen kannalta merkittäviksi kokonaisuuksiksi. Aineistokokonaisuuden analysoinnin jälkeen siirryttiin synteesin muodostamiseen kokoamalla tutkimusaineistosta tutkimuksen kannalta merkittäviä kokonaisuuksia. Lisäksi ilmiön suhdetta olemassa olevaan teoriaan hahmotettiin tulkitsemalla ja kuvailemalla.

Tutkimuksessa hyödynnettiin teoriaohjaavaa sisällönanalyysiä. Tutkimuksen sisältöä aloitettiin analysoimaan alustavasti haastatteluiden esikuuntelun ja litteroinnin yhteydessä. Haastatteluiden kirjalliseen muotoon saattamisen jälkeen tutkija tutustui tarkemmin haastatteluiden muodostamaan aineistoon lukemalla sen useita kertoja läpi ja muodostamalla kokonaisuudesta selkeämmän kuvan jatkokäsittelyä varten. Aineiston tarkastelun yhteydessä tutkija ryhtyi luokittelemaan aineistoa tutkimuksen teoreettisen osuuden ja tutkimusaineistosta nousseiden kokonaisuuksien muodostamiin teemoihin. Tutkimusaineiston teemoittelun jälkeen luokiteltiin teemojen sisältö vielä tarkemmin yhteneviin luokkiin ja alaluokkiin.



Kuvio 13 Haastatteluaineiston käsittely analyysista synteesiin (Hirsjärvi & Hurme, 2014, s. 144)

Aineistokokonaisuuden pilkkomisen ja luokittelujen jälkeen tutkija muodosti tutkimusaineistosta teoreettisen osuuden ja aineistostosta nousseiden kokonaisuuksien mukaisia teemakokonaisuuksia luokitteluihin perustuen. Digitaalisen turvallisuuden teemakokonaisuudet muodostuivat muun muassa digitaalisen turvallisuuden viitekehyksen mukaisista teemoista, kuten

riskienhallinnan ja kyberturvallisuuden teemoista. Teemakokonaisuudet sisälsivät teemoihin luokitteluiden perusteella sisältyvät aineistoluokat, kuten esimerkiksi kyberturvallisuuden kokonaisuuteen sisältyivät muun muassa tiedonsiirron ja toimintaympäristön monitorointi -luokat. Tutkimusaineistosta pilkkomisen ja luokitteluiden kautta muodostettuja kokonaisuuksia hyödynnettiin tutkimuksen tuloksien tulkinnassa ja raportoinnissa, joissa näistä pyrittiin muodostamaan käytänteitä mahdollisimman totuuden mukaisesti kuvaavia kokonaisuuksia.

6.4 Tutkimuksen laadullinen arviointi

Tutkimuksen toteutuksessa hyödynnettiin laadullisen tutkimuksen menetelmää. Laadullisen tutkimuksen laadukkuutta voidaan Eskola ja Suorannan (1998) mukaan arvioida tutkimustulosten siirrettävyyden, vahvistettavuuden, varmuuden ja uskottavuuden perusteella. Tutkimustuloksien uskottavuuteen vaikuttavat laadullisessa tutkimuksessa pääasiallisesti tutkijan vastuullisuus tutkimustilanteessa sekä empiirisen aineiston laadukkuudesta varmistuminen (Eskola & Suoranta, 1998). Tutkimuksen empiirinen aineisto kerättiin puolistrukturoiduilla teemahaastatteluilla, joissa haastateltavina olivat kunnanjohtajat ja asiantuntijat tai tietohallinnosta vastaava henkilö. Tutkimuksen haastattelurunko toimitettiin haastateltaville muutamaa päivää ennen varsinaista haastattelua. Edellisen lisäksi tutkija kävi haastateltavien kanssa tutkimuksen sisältämät käsitteet läpi haastatteluiden aluksi varmistuakseen, että kaikilla oli yhteinen ymmärrys käsitteiden tarkoituksesta. Tutkimukseen valittu puolistrukturoitu teemahaastattelu mahdollisti myös haastattelukysymyksien tarkentamisen ja selventämisen mahdollisten väärinkäsityksien minimoimiseksi.

Tutkimuksen varmuutta arvioitaessa tulee kiinnittää huomiota tutkijan mahdollisiin ennakkokäsityksiin ja oletuksiin (Eskola & Suoranta, 1998). Tutkimuksen teoreettinen konteksti oli tutkijalle entuudestaan osittain tuttu. Käsitteellisesti digitaalinen turvallisuus osa-alueittain eroaa kuitenkin jonkin verran kirjallisuudessa usein käytetyistä kokonaisuuksista sisältöjen osalta. Kuntasektorin digitaalisesta turvallisuudesta ei tutkijalla ollut tutkimuksen tekoa aloittaessa aiempaa tietämystä. Tästä johtuen ennakko-oletukset eivät päässeet vaikuttamaan tutkimustuloksiin.

Tutkimuksen vahvistuvuudella viitataan Eskola ja Suorannan (1998) mukaan siihen, miten tutkimuksessa tehdyt johtopäätökset tukevat vastaavaa ilmiötä tarkastelleita tutkimuksia. Tutkimuksen kohteena olevan digitaalisen turvallisuuden ilmiötä on tutkittu osa-alueittain sekä kuntasektoria kokonaisuutena koskien. Tutkimustulokset vaikuttaisivat olevan pääosin saman suuntaisia aikaisempien tutkimuksien kanssa, vaikka arviointia ei voida suorittaa kokonaisvaltaisesti tutkimuksien lähtökohtien eroavaisuuksista johtuen. Tutkimuksen vahvistuvuuteen voidaankin ottaa kantaa tarkemmin, kun saman aiheiset tutkimukset yleistyvät.

Tutkimustulosten siirrettävyys on Eskolan ja Suorannan (1998) mukaan mahdollista tietyin ehdoin, vaikka yleisesti naturalistisessa paradigmassa katsotaankin, etteivät yleistykset ole mahdollisia. Tämän tutkimuksen osalta siirrettävyyden arviointi mahdollistuu vahvistuvuuden tavoin vasta sitten, kun tutkimukset aiheesta yleistyvät.

Tutkimuksen luotettavuuden arvioinnissa käytetään usein validiteetin ja reliabiliteetin käsitteitä. Tutkimuksen reliaabelius tarkoittaa tutkimuksen mittaustulosten toistettavuutta eli kykyä antaa samanlaisia mittaustuloksia eri mittauskerroilla samasta ilmiöstä (Hirsjärvi ym., 2010). Tutkimuksen reliaabeliuden arvioinnissa voidaan hyödyntää kolmea eri menetelmää. Ensimmäisen menetelmän mukaan tutkimus on reliaabeli, mikäli samaa ilmiötä tutkittaessa saadaan kaikilla tutkimuskerroilla sama tulos. Toisen menetelmän mukaan tutkimuksen reliaabelius voidaan määrittää, mikäli kahden arvioitsijan päätelmät samasta tutkimusaiheesta päätyvät tutkimuksen arvioinnissa samaan tulokseen. Kolmas tapa arvioinnissa liittyy tutkimusmenetelmien arviointiin. Tämän näkemyksen mukaan tutkimus on reliaabeli kahden rinnakkaisen tutkimusmenetelmän tuottaessa samasta teemasta saman tutkimustuloksen. Tämän tutkimuksen reliaabeliuden arvioinnissa täytyy huomioida tutkimuksen empiirisen aineiston muodostuminen teemahaastatteluiden kautta, joiden täydellinen toistettavuus on tieteenfilosofian mukaisesti vähintäänkin vaikeaa. Tämän tutkimuksen tulokset ovat pääosin samansuuntaisia VAHTI Digiturvakyselyn tulosten kanssa, mikä tukee tutkimuksen reliaabeliutta. Tutkimuksen reliaabeliutta tukee myös Eskola ja Suoranta (1998) määritys laadullisen tutkimuksen tutkimusaineiston reliaabeliudesta aineiston ristiriidattomuuden osalta.

Tutkimuksen validius tarkoittaa Hirsjärvi ym. (2010) mukaan tutkimusmenetelmän kykyä mitata juuri sitä, mitä on pyritty mittaamaan. Validiuden arviointia voidaan suorittaa ennustevalidiuden, tutkimusasetelmavalidiuden ja rakennevalidiuden näkökulmista (Hirsjärvi ym., 2010). Ennustevalidiudella tarkoitetaan, että yhden tutkimuskerran toteutuksella ja tuloksien arvioinnilla voidaan ennustaa myöhemmin samasta aiheesta toteutettavien tutkimuksien tuloksia. Tutkimusasetelmavalidius voidaan jakaa neljään muotoon: tilastolliseen validiuden, rakennevalidiuden, sisäisen validiuden ja ulkoisen validiuden muotoihin (Hirsjärvi & Hurme, 2014). Tilastollinen validius liittyy tilastollisiin manipulaatioihin eikä ole siten relevantti tämän tutkimuksen osalta. Rakennevalidiuden arvioinnissa selvitetään, tutkitaanko tutkimuksessa sitä, mitä tutkimuksella on tarkoitettu tutkittavan. Tässä tutkimuksessa kerättiin teemahaastatteluita hyödyntämällä tutkimuksen kannalta tutkimusaineisto, jota analysoimalla saavutettiin tutkimustuloksien tulkinnan myötä vastaukset määriteltyihin tutkimuskysymyksiin. Edelliseen pohjautuen rakennevalidiutta arvioitaessa voidaan katsoa tutkimuksen olevan validi. Sisäisellä validiudella pyritään tarkastelemaan tutkimuksen sisäisiä riippuvuussuhteita. Laadullisen tutkimuksen riippuvuussuhteet eroavat kvantitatiivisen tutkimuksen tilastollisista riippuvuussuhteista, jota varten sisäisen validiuden arviointi on

alun perin määritetty. Sisäisen validiuden arviointi ei ole tämän tutkimuksen kannalta olennaista tutkimuksessa hyödynnetystä metodista johtuen. Ulkoisella validiudella tarkoitetaan tutkimustulosten yleistettävyyttä erilaisiin tilanteisiin tai erilaisiin henkilöihin. Tapaustutkimuksen yleistettävyyttä arvioitaessa tulee huomioida haastatteluiden ja niistä saatavan aineiston sitoutuminen kontekstiin ja ympäristöön, jossa haastattelut toteutetaan. Tapaustutkimuksen haastatteluiden kautta saatavia tutkimustuloksia ei voida yleistää koskemaan koko tutkittavaa ilmiötä, eikä sen pitäisi olla tapaustutkimuksessa tarkoituskaan. (Hirsjärvi & Hurme, 2014.)

Hirsjärvi ym. (2010) mukaan *laadullisen tutkimuksen luotettavuutta kohentaa tutkijan tarkka selostus tutkimuksen toteuttamisesta. Tarkkuus koskee tutkimuksen kaikkia vaiheita*. Tässä tutkimuksessa on pyritty selostamaan tutkimuksen toteutus (kts. luku 6.3) mahdollisimman tarkalla ja realistisella tavalla. Tutkimuksen luotettavuutta on pyritty edelleen lisäämään tutkimustuloksissa käytettyjen useiden haastattelusitaattien kautta.

7 TUTKIMUKSEN TULOKSET

Tässä luvussa esitellään tutkimuksen tulokset. Tutkimuksen havaintoaineistoa reflektoidaan ensiksi tiedonhallintalain asettamiin vaatimuksiin, jotka astuvat voimaan pääosin vuoden 2023 alusta siirtymäkauden päättyessä. Toisessa aliluvussa havaintoaineistoa esitellään digitaalisen turvallisuuden osa-alueiden näkökulmasta siten, että jokainen osa-alue käsitellään erikseen. Tutkimuksen tulokset -luvun viimeisessä aliluvussa esitellään digitaalisen turvallisuuden kokonaisuutta ja osa-alueita riskienhallinnan näkökulmasta.

7.1 Valmius tiedonhallintalain asettamiin vaatimuksiin

Tässä aliluvussa esitellään tutkimuksen tuloksia tiedonhallintalain asettamien vaatimuksien mukaisesti. Tiedonhallintalaki astuu kuntien osalta pääosin voimaan vuoden 2023 alusta. Tutkimus esittelee kuntien tämän hetkistä tilannetta tiedonhallintalain asettamien vaatimuksien suhteen.

7.1.1 Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

Tiedonhallintalain 12 § ohjaa tiedonhallintayksikköä tunnistamaan luotettavuutta edellyttävät tehtävät sekä arvioimaan näissä tehtävissä toimivien työntekijöiden luotettavuuden.

Tutkimukseen osallistuneista kunnista luotettavuutta edellyttävien tehtävien tunnistamisessa oli vaihtelua. Osassa kunnista ei ole luotettavuutta edellyttäviä tehtäviä tunnistettu lainkaan, kun taas osassa kunnista luotettavuutta edellyttäviä tehtäviä on tunnistettu toimialakohtaisesti tai laajemmin.

Luotettavuutta edellyttävissä tehtävissä toimivien työntekijöiden luotettavuutta ei pääsääntöisesti ole arvioitu pienissä ja keskisuurissa kunnissa. Luotettavuuden arviointeja on kunnissa teetetty säännöllisesti ainoastaan tietyillä toimialoilla, joissa toimitaan pääasiassa lasten parissa. Yhdessä tutkimukseen osallistuneista kunnista luotettavuuden arviointeja on teetetty tiettyihin, erityistä luotettavuutta edellyttäviin tehtäviin. Eräässä kunnassa työntekijöiden luotettavuuden arviointien tekemistä kuvattiin puolestaan seuraavasti:

> Turvallisuusselvityksiä ei ole tehty ja eikä ole noita, tämän voisi kyllä sanoa, että ei ole vielä tehty. Mutta varmaankin sellainen tarpeellinen asia jatkossa…mutta tämä korona on sotkenut tässä kuviot. (Haastateltava 4)

Tutkimukseen osallistuneissa kunnissa luotettavuuden edellyttävien tehtävien tunnistaminen ja työntekijöiden luotettavuuden varmistaminen koettiin tärkeiksi asioiksi, vaikka niiden käytännön toteuttaminen olikin vielä vaillinaista.

7.1.2 **Tietoaineistojen ja tietojärjestelmien tietoturvallisuus**

Tiedonhallintalain 13 § ohjaa tiedonhallintayksikön tietoaineistojen ja tietojärjestelmien tietoturvallisuutta. Lain pykälä asettaa useita vaatimuksia tiedonhallintayksikön tietoaineistojen ja tietojärjestelmien tietoturvallisuudelle. Lain pykälän mukaan tiedonhallintayksikön on (kohta 1) seurattava toiminympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus niiden elinkaaren ajalta. Tiedonhallintayksikön on myös (kohta 2) selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti. Viranomaisen tehtävien hoitamisen kannalta (kohta 3) olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti. Viranomaisen (kohta 4) tietojärjestelmät, tietovarantojen tietorakenteet ja tietojenkäsittely on suunniteltava siten, että asiakirjojen julkisuus voidaan toteuttaa vaivatta. Viranomaisen on (kohta 5) varmistettava hankittavien tietojärjestelmien asianmukaiset tietoturvallisuustoimenpiteet niitä hankittaessa.

Pienissä ja keskisuurissa kunnissa seurataan (1) kybertoimintaympäristön tilaa haavoittuvuuksien ja uhkien osalta aktiivisesti. Kaikki tutkimukseen osallistuneet haastateltavat kertoivat kunnan seuraavan käytössä olevien tietojärjestelmien uhkia ja haavoittuvuuksia sekä suorittavan niiden vaatimat toimenpiteet tietojärjestelmien tietoturvallisuuden takaamiseksi. Tutkimukseen osallistuneista kunnista kahdessa tehtiin seudullista yhteistyötä kybertoimintaympäristön valvonnassa. Yhdellä tutkimukseen osallistuneista kunnista oli seurantaa suorittamaan hankittu ulkopuoliselta palveluntarjoajalta SOC-palvelu seudullisena yhteistyönä.

> …meillä on niin kuin SOC/SIEM eli mikä tämä on security operation center, joka on niin kuin ostettu ulkopuoliselta taholta. Ja SIEM on sitten tämä mikä kokoaa tiedot ja hälyttelee ja tää SOC siihen reagoi. Jos sieltä tulee jotakin sellaista, niin kuin mille pitää jotain tehdä niin sitten taas lähtee viesti, meidän prosessien mukaan tukikeskukseen, joka on myös ulkoistettu tai hankittu ulkopuolelta palveluna. Ja he sitten organisoivat sitä eteenpäin. (Haastateltava 3)

Tietoaineistojen elinkaaren aikaisen tietoturvallisuuden osalta kunnissa ilmeni erilaisia epävarmuustekijöitä. Epävarmuustekijät liittyivät pääosin työntekijöiden tietoturvallisuuskäyttäytymiseen, mitä kunnissa ei tietoturva-koulutuksista huolimatta täysin pystytä takaamaan. Kaikista kunnilla käytössä olevista tietojärjestelmistä ei ole mahdollista kerätä lokitietoja, mikä osaltaan vaikeuttaa tietoaineistojen väärinkäytön havaitsemista.

