Tietoturvallisuuden riskienhallinnan kehittäminen valtioneuvoston kansliassa

Anthony Baxter

2021 Laurea

Laurea-ammattikorkeakoulu

Tietoturvallisuuden riskienhallinnan kehittäminen valtioneuvoston kansliassa

Anthony Baxter

Turvallisuus ja riskienhallinta

Opinnäytetyö

Toukokuu, 2021

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuus ja riskienhallinta

Tradenomi (AMK)

Anthony Baxter

Tietoturvallisuuden riskienhallinnan kehittäminen valtioneuvoston kansliassa

Vuosi 2021 Sivumäärä 62

Vuodet 2020 ja 2021 ovat jälleen osoittaneet tietoturvallisuuden merkityksen myös valtioneuvoston kanslian näkökulmasta. Toimintaympäristössä onnistuneiden kyberhyökkäysten ja tietovuotojen seurauksina voivat olla esimerkiksi kasvava epäluottamus viranomaisia kohtaan ja häiriöt viranomaisten palveluiden tuottamisessa. Menetettyä luottamusta on haastava saada takaisin, jonka takia tulisikin tehdä ennaltaehkäisevää tietoturvallisuuden riskienhallintaa.

Opinnäytetyön tavoitteena on kehittää valtioneuvoston kanslian tietoturvallisuuden riskienhallintaa. Kehittämistä varten selvitettiin valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan nykytilaa käyttäen kehittämistyön menetelmiä. Lisäksi perehdyttiin valtioneuvostoa ja sen toimintaympäristöä määrittelevään lainsäädäntöön. Tämän jälkeen tehtiin kehittämisehdotuksia tietoturvallisuuden riskienhallinnan kehittämiselle.

Nykytilan kartoitus tehtiin haastattelemalla valtioneuvoston kanslian johtohenkilöstöä sekä laatimalla kyselyn, joka suunnattiin kanslian yksiköiden ja toimintojen esihenkilöille. Haastatteluiden ja kyselystä saatujen tuloksien perusteella pystyttiin, arvioimaan kehittämiskohteita ja esittämään näille soveltuvia kehittämisehdotuksia.

Tuloksista ilmenee, että vaikka valtioneuvoston kanslian tietoturvallisuuden riskienhallinta on lain edellyttämällä tasolla, on kehitettävää erityisesti henkilöstön tietoturvallisuustietoisuuden ja -osaamisen alueilla. Lisäksi kehitettävää on organisatorisella tasolla tietoturvallisuuden vastuiden ja velvollisuuksien osalta. Opinnäytetyössä esitellään kehittämisehdotuksia tietoturvallisuuden riskienhallinnan kokonaisvaltaiseen kehittämiseen. Opinnäytetyön kehittämismenetelmistä saatuja tuloksia voidaan hyödyntää yksikkö- ja toimintakohtaisen tietoturvallisuustason tarkastelussa sekä kehittämisessä.

Asiasanat: tietoturvallisuus, riskienhallinta, valtioneuvoston kanslia

Laurea University of Applied Sciences **Abstract**

Safety, Security and Risk Management

Bachelor of Business Administration

Anthony Baxter

Developing Information Security Risk Management in the Prime Minister's Office

Year 2021 Pages 62

The years 2020 and 2021 have yet again demonstrated the importance of information security, especially from the perspective of the Prime Minister's Office. The main consequences of successful cyber attacks and information leaks in the operating environment are growing mistrust towards the authorities and disruptions in the provision of government services. It is challenging to regain lost trust, which is why preventive information security risk management should be carried out.

The aim of the thesis is to develop information security risk management in the Prime Minister's Office. As part of the process, the current state of information security risk management in the Prime Minister's Office was examined using development work methods. In addition, the legislation defining the Prime Minister's Office and its operating environment was reviewed.

The current state was evaluated by interviewing some leading staff members of the Prime Minister's Office and by preparing a questionnaire aimed at the senior management of the Prime Ministers Office. Based on the interviews and the results of the survey, it was possible to evaluate the development targets and present suitable development proposals.

The results show that although the information security risk management in the Prime Minister's Office is at the level required by law, it needs to be developed especially in the areas of staff member's information security awareness and competence. In addition, there is room for improvement at the organisational level in terms of defining information security responsibilities and obligations. The thesis presents development proposals that could be used to develop information security risk management holistically. The results obtained from the thesis development methods can be utilised in the assessment and development of the unit-specific information security level.

Keywords: information security, risk management, prime minister's office

Sisällys

1 Johdanto

Valtioneuvoston kanslian toimintaympäristö on jatkuvassa muutostilassa. Kansainväliset kriisitilanteet, digitalisaatio sekä kyberuhkien kehittyminen asettavat tietoturvallisuuden hallinnalle haasteita. Riittämätön tietoturvallisuus muodostaisi merkittävän riskin tavoitteiden saavuttamiselle sekä pääministerin sekä hallituksen toimintaedellytyksien turvaamisessa ja niiden jatkuvuudelle. Valtioneuvoston kanslialla on tärkeä rooli uusien toimintatapojen omaksumisessa sekä uuden teknologian käyttöönotossa valtionhallinnossa. Osana valtioneuvoston kanslian vuoden 2019 tulostavoitteita, aloitettiin tietoturvallisuuden hallintamallin käyttöönotto. Tietoturvallisuuden hallintamallin suunnittelu ja jalkauttaminen kuuluvat valmiusyksikölle. Tietoturvallisuuden ohjaus ja yhteensovittaminen on eräs valmiusyksikön lakisääteisistä tehtävistä (Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 162/2015). Hallintamallin suunnittelun tukena käytetään lainsäädännön asettamien vaatimusten lisäksi tapauskohtaisesti hyödynnettäviä standardeja, kriteeristöjä ja ohjeita, kuten valtioneuvoston tietoturvallisuusohjeita. Lainsäädäntö luo vähimmäisvaatimukset tietoturvallisuudelle, jota tulee sovittaa ja kehittää toimintaympäristöön sopivaksi. (Valtioneuvoston kanslia 2019a.)

Jatkuvasti muuttuvan toimintaympäristön lisäksi haasteita tietoturvallisuudelle toi kevään 2020 aikana alkanut COVID-19 pandemia. Erityinen huoli valtioneuvoston kanslialle nousi etätyön sekä omien laitteiden, kuten tablettien ja älytelevisioiden käytön kautta syntyvistä tietoturvallisuusriskeistä. Ilmiö ei kuitenkaan ole uusi ja vastaavia riskejä oli jo ennen pandemian aiheuttamia etätyösuosituksia. Sopivalla ja ajantasaisella tietoturvallisuuden hallintamallilla tämänkaltaiset haasteet saadaan ratkaistua, eivätkä muutokset työskentelytavoissa tällöin lisää merkittävästi tietoturvallisuusriskejä.

Hallintamallin suunnittelu ja käyttöönotto on monipolvinen ja laaja kokonaisuus. Tämän takia suunnittelutyö on pilkottu pienempiin osioihin ja sijoitettu tietoturvallisuuden vuosikelloon. Eräs näistä osista, on tietoturvallisuuden riskienhallinta, joka on tämän opinnäytetyön keskeinen aihe. Tarkoituksena oli selvittää valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan nykytila. Tämän jälkeen saatujen havaintojen pohjalta kehitettiin hallintamalliin sopivia menetelmiä lainsäädännön ja standardien sekä ohjeistuksien asettamien vaatimusten mukaisesti. Tavoitteena oli kehittää tietoturvallisuuden riskienhallintaa valtioneuvoston kansliassa. Kehittämistavoitteena oli selvittää, mitä kehittämistoimenpiteitä tietoturvallisuuden riskienhallinnalle voidaan vaatimusten ja havaintojen perusteella tunnistaa. Kehittämistavoitteen tueksi pyrittiin selvittämään mitä vaatimuksia lainsäädäntö, ohjeistus ja tilannekuva-arviot asettavat tietoturvallisuuden riskienhallinnalle valtioneuvoston kansliassa sekä mikä on tietoturvallisuuden riskienhallinnan

nykytila valtioneuvoston kansliassa. Tietoturvallisuuden riskienhallinnan nykytilaa pyrittiin selvittämään teemahaastatteluilla sekä kyselyllä. Valtioneuvoston kanslian vaatimuksia sekä mahdollisia kehittämisehdotuksia tutkittiin kirjallisuuskatsauksen menetelmien avulla.

Opinnäytetyössä on hyödynnetty ainoastaan julkisia dokumentteja eikä salassa pidettävää materiaalia ole käytetty lähdemateriaalina. Tietyt prosessit ja toiminnot ovat turvaluokiteltua tietoa, jonka takia niitä ei käsitellä opinnäytetyössä. Osioissa mainitaan erikseen, mikäli jokin osa jätetään huomioimatta turvaluokituksen takia. Opinnäytetyön tuloksia voi hyödyntää tietoturvallisuuden riskienhallinnan kehittämisen lisäksi muissa tietoturvallisuuden hallintamallin osa-alueissa. Vaikka tietoturvallisuuden hallintamalli koostuu useasta osa-alueesta, monet seikat, kuten lainsäädännön vaatimukset, ovat näille yhtenäisiä. Tietoturvallisuuden kehittämisen hyötyjä voi olla vaikea arvioida yksiselitteisesti. Luomalla vankka pohja tietoturvallisuudelle ja mahdollistamalla sen jatkuva kehittäminen, voidaan paremmin turvata pääministerin ja hallituksen toimintaedellytykset kaikissa olosuhteissa.

2 Valtioneuvoston kanslian tietoperusta

Tässä luvussa perehdytään opinnäytetyön tietoperustaan. Keskeisen tietoperustan opinnäytetyölle luo valtioneuvoston ja erityisesti valtioneuvoston kanslian määräykset ja ohjeet, sekä niiden toimintaansa määrittelevä lainsäädäntö. Tietoperustassa lisäksi perehdytään tietoturvallisuuden riskienhallinnan teoriaan, sen keskeisiin käsitteisiin sekä kansainvälisesti käytettyihin standardeihin.

Keskeiset käsitteet ja tietoperusta mahdollistavat tekstin luettavuuden ja ymmärrettävyyden (Vilkka 2015, 24). Tämän kehittämistyön tarkoituksena on kehittää valtioneuvoston kanslian tietoturvallisuuden riskienhallintaa. Ensimmäisessä alaluvussa käsitellään valtioneuvoston kansliaa ja sen toimintaympäristöä. Kehittämistyön kannalta keskeisiä käsitteitä ovat tietoturvallisuus ja riskienhallinta. Luvussa 2.2 avataan tarkemmin näitä käsitteitä. Luvussa 2.3 kerrotaan valtioneuvoston kanslian toimintaan vaikuttavasta lainsäädännöstä ja sen vaatimuksista tietoturvallisuuden riskienhallinnan osalta. Seuraavassa luvussa 2.4 tarkastellaan tietoturvallisuusohjeiden ja standardien asettamia vaatimuksia. Viimeisessä alaluvussa tarkastellaan tietoturvallisuuden riskienhallinnan teemasta tehtyä aiempaa tutkimusta ja kehittämistä.

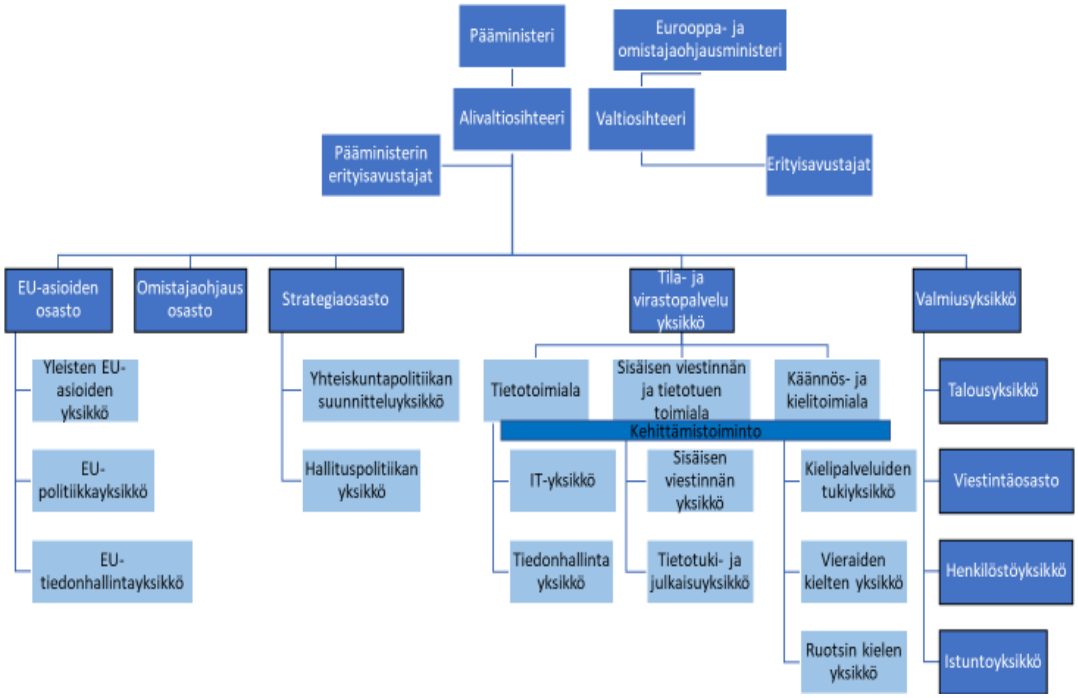
2.1 Valtioneuvoston kanslia ja sen toimintaympäristö

Valtioneuvostolla tarkoitetaan 12 ministeriön muodostamaa hallitus- ja hallintoasioiden päätöksentekoelintä sekä pääministerin ja ministereiden muodostamaa yleistä hallintovaltaa käyttävää toimielintä. Ministeriöt ovat: valtioneuvoston kanslia, ulkoministeriö, oikeusministeriö, sisäministeriö, puolustusministeriö, valtiovarainministeriö, opetus- ja

kulttuuriministeriö, maa- ja metsätalousministeriö, liikenne- ja viestintäministeriö, työ- ja elinkeinoministeriö, sosiaali- ja terveysministeriö sekä ympäristöministeriö. Ministeriöt vastaavat toimialallaan hallinnon toiminnasta sekä valtioneuvostolle kuuluvien asioiden valmistelusta. Ministeriön korkein virkamies johtaa ja valvoo ministeriön toimintaa. Korkeimman virkamiehen nimike on kansliapäällikkö, mutta ulkoministeriössä ja valtiovarainministeriössä virkanimike on valtiosihteeri. (Valtioneuvosto 2020.)

Valtioneuvoston kanslia yksi Suomen 12 ministeriöstä, jota johtaa pääministeri. Valtioneuvoston kanslia vastaa hallitusohjelman toimeenpanon valvonnasta ja avustaa pääministeriä valtioneuvoston johtamisessa. Lisäksi valtioneuvoston kanslia turvaa pääministerin ja hallituksen toimintaedellytykset kaikissa olosuhteissa. Yhtenä tärkeimmistä valtioneuvoston kanslian tehtävistä on Suomen EU-politiikan yhteensovittaminen. Tämän lisäksi kanslian tehtäviin kuuluu valtion omistajapolitiikka, valtioneuvoston kanslian alaisten valtio-omisteisten yhtiöiden omistajaohjaus, valtioneuvoston viestintä ja valtionhallinnon viestinnän yhteensovittaminen, valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus, häiriötilanteiden hallinnan yleinen yhteensovittaminen sekä valtion sektoritutkimuksen tavoitteiden yhteensovittaminen päätöksenteon tueksi. (Valtioneuvosto 2020.)