Tietojenkäsittelyyn (2) kohdistuvaa riskiarviointeja suoritetaan yhtä kuntaa lukuun ottamatta vuosittain. Yhdessä tutkimukseen osallistuneessa kunnassa tietojenkäsittelyyn kohdistuvaa riskiarviointia tehdään seudullisena yhteistyönä jatkuvasti ja nouseviin riskeihin pyritään reagoimaan välittömästi. Tietojenkäsit-

telyyn kohdistuvan riskiarvioinnin käytänteet vaihtelevat kuntakohtaisesti suuresti, eikä kuntia yhdistäviä tekijöitä riskiarviointeihin liittyen juurikaan ole. Riskiarviointeihin liittyvissä käytänteissä on suurimmassa osassa tutkimuksen kunnista vielä kehitettävää.

Pienien ja keskisuurien kuntien (3) käytännöt tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden testaamisessa vaihtelevat. Tietojärjestelmien ja toiminnan jatkuvuuden varmistaminen tapahtuu pääosin tuotannossa, ilman varsinaista vikasietoisuuden testausta:

> Toki tämmöinen tulee tuotannossa testattua niin kuin jatkuvasti. Että esimerkiksi nyt, kun alkoi tämä korona kriisi, niin meidän vpn-käyttäjien määrä on yli kymmenkertaistunut. Niin kuin parissa kolmessa päivässä. Niin silloin tuli heti pullonkaulat vastaan siinä ja meillä oli suunnitelmat, mitä sitten tehdään ja ne kyllä onnistuivat eli se kosketti kaikkia käyttäjiä, että se oli hidasta tai ei niin kuin onnistunut kirjautumiset jonkin aikaa, mutta siitä päästiin kyllä toipumaan. (Haastateltava 3)

Yksi tutkimukseen osallistuneista haastateltavista kertoi tietojärjestelmien jatkuvuuden testaamisen olevan kunnassaan säännöllistä erilaisten valtakunnallisten, maakunnallisten ja paikallisten harjoituksien kautta:

> Testausta suoritetaan säännöllisesti, elikkä meillä on ihan tämmöisiä valtakunnallisen tason, sitten on maakunnallisen tason ja sitten voi olla paikallisen tason harjoituksia, jossa me testataan, aina keskittyen tietenkin johonkin pääasiaan. Mutta kyllähän niissä tietysti aina joka kerta on digiturvallisuus ja digijatkuvuus aina ilman muuta mukana ja harjoitukset on ollut myös erittäin hyödyllisiä, että kyllä me on niitten kautta löydetty, että mitä puutteita meillä on ja missä pitää vielä ryhdistäytyä. (Haastateltava 1)

Kaikille tutkimukseen osallistuneille kunnille yhdistävänä tekijänä haastatteluiden perusteella oli työntekijöiden sitoutuminen tietojärjestelmien ja toiminnallisen käytettävyyden jatkuvuuden takaamiseen. Pienien ja keskisuurien kuntien vähäiset henkilöresurssit on saatu venymään äärimmilleen koronapandemian aiheuttamien muutostarpeiden toteuttamiseksi kaikissa tutkimuksen kunnissa.

Tutkimukseen osallistuneissa kunnissa on kaikissa (4) käytössä asianhallintajärjestelmät, jotka mahdollistavat julkisten asiakirjojen ja päätösten suoran julkaisun asianhallintajärjestelmästä.

> …meillä asianhallintajärjestelmä automaattisesti, tai ainakin suhteellisen automaattisesti julkaise nämä tuota, tai on ainakin suunniteltu siihen suuntaan, että pystytään julkaisemaan. (Haastateltava 2)

Asianhallintajärjestelmän ulkopuolisten, eri toimialojen, asiakirjojen osalta vastaavanlaisia julkaisujärjestelmiä ei ole käytössä. Näistä järjestelmistä asiakirjojen julkaiseminen vaatii vielä tällä hetkellä enemmän vaivannäköä.

> …mutta toimialojen omissa järjestelmissä aika vähän on varmaa sellaisia piirteitä niin kuin ohjelmistotoimittajillakaan, että sieltä suoraan, että siinä varmaan käsityötä aika paljon on sitten, mistä otetaan liitteitä tai karttoja tai muuta. (Haastateltava 1)

Kuntien käytössä olevat tietojärjestelmät ja tietovarantojen tietorakenteet tukevat siis ainakin osittain asiakirjojen julkisuuden vaivatonta toteuttamista.

Tietojärjestelmien hankintoihin (5) liittyvässä tietoturvallisuuden varmistamisessa on kuntien välisissä käytännöissä eroja. Pienissä kunnissa tietojärjestelmien tietoturvallisuutta ei ole huomioitu sopimuksissa yhtäläisellä tavalla kuin keskisuurissa kunnissa. Keskisuurissa kunnissa pyritään myös auditoimaan hankittavien tietojärjestelmien tietoturvallisuutta. Pienissä kunnissa vastaavaa auditointia ei hankittaville tietojärjestelmille ole tehty.

7.1.3 **Tietojen siirtäminen tietoverkossa**

Tiedonhallintalain 14 § määrittää tiedonsiirron turvallisen toteutuksen salassa pidettävien tietojen osalta. Lain 14 § mukaan salassa pidettävän tiedon tiedonsiirto täytyy toteuttaa suojattua tiedonsiirtoyhteyttä tai –tapaa käyttämällä yleisessä tietoverkossa.

Pienissä ja keskisuurissa kunnissa hyödynnetään suojattuja tiedonsiirtoyhteyksiä haastatteluiden mukaan laajasti:

> …tiedonsiirrossa käytetään salattuja yhteyksiä ja sitten niitä pyritään vaatimaan, ja käytännössä näin on, että salaamattomia yhteyksiä ei käytetä. (Haastateltava 1)

Erityisesti koronapandemia vauhditti suojattujen tiedonsiirtoyhteyksien kapasiteetin kasvatusta:

> …kun alkoi tämä korona kriisi, niin meidän vpn-käyttäjien määrä on yli kymmen kertaistunut. Niin kuin parissa kolmessa päivässä. Niin silloin tuli heti pullonkaulat vastaan siinä ja meillä oli suunnitelmat, mitä sitten tehdään ja ne kyllä onnistuivat. (Haastateltava 3)

Tutkimuksessa saatujen vastauksien perusteella pienissä ja keskisuurissa kunnissa vaikuttaisivat suojatun tiedonsiirron valmiudet ja kapasiteetti olevan hyvällä tasolla ja vastaavan tiedonhallintalain asettamia vaatimuksia.

7.1.4 **Tietoaineistojen turvallisuuden varmistaminen**

Tiedonhallintalain 15 § mukaan viranomaisen on varmistettava tietoturvallisuustoimenpitein tietoaineistojen turvallisuus. Tietoainestojen turvallisuudessa on huomioitava muun muassa tietoaineistojen muuttumattomuus, alkuperäisyys, ajantasaisuus ja virheettömyys. Lisäksi tietoaineistot on suojattava teknisiltä ja fyysisiltä vahingoilta ja ne on arkistoitava tarvittavilta osin.

Tietoaineistojen turvallisuuden osalta kuntien valmiudet vaihtelivat haastatteluiden perusteella jonkin verran. Kaikissa tutkimukseen osallistuneissa kunnissa ainakin tärkeimmät tietoainestot on pyritty suojaamaan koko elinkaaren ajalta. Tietoaineistojen käsittelyyn on kunnissa tehty perusohjeistus ohjaamaan tietoaineistojen oikeanlaista käsittelyä. Kaikkia tutkimukseen

osallistuneita kuntia yhdisti epävarmuus työntekijöiden tietoturva-käyttäytymisestä liittyen tietoaineistojen käsittelyyn, vaikka ohjeistusta asiaan liittyen onkin tarjolla.

Keskisuurissa kunnissa tietoaineistojen elinkaaren hallintaan ja turvallisuuteen on kiinnitetty pieniä kuntia enemmän huomiota:

> Kyllähän se (tietoturvallisuus) järjestelmien osalta on koko aineiston ajalta määritetty, ja meillähän on tietty TOS malli, eli tiedon ohjaus suunnitelma, missä on sitten määritelty tiedolle elin ajat ja näin. Sähköistä arkistoa ollaan vasta suunnittelemassa, tällaista käyttöarkistoa. (Haastateltava 1)

Keskisuurissa kunnissa tietoaineistojen elinkaaren hallinta ja turvallisuuden varmistaminen tietoturvallisuustoimenpitein on haastattelujen perusteella myös selvästi suunnitelmallisempaa kuin pienissä kunnissa. Keskisuurissa kunnissa oli kiinnitetty huomiota tietoaineistojen arkistointiin, mikä ei käynyt haastatteluissa ilmi pienien kuntien osalta. Pienissä kunnissa saattaa tietojärjestelmien tietoturvantasossa olla myös pieniä puutteita ainakin ei kriittisien tietojärjestelmien osalta.

7.1.5 **Tietojärjestelmien käyttöoikeuksien hallinta**

Tiedonhallintalain 16 § mukaan tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestemän käyttöoikeudet käyttäjän tehtävien mukaan ja ne on pidettävä ajantasaisina.

Tutkimukseen osallistuneissa pienissä kunnissa tietojärjestelmien käyttöoikeuksien hallinta on toteutettu tietojärjestelmäkohtaisesti. Jokaiselle käyttäjälle on luotu erilliset tunnukset jokaiseen työtehtävässä tarvittavaan tietojärjestelmään, joita tietojärjestelmän pääkäyttäjät hallinnoivat.

> …sanotaan että ne ovat ainakin joka sovellukselle erikseen eli mitään yhteistä ad integraatiota esimerkiksi ei ole olemassa, vaan se on joka sovellukseen oma. (Haastateltava 2)

Keskisuurissa kunnissa on pyritty toteuttamaan tietojärjestelmäoikeudet keskitetysti työroolien mukaan. Tietojärjestelmien tunnistus on integroitu keskitetysti ylläpidettyyn tunnistuspalveluun.

> …jos puhutaan näistä yleisistä käyttöoikeuksista, niin vaikka tähän infraan, tai tietokoneille, niin meillä on keskitetty käyttäjähallinta… (Haastateltava 3)

Kunnissa käytössä olevat toimialakohtaiset hallinnolliset järjestelmät eivät kuitenkaan kaikki mahdollista tunnistuksen integroimista keskitettyyn tunnistuspalveluun, mistä syystä tietyissä tietojärjestelmissä on myös keskisuurissa kunnissa edelleen tietojärjestelmäkohtaisia tunnuksia, joita tietojärjestelmien pääkäyttäjät hallinnoivat:

> Ja sitten on olemassa näitä hallinnollisia järjestelmiä, nyt vaikkapa tämä asianhallintajärjestelmä, niin siihen on sitten edelleenkin … niin kuin omat tunnuksensa. Jota hallinnoi sitten sen järjestelmän pääkäyttäjä. Ja se on vähän ongelmallista. Ongelmallista siinä mielessä, että jos hän vaikka lähtee pois töistä, tämä kyseinen käyttäjä, niin silloin miellä on integraatio olemassa henkilöstöjärjestelmiin, että jos käyttäjä poistuu organisaatiosta, niin tunnus lukitaan, että hän ei pääse koneelle kirjautumaan mutta siihen järjestelmään pääsee, koska hänellä on eri tunnukset. (Haastateltava 3)

Kunnissa käytössä olevien tietojärjestelmien käyttöoikeuksien keskitetty, esimerkiksi roolipohjainen, hallinta on vielä tällä hetkellä ongelmallista. Kaikki käytössä olevat toimialakohtaiset tietojärjestelmät eivät tue tunnistuksen integroimista keskitettyyn tunnistuspalveluun. Osassa kunnista ongelma on tiedostettu ja hankittavissa uusissa tietojärjestelmissä tunnistukseen liittyvät vaatimukset huomioidaan osana hankintaprosessia.

7.1.6 **Lokitietojen kerääminen**

Tiedonhallintalain 17 § mukaan viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot.

Pienien ja keskisuurien kuntien lokitietojen kerääminen on tietojärjestelmästä riippuvaa. Kaikki tietojärjestelmät eivät mahdollista lokitietojen keräämistä, mikä vaikeuttaa osaltaan lokitietojen keräämistä. Tutkimukseen osallistuvista kunnista suurimmassa osassa on lokitietojen keräämistä suunniteltu ja toteutettu niistä tietojärjestelmistä, joista se on teknisesti mahdollista toteuttaa. Lokitietojen keräämisen, tallentamisen ja mahdollisen jatkokäsittelyn tärkeys oli tutkimukseen osallistuneista kunnista huomioitu yhtä poikkeusta lukuunottamatta.

> lähtökohtaisesti tämä tietohallintolakihan nyt määrää, että jonkinlaista lokia on kerättävä koko ajan… myös GDPR vaatii, että meidän täytyy tietää, kuka tietoa on käsitellyt. Että se täytyy pystyä todentamaan. Että se on ihan oletuksena, että kaikista järjestelmistä pitää jotakin lokia jäädä. (Haastateltava 3)

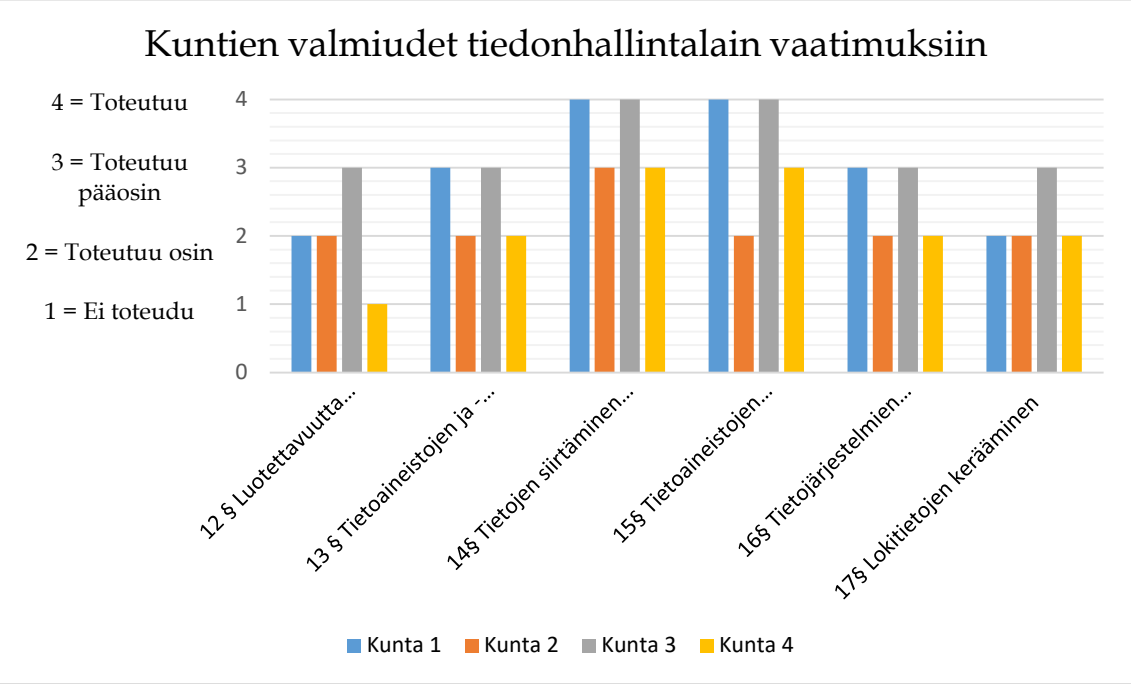
Pienissä ja keskisuurissa kunnissa lokitiedoista kerätään vähintään tietojärjestelmien oletuslokitiedot. Suuressa osassa kunnista lokitietojen kerääminen on suunnitelmallista ja niitä kerätään kaikista tietojärjestelmistä, mistä kerääminen on teknisesti mahdollista.

7.1.7 **Yhteenveto**

Pienien ja keskisuurien kuntien tämän hetkiset valmiudet tiedonhallintalain asettamien vaatimuksien noudattamiseen vaihtelevat suuresti. Suurin osa tiedonhallintalain asettamista vaatimuksista astuu kuntasektorille voimaan vuoden 2023 alusta siirtymäkauden loputtua, joten korjaaviin toimenpiteisiin on vielä aikaa.

Pienissä ja keskisuurissa kunnissa luotettavuutta edellyttävien tehtävien tunnistamisessa ja näissä tehtävissä työskentelevien työntekijöiden luotettavuudesta varmistuminen on vielä työn alla. Tutkimukseen osallistuneista (taulukko 2) kunnista yhdessä luotettavuutta edellyttäviä tehtäviä ei ole tunnistettu eikä työntekijöiden luotettavuutta ole varmistettu. Toisessa tutkimukseen osallistuneessa kunnassa tiedonhallintalain 12 §:n vaatimukset puolestaan toteutuivat pääosin eli kuntien välillä on suurta vaihtelua 12 §:n asettamien vaatimuksien toteuttamisessa.