Valtioneuvoston kanslia koostuu useasta monialaisesta osastosta. Osastoja ovat EU-asioiden osasto, valtioneuvoston hallintoyksikkö, omistajaohjausosasto, viestintäosasto, strategiaosasto, istuntoyksikkö, valmiusyksikkö, henkilöstöyksikkö ja talousyksikkö. Tietoturvallisuuden näkökulmasta, osastoilla on keskenään erilaisia tarpeita ja haasteita. Valtioneuvoston kanslian organisaatio on kuvattu kuviossa 1. Ministeriön tehtävät määrittelee tarkemmin valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 13 § (162/2015). Valtioneuvoston kanslian valmiusyksikölle kuuluu lisäksi valtioneuvoston ja ministeriöiden yhteisen turvallisuuden ja tietoturvallisuuden ohjaus sekä yhteensovittaminen. Valtioneuvoston ja ministeriöiden yhteisen tieto- ja viestintätekniikan sekä tietojärjestelmien teknisen tietoturvallisuuden hallinta kuuluu valtioneuvoston kanslian tietotoimialalle. Lisäksi tietotoimialalle kuuluu yhteisten tieto- ja viestintätekniikan palveluiden sekä tietojärjestelmien hallinta ja kehittäminen. Valtioneuvoston kanslian tietotoimiala kuuluu hallintoyksikön alaisuuteen. (Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 162/2015.)



Kuvio 1: Valtioneuvoston kanslian organisaatio (Valtioneuvoston kanslia 2020a)

Kansliapäällikkökokous on korkean virkamiestason yhteistyöryhmä ja valtiokonsernin johtamisen foorumi (Valtioneuvoston kanslia 2020b). Kansliapäällikkökokous vastaa toiminnan yhteensovittamisesta vakavissa tietoturvahäiriötilanteissa. Valtioneuvoston tietoturvallisuuden ohjausryhmä käsittelee valtioneuvoston tietoturvallisuuden tilannekuvaa puolivuosittain. Ministeriöt vastaavat toimialansa tietoturvallisuuteen liittyvän tiedon toimittamisesta. Tilannekuvan koostaminen kuuluu lakisääteisesti valtioneuvoston kanslian valmiusyksikölle. Tietoturvallisuuden hallinnan asiantuntijaorganisaationa toimii valtioneuvoston tietoturvallisuuden yhteistyöryhmä. Yhteistyöryhmä kokoontuu neljä kertaa vuodessa. Lisäksi vakavan häiriön sattuessa ryhmä voidaan kutsua koolle ylimääräiseen kokoukseen. (Valtioneuvoston kanslia 2018.)

Valtioneuvoston kanslian ja sen tietojärjestelmien tietoturvallisuuden tilaa käsittelee valtioneuvoston tietoturvaryhmä. Lisäksi se käsittelee kanslian tietoturvallisuussuunnitelmia ja niiden etenemistä, sekä tietoturvallisuuden riskien ja poikkeamien hallintaa. Ryhmä on valmiusyksikön koordinoima, johon kuuluu henkilöstöä useammasta eri yksiköstä. (Valtioneuvoston kanslia 2019c.)

Valtorina tunnettu valtion tieto- ja viestintätekniikkakeskus tuottaa valtiohallinnolle ICT-palvelut. Valtori vastaa suurelta osin digitaalisista palveluista ja työkaluista, joita valtioneuvostossa käytetään. Valtorilla on myös merkittävä rooli tietoturvallisuuden

ylläpitämisessä valtionhallinnossa, sillä valtionhallinnon käyttämät tietoverkot ja palvelut ovat Valtorin tuottamia. Valtoriin on viime vuosina kehitetty kyberpoikkeamien havainnointi-, reagointi- ja analysointikyvykkyyttä palveluiden tietoturvallisuuden takaamiseksi.

Valtorin toimintaa ohjaa laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013) sekä valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014). Valtori tehtäviin kuuluu esimerkiksi tietoliikennepalveluihin liittyvät tietoturvapalvelut. (Valtori 2021.)

Lainsäädäntö luo viitekehyksen valtioneuvoston toiminnalle. Valtioneuvostoa ja sen ministeriöitä koskee ja velvoittaa suuri määrä erilaisia lakeja. Yksiköt joutuvat usein itse tulkitsemaan lait, jotka säätelevät heidän toimintaansa. Tässä opinnäytetyössä valtioneuvoston kansliaa säätelevää lainsäädäntöä tarkastellaan lainopin perusteilla. Lainoppi on oikeudellisten tekstien tulkintaa. Se on argumentatiivinen tutkimusmenetelmä, jossa esitetään väitteitä lain merkityssisällöstä oikeuslähteiden avulla. Lainopin mukaan täydellistä totuutta lain sisällöstä ei ole. Vaatimuksia asettavaa lainsäädäntöä on tulkittu tietoturvallisuuden riskienhallinnan näkökulmasta. (Hirvonen 2011, 21-26.)

Lainsäädäntö määrittelee valtioneuvoston kanslian toiminnalle toimivaltuudet ja edellytykset. Oleellinen tietoperusta täten löytyy toimintaa ohjaavasta lainsäädännöstä. Valtioneuvoston kanslian tietoturvallisuutta määrittelevä lainsäädäntö on pirstaleinen ja koostuu eri tarkoituksiin asetetuista laeista. Osa lainsäädännöstä määrittelee yleisesti valtioneuvoston kanslian tehtäviä ja roolia valtiohallinnossa. Osa taas käsittelee tiedon hallintaa ja asettaa vaatimuksia tietoturvallisuudelle. Seuraavat lait ohjaavat valtioneuvoston kansliaa eri näkökulmista: laki valtioneuvostosta (175/2003), valtioneuvoston ohjesääntö (262/2003), laki julkisen hallinnon tiedonhallinnasta (906/2019), asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999), josta on voimassa enää luku 2a, valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) sekä laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004). Lakien asettamat vaatimukset tarkennetaan liitteessä 1.

2.1.1 Määrittelevä lainsäädäntö

Laki valtioneuvostosta (175/2003) ja valtioneuvoston ohjesääntö (262/2003) toimivat valtioneuvoston sekä ministeriöiden toimintaa ohjaavina säädöksinä. Laeista ilmenee organisaatio ja toimialajako sekä ministeriöiden toimialat. Laki valtioneuvostosta ei määrittele tarkemmin tehtäviä ja vastuita valtioneuvoston kanslian tietoturvallisuuden näkökulmasta. Valtioneuvoston ohjesääntö antaa tarkempia säännöksiä valtioneuvoston toimintaan ja järjestysmuotoon. Valtioneuvoston ohjesääntö (262/2003) toteaa valtioneuvoston kanslian toimialaan kuuluvan ”valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus, häiriötilanteiden hallinnan yleinen yhteensovittaminen sekä

valmiuslaissa määriteltyjen poikkeusolojen toteamisen ja käyttöönottoasetuksen antamisen yleinen yhteensovittaminen". Valtioneuvoston ohjesäännöstä voidaan tulkita täten, että valtioneuvoston yhteinen tietoturvallisuus kuuluu valtioneuvoston kanslian toimialaan.

Laki valtioneuvostosta (175/2003) ja valtioneuvoston ohjesääntö (262/2003) eivät suoraan määrittele vaatimuksia riskienhallinnalle. Vaatimukset kuuluvat tekniseen, hallinnolliseen ja fyysisen tietoturvaan. Suurin osa vaatimuksista on kuitenkin luonteeltaan ennaltaehkäiseviä. Niiden voidaan tulkita kuuluvan osaksi myös tietoturvallisuuden riskienhallintaa. Laissa ainoastaan säädetään kuka johtaa ja kenelle lankeaa vastuu.

Lain valtioneuvostosta (175/2003) nojalla on säädetty valtioneuvoston asetus valtioneuvoston kansliasta (393/2007). Asetus tarkentaa valtioneuvoston ohjesääntöä (262/2003) yksityiskohtaisemmin valtioneuvoston kanslian tehtäviä. Tietoturvallisuuteen liittyviä tehtäviä ovat: "valtioneuvoston yhteisen tilannekuvan kokoaminen ja häiriötilanteiden hallinnan yleinen yhteensovittaminen sekä valtioneuvoston yhteinen poikkeusoloihin ja häiriötilanteisiin varautuminen, valtioneuvoston ja sen ministeriöiden yhteisen turvallisuuden ohjaus ja yhteensovittaminen sekä turvallisuuspalvelut, valtioneuvoston ja sen ministeriöiden yhteisen tietoturvallisuuden ja tietosuojan ohjaus ja yhteensovittaminen sekä yhteiseen tieto- ja viestintätekniikkaan ja yhteisiin tietojärjestelmiin kuuluvan tietoturvallisuuden hallinta" (Valtioneuvoston asetus valtioneuvoston kansliasta (393/2007).

Lain valtioneuvostosta (175/2003) 7 §:n mukaan toiminnasta voidaan antaa tarkempia säännöksiä asiasta ministeriön asetuksena annettavalla ministeriön työjärjestyksellä. Lain nojalla on säädetty valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä (162/2015). Asetus tarkentaa organisaation tehtäviä ja vastuita. Asetuksessa erotellaan hallinnollinen tietoturvallisuus ja tekninen tietoturvallisuus. Valtioneuvoston ja ministeriöiden yhteisten tieto- ja viestintätekniikan ja yhteisten tietojärjestelmien teknisen tietoturvallisuuden hallinnasta vastaa hallintoyksikön alainen tietotoimiala. Valmiusyksikön tehtäviä tietoturvallisuuden osalta ovat "häiriötilanteiden hallinnan yleinen yhteensovittaminen, valtioneuvoston yhteinen poikkeusoloihin ja häiriötilanteisiin varautuminen sekä valtioneuvoston ja sen ministeriöiden yhteisen turvallisuuden ja tietoturvallisuuden ohjaus ja yhteensovittaminen" (Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 162/2015).

2.1.2 Muu lainsäädäntö

Laki julkisen hallinnon tiedonhallinnasta (906/2019) yhtenä tarkoituksena on varmistaa viranomaisten tietoaineistojen tietoturvallinen käsittely. Lisäksi tarkoituksena on mahdollistaa tiedon turvallinen hyödyntäminen sekä edistää tietojärjestelmien yhteentoimivuutta. Vaatimuksissa korostuu erityisesti riskienhallinta sekä elinkaariajattelu, tarkoittaen esimerkiksi tietojärjestelmien säännöllistä testaamista.

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019) ja laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004) säätävät toimenpiteistä tietoturvallisuusvelvoitteiden toteuttamiseksi. Lait asettavat samankaltaisia vaatimuksia ja velvollisuuksia. Ne asettavat vaatimuksia esimerkiksi turvallisuusluokitteluun, monitasoiseen suojaukseen sekä turvallisuusalueisiin.

2.2 Tietoturvallisuuden riskienhallinta

Kyberuhat kehittyvät kasvavaa vauhtia, eikä olekaan tarkoituksenmukaista pyrkiä aina pysymään uusimpien kybertrendien edellä. Sen sijaan merkityksellisempää on juurruttaa tietoturvayhteistyö organisaatiossa osaksi jokaista toimintoa sekä henkilöstön arkea. Kasvattamalla henkilöstön tietoturvallisuustietoisuutta parannetaan kokonaisvaltaisesti turvallisuuden tasoa. Yleisimmin käytetyt huijausyritykset ja haittaohjelmien levitysyritykset hyödyntävät edelleen perinteisiä menetelmiä, kuten sähköpostia. Vaikka tekninen tietoturvallisuuskontrolli ei tunnistaisi potentiaalisesti vaarallista sähköpostia, turvallisuusorientoituneella henkilöstöllä on paremmat mahdollisuudet tunnistaa vaaran paikat ja välttää huijaukset ja haittaohjelmat.

Tietoturvallisuus ja riskienhallinta saatetaan nähdä toisistaan irrallisina kokonaisuuksina, ja usein organisaatiossa näistä vastaa kaksi erillistä tahoa. Riskienhallinnan tulisi kuitenkin olla kokonaisvaltaista kaikkiin toimintoihin ja osa-alueisiin ulottuvaa. Riskienhallinta nähdään yhtenä merkittävimmistä osa-alueista ICT-hallinnassa ja tietoturvallisuudessa. Tietoturvallisuuden riskienhallinta on prosessi, jonka avulla valtioneuvoston kanslian johto voi tasapainottaa operatiivisia sekä taloudellisia kustannuksia. Lisäksi sen avulla pyritään saavuttamaan kanslian tavoitteita, suojaamalla järjestelmiä sekä tietoja, jotka tukevat tavoitteiden saavuttamista. (Stoneburner, Goguen & Feringa 2002, 1-4.)

Tietoturvallisuuden riskienhallinta ei ole ainoastaan ICT:stä ja turvallisuudesta vastaavien tehtävä, vaan koko organisaation alkaen ylimmästä johdosta. Valtioneuvoston kanslian johdon tulee varmistua, että organisaatiolla on riittävä kyky suorittaa sen tehtäviä. Tehtävien hoitamisen turvaamiseksi tulee varmistaa riittävät resurssit sekä kyetä varmistamaan tietoturvallinen toimintaympäristö suhteessa uhkiin. Hyvin jäsennelty riskienhallinta metodologia voi auttaa kanslian johtoa tunnistamaan sopivat kontrollit tarjoamaan tehtävien kannalta riittävä turvallisuustaso. (Stoneburner, Goguen & Feringa 2002, 1-4.)

Valtioneuvoston kansliaan kohdistuvat riskit kehittyvät ajan saatossa. Toimintaympäristön painopisteiden siirtyessä uusia riskejä ja kohteita saattaa ilmaantua. Tämän takia on tärkeää, että riskienhallinnassa jatkuvasti arvioidaan riskejä ja toimintaympäristöä. Lisäksi tulisi säännöllisesti arvioida suojattavia arvoja. Kanslian tietoturvallisuusriskejä arvioidaan tietoturvallisuuspolitiikan vuosikellon mukaisesti. Ydintoimintojen riskejä arvioidaan vuosittain tammi-maaliskuussa (toinen kvartaali). Tietoturvallisuustilannetta tarkastellaan

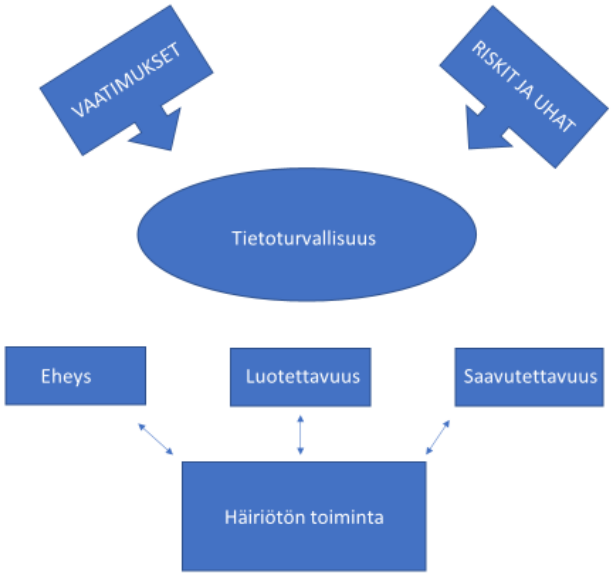
huhti-kesäkuussa (kolmas kvartaali). Heinä-syyskuussa (neljäs kvartaali) jälleen tarkastellaan tietojärjestelmien riskienhallintatasoa. Loka-joulukuussa (ensimmäinen kvartaali) suunnitellaan seuraavan vuoden tietoturvatoimintaa. Tietojärjestelmien osalta tietoturvallisuusriskejä arvioidaan heinä-syyskuussa (neljäs kvartaali). (Valtioneuvoston kanslia 2019, 8-9; (Wheeler 2013, 43.)

2.2.1 Tietoturvallisuus

Tietoturvallisuus jaotellaan yleisesti hallinnolliseen, tekniseen sekä fyysiseen tietoturvallisuuteen. Ohjeistukset, riskienhallinta sekä koulutus ovat esimerkkejä hallinnollisesta tietoturvallisuudesta. Haittaohjelmien torjunta sekä palomuuriratkaisut ovat esimerkkejä tekniseen tietoturvallisuuteen kuuluvista asioista. Fyysisen tietoturvallisuuden tavoitteena on luoda toiminnalle tarkoituksenmukaisen, turvallinen sekä vaatimustenmukainen toimintaympäristö. (Vacca 2013.)