TAULUKKO 2 Kuntien valmiudet tiedonhallintalain vaatimuksiin



Pienien ja keskisuurien kuntien tietoaineistojen ja tietojärjestelmien tietoturvallisuudesta löytyy myös jonkin verran eroavaisuuksia. Tietojenkäsittelyyn kohdistuvien riskien kartoituksessa ja riskiarvioinnin prosesseissa on vaihtelua kuntien kesken. Osassa kunnista digitaaliseen toimintaympäristöön kohdistuvia riskiarvoita tehdään aktiivisesti jatkuvan prosessin omaisesti, kun osassa kunnista riskiarvioita tehdään korkeintaan satunnaisesti. Tietojärjestelmien vikasietoisuutta ja toiminnallista käytettävyyttä testataan kunnissa harvoin. Tietojärjestelmien vikasietoisuuden ja toiminnallisen käytettävyyden testaaminen tapahtuu pääosin erilaisien harjoituksien yhteydessä, joissa digitaalinen toimintaympäristö kuuluu osaksi harjoitusta. Asiakirjojen julkisuuden vaivaton toteutus on pääosin kunnossa kaikissa kunnissa. Asiakirjojen julkisuuden toteuttaminen vaatii hieman enemmän vaivaa ainoastaan tiettyjen kunnallisten toimialojen kohdalta. Hankittavien tietojärjestelmien tietoturvallisuuden varmistamisessa on kuntakohtaisia eroja. Keskisuurissa kunnissa huomioitiin sopimuksissa selkeästi laajemmin tietoturvallisuuteen ja tietosuojaan liittyvät vaatimukset kuin pienissä kunnissa.

Tietojen siirtäminen tietoverkossa tapahtuu pienissä ja keskisuurissa kunnissa pääosin suojattua tiedonsiirtoyhteyttä pitkin. Koronapandemia ja siihen liittyvä etätyöskentelyn tarpeellisuus ovat parantaneet kuntien suojatun tiedonsiirtoyhteyden kapasiteettia ja käyttömahdollisuuksia.

Tietoaineistojen turvallisuuden varmistamisen taso vaihtelee pienissä ja keskisuurissa kunnissa. Kriittiset tietoaineistot on kaikissa kunnissa varmistettu ja suojaukset teknisiltä ja fyysisiltä vahingolta ovat pääosin kunnossa. Keskisuurissa kunnissa on edellisten lisäksi olemassa myös suunnitelmat tiedon ohjaukselle ja tietoaineistojen arkistoinnille. Suurimmat epävarmuustekijät tietoaineistojen turvallisuudelle kunnissa liittyvät henkilöstön tietoturvallisuuskäyttäytymiseen ja vanhempien tietojärjestelmien puutteisiin lokitietojen keräämisessä.

Tietojärjestelmien käyttöoikeuksien hallinnan toteutukset ja niihin liittyvät prosessit eroavat pienien ja keskisuurien kuntien välillä. Pienissä kunnissa tietojärjestelmien käyttäjätunnukset ja niihin liittyvät käyttöoikeudet määritetään järjestelmäkohtaisesti. Keskisuurissa kunnissa käyttöoikeudet määräytyvät pääasiallisesti roolipohjaisesti keskitetystä tunnistuspalvelusta. Pienissä kunnissa tietojärjestelmien käyttöoikeuksien hallinta on yhden työntekijän vastuulla, mikä koettiin myös epävarmuustekijäksi hallinnoinnin kannalta.

Lokitietojen kerääminen osasta, tällä hetkellä kunnissa käytössä olevista, tietojärjestelmistä on teknisesti vaikeaa. Tietojärjestelmistä, jotka mahdollistavat lokitietojen keräämisen, kerätään kunnissa ainakin oletuslokitiedot. Yhdessä tutkimukseen osallistuneessa kunnassa lokitietoja kerättiin järjestelmällisesti ja niitä hyödynnettiin tietojärjestelmien tarkkailussa suunnitelmallisesti.

7.2 Kuntien digitaalinen turvallisuus

Tässä aliluvussa esitellään tutkimuksen tuloksia kuntien digitaalisen turvallisuuden näkökulmasta. Tulokset esitellään digitaalisen turvallisuuden osa-alueittain. Lisäksi tässä aliluvussa esitellään tutkimuksen esiin nostamat haasteet digitaalisen turvallisuuden toteuttamiselle sekä digitaalisen turvallisuuden ohjaukseen liittyvät tutkimustulokset.

7.2.1 **Digitaaliseen turvallisuuteen liittyvät haasteet**

Tutkimuksessa kuntien esiin nostamat digitaaliseen turvallisuuteen kohdistuvat haasteet ovat kaikissa kunnissa resursseihin liittyviä sekä käyttäjien tietoturvakäyttäytymiseen liittyviä haasteita. Käyttäjille oli tarjolla ohjeistusta oikeanlaiseen, tietoturvalliseen käyttäytymiseen mutta siitä huolimatta tietoturvakäyttäytyminen koettiin ongelmaksi tutkimukseen osallistuneissa kunnissa.

> …on myös se, että nämä meidän omat käyttäjät, että me ollaan kyllä koulutettu meidän henkilökuntaa mutta silti minä väitän, että meidän henkilökunta ei ota kovin vakavasti tätä, niin kuin digiturvallisuus kysymystä, että niitä kyllä ympärillä sattuu ja tapahtuu, mutta kun ei osu ihan kohdilleen, niin ei oteta niin vakavasti. (Haastateltava 2)

Kunnissa on tarjottu henkilökunnalle ohjeistuksien lisäksi myös tietoturvaan liittyviä koulutuksia tietoturvatietoisuuden ja tietoturvakäyttäytymisen parantamiseksi. Yhdessä tutkimukseen osallistuneessa kunnassa oli mietitty edellä mainittujen toimenpiteiden lisäksi myös sanktioiden käyttöönottoa tietoturvakäyttäytymisen ohjaamiseksi.

Digitaaliseen turvallisuuteen käytettävien resurssien vähyys näkyy kunnissa sekä henkilöstöresurssien että taloudellisten resurssien vähyytenä. Tutkimukseen osallistuneista kunnissa digitaalisesta turvallisuudesta vastaava henkilö huolehtii digitaalisesta turvallisuudesta oman työnsä ohessa eli erillistä digitaaliseen turvallisuuteen keskittynyttä henkilöresurssia ei tutkimukseen osallistuneissa kunnissa ollut.

> …Meillä ei ole paljon henkilöresursseja, tähän niin kuin käyttää. Se on yksi haaste. Kun on ohut resurssi niin tämä ympäristö, digiympäristön hallinta aiheuttaa haasteita siitä johtuen. (Haastateltava 4)

Henkilöresurssien vähyys näkyy erityisesti pienien kuntien toiminnassa, joissa digitaalisen toimintaympäristön ylläpito, kehitys sekä turvallisuus ovat yleensä yhden ihmisen vastuulla. Digitaaliseen turvallisuuteen suunnatut taloudelliset resurssit ovat haastavat kaikissa tutkimukseen osallistuneissa kunnissa. Henkilöstöresurssien lisäksi haasteita on myös digitaaliseen toimintaympäristön turvallisuuteen suunnatuissa taloudellisissa resursseissa.

> …sitten taas toivoisi päättäjiltä, että budjeteista päättäessä saisi ymmärtämään tämän (digitaalinen turvallisuus) tärkeyden. (Haastateltava 3)

Pienissä kunnissa taloudellisten resurssien vähyys näkyy digitaalisen turvallisuuden lisäksi myös jokapäiväisessä digitaalisen toimintaympäristön ylläpidossa. Toimintaympäristön ylläpitäjän sairastuessa ei tutkimukseen osallistuneissa pienissä kunnissa ollut varahenkilöä toimintaympäristön ylläpitoon.

7.2.2 **Digitaaliseen turvallisuuteen sitoutuminen kuntajohdossa**

Kuntajohdon sitoutuminen digitaaliseen turvallisuuteen näkyy periaatteellisella tasolla mutta ei juurikaan digitaalisen turvallisuuden budjetoinnissa. Digitaaliseen turvallisuuteen periaatteellisella tasolla sitoutumisella kuntajohto tarkoittaa, että digitaalisen turvallisuuden tärkeys on ymmärretty mutta mahdollisuudet taloudellisien resurssien suuntaamiseksi siihen ovat vähäiset.

> Me ollaan semmoisella, niin kuin periaatteellisella tasolla sitoutuneita, mutta se näkyy tosi vähän. Se näkyy esimerkiksi näinä koulutuksina, mutta ei tämä ole sellainen aktiivinen teema, enemmänkin siellä taustalla on hyvä myös muistaa, että tästä täytyy pitää hyvää huolta. (Haastateltava 2)

Digitaalisen turvallisuuden resursointia on kunnissa kohdennettu muun muassa tietoturvakoulutuksiin. Tietoturvakoulutuksia on järjestetty kaikissa kunnissa ainakin virkamiesjohdolle mutta erityisesti keskisuurissa kunnissa myös laajasti koko henkilöstölle. Osassa tutkimukseen osallistuneista kunnista tehtiin myös alueellista yhteistyötä digitaalisessa turvallisuudessa, mihin on myös ohjattu taloudellisia resursseja. Alueellisesta yhteistyöstä digitaalisen turvallisuuden osalta on siihen osallistuneissa kunnissa hyviä kokemuksia. Alueellinen yhteistyö koettiin kunnissa myös kustannustehokkaaksi tavaksi parantaa kunnan digitaalista turvallisuutta.

7.2.3 **Jatkuvuuden hallinta ja varautuminen**

Jatkuvuuden hallinnan ja varautumisen suunnittelun ja testaamisen käytänteet vaihtelevat kuntakohtaisesti. Keskisuurissa kunnissa jatkuvuuden hallintaan ja varautumiseen liittyvät suunnitelmat ja käytänteet ovat hyvällä tasolla. Keskisuurissa kunnissa on kriittisten järjestelmien jatkuvuuden varmistamiseksi varauduttu muun muassa toipumissuunnitelmien ja varajärjestelmien muodossa. Pienien kuntien tilanne jatkuvuuden hallinnan ja varautumisen osalta eroaa keskisuurista kunnista. Pienien kuntien jatkuvuuden hallinta ja varautuminen on resurssien vähäisyydestä johtuen heikompaa, ja tilanteisiin joudutaan reagoimaan enemmän tilannekohtaisesti.

Jatkuvuus- ja toipumissuunnitelmien testausta tehdään pienissä ja keskisuurissa kunnissa vähän. Testaamista suoritetaan lähinnä erilaisten varautumisharjoituksien osana, mikäli harjoituksiin sisältyy digitaaliseen turvallisuuteen liittyviä osioita. Pienissä ja keskisuurissa kunnissa on pystytty reagoimaan muuttuviin tilanteisiin kohtalaisen hyvin varautumisen tasosta riippumatta. Kaikissa tutkimuksen kunnissa pystyttiin esimerkiksi reagoimaan tehokkaasti koronapandemian vaatimiin etätyöyhteyksien kapasiteetin kasvattamiseen.

7.2.4 **Tietoturvallisuus**

Pienissä ja keskisuurissa kunnissa on pääosin tietoturvapolitiikat ja tietoturvatavoitteet määritetty. Tutkimukseen osallistuneista kunnista ainoastaan yhdeltä kunnalta puuttuivat tietoturvaan liittyvät tavoitteet ja politiikat. Tietoturvaan liittyvät tavoitteet on myös käsitelty kunnanjohdon toimesta niissä kunnissa, joissa ne on määritetty.

Tietoturvaohjeistukset ovat käytössä kaikissa tutkimuksen kunnissa. Keskisuurissa kunnissa tietoturvaohjeistukset käsittävät yleisien tietoturvaohjeiden lisäksi myös muun muassa mobiililaitteiden sekä sosiaalisen

median käyttöön liittyvää ohjeistusta. Seudullista yhteistyötä digitaalisessa turvallisuudessa tekevissä kunnissa tietoturvaan liittyvät ohjeistukset ovat kattavammat yhteistyön ansiosta.

Pienien ja keskisuurien kuntien sopimuksiin liittyvät tietoturvallisuuskäytänteet vaihtelevat. Pienissä kunnissa tietoturvallisuutta on huomioitu sopimuksissa vain vähän tai ei ollenkaan. Keskisuurissa kunnissa tietoturvallisuuteen liittyvät tekijät on huomioitu sopimuksissa laajemmin ja niissä on huomioitu myös kuntakohtaisia vaatimuksia tietoturvallisuuteen ja yhteensopivuuteen liittyen. Hankittujen tietojärjestelmien tietoturvallisuuden testaus ja auditointi vaihtelevat myös kuntakohtaisesti. Pienissä kunnissa hankittujen tietojärjestelmien tietoturvallisuutta ei ole testattu tai auditoitu. Keskisuurissa kunnissa tietoturvallisuuteen liittyvät ominaisuudet pyritään huomioimaan jo sopimusvaiheessa. Sopimusvaiheen lisäksi tietoturvallisuutta pyritään keskisuurissa kunnissa jollakin tavalla testaamaan tai auditoimaan käyttöönoton jälkeen.

Käyttöoikeuksien ja pääsynhallinta on pienissä kunnissa toteutettu tietojärjestelmäkohtaisesti. Keskisuurissa kunnissa pääsynhallinta ja käyttöoikeuksien hallinta on toteutettu keskitetysti ja roolipohjaisesti niissä tietojärjestelmissä, jotka tukevat vaadittavaa järjestelmäintegraatiota. Kuntasektorin monitoimialaisuus asettaa tietojärjestelmien keskitetylle käyttöoikeuksien ja pääsynhallinnalle haasteita, joita ei pienissä ja keskisuurissa kunnissa vielä ole ratkaistu.

Tietoaineistojen tietoturvallisuuteen on pienissä ja keskisuurissa kunnissa pyritty panostamaan käytössä olevien resurssien ja lain vaatimusten mukaisesti. Tietoaineistojen tietoturvallisuuteen käytössä olevien resurssien suuruus vaikuttaa kuntakohtaisiin käytänteisiin, jotka eroavat suuresti toisistaan. Pienissä kunnissa tietoaineistojen järjestelmäturvallisuuden taso on keskimäärin heikompaa kuin keskisuurissa kunnissa. Keskisuurissa kunnissa tietoainestoille on määritetty tiedonohjaussuunnitelmat, joissa tiedolle on määritetty muun muassa elinajat. Tietoaineistojen järjestelmäturvallisuuden lisäksi kunnissa on ymmärretty myös tietoaineistojen käsittelyyn liittyvät riskit. Suurimmat epävarmuudet tietoaineistojen tietoturvallisuudesta liittyvätkin sekä pienissä että keskisuurissa kunnissa tietoaineistojen asianmukaiseen ja tietoturvalliseen käsittelyyn.

> Tietysti tähän liittyy riskejä, jos joku jostain järjestelmästä kopioi omalle koneelleen, niin käyttäjä on tässäkin sitten se, tavallaan se heikoin lenkki, et jos joku säilöö jotain materiaalia muistitikulla tai omalla koneella, jemmailee jostain mitä saa käsiinsä, sitähän ei voi täysin estää. (Haastateltava 1)

Tietoturvallisuuteen liittyvä tilaturvallisuus on saanut viimeisien vuosien aikana huomiota niin pienissä kuin keskisuurissa kunnissa. Yleisen fyysisen pääsynhallinnan lisäksi kunnissa on huomioitu myös tietoaineistojen tilaturvallisuuteen liittyviä vaatimuksia asianmukaisella tavalla.

7.2.5 **Kyberturvallisuus**

Kyberturvallisuuden toteuttamisessa pienissä ja keskisuurissa kunnissa näkyy ainakin osittain siihen varattujen resurssien pienuus. Keskisuurissa kunnissa tietojärjestelmiin ja tietoliikenteeseen liittyvät käytänteet ovat pieniä kuntia paremmalla tasolla. Pienissäkin kunnissa pyritään tietojärjestelmien haavoittuvuuksiin ja uhkiin reagoimaan aktiivisesti.

Tietojärjestelmien lokitietoja pienissä ja keskisuurissa kunnissa kerätään tietojärjestelmien mahdollistamalla tavalla. Käytettävistä tietojärjestelmistä kaikki eivät kuitenkaan mahdollista lokitietojen keräämistä, joten näistä tietojärjestelmistä ei lokitietoja kerätä.

> Lokien kerääminen on järjestelmästä riippuvainen. Kaikista järjestelmistä ei ole ollut mahdollista kerätä lokitietoja. (Haastateltava 4)

Kyberturvallisuuteen liittyvää tietojärjestelmien ja tietoliikenteen valvontaa suoritetaan tutkimuksen kunnista kahdessa. Turvallisuusvalvonta on molemmissa kunnissa hankittu seudullisena yhteistyönä ulkopuoliselta toimijalta.

Tiedonsiirron turvallisuus on huomioitu kaikissa tutkimukseen osallistuneissa kunnissa ainakin jollakin tasolla. Koronapandemian pakottamana kunnissa on kasvatettu tietoturvallisien yhteyksien kapasiteettia, jonka kautta kunnan tietojärjestelmiä voidaan hyödyntää.

Pienissä ja keskisuurissa kunnissa tietojärjestelmiä ja tietoliikennejärjestelyitä auditoidaan korkeintaan satunnaisesti. Pienissä kunnissa tietojärjestelmien ja tietoliikennejärjestelyiden auditointia ei koettu tarpeelliseksi, mistä syystä niitä ei järjestetty. Keskisuurissa kunnissa auditoinnit koettiin tärkeämmiksi ja niitä järjestettiin satunnaisesti.

7.2.6 **Tietosuoja**

Tutkimukseen osallistuneista kunnista kaikkiin on nimetty tietosuojasta vastaava henkilö. Tietosuojasta vastaavista henkilöistä osa toimii tietosuojavastaavan tehtävässä oman varsinaisen toimensa ohessa. Tietosuojavastaavan työhön liittyvät vastuut on myös määritetty kaikissa tutkimukseen osallistuneissa kunnissa. Osassa kunnista on myös perustettu tietosuojaryhmä pohtimaan tietosuojaan liittyviä asioita. Lisäksi osassa tutkimukseen osallistuneista kunnista tehdään tietosuojaan liittyvissä asioissa seudullista yhteistyötä:

> …tietosuojavastaavat kokoontuu myös säännöllisesti. Eli on tämmöinenkin rakenne olevassa, missä jaetaan sitten niitä oppeja ja muuta eli tämä on vähän niin kuin tämmöinen communities of practice, myös tällä saralla. (Haastateltava 3)

Luotettavuutta vaativien tehtävien tunnistaminen vaihtelee tutkimukseen osallistuneissa kunnissa. Keskisuurissa kunnissa luotettavuutta edellyttävien

tehtävien tunnistaminen on haastatteluiden perusteella hieman paremmalla tasolla, joskin työntekijöiden luotettavuuden varmistaminen on ainakin osittain myös keskisuurissa kunnissa tekemättä.

Tietosuojakoulutusta on annettu kaikissa tutkimukseen osallistuneissa kunnissa, pois lukien yksi kunta, jossa tietosuojaan liittyvät asiakokonaisuudet ovat vasta suunnitteluasteella. Tietosuojakoulutusta on pidetty keskisuurissa kunnissa laajasti koko henkilökunnan käsittäen.

> Kaikki on koulutettu läpi, eli tietosuojavastaava on käynyt läpi joka ikisin toimialan, kaikki henkilöt sikäli, kun ovat olleet paikalla, mutta meillä on tietty testi tehty tietosuoja asioista jokaiselle työntekijälle eli meillä on tietosuojamalli käytössä. (Haastateltava 1)

Pienissä kunnissa tietosuojakoulutusta ei ole tarjottu tai se on kohdennettu ainoastaan pienelle henkilötietoja käsittelevälle ryhmälle.

7.2.7 **Riskienhallinta**

Riskienhallintaa käsitellään seuraavassa 7.3 aliluvussa.

7.2.8 **Yhteenveto**

Pienien ja keskisuurien kuntien digitaalisessa turvallisuudessa on vielä kehitettävää. Suurimmat pienien ja keskisuurien kuntien digitaalista turvallisuutta koskevat haasteet liittyvät käytettävissä olevien taloudellisten ja henkilöstöresurssien vähyyteen sekä henkilökunnan tietoturvakäyttäytymiseen. Edellä mainittujen haasteiden lisäksi pienissä ja keskisuurissa kunnissa on kunnasta riippuen kehitettävää myös muilla digitaalisen turvallisuuden osa-alueilla. Keskisuurien kuntien digitaalisen turvallisuuden kokonaistilanne on keskimäärin pieniä kuntia parempi. Seudullisesta yhteistyöstä digitaaliseen turvallisuuteen liittyen vaikuttaisi olevan hyötyä siihen osallistuville kunnille, kuntakoosta riippumatta.

7.3 Riskienhallinta kuntien digitaalisessa turvallisuudessa

Digitaalisen riskienhallinnan prosessit ja käytänteet erovat toisistaan monella tavalla kuntien välillä. Tässä aliluvussa esitellään tutkimuksen tuloksia kuntien digitaalisen riskienhallinnan näkökulmasta.

7.3.1 **Riskienhallinnan periaatteet ja tavoitteet**

Pienistä ja keskisuurista kunnista on suurimmassa osassa määritetty digitaalisen turvallisuuden riskienhallinnalle tavoitteet ja periaatteet. Pienissä kunnissa

riskienhallintaan on asetettu periaatteet ja tavoitteet vasta viime vuosien aikana tai ne on vielä asettamatta.

> meidän päätökset, meillä ei ole mitään, tämä on niin pieni organisaatio, ettei meillä ole mitään tietohallintopolitiikkaohjelmaa, että kyllä tämä on hyvin arkista askartelua meillä, niin ehkä meillä ei ole, kun kysyt tuolla tasolla. Että meillä ei ole tuota tasoa olemassa. (Haastateltava 2)

Keskisuurissa kunnissa tilanne on keskimäärin huomattavasti parempi kuin pienissä kunnissa. Digitaaliselle turvallisuudelle on määritetty selkeät periaatteet ja tavoitteet, jotka on käsitelty ja hyväksytty kunnan päättävissä elimissä. Keskisuurissa kunnissa digitaalisen turvallisuuden periaatteet ja tavoitteet noudattavat lainsäädännön asettamia vaatimuksia.

> …se, että pitää pystyä kuntien tekemään ne lainsäädännön määräämät tehtävät, sehän se on niin kuin mikä sen sanelee, plus sitten, että täytyy noudattaa lakeja niin kuin hyvää tietohallintotapaa… (Haastateltava 3)

Riskienhallinnan periaatteiden ja tavoitteiden määrittämisen toteutukset vaihtelevat kunnittain. Osassa pienissä ja keskisuurissa kunnissa hyödynnetään riskienhallinnassa seudullista yhteistyötä, joka näyttää parantavan myös riskienhallinnan tehokkuutta.

7.3.2 **Riskihallinta ja johtaminen**

Digitaalisten riskienhallinnan prosessit ja käytänteet eroavat toisistaan tutkimukseen osallistuneiden kuntien välillä. Kaikissa kunnissa käsitellään digitaalista riskienhallintaa strategisella tasolla vähintään pintapuolisesti, mutta sen vaatimat toimenpiteet eivät kaikissa kunnissa jalkaudu taktiselle tai operatiiviselle tasolle.

> …varsinaisesti tosi kattavaa riskikartoitusta me ei olla tehty. Me tehdään parasta aikaa meidän valmiussuunnitelman yleistä osaa, siinä on kyllä määritetty niin kuin ylätasolla erilaisia uhkakuvia, uhka mahdollisuuksia, joista yksi on tämä digitaalinen haitta tai –hyökkäys, miten sen nyt haluaakin sanoa. Mutta joo, ei meillä ole mitään semmoista manuaalia, josta katsotaan, että tässä on meidän riskikartoitus ja sitten tavallaan heijastumisvaikutukset. (Haastateltava 2)

Toimenpiteiden ja resurssien puute näkyy esimerkiksi siten, että yhdessäkään tutkimukseen osallistuneista kunnista ei ole omaa digitaalisen turvallisuuden asiantuntijaa kunnan henkilöstössä. Digitaalista turvallisuutta pyritäänkin pienissä ja keskisuurissa kunnissa hoitaman oman varsinaisen toimen ohessa tai seudullisena yhteistyönä, jolloin henkilöresurssi jakautuu usean kunnan kesken.

> kyllä varmaan jossain … tehtävän kuvauksessa saattaa olla jokin sivulause olla tämmöisestä kokonaisesta tietohallinnoinnista mutta kyllä vastuuta on hajautettu käyttäjille asti, ja levitetty sitä, että jokaisella on se vastuu. Varmaan tässä voitaisiin olla paljon selkeämpiä ja suoraan sanottuna ryhdikkäämpiäkin. (Haastateltava 1)

Kaikissa tutkimukseen osallistuneista kunnista on pyritty ylläpitämään valmius-, varautumis- tai jatkuvuussuunnitelmia kunnan kriittisten palveluiden ylläpitämiseksi normaaliolojen häiriötilanteissa ja poikkeusoloissa. Suurimmassa osassa kunnista digitaalinen riskienhallinta huomioidaan johtamisessa yleisen kuntastrategian lisäksi myös toimialakohtaisesti.

> …sitä hyödynnetään sillä tavalla, että kun tehdään näitä korkeamman tason suunnitelmia, lähtien kuntastrategioista, toimialojen strategioihin ja toimintaohjelmiin, joka vuotisiin talousarvioihin, toimintasuunnitelmiin niin näissähän näitä asioita otetaan tietysti huomioon. (Haastateltava 1)

Seudullinen yhteistyö digitaalisessa turvallisuudessa vaikuttaisi tutkimuksen mukaan edesauttavan digitaalisen turvallisuuden riskienhallinnan strategisen tason lisäksi myös riskienhallinnan taktista ja operatiivista tasoa.

7.3.3 **Riskiarvioinnit kunnissa**

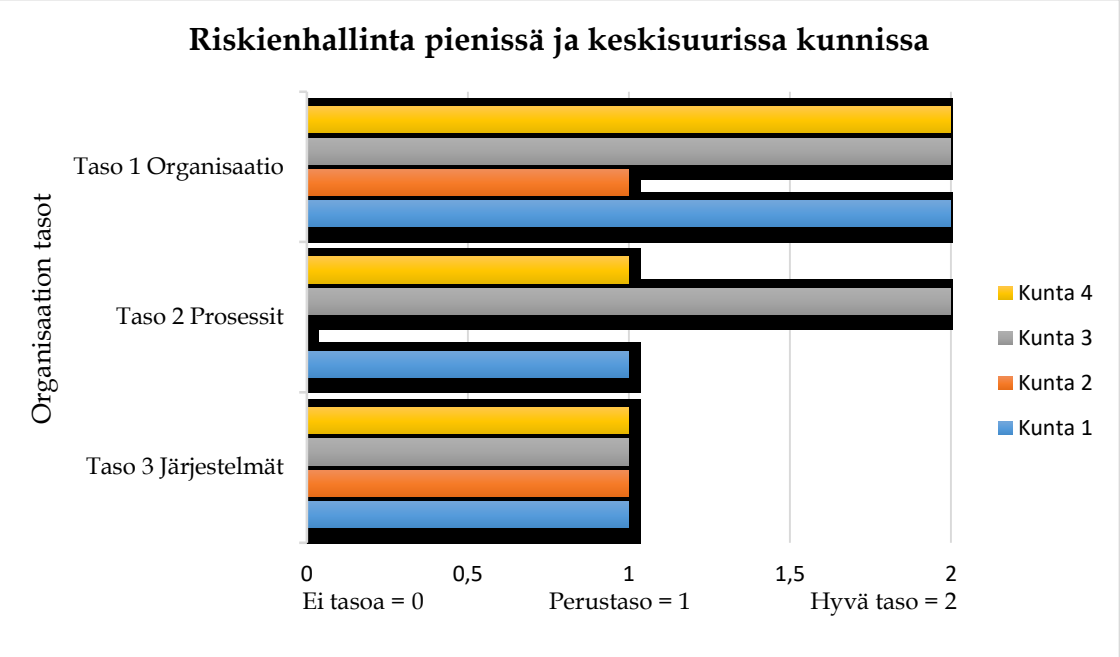
Riskiarviointien suorittaminen vaihtelee pienissä ja keskisuurissa kunnissa suuresti. Pienissä kunnissa riskiarviointien teko vaihtelee satunnaisista arvioinneista vuosittaisiin arviointeihin. Keskisuurissa kunnissa riskiarviointeja tehdään vähintään vuosittain mutta myös jatkuvaluonteisesti. Riskiarviointien suorittamiseen vaikuttaa tutkimuksen mukaan se, millä tavalla kunnassa on organisoitu digitaalisen turvallisuuden toiminnot ja tehdäänkö kunnissa seudullista yhteistyötä muiden kuntien kanssa.

Riskiarviointien prosessi vaihtelee myös kuntakohtaisesti. Kunnissa, joissa riskiarviointeja suoritetaan vähintään vuosittain, on niiden tekeminen sidoksissa kunnan muihin prosesseihin. Digitaaliseen turvallisuuteen liittyvää seudullista yhteistyötä tekevissä kunnissa riskiarviointeja suoritetaan enemmän kuin kunnissa, joissa yhteistyötä ei tehdä.

7.3.4 **Yhteenveto**

Digitaalisen turvallisuuden riskienhallinnan periaatteet, johtaminen ja muut riskienhallinnan käytänteet vaihtelevat kunnittain. Useammassa tutkimukseen osallistuneista kunnista riskienhallintaan (taulukko 4) liittyvät prosessit ovat vähintään perustasolla eli niitä käsitellään kaikilla organisaation tasoilla. Kaikissa pienissä ja keskisuurissa kunnissa digitaalisen turvallisuuden riskienhallintaa käsitellään organisaatiotasolla eli organisaation johdossa. Strateginen riskienhallinta ei kuitenkaan heijastunut digitaalisen turvallisuuden resursseihin, mikä näkyy resurssipulana sekä (kuvio 8) toiminnan prosessit ja tietojärjestelmät tasoilla.

TAULUKKO 3 Riskienhallinta pienissä ja keskisuurissa kunnissa



Digitaaliseen turvallisuuteen liittyviä riskiarviointeja tehdään keskisuurissa kunnissa useammin kuin pienissä kunnissa. Keskisuurissa kunnissa riskiarvioinnit ja digitaalisen turvallisuuden riskienhallinta ovat myös kiinteämmin osa tietohallinnon toimintaa. Kuntien välinen seudullinen yhteistyö digitaalisessa turvallisuudessa vaikutti lisäävästi myös riskienhallintaan liittyviin toimenpiteisiin.

8 JOHTOPÄÄTÖKSET JA POHDINTA

Tässä luvussa käsitellään tutkimuksen tuloksia tutkimuskysymyksiin nähden. Tutkimuksen tuloksista tehdään johtopäätökset, minkä jälkeen pohditaan tutkimustuloksia olemassa olevaan tutkimustietoon nähden sekä sitä, mitkä asiat tuloksiin ovat vaikuttaneet.

8.1 Digitaalisen turvallisuuden tilanne pienissä ja keskisuurissa kunnissa

Tässä aliluvussa tehdään digitaalisen turvallisuuden osa-alueittain johtopäätökset ja pohditaan pienien ja keskisuurien kuntien digitaaliseen turvallisuuden tilanteeseen liittyviä tutkimustuloksia olemassa olevaan tutkimustietoon nähden.

Digitaalisen turvallisuuden eri osa-alueiden tilanteet pienissä ja keskisuurissa kunnissa vaihtelevat suuresti. Kaikissa tutkimukseen osallistuneissa kunnissa suurimmat tunnistetut haasteet liittyvät henkilöstön tietoturvakäyttäytymiseen ja digitaalisen turvallisuuteen käytettävissä oleviin henkilöstö- ja taloudellisiin resursseihin. Henkilöstö- ja taloudellisten resurssien ohjauksesta digitaaliseen turvallisuuteen vastaa muun muassa ISO/IEC- (International Organization for Standardization, 2013c) ja NIST-standardien (National Institute of Standards and Technology, 2011) mukaan organisaation johto eli kuntasektorilla kuntajohto. Kuntajohdossa digitaalisen turvallisuuden vähäinen resurssitilanne on havaittu mutta mahdollisuuksia sen lisäämiseen ei pienissä ja keskisuurissa kunnissa resurssitilanteesta johtuen tällä hetkellä ole. Henkilöstön tietoturvatietoisuutta ja –käyttäytymistä on pienissä ja keskisuurissa kunnissa pyritty parantamaan tietoturvakoulutuksilla ja ohjeistuksilla. Suoritetuista toimenpiteistä huolimatta kunnissa tunnetaan epävarmuutta asian suhteen. Henkilöstöön liittyvät epävarmuudet täytyykin huomioida organisaation tietoturvanhallinnassa (Nazareth & Choi, 2015; Soomro ym., 2016) riittävän tietoturvatason varmistamiseksi. Kuntien henkilöstön tietoturvakäyttäytymiseen liittyviä epävarmuustekijöitä aiheuttavat kuntien toiminnan monialaisuudesta johtuvan seurannan vaikeus sekä tietojärjestelmien lokien keräämiseen liittyvät haasteet.

Pienien ja keskisuurien kuntien kuntajohto on tutkimuksen kunnissa periaatteellisella tasolla sitoutunut digitaaliseen turvallisuuteen kuntien toiminnassa. Taloudellisten resurssien vähäisyys heijastuu kuitenkin voimakkaasti digitaalisen turvallisuuden kaikille muille toiminnan tasoille tutkimukseen osallistuneissa kunnissa. Erityisesti pienissä kunnissa henkilöresurssien vajaus näkyy digitaalisen turvallisuuden kehittämisen lisäksi myös tietohallinnon operatiivisella tasolla. Tutkimukseen osallistuneissa kunnissa on digitaalisen turvallisuuden resursseja ohjattu henkilöstön

tietoturvatietoisuuden lisäämiseen. Henkilöstön tietoturvatietoisuuden ja -käyttäytymisen varmistaminen onkin organisaation näkökulmasta tärkeää (Nazareth & Choi, 2015).