Tiedolla ja tietojärjestelmillä on luonnollinen elinkaari aina sen luomisesta sen hävittämiseen. Suojattavan kohteen arvo ja siihen kohdistuvat riskit voivat muuttua sen elinkaaren aikana. Tietoturvallisuus tulisi ottaa huomioon elinkaaren kaikissa vaiheissa. (SFS-EN ISO/IEC 27002:2017, 7.)

CIA-mallin (confidentiality, integrity and availability) mukaan tietoturvallisuudella ylläpidetään kolmea tekijää: tiedon eheyttä, saatavuutta sekä luottamuksellisuutta. Useimmat yritykset sekä valtaosa alan julkaisuista ovat omaksuneet CIA-mallin. Tieto voi ilmetä monessa erilaisessa muodossa, kuten fyysisinä dokumentteina, sähköisinä asiakirjoina tai tietopääomana. Tietoturvallisuutta ohjaavat erilaiset vaatimukset sekä monenlaiset riskit ja uhat. Ylläpitämällä tietoturvallisuutta tavoitellaan kriittisten toimintojen häiriötöntä toimintaa, kuten kuviossa 2 ilmaistaan. Voidaan sanoa tietoturvallisuuden olevan yleinen tavoitetila, jossa pyritään parempaan. Tietoturvallisuuden ei tulisi olla kertaluonteinen projekti, vaan jatkuva prosessi. Toimintaympäristöön ilmestyy uusia menetelmiä, riskejä ja uhkakuvia, jotka pakottavat kehittämään tietoturvallisuutta. (Raggad 2010, 20.)



Kuvio 2: Tietoturvallisuuden prosessi

Tiedon luottamuksellisuudella tarkoitetaan ominaisuutta, ettei suojattava tieto ole rajattomasti saatavilla tai ettei sitä luovuteta luvattomille henkilöille, organisaatioille tai prosesseille. Tiedon luottamuksellisuuden suojaamisella pyritään välttämään tiedon vuotamista ulkopuolisille sekä varmistumaan että ainoastaan valtuutetut henkilöt, organisaatiot tai prosessit pääsevät tietoihin. Tietovuodolle voi altistaa esimerkiksi epäasiallisesti hävitetty henkilötietoja sisältävä dokumentti tai salaamaton verkkoyhteys, jotka vaarantavat luottamuksellisuuden. Luotettavuus voidaan varmistaa esimerkiksi salausmekanismeilla. (Raggad 2010, 20; Yeboah-Boateng 2013, 42.)

Tiedon eheydellä tarkoitetaan kykyä varmistua tietojen muuttamattomuudesta. Eheys varmistaa, ettei tietoja ole muutettu esimerkiksi tallennuksessa tai siirrossa. Eheyttä rikotaan aina, kun tietoja on luvattomasti käsitelty, joko tahattomasti tai tahallisesti. Toimijana voi olla henkilö, haittaohjelmisto tai järjestelmä. Tiedon korruptoimista voi olla laskutustietojen muokkaaminen siten että toimija hyötyy taloudellisesti. (Raggad 2010, 20; Yeboah-Boateng 2013, 42-43.)

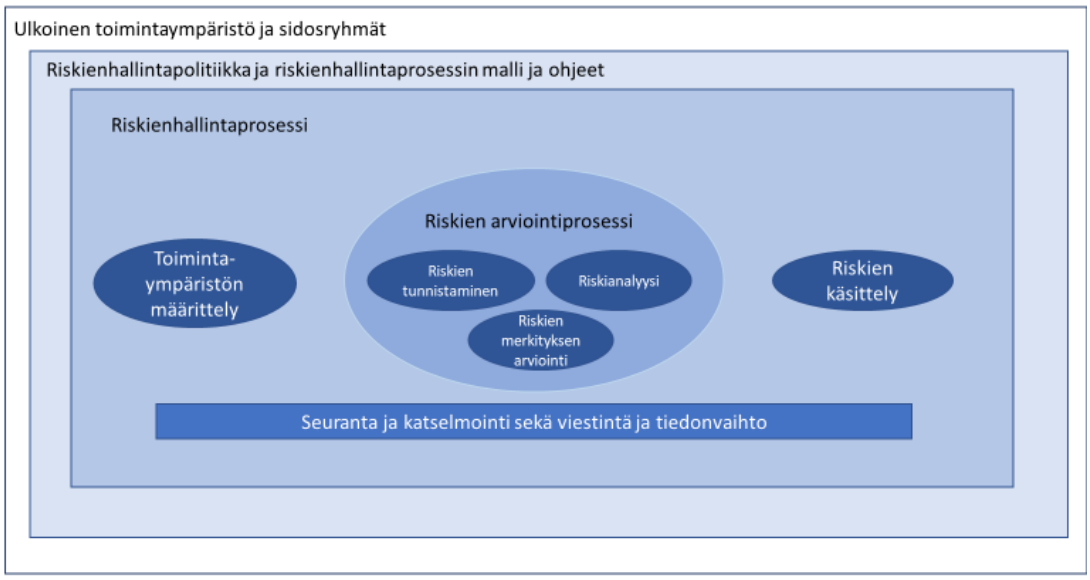
Saatavuudella tarkoitetaan, että tieto on saatavilla sitä tarvittaessa. Sillä varmistetaan, että käyttäjä tai järjestelmä saa tiedon esitettyään oikeutetun pyynnön. Kriittiseksi luokiteltujen tietojen tulisi varmistua saatavuudesta esimerkiksi varmuuskopioinneilla. Järjestelmissä saatavuus tarkoittaa kaikkia tarvittavia komponentteja, jotta voidaan tuottaa tai hakea käytettävää tietoa. Tiedon saatavuuden suojaamisella pyritään tiedon käytettävyyteen. Tiedon eheys ja luotettavuus voidaan varmistaa hyvinkin raskain toimenpitein, jolloin kuitenkin tiedon saatavuus ja käytettävyys heikkenee. Tiedon saatavuuden tarvetta

määrittelee tiedon käyttötarve. Saatavuuteen voidaan vaikuttaa esimerkiksi tahallisilla palvelunestohyökkäyksillä. (Raggad 2010, 20; Yeboah-Boateng 2013, 43.)

2.2.2 Riskienhallinta

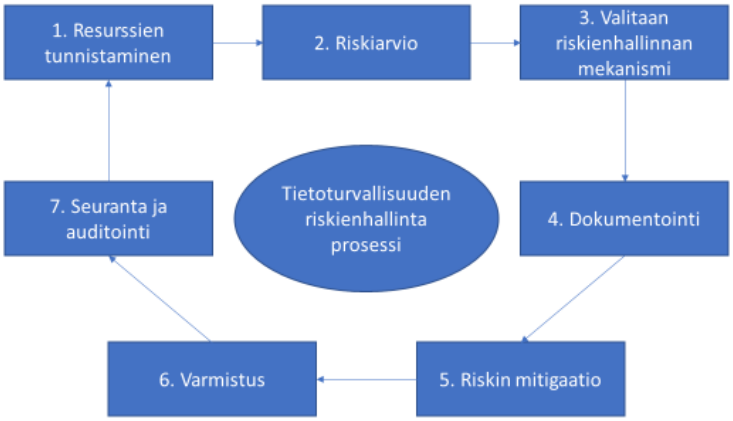
Eräs määritelmä riskistä on, että se on poikkeama odotuksesta. Riski on epävarmuuden vaikutus tavoitteisiin ja tämä vaikutus voi olla joko negatiivinen tai positiivinen odotuksiin nähden. Riski usein rinnastetaan uhkaan, mutta riskillä voidaan tarkoittaa myös positiivisia asioita, jotka voivat hyödyttää organisaatiota jollakin tavalla. (Rousku 2017.)

Riskienhallinnan tavoitteena on organisaation tavoitteiden saavuttamisen sekä jatkuvuuden varmistamisen. Riskienhallinnan tulisi olla järjestelmällistä ja tavoitteellista toimintaa, jolla tuetaan organisaatiota esimerkiksi johtamisessa ja kehittymisessä. Valtioneuvoston riskienhallintaprosessi koostuu toimintaympäristön määrittelystä, riskien arviointiprosessista sekä riskien käsittelystä. Lisäksi prosessiin kuuluu jatkuva seuranta ja katselmointi sekä viestintä ja tiedonvaihto. Alla olevassa kuviossa 3 on kuvattu riskienhallinnan viitekehys. (Rousku 2017; Valtioneuvoston kanslia 2019d.)