Osassa tutkimukseen osallistuneista kunnista tehdään seudullista yhteistyötä digitaalisen turvallisuuden kehittämiseen liittyen. Alueellisesta yhteistyöstä saadut kokemukset ovat niihin osallistuneissa kunnissa myönteisiä, ja sen koetaan olevan kustannustehokas tapa parantaa kunnan digitaalista turvallisuutta.

Jatkuvuuden hallintaan ja varautumiseen liittyvät käytänteet vaihtelevat tutkimustuloksien mukaan kuntakohtaisesti. Kaikissa tutkimuksen kunnissa on pyritty toteuttamaan lainsäädännön (Valmiuslaki 1552/2011) edellyttämät valmiussuunnitelmat takaamaan elintärkeiden toimintojen jatkuvuus eri tilanteissa. Tarkemmat jatkuvuuden hallintaan ja varautumiseen liittyvät suunnitelmat ja käytänteet ovat keskisuurissa kunnissa hyvällä tasolla (Swanson ym., 2010). Pienissä kunnissa jatkuvuuden hallinta ja varautuminen ovat keskisuuria kuntia huonommalla tasolla. Pienien kuntien jatkuvuuden hallinta on keskisuuria kuntia enemmän nouseviin tilanteisiin reagoimista kuin proaktiivista varautumista. Jatkuvuus- ja toipumissuunnitelmien testausta ei suoriteta tutkimustiedon (Niemimaa & Järveläinen, 2013) edellyttämällä tavalla pienissä eikä keskisuurissa kunnissa riittävästi. Jatkuvuuden ja varautumisen testaaminen tapahtuu pääosin erilaisten varautumisharjoituksien osana, mikäli harjoituksiin sisältyy jatkuvuuden varmistamiseen liittyviä osioita. Vähäisestä testaamisesta riippumatta, on pienissä ja keskisuurissa kunnissa pystytty reagoimaan muuttuviin tilanteisiin hyvin. Tämä reagointinopeus näkyi esimerkiksi etätyöyhteyksien nopeana kapasiteetin kasvattamisena koronapandemian yhteydessä.

Tietoturvapolitiikat ja tietoturvatavoitteet ovat määritetty lähes kaikissa tutkimukseen osallistuneissa kunnissa. Näissä kunnissa tietoturvatavoitteet on myös käsitelty ja hyväksytty kunnanjohdon toimesta. Tietoturvapolitiikat ja -tavoitteet toimivat pohjana koko tietoturvallisuuden määrityksessä, mistä syystä niiden määritys on organisaation kannalta tärkeää (Humphreys, 2008).

Kaikissa tutkimuksen kunnissa on käytössä tietoturvaohjeistukset, joilla pyritään ohjaamaan henkilöstön tietoturvakäyttäytymistä tietoturvallisempaan suuntaan (Nazareth & Choi, 2015). Ohjeistukset käsittävät yleisien tietoturvaohjeiden lisäksi myös esimerkiksi mobiililaitteiden ja sosiaalisen median käyttöön liittyvää ohjeistusta. Seudullinen yhteistyö mahdollistaa tutkimustulosten mukaan myös tietoturvaohjeistuksien suuremman kattavuuden lisääntyneiden henkilöresurssien myötä.

Tietoturvallisuuden huomioiminen sopimuksiin liittyen on keskisuurissa kunnissa paremmalla tasolla kuin pienissä kunnissa. Pienissä kunnissa ei sopimuksissa välttämättä huomioida tietoturvallisuuteen liittyviä tekijöitä laisinkaan. Keskisuurissa kunnissa sopimuksissa huomioidaan tietoturvallisuuden lisäksi myös järjestelmien yhteensopivuus muiden kunnan käytössä olevien tietojärjestelmien kanssa. Keskisuurissa kunnissa testataan ja auditoidaan hankittuja järjestelmiä myös hieman pieniä kuntia enemmän, joskin

testausta ja auditointeja ei suoriteta riittävän järjestelmällisesti keskisuurissakaan kunnissa. Tietoturvallisuuden huomioiminen sopimuksissa sekä hankittujen järjestelmien tietoturvallisuuden testaamisella ja riittävien hallintakeinojen käyttöönotolla voidaan vaikuttaa organisaation tietoaineistojen tietoturvallisuuteen (Humphreys, 2008). Näihin asioihin tuleekin kiinnittää enemmän huomiota keskisuurissa ja erityisesti pienissä kunnissa tietoaineistojen tietoturvallisuuden takaamiseksi.

Tietoturvallisuuteen liittyvä käyttöoikeuksien ja pääsynhallinta on pienissä kunnissa toteutettu tietojärjestelmäkohtaisesti. Keskisuurissa kunnissa pääsynhallinta ja käyttöoikeuksien hallinta on toteutettu keskitetysti ja roolipohjaisesti niissä tietojärjestelmissä, jotka tukevat sitä. Kuntien monitoimialaisuus ja vähäiset henkilöstö- ja taloudelliset resurssit asettavat käyttöoikeuksien ja pääsynhallinnalle haasteita, jotka ovat ainakin vielä osin ratkaisematta. Tietoturvaperiaatteista esimerkiksi vähimpien oikeuksien periaatetta on vaikea valvoa, jos käyttöoikeuksia ei ole sidottu työrooliin (Grance ym., 2003). Digitaalisen toimintaympäristön yhteensopivuuteen tulee kunnissa kiinnittää entistä enemmän huomiota, jotta käyttöoikeuksien ja pääsynhallinnan haasteet saadaan ratkaistua.

Tietoaineistojen tietoturvallisuuteen on tutkimuksen kunnissa pyritty panostamaan käytettävissä olevien resurssien ja lainsäädännön vaatimusten mukaisesti. Kuntakohtaiset käytänteet tietoaineistojen tietoturvallisuuden osalta eroavat käytössä olevien resurssien mukaan. Keskisuurissa kunnissa on tietoaineistojen tietoturvallisuudenkin osalta pieniä kuntia parempi tilanne. Keskisuurissa kunnissa tietoaineistoille on määritetty tiedonohjaussuunnitelmat, jotka parantavat osaltaan tietoaineistojen hallintaa ja siten myös tietoturvallisuutta. Tietoaineistoihin liittyvän järjestelmäturvallisuuden lisäksi kunnissa on huomioitu myös tietoaineistojen käsittelyyn liittyvät riskit, jotka muodostavatkin suurimmat epävarmuudet tietoaineistojen tietoturvallisuuteen liittyen. Tietoaineistojen tietoturvallisuuden hallinnassa, kuten koko organisaation tietoturvanhallinnassa, tuleekin huomioida organisaation kaikki työntekijät (Soomro ym., 2016). Tietoaineistojen tietoturvallisuuden osalta on erityisesti pienissä kunnissa vielä kehitettävää. Tietoaineistojen tietoturvalliseen säilytykseen ja käsittelyyn tulee kiinnittää nykyistä enemmän huomiota tietoturvallisuuden takaamiseksi.

Tilaturvallisuuteen on pienissä ja keskisuurissa kunnissa kiinnitetty viime vuosien aikana entistä enemmän huomiota. Yleisen fyysisen pääsynhallinnan lisäksi kunnissa on huomioitu myös tietoaineistojen tilaturvallisuuteen liittyviä vaatimuksia (Chapple ym., 2018). Tutkimuksen tuloksien perusteella tilaturvallisuuteen liittyvät käytänteet vaikuttaisivat olevan kohtalaisen hyvin hoidettu pienissä ja keskisuurissa kunnissa.

Kyberturvallisuuden käytännön toteutuksissa pienissä ja keskisuurissa kunnissa näkyy siihen käytössä olevien resurssien vähyys. Keskisuurissa kunnissa tietojärjestelmiin ja –liikenteeseen liittyvät turvallisuuskäytänteet ovat erityisesti teknisien ja hallinnollisien hallintakeinojen osalta (D'Arcy & Herath, 2011) pieniä kuntia paremmalla tasolla. Keskisuurien kuntien

kyberturvallisuuteen suunnatut resurssit ja niihin liittyvä organisointi ovat pieniä kuntia paremmalla tasolla, mikä näkyy käytännön tasolla usealla eri tavalla. Keskisuurissa kunnissa on esimerkiksi tietojärjestelmien ja tietoliikenteen hallinta sekä niiden valvonta organisoitu tehokkaasti resursseihin nähden. Tutkimusaineisto ja tutkimustulokset tarjoavat ainoastaan suuntaa antavia tuloksia kyberturvallisuustilanteesta ja siihen liittyvistä käytänteistä pienissä ja keskisuurissa kunnissa. Näiden perusteella keskisuurissa kunnissa on kyberturvallisuuden kokonaistilanne pieniä kuntia paremmalla tasolla.

Tietosuojan ja siihen liittyvien lainsäädännöllisien vaatimuksien toteuttamisen osalta kuntien välillä on suuria eroja. Kaikissa tutkimukseen osallistuneissa kunnissa on nimetty tietosuojasta vastaava henkilö EU-asetuksen (2016/679) mukaisesti. Tietosuojavastaavan työhön liittyvät vastuut ovat myös määritelty kaikissa tutkimuksen kunnissa. Tietosuojan suunnittelussa ja toteutuksessa on kuntien välillä kuitenkin suuria eroja. Yhdessä tutkimuksen kunnassa tietosuojaan liittyvät asiat olivat vielä käytännöntasolla kokonaisuudessaan suunnittelematta ja toteuttamatta. Toisessa kunnassa puolestaan tietosuojaan liittyvissä asioissa tehdään seudullista yhteistyötä, jossa tietosuojaan liittyvää osaamista ja tietoa jaetaan seudun tietosuojavastaavien kesken säännöllisesti. Keskisuurissa kunnissa tietosuojaan liittyvät asiat on hyvin suunniteltu ja toteutettu. Tutkimustuloksien mukaan kaikissa tutkimuksen kunnissa oli vielä kehitettävää luotettavuutta edellyttävien tehtävien tunnistamisessa ja niissä toimivien työntekijöiden luotettavuuden varmistamisessa.

Digitaalisen turvallisuuden tilanteet pienissä ja keskisuurissa kunnissa vaihtelevat digitaalisen turvallisuuden osa-alueittain suuresti. Pienien kuntien digiturvallisuuden tilanne on keskisuuria kuntia huonommalla tasolla, ja tietyt osa-alueet vaativat kehittämistä jo lainsäädännön asettamien vaatimuksien näkökulmasta. Kuntien taloudellisien resurssien vähäisyys asettaa haasteita digitaalisen turvallisuuden kehittämiselle. Näihin haasteisiin on pystytty ainakin osittain vastaamaan seudullisen yhteistyön kautta, joka on tarjonnut kustannustehokkaan tavan parantaa digitaalisen turvallisuuden käytänteitä. Keskisuurien kuntien digiturvallisuuden tilanne on kohtalaisen hyvällä tasolla. Keskisuurissa kunnissa on huomioitu kaikki digitaalisen turvallisuuden osa-alueet, vaikka joissakin osa-alueissa on vielä kehitettävää. Keskisuurien kuntien parempaa tilannetta selittävät osittain hieman parempi resurssitilanne tietohallinnossa, mikä on mahdollistanut myös digitaalisen turvallisuuden käytänteiden kehittämisen. Toisena selittävänä tekijänä parempaan digiturvallisuustilanteeseen on tietohallinnon taktisen-/prosessitason olemassa olo, joka osaltaan mahdollistaa tehokkaamman viestinnän kuntajohdon suuntaan sekä digiturvallisuuden kehittämiseen vaadittavan resurssit organisoinnin ja toimivien prosessien kehittämiseen.

8.2 Digitaalisen turvallisuuden riskienhallinnan organisointi ja käytänteet pienissä ja keskisuurissa kunnissa

Tässä aliluvussa tehdään johtopäätökset ja pohditaan pienien ja keskisuurien kuntien digitaalisen turvallisuuden riskienhallinnan organisointiin ja käytänteisiin liittyvistä tutkimustuloksista olemassa olevaan tutkimustietoon nähden.

Digitaalisen turvallisuuden riskienhallinnalle on asetettu suurimmassa osassa tutkimukseen osallistuneista kunnista tavoitteet ja periaatteet, kuten esimerkiksi ISO 27005-standardi määrittää ja Andress & Leary (2017) teoksessaan ohjeistavat. Riskienhallinnan tavoitteiden ja periaatteiden määrityksen osalta keskisuurissa kunnissa on henkilöresursseista johtuen pieniä kuntia parempi tilanne. Keskisuurien kuntien digitaaliselle turvallisuudelle määrittämät periaatteet ja tavoitteet käsitellään ja hyväksytään kunnan päättävissä elimissä. Pienissä kunnissa näin ei aina tapahdu vaan digitaalisen turvallisuuden riskienhallinta käsitellään osittain operatiivisella tasolla riskien ilmaannuttua. Keskisuurien kuntien digitaaliselle turvallisuudelle asettamat vaatimukset noudattavat myös pieniä kuntia tarkemmin lainsäädännön asettamia vaatimuksia.

Seudullinen yhteistyö digitaalisessa turvallisuudessa parantaa riskienhallinnan tehokkuutta sekä pienien että keskisuurien kuntien osalta. Riskienhallinnan tehokkuuden lisääntymiseen seudullisessa yhteistyössä vaikuttavat henkilöresurssien lisääntyminen sekä mahdollisuus hyödyntää digitaaliseen turvallisuuteen perehtyneen asiantuntijan osaamista.

Digitaalisen riskienhallinnan käytänteet ja prosessit eroavat tutkimustuloksien mukaan kuntien välillä. Kaikissa tutkimukseen osallistuneissa kunnissa digitaalista riskienhallintaa käsitellään strategisella tasolla vähintään periaatteellisesti mutta tarvittavat toimenpiteet eivät kaikissa tutkimuksen kunnissa jalkaudu taktiselle ja operatiiviselle tasolle NIST-standardin (kuvio 8) osoittamalla tavalla (National Institute of Standards and Technology, 2011). Pienissä kunnissa riskienhallinnan prosessin vajaavaisuus johtuu ainakin osittain taktisen eli prosesseista vastaavan tason puuttumisesta kunnan tietohallinnosta. Riskienhallinnan strategisen tason toimenpiteiden ja sen myöntämien resurssien puute näkyy tutkimuksen kaikissa kunnissa digitaalisen turvallisuuden henkilöresurssien sekä taloudellisten resurssien puutteena. Tutkimustulosten mukaan ainoastaan yhdessä tutkimukseen osallistuneista kunnista pystytään noudattamaan riskienhallinnan prosessissa Shameli-Shendi ym. (2016) ja ISO 27005-standardin (2013) mukaista riskienhallinnan prosessia. Riskienhallinnan prosessin kehittämisessä on tutkimustulosten mukaan tarvetta suurimmassa osassa pieniä ja keskisuuria kuntia.

Kaikissa tutkimukseen osallistuneissa kunnissa kriittisten palveluiden ylläpito on huomioitu eri tilanteissa valmius-, varautumis- tai jatkuvuussuunnitelmin. Varautumis- ja jatkuvuussuunnitelmia ei kuitenkaan ole testattu tutkimukseen osallistuneissa kunnissa tutkimustiedon (Botha & Von Solms, 2004; Niemimaa & Järveläinen, 2013) mukaisesti käytännön tilanteissa juuri ollenkaan.

Digitaalisen turvallisuuden riskienhallinta on pyritty huomioimaan yleisen kuntastrategian lisäksi myös toimialakohtaisesti suurimmassa osassa tutkimuksen kunnista. Tutkimustuloksien mukaan Fenz ym. (2014) tutkimuksen mukainen riskienhallinnan laajuus ja rajat ovat määriteltynä suurimmassa osassa pienissä ja keskisuurissa kunnissa. Seudullinen yhteistyö digitaalisessa turvallisuudessa vaikutti tutkimustuloksien mukaan tehostavasti riskienhallinnan strategisen tason käytänteiden lisäksi myös taktisen ja operatiivisen tason käytänteisiin.

Digitaaliseen turvallisuuteen liittyvien riskiarviointien käytänteet vaihtelevat kuntakohtaisesti. Keskisuurissa kunnissa suoritetaan riskiarviointeja useammin ja suunnitelmallisemmin kuin pienissä kunnissa. Riskiarviointien prosessiin, frekvenssiin ja muihin käytänteisiin vaikuttavat kunnan digitaalisen turvallisuuden toimintojen organisointi sekä digitaaliseen turvallisuuteen liittyvä seudullinen yhteistyö. Pienissä ja keskisuurissa kunnissa tehdään Shameli-Sendi ym. (2016) ja Fenz ym. (2014) mukaista haavoittuvuuksien ja uhkien tunnistamista aktiivisesti seuraamalla esimerkiksi kyberturvallisuuskeskuksen jakamaa tilannekuvaa.

Tutkimustuloksien mukaan lähes kaikissa tutkimuksen kunnissa on vielä kehitettävää riskienhallinnan organisoinnissa ja käytänteissä. Keskisuurissa kunnissa on digitaalisen turvallisuuden riskienhallinta organisoitu tehokkaammin kuin pienissä kunnissa ja käytänteet ovat vähintään kohtalaisella tasolla. Pienissä kunnissa on digitaalisen turvallisuuden riskienhallinnassa enemmän kehitettävää niin organisoinnin kuin käytänteidenkin osalta.

8.3 Pienien ja keskisuurien kuntien valmiudet laki julkisen hallinnon tiedonhallinnasta (906/2019) tietoturvallisuus vaatimuksiin

Laki julkisen hallinnon tiedonhallinnasta siirtymäkausi kuntasektorin osalta päättyy 1.1.2023, jolloin lain kuntasektoria koskettavat vaatimukset astuvat voimaan. Tässä tutkimuksessa oli tarkoituksena selvittää pienien ja keskisuurien kuntien valmiuksia tiedonhallintalain 4 luvun tietoturvallisuudelle asettamiin vaatimuksiin. Tässä aliluvussa pohditaan pienien ja keskisuurien kuntien tämän hetken valmiuksia toteuttaa lainsäädännön asettamat vaatimukset.

Tiedonhallintalain (906/2019 12 §) mukaan kuntien on tunnistettava luotettavuutta edellyttävät tehtävät sekä varmistettava näissä tehtävissä toimivien henkilöiden luotettavuus. Tutkimusaineiston perusteella pienien ja keskisuurien kuntien valmiudet tiedonhallintalain 12 § asettamiin vaatimuksiin vaihtelivat suuresti. Yhdessä tutkimukseen osallistuneessa kunnassa vaatimukset toteutuivat pääosin, kun toisessa kunnassa luotettavuutta edellyttäviä tehtäviä ei ole tunnistettu lainkaan eikä täten työntekijöiden luotettavuuttakaan ole varmistettu. Luotettavuuden varmistamisen käytänteiden vaihtelut selittyvät ainakin osittain vakiintuneiden

henkilöstöhallinnon prosessien kautta. Myös kuntasektorin resurssien kapeus vaikuttaa osaltaan prosessien kehittämisen mahdollisuuksiin.

Tiedonhallintalain (906/2019 13 §) mukaan kuntien on:

1. varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.
2. Tietojenkäsittelyyn kohdistuvat olennaiset riskit on selvitettävä ja tietoturvallisuustoimenpiteet on mitoitettava riskiarvioinnin mukaisesti.
3. Viranomaisen olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.
4. Viranomaisen tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely on suunniteltava siten, että asiakirjojen julkisuus voidaan toteuttaa vaivatta.
5. Hankittavista tietojärjestelmistä on varmistettava asianmukaiset tietoturvallisuustoimenpiteet.

Tiedonhallintalain 13 § asettamat vaatimukset käsittävät laajasti digitaaliseen turvallisuuteen liittyviä vaatimuksia. Tutkimusaineiston mukaan pienien ja keskisuurien kuntien valmiudet lain asettamiin vaatimuksiin vaihtelevat suuresti. Digitaalisen toimintaympäristön (13 § kohta 1) haavoittuvuuksia ja uhkia seurataan tutkimustulosten mukaan aktiivisesti sekä pienissä että keskisuurissa kunnissa. Toimintaympäristön laajempaa valvontaa suoritettiin seudullisena yhteistyönä kahdessa tutkimukseen osallistuneista kunnissa. Tietoaineistojen tietoturvallisuuden varmistamiseen liittyi kaikissa tutkimuksen kunnissa epävarmuustekijöitä. Tietoaineistojen tietoturvallisuuteen liittyvät epävarmuudet liittyivät pääosin henkilökunnan tietoturvakäyttäytymiseen, jota ei tietoturvakoulutuksista huolimatta pystytä takaamaan. Toisena tietoaineistojen tietoturvallisuuden epävarmuutta lisäävänä tekijänä tutkimustuloksista nousivat esiin tietojärjestelmät, joista ei ole mahdollista kerätä lokitietoja. Lokitietojen puute vaikeuttaa osaltaan tietoaineistojen käytön valvontaa ja väärinkäytöksien havaitsemista.

Tietojenkäsittelyyn (13 § kohta 2) kohdistuvaa riskiarviointia tehdään tutkimustulosten mukaan yhtä kuntaa lukuun ottamatta vuosittain. Yhdessä tutkimukseen osallistuneessa kunnassa tietojenkäsittelyyn kohdistuvaa riskiarviointia tehdään seudullisena yhteistyönä jatkuvasti ja nouseviin riskeihin reagoidaan välittömästi. Tietojenkäsittelyyn kohdistuvan riskiarvioinnin käytänteet vaihtelivat kuntakohtaisesti suuresti, eikä tutkimustuloksista noussut kuntia yhdistäviä tekijöitä riskiarviointeihin liittyen. Osassa tutkimukseen osallistuneista kunnista riskiarviointiin liittyvissä käytänteissä on kuitenkin vielä kehitettävää.

Viranomaisen (13 § kohta 3) olennaisien tietojärjestelmien vikasietoisuuden ja toiminallisuuden testauskäytänteet vaihtelivat kunta kohtaisesti. Toiminnallisuuden ja vikasietoisuuden testaus tapahtuvat pääasiallisesti tuotantoympäristössä eli ongelmiin pyritään reagoimaan niiden ilmaannuttua. Tutkimusaineis-

ton mukaan yhdessä tutkimukseen osallistuneista kunnista jatkuvuuden testausta suoritetaan säännöllisesti erilaisissa valtakunnallisissa, maakunnallisissa ja paikallisissa harjoituksissa. Kaikkia tutkimuksen kuntia yhdistävänä tekijänä tutkimustuloksista nousi esiin työntekijöiden sitoutuminen tietojärjestelmien ja toiminnallisen käytettävyyden jatkuvuuden takaamiseksi.

Pienissä ja keskisuurissa kunnissa (13 § kohta 4) käytössä olevat asianhallintajärjestelmät tukevat kattavasti julkisten asiakirjojen julkaisua. Kaikkia tutkimukseen osallistuneita kuntia yhdistikin julkisten asiakirjojen julkaisun mahdollisuus asianhallintajärjestelmiin integroitujen julkaisujärjestelmien kautta. Asianhallintajärjestelmän ulkopuolisten toimialojen osalta julkisten asiakirjojen julkaisu vaatii vielä tällä hetkellä kaikissa kunnissa enemmän vaivannäköä.

Pienissä ja keskisuurissa kunnissa (13 § kohta 5) hankittavien tietojärjestelmien tietoturvallisuuden huomioiminen vaihteli sekä sopimustasolla että testauskäytänteiden tasolla. Tutkimustuloksien mukaan pienissä kunnissa hankittavien tietojärjestelmien tietoturvallisuutta ei huomioitu sopimuksissa eikä auditoinneissa yhtä laajasti kuin keskisuurissa kunnissa. Tietoturvallisuuden huomioimisen vähyys hankittavien tietojärjestelmien osalta pienissä kunnissa johtunee pitkälti asiantuntemuksen ja resurssien puutteesta.

Tiedonhallintalain (906/2019 14 §) mukaan tietojensiirto yleisessä tietoverkossa on toteutettava salattua tai muuten suojattua tiedonsiirtoyhteyttä tai –tapaa käyttämällä, mikäli siirrettävät tiedot ovat salassa pidettäviä. Tiedonsiirrossa on myös varmistettava tai tunnistettava vastaanottaja riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettäviä salassa pidettäviä tietoja. Tutkimustuloksien mukaan pienissä ja keskisuurissa kunnissa hyödynnetään suojattuja tiedonsiirtoyhteyksiä laajasti. Koronapandemian myötä pienissä ja keskisuurissa kunnissa on lisätty suojattujen tiedonsiirtoyhteyksien kapasiteettia vastaamaan kasvanutta tarvetta. Tutkimustulosten mukaan kunnissa on otettu käyttöön myös turvaposti, joka mahdollistaa viestien vastaanottajan tunnistamisen riittävän tietoturvallisella tavalla. Pienien ja keskisuurien kuntien resurssien pienuudesta riippumatta on kaikissa kunnissa koronapandemian myötä pystytty lisäämään suojattujen tiedonsiirtoyhteyksien kapasiteettia huomattavasti. Tiedonhallintalain 14 § vaatimuksien näkökulmasta pienien ja keskisuurien kuntien valmiudet vaikuttavat vastaavan pääosin lain asettamia vaatimuksia.

Tiedonhallintalain (906/2019 15 §) mukaan viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein tietoaineistojen turvallisuus. Tietoaineistojen turvallisuudessa on huomioitava muun muassa tietoaineistojen muuttumattomuus, alkuperäisyys, ajantasaisuus ja virheettömyys. Lisäksi tietoaineistot on suojattava teknisiltä ja fyysisiltä vahingoilta ja ne on arkistoitava tarvittavilta osin. Tutkimustuloksien mukaan pienien ja keskisuurien kuntien valmiudet tietoaineistojen turvallisuuden varmistamiseksi vaihtelevat jonkin verran. Kaikissa tutkimukseen osallistuneissa kunnissa on tärkeimmät tietoaineistot pyritty suojaamaan koko tiedon elinkaaren ajalta. Tietoaineistojen tietoturvalliseen käsittelyyn on kunnissa tehty perusohjeistukset ohjaamaan tietoaineistojen käsittelyä. Keskisuurissa kunnissa on tutkimustuloksien mukaan kiinnitetty pieniä

kuntia enemmän huomiota tietoaineistojen elinkaaren hallintaan, mikä osaltaan tukee tietoaineistojen turvallisuuden hallintaa. Tutkimustuloksista nousi esiin kaikkia kuntia yhdistävä epävarmuus työntekijöiden tietoaineistojen käsittelyyn liittyvästä tietoturvakäyttäytymisestä. Tietoaineistojen tietoturvallisen käsittelyn varmistamisen lisäksi on erityisesti pienissä kunnissa tietoaineistojen turvallisuuden varmistamisessa vielä kehitettävää muillakin osa-alueilla.

Tiedonhallintalain (906/2019 16 §) mukaan tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet käyttäjän tehtävien mukaan ja ne on pidettävä ajantasaisina. Pienissä kunnissa tietojärjestelmien käyttöoikeuksien hallinnassa ei ole käytössä roolipohjaista keskitettyä pääsynhallintaa vaan käyttöoikeuksien hallinta tapahtuu tietojärjestelmäkohtaisesti. Tietojärjestelmäkohtainen käyttöoikeuksien ja pääsynhallinta vaikeuttaa käyttöoikeuksien hallintaa ja käyttöoikeuksien ajantasaisena pitämistä. Keskisuurissa kunnissa käytössä on keskitetty roolipohjainen pääsynhallinta niiltä osin kuin tietojärjestelmät mahdollistavat pääsynhallinnan integraatiota. Keskisuurissa kunnissa on lain asettamien vaatimuksien suhteen parempi tilanne mutta niilläkin on toimialakohtaisia tietojärjestelmiä käytössä, jotka eivät mahdollista keskitettyä roolipohjaista pääsynhallintaa.

Tiedonhallintalain (906/2019 17 §) mukaan viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Pienien ja keskisuurien kuntien lokitietojen kerääminen on tietojärjestelmästä riippuvaa ja kaikki käytössä olevat tietojärjestelmät eivät tue lokitietojen keräämistä. Tutkimustuloksien mukaan lokitietoja kerätään niistä tietojärjestelmistä, joista se on teknisesti mahdollista. Lokitietojen tärkeys on huomioitu useimmissa tutkimukseen osallistuneissa kunnissa. Lokitietojen hallinnassa on pienissä ja keskisuurissa kunnissa vielä kehitettävää. Uusien tietojärjestelmähankintojen yhteydessä kunnissa täytyy huomioida lain asettamat vaatimukset myös lokitietojen keräämisen osalta.

9 Yhteenveto

Tutkimuksen tavoitteena oli selvittää pienien ja keskisuurien kuntien digitaalisen turvallisuuden ja siihen liittyvän riskienhallinnan käytänteitä sekä valmiutta vastata laki julkisen hallinnon tiedonhallinnasta tietoturvallisuudelle asettamiin vaatimuksiin. Tutkimusmenetelmäksi tutkimukseen valikoitui laadullinen tutkimus, jonka avulla tutkittavasta ilmiöstä on mahdollista saada syvällisempää tietämystä. Tutkimuksen aineisto koostui neljän pienen ja keskisuuren kunnan kunnanjohtajan ja asiantuntijan tai tietohallinnosta vastaavan teemahaastatteluista. Tutkimukseen osallistuneiden kuntien vähyydestä johtuen tutkimuksen tuloksia ei voida yleistää koskemaan koko kuntasektoria vaan tutkimuksen tulokset kuvaavat tutkimukseen osallistuneiden kuntien tilannetta ja antavat suuntaa muiden pienien ja keskisuurien kuntien digitaaliseen turvallisuuteen liittyvistä käytänteistä. Tutkimuksen tulokset vastaavat pääosin esimerkiksi VAHTI Digiturvakyselyiden tuloksia, joskin tutkimusmenetelmien erilaisuuden vuoksi suoraa vertailua tutkimuksien välillä ei voida suorittaa.

Digitaaliseen turvallisuuteen liittyvän riskienhallinnan käytänteet vaihtelevat kunnittain. Keskisuurissa kunnissa digitaalisen turvallisuuden riskienhallinnan käytänteet ovat pieniä kuntia paremmalla tasolla osittain parempien henkilöstö- ja taloudellisten resurssien sekä organisaation tietohallinnon hierarkiarakenteen ansiosta, mikä mahdollistaa osaltaan riskienhallinnan (kuvio 8) monitasoisen hallinnan. Kuntajohto on vähintäänkin periaatteellisella tasolla sitoutunut digitaalisen turvallisuuden riskienhallinnan johtamiseen, mikä ei kuitenkaan heijastu riittävällä tavalla digitaalisen turvallisuuden henkilöstö- tai taloudellisiin resursseihin. Resurssien vähäisyys vaikuttaakin pienissä ja keskisuurissa kunnissa digitaalisen turvallisuuden riskienhallinnan prosessin lisäksi myös muihin digitaalisen turvallisuuden osa-alueisiin. Pienissä kunnissa digitaalisen turvallisuuden riskienhallinta on pitkälti operatiivisella eli toiminnan tasolla tapahtuvaa nouseviin riskeihin reagoimista. Riskienhallinnan prosessin puutteellisuuden vuoksi riskienhallintaa ei ole pienissä kunnissa mahdollista kehittää suunnitelmallisesti koko digitaalista toimintaympäristöä tukevaksi nykyisillä resursseilla. Keskisuurissa kunnissa tilanne on digitaalisen turvallisuuden resurssien suhteen hieman pieniä kuntia parempi, mikä heijastuu myös riskienhallintaan. Keskisuurissa kunnissa riskienhallinta käsittää kaikki organisaation tasot, mikä parantaa osaltaan myös riskienhallinan prosessin toimivuutta. Keskisuurissakin kunnissa oli puutetta tietohallinnon henkilöstöresursseista ja erityisesti digitaalisen turvallisuuden asiantuntijoista, mikä vaikuttaa riskienhallinnan käytänteisiin.

Seudullisesta yhteistyöstä kuntien kesken koetaan olevan hyötyä digitaalisen turvallisuuden riskienhallinnassa. Seudullisen yhteistyön kautta henkilöstöresursseja ja asiantuntemusta pystytään jakamaan kuntien kesken, mikä mahdollistaa muun muassa digitaalisen riskienhallinnan kehittämisen yhteistyössä. Pienien ja keskisuurien kuntien digitaalisen turvallisuuden riskienhallinnan koko-

naisuudet eroavat toisistaan huomattavasti. Suurimmalla osalla pienistä ja keskisuurista kunnista on kuitenkin edelleen tarvetta riskienhallinnan kehittämiselle.

Digitaalisen turvallisuuden tilanne vaihtelee pienissä ja keskisuurissa kunnissa suuresti. Lähes kaikissa tutkimuksien kunnissa on tietoturvapolitiikat ja –tavoitteiden määritetty ja käsitelty kunnanjohdon toimesta. Tietoturvatavoitteiden toteuttamiseen ei kuitenkaan ole, erityisesti pienissä kunnissa, riittäviä resursseja. Pienien kuntien resurssien vähyys heijastuukin lähes kaikille digitaalisen turvallisuuden osa-alueille. Pienissä kunnissa digitaalisen turvallisuuden henkilöresurssit sitoutuvat operatiivisten toimintojen ylläpitoon, mistä syystä digitaalisen turvallisuuden kehittämiseen ei juurikaan ole resursseja käytettävissä. Operatiivisen tason henkilöstövajauksen lisäksi pienistä kunnista puuttuu prosesseista ja projekteista vastaava taktinen taso, joka yleensä vastaavat myös digitaalisen turvallisuuden prosesseista. Pienissä kunnissa onkin tarvetta digitaalisen turvallisuuden kehittämisen resurssien lisäksi myös normaalin tietohallinnon toimintojen resurssien lisäämiselle. Keskisuurissa kunnissa tilanne resurssien osalta on pieniä kuntia hieman parempi. Keskisuurissa kunnissa on tietohallinnon kehittämiseen henkilöresurssi, joka vastaa myös digitaalisen turvallisuuden toiminnoista.