Kuvio 3: Riskienhallinnan viitekehys (Rousku 2017).

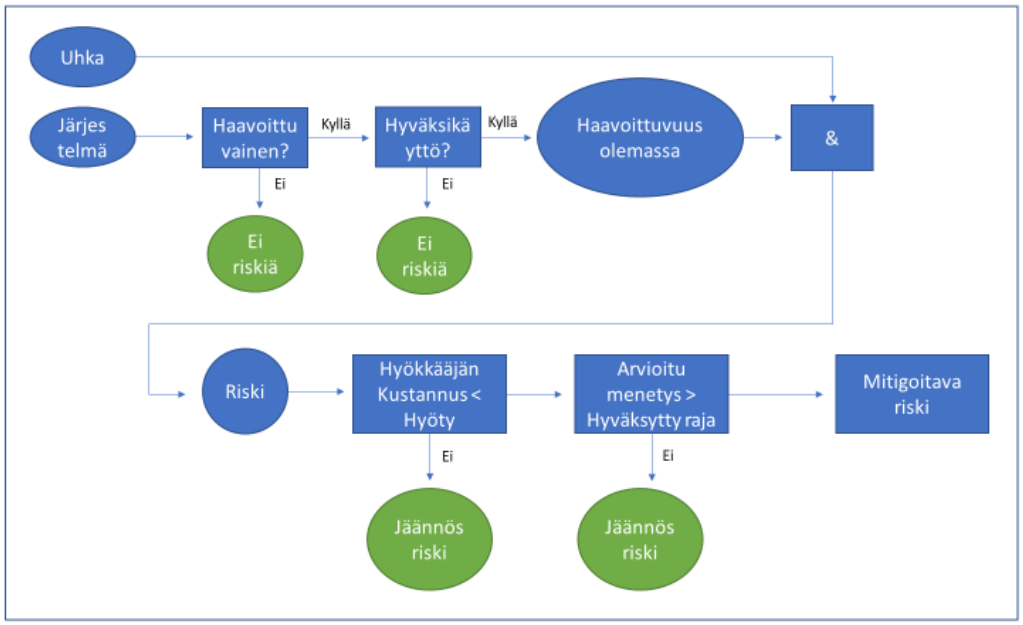
Riskienhallinnan elinkaari, kuvattu kuviossa 4, alkaa resurssien tunnistamisesta ja arvioinnista. Tämän jälkeen tehdään riskiarvio ja valitaan sopivin mekanismi riskin käsittelyyn. Sitten päätökset ja arviot dokumentoidaan. Suunnitelma laitetaan täytäntöön ja se todennetaan toimivaksi ja sopivaksi. Lopuksi arvioidaan ja tarkistetaan ketjun toimivuus ja sopivuus. Elinkaariajattelussa työ ei lopu tähän, vaan siirrytään jälleen ensimmäiseen kohtaan. (Wheeler 2011, 46.)



Kuvio 4: Riskienhallinnan elinkaari (Wheeler 2011, 46).

Riskiarviointiprosessi tulisi toistaa säännöllisesti, eikä sitä tulisi toteuttaa ainoastaan lakisääteisten vaatimusten takia vaan riskienhallinnan mahdollistamasta tuesta valtioneuvoston kanslian tavoitteille ja tehtäville. Riskiarvioinnilla tulisi olla selkeä aikataulu, mutta sen tulisi myös olla joustava ja kyetä ottamaan huomioon mahdolliset muutokset tietojärjestelmissä sekä toimintaympäristössä. Riskiarvioinnissa tulee arvioida riskien vaikutuksia ja priorisoida ne. Kun riskit on perustellusti arvioitu, pystytään päättämään mikä riskienhallinnan mekanismeista on sopivin. Riskienhallinnassa on yleisesti neljä mekanismia: riskin poisto, riskin todennäköisyyden vähentäminen, riskin vaikutusten pienentäminen sekä riskin hyväksyminen. Nämä pätevät kaikkien riskien hallintaan, eikä ainoastaan tietoturvallisuuteen. (Stoneburner, Goguen & Feringa 2002, 41; Wheeler 2011, 54-57.)

Riskin mitigaatioprosessilla, mikä on kuvattu kuviossa 5, kuvataan miten luokitella uhkia ja riskejä ja ovatko ne hyväksyttäviä vai mitigoitavia. Mitigoitavia mekanismeja ovat riskin poisto, riskin todennäköisyyden vähentäminen sekä riskin vaikutusten pienentäminen. Riskin hyväksymisestä usein käytetään termiä jäännösriski. Jäännösriski on riski, joka on todettu olevan sellainen, että kustannuksellisista tai käytännön syistä riski hyväksytään, eikä se välttämättä aiheuta toimenpiteitä. (Stoneburner, Goguen & Feringa 2002, 28; Wheeler 2011, 54-57.)



Kuvio 5: Riskin mitigaatioprosessi (Stoneburner, Goguen & Feringa 2002, 28).

Riskin poistamisella tarkoitetaan sellaisia toimenpiteitä, jotka poistavat riskin aiheuttavat seikat sekä itse riskin. Riskin poistoa voi olla esimerkiksi korjaamalla haavoittuvuus tai poistamalla haavoittuvainen palvelu kokonaan käytöstä. Täydellinen tietoturvallisuusriskien poistaminen on kallista ja useimmiten mahdotonta. (Valtioneuvoston kanslia 2019d; Wheeler 2011, 54-57.)

Riskin todennäköisyyttä voidaan vähentää esimerkiksi rajoittavilla toimenpiteillä, jotka eivät poista riskiä. Riskin todennäköisyyttä voidaan vähentää alentamalla tapahtuman todennäköisyyttä, rajoittamalla tapahtuman vaikutuksia tai vähentämällä resurssin herkkyyttä. Tietoturvallisuuden näkökulmasta, useimmat näistä toimenpiteistä ovat ennaltaehkäiseviä tai palauttavia. Ennaltaehkäisevä toimenpide voi olla esimerkiksi tekninen hälytysjärjestelmä. Hälytyksen avulla ei voida estää hyökkäystä. Hälytyksestä tietoisena voidaan kuitenkin sulkea esimerkiksi käyttäjätili ja täten rajoittaa tapahtuman vaikutuksia. Palauttavia toimenpiteitä ovat esimerkiksi varmuuskopiot. Varmuuskopiot eivät estä hyökkäystä, mutta hyökkäyksen jälkeen mahdollisesti menetetyt tiedot saadaan palautettua. (Wheeler 2011, 54-57.)

Riskin vaikutuksen pienentämisellä usein tarkoitetaan myös riskin siirtoa. Yleisin esimerkki riskin siirrosta on vakuuttaminen. Tällöin vahingon sattuessa, taloudellinen riski on vakuutusyhtiöllä, eikä toimijalla. (Wheeler 2011, 54-57.)

Käytännössä riskienhallintaprosessi etenee niin, että riskien todennäköisyyttä ja niiden vaikutuksia pyritään alentamaan eri toimenpiteillä, kunnes jäljelle jäävä riski on toimijan arvion mukaan niin pieni, että se voidaan hyväksyä. Riskienhallinnan tulisi olla jatkuvaa ja

mukana kaikissa toiminnoissa sekä prosesseissa. Näin saadaan lisäksi aiemmin tunnistamattomat riskit hahmoteltua ajoissa. (Wheeler 2011; Valtioneuvoston kanslia 2019d.)

2.3 Ohjaavat määräykset ja vaatimukset

Lainsäädännön lisäksi vaatimuksia asettavat valtioneuvoston kanslian omat määräykset ja ohjeet. Omien sisäisten määräyksien ja ohjeiden lisäksi, on valtioneuvoston asettamat tavoitteet sekä tapauskohtaisesti hyödynnettävät muiden organisaatioiden kriteeristöt. Täyttämällä lainsäädännön edellyttämän tason, täytetään minimivaatimukset. Täydentämällä minimivaatimuksiaan valtioneuvoston kanslia pystyy tehokkaammin varautumaan muutoksiin toimintaympäristössään.