Pienien ja keskisuurien kuntien digitaaliseen turvallisuuteen liittyvät suurimmat epävarmuudet ovat haastatteluiden perusteella henkilöstön tietoturvakäyttäytymiseen liittyvät epävarmuudet ja digitaalisen turvallisuuden resursseihin liittyvät puutteet. Tietoturvakäyttäytymistä ja –tietoisuutta on pienissä ja keskisuurissa kunnissa pyritty parantamaan tietoturvakoulutuksien ja –ohjeistuksien avulla.

Jatkuvuuden hallinnan osalta on kaikissa kunnissa määritetty valmiussuunnitelmat, joiden avulla kriittiset palvelut voidaan toteuttaa eri tilanteissa. Muiden jatkuvuus- ja varautumissuunnitelmien osalta keskisuurien kuntien tilanne on parempi kuin pienien kuntien. Jatkuvuussuunnitelmien testaus on lähes kaikissa kunnissa vähäistä tai sitä ei ole lainkaan.

Tietoturvallisuuden toteuttamisen osalta keskisuurissa kunnissa on pieniä kuntia parempi tilanne. Keskisuurissa kunnissa on huomioitu tietoturvallisuusvaatimukset sopimuksissa pieniä kuntia tarkemmin. Tietojärjestelmien pääsynhallinta eroaa myös pienien ja keskisuurien kuntien osalta. Pienissä kunnissa pääsynhallinta on toteutettu tietojärjestelmäkohtaisesti, kun keskisuurissa kunnissa pääsynhallinta on toteutettu keskitetysti ja roolipohjaisesti niissä tietojärjestelmissä, joissa se on teknisesti mahdollista. Kriittisimmät tietoaineistot on pyritty suojaamaan kaikissa tutkimuksen kunnista. Keskisuurissa kunnissa on kokonaisuudessaan tietoaineistojen tietoturvallisuuden osaltakin parempi tilanne kuin pienissä kunnissa. Tietoturvallisuuteen liittyvään tilaturvallisuuteen oli viimeisien vuosien aikana kiinnitetty kaikissa tutkimuksen kunnissa vaadittavaa huomiota.

Kyberturvallisuuden osalta suojattuun tietoliikenteeseen on panostettu tämän vuoden aikana kaikissa kunnissa, ja tilanne on kohentunut huomattavasti.

Keskisuurissa kunnissa ovat tietoverkon ja tietojärjestelmien turvallisuuskäytänteet erityisesti teknisien ja hallinnollisien hallintakeinojen osalta pieniä kuntia paremmalla tasolla. Tutkimusaineisto ja tutkimustulokset tarjoavat kyberturvallisuuden osalta ainoastaan suuntaa antavia tuloksia, joiden perusteella keskisuurissa kunnissa kyberturvallisuuden kokonaistilanne vaikuttaa pieniä kuntia paremmalta.

Tietosuojavastaava ja siihen liittyvät vastuut on määritetty kaikissa tutkimuksen kunnissa. Tietosuojan osalta tutkimuksen kunnista löytyivät suurimmat digitaaliseen turvallisuuteen liittyvät erot. Tietosuojan toteutuksen osalta yhdessä kunnassa ei ole tehty mitään toimenpiteitä, kun taas toisessa kunnassa tietosuoja-asiat ovat toteutettu lainsäädännön edellyttämällä tavalla ja tietosuojan kehityksessä tehdään seudullista yhteistyötä kuntien tietosuojavastaavien kesken aktiivisesti.

Digitaalisen turvallisuuden tilanne vaihtelee suuresti pienien ja keskisuurien kuntien kesken. Lähes kaikissa pienissä ja keskisuurissa kunnissa on tarvetta digitaalisen turvallisuuden aktiiviselle kehittämiselle turvallisen tietojenkäsittelyn toimintaympäristön takaamiseksi. Tutkimustuloksista nousi esille resurssien puute digitaalisen toimintaympäristön turvallisuuden kehittämiseen liittyen. Resurssien lisäämiseen ei erityisesti pienissä kunnissa ole tällä hetkellä mahdollisuutta. Tutkimustuloksista nousivat esille myös seudullisen yhteistyön tuomat hyödyt. Seudullisen yhteistyön puitteissa henkilöstöresursseihin liittyviä vastuita on jaettu kuntien kesken ja digitaalisen turvallisuuden kehittämiseen on palkattu ulkopuolisia asiantuntijoita yhteisesti kustannuksien säästämiseksi.

Kuntien valmiudet vaihtelevat tutkimustuloksien mukaan **laki julkisen hallinnon tiedonhallinnasta (906/2019) tietoturvallisuudelle asettamien vaatimuksien** suhteen. Kuntien valmiudet vaihtelevat lain kaikkien pykälien (taulokko 2) kohdalla. Keskisuurien kuntien tilanne on kokonaisuudessaan pieniä kuntia parempi lainsäädännön tietoturvallisuudelle asettamien vaatimuksien suhteen. Lainsäädännön näkökulmasta yllättävintä tutkimustuloksissa on tietosuojaan liittyvien käytänteiden puutteellisuus. Kaikissa tutkimukseen osallistuneissa kunnissa on tiedonhallintalain tietoturvallisuudelle asettamien vaatimuksien näkökulmasta vielä kehitettävää digitaalisessa turvallisuudessa.

Tutkimuksen tuloksien perusteella pienien ja keskisuurien kuntien digitaaliseen turvallisuuteen keskittyville tutkimuksille on edelleen tarvetta. Jatkotutkimuksissa voidaan tutkia esimerkiksi pienien ja keskisuurien kuntien digitaalisen turvallisuuden osa-alueita syvällisemmin tai laajemmalla otoksella, jolloin tutkimustuloksia voitaisiin yleistää myös laajemmin. Pienien ja keskisuurien kuntien digitaalinen turvallisuus tarjoaa mielenkiintoisen tutkimuskentän myös jatkoopintoja tai laajempaa tutkimusta ajatellen.

LÄHTEET

Alasuutari, P. (2011). *Laadullinen tutkimus 2.0*. Tampere: Osuuskunta Vastapaino.

Andress, J., & Leary, M. (2017). Building a Practical Information Security Program. Teoksessa *Building a Practical Information Security Program*. https://doi.org/10.1016/c2014-0-01691-7

Bélanger, F., & Crossler, R. E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarter*, *34*(3), 567–594.

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). *Operational Role of Security Information and Event Management Systems*.

Blakley, B., McDermott, E., & Geer, D. (2001). Information security is information risk management. *Proceedings of the 2001 workshop on New security paradigms - NSPW '01*, 97. https://doi.org/10.1145/508185.508187

Bojanc, R., & Jerman-Blažič, B. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management*, *28*(5), 413–422. https://doi.org/10.1016/j.ijinfomgt.2008.02.002

Botha, J., & Von Solms, R. (2004). A cyclic approach to business continuity planning. *Information Management and Computer Security*, *12*(4), 328–337. https://doi.org/10.1108/09685220410553541

Bryant, B., & Saiedian, H. (2020). Improving SIEM Alert Metadata Aggregation with a Novel Kill-Chain Based Classification Model. *Computers & Security*. https://doi.org/10.1016/j.cose.2020.101817

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness*. *34*(3), 523–548.

Chapple, M., Steward, J. M., & Gibson, D. (2018). *CISSP- Certified Information Systems Security Professional: Official Study Guide* (8th p.). Indianapolis: John Wiley & Sons.

Conboy, K., Fitzgerald, G., & Mathiassen, L. (2012). European Journal of Information Systems Qualitative methods research in information systems: motivations, themes, and contributions Qualitative methods research in information systems: motivations, themes, and contributions. *European Journal of Information Systems*, *21*, 113–118. https://doi.org/10.1057/ejis.2011.57

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems*, *20*(6), 643–658. https://doi.org/10.1057/ejis.2011.23

Dempsey, K. L., Chawla, N. S., Johnson, L. A., Johnston, R., Jones, A. C., Orebaugh, A. D., … Stine, K. M. (2011). *Information Security Continuous Monitoring (ISCM) for federal information systems and organizations*. https://doi.org/10.6028/NIST.SP.800-137

Digi- ja väestötietovirasto. (2020). Digiturva. Noudettu osoitteesta

https://dvv.fi/digiturva

Dionne, G. (2013). Risk management: History, definition, and critique. *Risk Management and Insurance Review*, *16*(2), 147–166. https://doi.org/10.1111/rmir.12016

Ekelhart, A., Fenz, S., Klemen, M., & Weippl, E. (2007). Security ontologies: Improving quantitative risk analysis. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 1–7. https://doi.org/10.1109/HICSS.2007.478

Euroopan parlamentti ja neuvosto. *Euroopan unionin L 119/2016.* , (2016).

European Union Agency for Cybersecurity. (2019). IT Continuity Home — ENISA. Noudettu 30. joulukuuta 2019, osoitteesta https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience

Fazlida, M. R., & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*(April), 243–248. https://doi.org/10.1016/s2212-5671(15)01106-5

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management and Computer Security*, *22*(5), 410–430. https://doi.org/10.1108/IMCS-07-2013-0053

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness – A systematic review of the literature. *Computers & Security*, *46*, 18–31. https://doi.org/10.1016/j.cose.2014.06.008

Gabriel, R., Hoppe, T., Pastwa, A., & Sowa, S. (2009). Analyzing Malware Log Data to Support Security Information and Event Management: Some Research Results. *2009 First International Confernce on Advances in Databases, Knowledge, and Data Applications*, 108–113. https://doi.org/10.1109/DBKDA.2009.26

Galder, A., & Watkins, S. G. (2010). *Information Security Risk Management for ISO27001/ISO27002*. Cambridgeshire : IT Governance Publishing.

Grance, T., Stevens, M., & Myers, M. (2003). *NIST SP 800-36*.

Hayel, Y., & Quanyan Zhu. (2015). Resilient and secure network design for cyber attack-induced cascading link failures in critical infrastructures. *2015 49th Annual Conference on Information Sciences and Systems (CISS)*, 1–3. https://doi.org/10.1109/CISS.2015.7086855

Hirsjärvi, S., & Hurme, H. (2014). *Tutkimushaastattelu*. Helsinki: Gaudeamus Oy.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2010). *Tutki ja kirjoita*. Helsinki: Kustannusosakeyhtiö Tammi.

Hoque, N., Bhuyan, M. H., Baishya, R. C., Bhattacharyya, D. K., & Kalita, J. K. (2014, huhtikuuta). Network attacks: Taxonomy, tools and systems. *Journal of Network and Computer Applications*, Vsk. 40, ss. 307–324. https://doi.org/10.1016/j.jnca.2013.08.001

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*. https://doi.org/10.1016/j.istr.2008.10.010

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

Insta Group. (2017). SIEM-järjestelmä on organisaation kyberturvallisuuden hermokeskus - Insta Group. Noudettu 20. toukokuuta 2019, osoitteesta https://www.insta.fi/ajankohtaista/uutiset/insta-defsec/siem-jarjestelma-on-organisaation-kyberturvallisuuden-hermokeskus.html

International Organization for Standardization. (2011). *ISO/IEC 27031:2011*. Noudettu osoitteesta https://www.iso.org/standard/44374.html

International Organization for Standardization. (2013a). *ISO/IEC 27001:2013*. Suomen Standardisoimisliitto SFS Ry.

International Organization for Standardization. (2013b). *ISO/IEC 27002:2013*. Suomen Standardisoimisliitto SFS Ry.

International Organization for Standardization. (2013c). ISO/IEC 27005:2013. *ISO/IEC 27005*.

International Organization for Standardization. (2018). ISO/IEC 31000:2018. *ISO/IEC 31000:2018*.

Islam, S., & Falcarin, P. (2011). Measuring security requirements for software security. *Proceedings of 2011, 10th IEEE International Conference on Cybernetic Intelligent Systems, CIS 2011*, 70–75. https://doi.org/10.1109/CIS.2011.6169137

Jennex, M. E., & Zyngier, S. (2007). Security as a contributor to knowledge management success. *Information Systems Frontiers*, *9*(5), 493–504. https://doi.org/10.1007/s10796-007-9053-4

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. https://doi.org/10.1016/S0268-4012(02)00105-6

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: Information security risk analysis method. *Computers and Security*, *24*(2), 147–159. https://doi.org/10.1016/j.cose.2004.07.004

Kowtha, S., Nolan, L. A., & Daley, R. A. (2012). Cyber security operations center characterization model and analysis. *2012 IEEE International Conference on Technologies for Homeland Security, HST 2012*, 470–475. https://doi.org/10.1109/THS.2012.6459894

Kuntaliitto. (2019a). Kaupunkien ja kuntien lukumäärät ja väestötiedot. Noudettu 3. helmikuuta 2020, osoitteesta 2019 website: https://www.kuntaliitto.fi/tilastot-ja-julkaisut/kaupunkien-ja-kuntien-lukumaarat-ja-vaestotiedot

Kuntaliitto. (2019b). Kunnan johtamisjärjestelmä | Kuntaliitto.fi. Noudettu 8. helmikuuta 2020, osoitteesta https://www.kuntaliitto.fi/osallistuminen-ja-vuorovaikutus/johtaminen-ja-kehittaminen/kuntajohtaminen/kunnan-johtamisjarjestelma

Kuntaliitto. (2020). Kuntayhtymät (kuntalaki 2015) | Kuntaliitto.fi. Noudettu 1. kesäkuuta 2020, osoitteesta https://www.kuntaliitto.fi/laki/kuntien-ja-kuntayhtymien-yhteistoiminta/kuntayhtymat-kuntalaki-2015

Matulevičius, R., Mayer, N., & Heymans, P. (2008). Alignment of misuse cases with security risk management. *ARES 2008 - 3rd International Conference on Availability, Security, and Reliability, Proceedings*, 1397–1404. https://doi.org/10.1109/ARES.2008.88

Myers, M. D. (1997). Qualitative research in information systems. *MIS Quarterly: Management Information Systems*, *21*(2), 241–242. https://doi.org/10.4018/978-1-59140-144-5.ch016

National Institute of Standards and Technology. (2011). Managing Information Security. *Kybernetes*, *40*(3/4), 5–9. https://doi.org/10.1108/k.2011.06740caa.012

National Institute of Standards and Technology. (2012). Guide for conducting risk assessments. Teoksessa *NIST Special Publication 800-30 Revision 1*. https://doi.org/10.6028/NIST.SP.800-30r1

National Institute of Standards and Technology. (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. https://doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology. (2018a). *Framework for improving critical infrastructure cybersecurity*.

National Institute of Standards and Technology. (2018b). *NIST Special Publication 800-37 Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy JOINT TASK FORCE*. 183. https://doi.org/10.6028/NIST.SP.800-37r2

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information and Management*, *52*(1), 123–134. https://doi.org/10.1016/j.im.2014.10.009

Niemimaa, M. (2017). Information systems continuity process: Conceptual foundations for the study of the "social". *Computers and Security*, *65*, 1–13. https://doi.org/10.1016/j.cose.2016.11.001

Niemimaa, M., & Järveläinen, J. (2013). IT service continuity: Achieving embeddedness through planning. *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, 333–340. https://doi.org/10.1109/ARES.2013.45

NVD. (2020). NVD - Home. Noudettu 16. toukokuuta 2020, osoitteesta 2020 website: https://nvd.nist.gov/

Offensive Security. (2020). Exploit Database - Exploits for Penetration Testers, Researchers, and Ethical Hackers. Noudettu 16. toukokuuta 2020, osoitteesta https://www.exploit-db.com/

Oikeusministeriö. *FINLEX ® - Ajantasainen lainsäädäntö: Kuntalaki 410/2015*. , (2015).

Oikeusministeriö. (2018). *FINLEX ® - Säädökset alkuperäisinä: Tietosuojalaki 1050/2018*.

Oikeusministeriö. *FINLEX ® - Säädökset alkuperäisinä: Laki julkisen hallinnon tiedonhallinnasta 906/2019*. , (2020).

Oikeusministeriö, E. P. O. *FINLEX ® - Ajantasainen lainsäädäntö: Valmiuslaki 1552/2011*. , (2011).

Puolustusministeriö. (2015). Katakri. Noudettu osoitteesta

http://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Rostami, M., Koushanfar, F., & Karri, R. (2014). A primer on hardware security: Models, methods, and metrics. *Proceedings of the IEEE*, *102*(8), 1283–1295. https://doi.org/10.1109/JPROC.2014.2335155

Rot, A. (2008). IT Risk Assessment : Quantitative and Qualitative Approach. *Proceedings of The World Congress on Engineering and Computer Science 2008*, 1073–1078. Noudettu osoitteesta http://www.iaeng.org/publication/WCECS2008/WCECS2008_pp1073-1078.pdf

Sanastokeskus TSK. (2018). *Kyberturvallisuuden sanasto*. Noudettu osoitteesta https://www.tsk.fi

Sanastokeskus TSK. (2020). Tietotekniikan termitalkoot - Henkilötiedot. Noudettu osoitteesta http://www.tsk.fi/tsk/termitalkoot/fi/node/266?page=resurssi&tiedosto=henkilotiedot.svg

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers and Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Stawowski, M. (2009). Network Security Architecture. *Insurance Fraud Casebook*. Noudettu osoitteesta https://pdfs.semanticscholar.org/5756/859705f57cfdf799fd2f790f5b7b0ccf334a.pdf

Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency Planning Guide for Information Technology Systems. *Computer Security Division*, (May), 150. https://doi.org/10.6028/NIST.SP.800-34r1

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide. *Proceedings - International Conference on Availability, Reliability and Security, ARES 2009*, 726–731. https://doi.org/10.1109/ARES.2009.75

Thakur, M. A., & Gaikwad, R. (2015). User identity and access management trends in it infrastructure- An overview. *2015 International Conference on Pervasive Computing: Advance Communication Technology and Application for Society, ICPC 2015*, *00*(c), 4–7. https://doi.org/10.1109/PERVASIVE.2015.7086972

Tietosuojavaltuutetun toimisto. (2010). Tietosuojavaltuutetun toimisto. Noudettu 19. toukokuuta 2020, osoitteesta https://tietosuoja.fi/etusivu

Traficom. (2020). Kyberturvallisuuskeskus. Noudettu 16. toukokuuta 2020, osoitteesta https://www.kyberturvallisuuskeskus.fi/fi/palvelumme

Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällön analyysi*. Helsinki: Kustannusosakeyhtiö Tammi.

Valtionvarainministeriö. (2016). *Julkisen hallinnon ICT Toiminnan jatkuvuuden*

hallinta. Noudettu osoitteesta https://www.vahtiohje.fi/c/document_library/get_file?uuid=11459f91-91c8-4ebe-a34f-9d8d9bfc964c&groupId=10229

Valtionvarainministeriö. (2020). Kuntien tehtävät ja toiminta - Valtiovarainministeriö. Noudettu 3. helmikuuta 2020, osoitteesta https://vm.fi/kuntien-tehtavat-ja-toiminta

Valtiovarainministeriö. (2019). *Kuntien tehtävien ja velvoitteiden vähentäminen*.

Valtiovarainministeriö. (2020a). Digitaalinen turvallisuus. Noudettu osoitteesta https://vm.fi/digitaalinen-turvallisuus

Valtiovarainministeriö. (2020b). *Digitaalisen turvallisuuden ohjaus*. Noudettu osoitteesta https://vm.fi/digitaalisen-turvallisuuden-ohjaus

Valtiovarainministeriö. (2020c). *Julkisen hallinnon digitaalinen turvallisuus*. Noudettu osoitteesta http://urn.fi/URN:ISBN:978-952-287-857-1 Sivumäärä

Valtiovarainministeriö. (2020d). Tiedonhallintalain täytäntöönpano - Valtiovarainministeriö. Noudettu 18. toukokuuta 2020, osoitteesta https://vm.fi/tiedonhallintalain-taytantoonpano

Valtiovarainministeriö. (2020e). Tieto- ja tiedonhallinnan ohjaus. Noudettu osoitteesta https://vm.fi/tietohallinnon-ohjaus

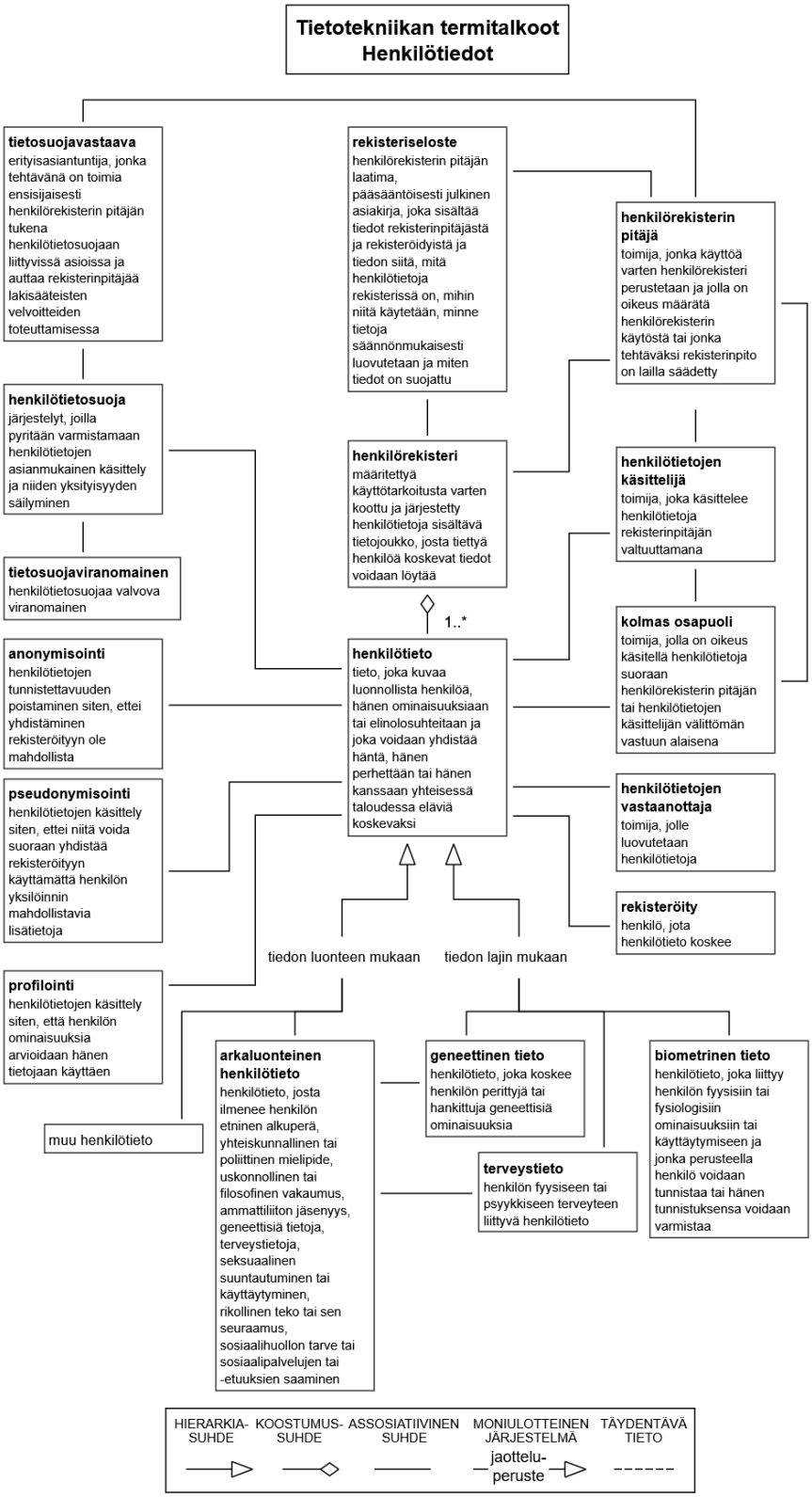
Voutilainen, T., & Kurvinen, E. (2015). *KUNTIEN TIETOHALLINNON JÄRJESTÄMINEN - VASTUUT JA RAJOITTEET ULKOISTAMISESSA*.

Walker, R. (2013). *Winning With Risk Management*. Singapore.

Wan, S. H. C., & Chan, Y.-H. C. Y.-H. (2008). Adoption of business continuity planning processes in IT service management. *2008 3rd IEEEIFIP International Workshop on Businessdriven IT Management*, 21–30. https://doi.org/10.1109/BDIM.2008.4540071

Yleisradio. (2019). Kaupunginjohtaja Lahden kyberhyökkäyksestä: ”Tietoturvan taso ei ole ollut riittävä”. Noudettu 12. syyskuuta 2020, osoitteesta https://yle.fi/uutiset/3-10869368

LIITE 1 HENKILÖTIEDOT KÄSITEKAAVIO (SANASTOKESKUS)



LIITE 2 JULKISEN HALLINNON ICT:N OHJAUS

Julkisen hallinnon ICT:n ohjaus	Laki	Asetus	Määräys	Sopimus	Periaatep.	Strategia	Linjaus	Ohje	Suositus	Auditointi	Tila	Vuosi	Vastuu	Lisätietoja JulkICT:sta	Huom.
Julkisen hallinnon tietohallinto	L	As									Voimassa	2011	JulkICT	Hannele Kerola	Tietohallintolaki. Uusiminen suunnitteilla
Toimialariippumaton ICT	L	As									Voimassa	2014	JulkICT	Tuomo Pigg	Lyhenne = TORI
Hallinnon turvallisuusverkko	L	As			P						Voimassa	2015	JulkICT	Timo Saastamoinen	Lyhenne = TUVE
Kansallinen palveluarkkitehtuuri	L										Esitys annettu	2016	JulkICT	Eeva Lantto	Lyhenne = KaPA
Hallituksen strateginen ohjelma						St					Voimassa	2015	VN	Anna-Maija Karjalainen	Hallitusohjelma
Hallintolaki	L										Voimassa	2003	OM	Sami Kivivasara	Tärkein ICT:tä koskeva yleislaki
Valtioneuvoston ohjesääntö		As									Voimassa	2003	VNK	Sami Kivivasara	
Valtiovarainministeriö		As									Voimassa	2003	VN	Sami Kivivasara	Valtioneuvoston asetus, päivitetty 2015
Viranomaisten toiminnan julkisuus	L	As									Voimassa	1999	OM	Sami Kivivasara	Julkisuuslaki
Sähköinen tunnistaminen	L		M								Voimassa	2009	LVM	Olli-Pekka Rissanen	Päivitys 2015
Sähköinen asiointi	L										Voimassa	2003	OM	Kimmo Mäkinen	Koskee viranomaisten välistä toimintaa
Valmiuslaki	L	As									Voimassa	2011	OM	Tuomo Pigg	Erityisesti § 105
Tietoyhteiskuntakaari	L										Voimassa	2014	LVM	Olli-Pekka Rissanen	Sisältää VM:n asioita
Tietohallinnon neuvottelukunta		As									Voimassa	2016	JulkICT	Heikki Talkkari	JUHTA. Tietohallintolain asetus.
Lausuntomenettely hankinnoissa		As									Voimassa	2014	JulkICT	Toni Äikäs	Tietohallinnon hankinnat. Tietohallintolain asetus.
Valtionhallinnon tietoturvallisuus		As			P						Voimassa	2010	JulkICT	Saana Seppänen	Uusitaan 2017. OM:n antama julkisuuslain asetus.
Julkisen tiedon saatavuus					P						Voimassa	2011	JulkICT	Kauhanen-Simanainen	
Avoin data opas								O			Julkaistu	2016	JulkICT	Kauhanen-Simanainen	Oppaassa on mukana katsaus alan säädöksiin
Yhteiskunnan turvallisuusstrategia					P						Julkaistu	2010	PLM	Tuija Kuusisto	YTS. Erityisesti ICT osuus. Uusitaan 2017.
Kyberturvallisuusstrategia					P						Julkaistu	2013	PLM	Tuija Kuusisto	Erillinen toimeenpanosuunnitelma
JulkICT strategia 2012-20120						St					Vahvistamatta	2012	JulkICT	Anna-Maija Karjalainen	Korvataan digistrategialla
Digistrategia						St					Tekeillä	2016	JulkICT	Riikka Pellikka	
Digitalisoinnin periaatteet						St					Valmis	2016	JulkICT	Aleksi Kopponen	
Suomen tietoturvallisuusstrategia						St					Julkaistu	2016	LVM	Kimmo Rousku	LVM:n julkaisu
Tietoliikenne, päätelaite ja viestintä							Li				Tekeillä	2017	JulkICT	Yrjö Benson	Julkisen hallinnon palvelulinjaukset
Konesali- ja kapasiteettipalvelu							Li				Julkaistu	2014	JulkICT	Yrjö Benson	Toteutusprojekti VAKSI 2014-2016, valtionhallinto.
Tietohallintomalli							Li				Tekeillä	2017	JulkICT	Yrjö Benson	Julkinen hallinto
Kokonaisarkkitehtuuri								O			Valmis	2014	JulkICT	Jari Kallela	Tietohallintolakiin perustuen
Viitearkkitehtuurit								O			Valmis	2016	JulkICT	Jari Kallela	12 kappaletta
Yhteentoimivuus								O			Tekeillä	2016	JulkICT	Jari Kallela	
ICT hankkeiden raportointi								O			Valmis	2015	JulkICT	Toni Äikäs	
Tietoturvapalvelut				S							Allekirjoitettu	2016	JulkICT	Kirsi Janhunen	GovCERT ja GovHAVARO
Tietoturvallisuuden auditointi			M							A	Hyväksytty	2015	NSA	Kimmo Rousku	Katakri. Määräys moniin kansainvälisiin asioihin.
Turvallisuus käsikirja yrityksille								O			Julkaistu	2015	NSA	Kirsi Janhunen	Turvallisuusviranomaisten käsikirja yrityksille
VAHTI ohjeet (41 kpl)								O			Jatkuva	2015	JulkICT	Kimmo Rousku	Valtiohallinnon tieto- ja kyberturvallisuuden ohjausryhmä
Julkisen hallinnon suositukset (50 kpl)									Su		Jatkuva	2016	JulkICT	Pekka Niemi	JUHTA antaa suositukset

Taulukossa olevien lisäksi on raha- ja budjettiohjaus voimakas ohjauskeino.
Lisätietoja koko taulukosta antaa Yrjö Benson, yrjo.benson@vm.fi

LIITE 3 HAASTATTELUISSA KÄYTETYT TUTKIMUSKYSYMYKSET

1. Millaiseksi arvioitte kuntaorganisaationne digitaalisen turvallisuuden kokonaisuudessaan (1-10)?
2. Minkälaisia haasteita kunnassanne on digitaaliseen turvallisuuteen liittyen?
3. Millaista tukea tai ohjeistusta toivoisitte saavanne digitaalisen turvallisuuden riskienhallintaan tai digitaalisen turvallisuuden yleiseen parantamiseen?
4. Pohjautuuko kuntanne riskienhallinta riskiarvioinnin tuloksiin ja miten sitä hyödynnetään johtamisessa ja päätöksenteossa?
5. Kuinka usein kuntanne ydintoimintojen riskit arvioidaan ja miten niistä raportoidaan kunnan johdolle?
6. Miten kuntanne tietoturvatavoitteet on määritetty ja miten se näkyy toiminnan ja tavoitteiden suunnittelussa?
7. Miten digiturvallisuuteen liittyvät tehtävät ovat kunnassanne organisoita ja onko niihin liittyvät vastuut määritetty?
8. Onko kunnassanne määritetty digiturvallisuuteen liittyvät ohjeistukset henkilökunnanalle? Mitä digiturvallisuuden osa-alueita ohjeet käsittelevät?
9. Onko kuntanne johto sitoutunut digiturvallisuuden toteuttamiseen ja millä tavalla se näkyy kuntanne toiminnassa?
10. Onko kunnassanne tehty jatkuvuuden hallintaan ja varautumiseen liittyviä suunnitelmia?
11. Onko suunnitelmien (jatkuvuussuunnitelmat ja palautumissuunnitelmat) toimivuutta testattu ja kuinka usein testausta suoritetaan?
12. Miten kunnassanne seurataan tietoturvallisuuden tilaa ja millä keinoilla tietojärjestelmien turvallisuus varmistetaan?
13. Onko kuntaanne nimetty tietosuojasta vastaava henkilö ja onko siihen liittyvät vastuut määritetty?
14. Onko kunnassanne tunnistettu luotettavuutta edellyttävät tehtävät ja onko niissä toimiville henkilöille teetetty turvallisuusselvitykset?
15. Onko luotettavuutta edellyttävissä tehtävissä toimiville henkilöille annettu siihen liittyvää koulutusta?
16. Onko kuntanne tietosuojaan liittyvät prosessit määritetty ja millä tavalla se näkyy johtamisessa?
17. Miten kuntanne sopimuksissa huomioidaan tietoturvaan liittyvät vaatimukset?
18. Onko kuntanne toiminnassa huomioitu tiloihin liittyvät tietoturvavaatimukset?
19. Onko kunnassanne määritetty lokipolitiikka (kerääminen, tallentaminen, käsittely, analysointi)?

20. Miten kunnassanne on varmistettu tiedonsiirron turvallisuus (tietoliikenteen salaus ja käyttäjätunnistus/-valtuutus)?
21. Miten kunnassanne on varmistettu tietoaineistojen tietoturvallisuuden (fyysinen turvallisuus ja järjestelmäturvallisuus)? Onko tietoaineistojen tietoturvallisuus varmistettu koko tiedon elinkaaren osalta?
22. Millä tavoin kuntanne tietojärjestelmien ja tietovarantojen suunnittelussa on huomioitu niiden soveltuvuus julkisten asiakirjojen julkaisuun (esim. asianhallintajärjestelmä)?
23. Miten kuntaanne hankittujen tietojärjestelmien tietoturvallisuus on varmistettu sopimuksia tehtäessä ja onko hankittujen tietojärjestelmien tietoturvallisuutta testattu ja auditoitu? (sopimukset ja testaus/auditointi)
24. Kuinka laajasti kuntanne käytössä olevia tietojärjestelmiä ja tietoliikennejärjestelyitä on arviointi/auditointi? Kuinka usein arviointia/auditointia suoritetaan?
25. Miten kuntanne tietojärjestelmien käyttöoikeuksien hallinta on toteutettu?