Tietoturvallisuuden hallinta muodostuu kokonaisuudesta, jonka luo politiikat, standardit sekä ohjeistukset. Raggadin (2010) mukaan politiikka vastaa kysymykseen ”miksi”, kun standardit ja ohjeistukset vastaavat kysymyksiin ”mitä” ja ”miten”. Tietoturvallisuuden hallintamallin kriittisin elementti on tietoturvallisuuspolitiikka. Politiikka määrittelee säännön ja toimintatavat, joilla varmistetaan organisaation tietoturvallisuus. Lisäksi niissä määritellään tietoturvallisuusvastuut ja -toiminnot sekä ilmaistaan johdon asenne tietoturvallisuutta kohtaan. Standardit tukevat ja vahvistavat politiikan sanomaa. Standardeista tulee käyttöönottaessa velvoittavia. Organisaation omien standardien tulisi tehdä politiikasta merkityksellisemmän ja tehokkaamman. Standardissa tulisi olla vähintään yksi tarkennus esimerkiksi ohjelmistoihin tai käyttäytymiseen. Valtioneuvoston kanslian määräykset voidaan tulkita standardeiksi Raggadin määrittelyn mukaan. Ohjeet eivät Raggadin määritelmän mukaan ole velvoittavia, mutta valtioneuvoston kanslian ohjeet ovat velvoittavia. (Raggad 2010, 166-167.)

2.3.1 Valtioneuvoston määräykset

Määräys tietoturvallisuuden hallinnasta valtioneuvostossa ja sen ministeriöissä on valtioneuvoston tietoturvapolitiikka. Määräyksen tavoitteena on pyrkiä varmistamaan valtioneuvoston tietoturvallisuuden vaatimustenmukainen ja riskilähtöinen hallinta ja toteuttaminen. Politiikassa kerrotaan tietoturvallisuuden organisoinnista sekä vastuujaoista valtioneuvostosta. Lisäksi se kertoo valtioneuvoston tietoturvallisuusriskeistä, tietoturvallisuuden kehittämisestä ja raportoinnista. Määräystä täydentää valtioneuvoston kanslian tarkentavat määräykset, ohjeet ja periaatteet. (Valtioneuvoston kanslia 2018.)

Politiikka toteaa tietoturvallisuuden riskienhallinnan tukevan valtioneuvoston toiminnan jatkuvuutta sekä varautumista normaaliolojen häiriötilanteisiin. Määräys määrittelee, että kukin ministeriö arvioi vuosittain omaan toimintaansa liittyvät keskeiset tietoturvallisuusriskit. Ministeriön johto on vastuussa riskienhallinnan toteutumisesta osana ministeriön toiminallista johtamista. Tietojärjestelmien ja tietoteknisten palveluiden

tietoturvallisuusriskeistä vastaa järjestelmän tai palvelun omistaja. Nämäkin riskit on arvioitava vuosittain. Lisäksi hankinnoissa ja projekteissa tulee huolehtia tietoturvallisuusriskien hallinnasta ja niistä vastuu on hankkeen tai projektin päälliköllä. Valtioneuvoston kanslian asiantuntijat tukevat ministeriöitä tietoturvallisuusasioissa. (Valtioneuvoston kanslia 2018.)

2.3.2 Valtioneuvoston kanslian määräykset ja ohjeet

Alaluvussa käsitellään täydentävät määräykset, ohjeet ja periaatteet ja niistä muodostuva oma kriteeristö. Ne täydentävät valtioneuvoston kanslian tietoturvallisuuspolitiikkaa ja vahvistavat sekä tarkentavat tietoturvallisuuden riskienhallinnan toteuttamista. Monet ohjeet ovat itsessään osa riskienhallintaa, sillä on jokaisen henkilökuntaan kuuluvan velvollisuus tutustua ohjeisiin ja noudattaa niitä (Valtioneuvoston kanslia 2019a).

Valtioneuvoston kanslian tavoitteet määritellään vuosittain. Yksi valtioneuvoston kanslian tavoitteista (2019b) on yhteinen, ajantasainen ja yhteismitallinen tietopohja ministeriöille. Tätä tietopohjaa jaettaisiin aktiivisesti ja turvallisesti valtioneuvostossa valmistelun ja päätöksenteon tueksi. Eräs toimenpide tämän tavoitteen saavuttamiseksi on valtioneuvoston tietoturvallisuuden hallintamallin käyttöönotto. Tietoturvallisuuden hallintamallin suunnittelu ja käyttöönotto on pitkä ja monivaiheinen projekti. Eräs toinen valtioneuvoston kanslian tavoite on yhteisiin kustannustehokkaisiin ja turvallisiin ratkaisuihin perustuva digitaalinen valtioneuvosto. Tämän tavoitteen saavuttamiseksi tulee toteuttaa valtioneuvoston yhteisen tietoturvallisuuden riskienhallintaa. Tulostavoite määrittelee siihen kuuluvan riskiarviot, stressitestit sekä toipumissuunnitelmat. (Valtioneuvoston kanslia 2019a; Valtioneuvoston kanslia 2019b.)

Määräys tietoturvallisuuden hallinnasta valtioneuvoston kansliassa (2019c) on kanslian tietoturvallisuuspolitiikka. Määräyksen tavoitteena on varmistaa valtioneuvoston kanslian tietoturvallisuuden vaatimustenmukainen ja riskilähtöinen toteuttaminen. Politiikka määrittelee kanslian tietoturvallisuuden painopisteen olevan tietoaineiston käsittelyssä, tietojärjestelmien tietoturvallisuuden varmistamisessa, henkilöstön tietoturvaosaamisen ylläpidossa ja kehityksessä sekä toiminnan jatkuvuuden varmistamisessa kaikissa olosuhteissa. Määräyksen vaatimat toimenpiteet esitellään taulukossa 1. (Valtioneuvoston kanslia 2019c.)

Valtioneuvoston kansliassa on tietoturvallisuuden näkökulmasta varmistettava:
Ydintoimintoihin liittyvät keskeiset tietoturvallisuusriskit on tunnistettu ja analysoitu.

Tietoturvallisuuden varmistamiseksi on riittävät asiantuntemus ja tietoturvallisuuden keskeiset tehtävät ja vastuut on määritelty.
Asiakirjojen käsittelyä koskevat tehtävät ja vastuut on määritelty.
Tietojen saanti ja käytettävyys on turvattu sekä poikkeamienhallinnan menettelytavat määritelty.
Asiakirjojen salassapito on varmistettu antamalla pääsy vain niitä työssään tarvitseville.
Tietojen muuttaminen tai luvaton käsittely on pyritty teknisesti ennaltaehkäisemään ja estämään.
Asiakirjojen tietojenkäsittely ja -säilytystilat on riittävästi valvottuja ja suojattuja.
Henkilöstön luotettavuus on arvioitu ja varmistettu.
Henkilöstölle on annettu asiakirjojen käsittelyyn ja säilytykseen liittyviä ohjeita ja koulutusta.
Tietoturvallisuusohjeiden noudattamisesta valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

Taulukko 1: Valtioneuvoston kanslian tietoturvallisuuspolitiikan (Valtioneuvoston kanslia 2019c) vaatimat toimenpiteet tietoturvallisuuden näkökulmasta

Tietoturvallisuusvastuut valtioneuvoston kansliassa on jaettu tietojärjestelmien omistajille, hanke- ja projektipäälliköille, johdolle ja esimiehille sekä henkilöstölle. Tietoturvallisuuden riskienhallinnan osalta vastuut ovat samat. Jokaiselle kanslian tietojärjestelmälle on toiminnallinen omistaja. Omistaja johtaa, ohjaa ja kehittää sitä toimintaa, jota järjestelmä tukee. Omistajalla on vastuu kyseisen järjestelmän tietoturvallisuudesta. Omistajan tukena toimii tekninen omistaja, joka vastaa teknisestä toimivuudesta ja tukee teknisen tietoturvallisuuden osalta. Tietojärjestelmien tietoturvallisuutta tuetaan valtioneuvoston kanslian vuosikellolla, joka on käytössä valtioneuvoston ja valtioneuvoston kanslian järjestelmien osalta. Vuosikellon ylläpitämisestä ja sen mukaisten toimien toteutumisesta, seurannasta ja raportoinnista vastaa valmiusyksikön tietoturvallisuusasiantuntijat. Hankkeisiin ja hankintoihin kohdistuvat tietoturvallisuusvelvoitteet tulee yksilöidä sopimus- tai hankekohtaisesti. Nämä velvoitteet tulee ottaa huomioon jo hankinnan suunnitteluvaiheessa. Velvoitteiden tunnistamisesta ja dokumentoinnista vastaa sopimuksesta vastaava taho ja hankkeissa hankkeen tai projektin päällikkö. Hankkeen tai projektin päällikkö vastaa niihin liittyvien asiantuntijoiden tietoturvallisuusperehdytyksestä ja luotettavuuden arvioinnista.

Johdon sekä esimiesten vastuulla on tietoturvallisuuden organisointi sekä resurssointi. Tietoturvallisuutta koskevien määräysten, periaatteiden ja ohjeiden toteutumisen valvonta ja seuranta osana toiminallista johtamista on johdon sekä esimiesten vastuulla. Lisäksi näistä määräyksistä, periaatteista ja ohjeista tulee tiedottaa henkilöstöä yhteistyössä sisäisen viestinnän ja valmiusyksikön kanssa. Henkilöstöllä on velvollisuus tutustua ja noudattaa valtioneuvoston sekä valtioneuvoston kanslian tietoturvallisuusmääräyksiin, -periaatteisiin ja -ohjeisiin. Lisäksi henkilöstön tulee osallistua tietoturvallisuuskoulutuksiin sekä ilmoittaa havaituista tietoturvallisuutta vaarantavista asioista. (Valtioneuvoston kanslia 2019c, 3-5.)

Valtioneuvoston kanslian riskienhallintapolitiikka (2017) on tarkoitettu kattamaan kaiken kanslian toiminnan. Politiikka kertoo ”riskienhallinnan olevan kiinteä osa kanslian toimintaa, johtamisjärjestelmää ja asioiden valmistelua” (Valtioneuvoston kanslia 2017, 1-2). Riskienhallintapolitiikka on osa sisäisen valvonnan toimialaa ja siten lakisääteinen tehtävä valtioneuvoston kanslialle. Riskienhallinta auttaa valtioneuvoston kansliaa toteuttamaan tehtävänsä sekä saavuttamaan tavoitteensa. Lisäksi sillä turvataan toiminnan jatkuvuus, häiriöttömyys ja turvallisuus sekä toimintaedellytysten säilyminen. Vaikka politiikka ei ole yksinomaan tietoturvallisuuden riskienhallintaa koskeva, se antaa viitekehyksen sille. Valtioneuvoston kanslian tietoturvallisuusriskien arvioinnissa noudatetaan riskienhallintapolitiikkaa (Valtioneuvoston kanslia 2019c). Politiikka on lisäksi osoitus ylimmän johdon sitoutumisesta riskienhallintaan. (Valtioneuvoston kanslia 2017, 1-2.)

Riskienhallinnan vastuita on jaettu kanslian johtoryhmälle, esimiehille, hankkeen tai projektin omistajille sekä yleisesti henkilöstölle. Johtoryhmän vastuulla on sisällyttää riskienhallinta osaksi ohjaus- ja johtamisjärjestelmää ja johtoryhmätyöskentelyä kaikilla organisaatiotasoilla. Johtoryhmä lisäksi käsittelee valtioneuvoston kanslian riskit ja riskienhallintatoimenpiteet. Johdon vastuulla on myös varmistua siitä, että koko henkilöstö on ohjeista tietoisia ja että, koulutus ja perehdytys on ollut riittävää. Esimiehet, eli osastopäälliköt, toimialajohtajat, yksikön päälliköt sekä ryhmäjohtajat vastaavat oman vastuuorganisaationsa riskienhallinnasta ja sen toimeenpanosta. Lisäksi he tunnistavat oman vastuuorganisaationsa toimintaan liittyviä riskejä sekä raportoivat niistä eteenpäin. Esimiesten tulee viestiä riskienhallinnan periaatteista ja vaadittavista toimenpiteistä alaisilleen. Henkilöstön tulee arvioida ja tunnistaa omaan työhönsä liittyviä riskejä ja raportoida näistä ja mahdollisista poikkeamista esimiehelleen. Henkilöstön tulee omalta osaltaan vastata riskienhallinnan periaatteiden noudattamisesta sekä voimassa olevien ohjeiden, säädösten ja määräysten noudattamisesta. (Valtioneuvoston kanslia 2017, 3-4.)

Kanslian tietoturvallisuusriskien hallintaohje (2019d) kuvaa valtioneuvoston tietoturvallisuusriskien hallintamenetelmät. Tietoturvallisuuden riskienhallinnan tavoitteena on ohjeen mukaan löytää suojattavan kohteen tietoturvallisuuden kannalta merkittävät uhat sekä tarpeenmukaiset tietoturvallisuuskontrollit. Tietoturvallisuuden riskienhallinnan vastuut

on määritelty sekä tietoturvallisuuspolitiikassa että hallintaohjeessa. Ohje tarkentaa, että riskienhallintametodeista vastaa riskiarvioista vastaava taho. Projektin tai hankkeen metodeista, suojauskeinoista sekä jäännösriskien hyväksymisestä vastaa projektipäällikkö. Omistaja voi tarvittaessa palauttaa riskit uudelleenkäsiteltäväksi ja lisäksi tarvittaessa projektin tai hankkeen ohjausryhmä voivat ottaa kantaa. (Valtioneuvoston kanslia 2019d.)

2.3.3 Katakri: Viranomaisten auditointityökalu tietoturvallisuudelle

Kansallinen turvallisuusviranomainen, NSA (National Security Authority), on julkaissut päivitetyn version Katakrista, eli viranomaisten tietoturvallisuuden auditointityökaluksi tarkoitetun kansallisen auditointikriteeristön, joulukuussa 2020. Katakrilla on koettu myös olevan merkittävä arvo Suomen tietoturvallisuusmaineelle. Katakrin tarkoituksena on toimia työkaluna, jonka avulla arvioidaan organisaation ”kykyä suojata kansallista tai kansainvälistä turvallisuusluokiteltua tietoa”. Työkaluun on kerätty kansallisia ja kansainvälisiä vähimmäisvaatimuksia, eikä se aseta tietoturvallisuudelle vaatimuksia, vaan vaatimukset tulevat voimassa olevasta lainsäädännöstä ja velvoitteista. Lisäksi on hyödynnetty erilaisia standardeja kuten ISO/IEC 27001. Katakrin päivitetyssä versiossa on kuitenkin muutamia puutteita, kuten esimerkiksi vaatimuksia jatkuvuudenhallintaan tai varautumiseen ei ole. Katakri on jaettu kolmeen osa-alueeseen: turvallisuusjohtaminen (T), fyysinen turvallisuus (F) sekä tekninen tietoturvallisuus (I). (Katakri 2020; Ulkoministeriö 2021.)

T-osion kolmas vaatimus on, että ”organisaatio on arvioinut olennaiset turvallisuusluokiteltuihin tietoihin kohdistuvat riskit ja mitoittanut tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti”. Alla olevassa taulukossa (taulukko 2) kuvataan Katakrin toteutusesimerkki. Tämä on ainoa vaatimus, joka suoraan koskettaa tietoturvallisuuden riskienhallintaa hallinnollisena kokonaisuutena. Muissa osioissa ja vaatimuksissa tulee esille vaatimuksia ja toimia, jotka koskettavat omalta osaltaan tietoturvallisuuden riskienhallintaa, kuten esimerkiksi F-osion toinen vaatimus riskien arvioinnista, jossa todetaan, että fyysisten turvatoimien tulee perustua riskien arviointiin. (Katakri 2020, 11.)

Toteutusesimerkki tietoturvallisuuden riskienhallinnasta	
1.	Tietoturvallisuuden riskienhallinta on osana organisaation toimintaa.
2.	Turvallisuusluokiteltujen tietojen turvaamiseksi riittävät toimenpiteet varmistetaan tietoturvallisuuden riskienhallinnalla.

3.	Tietoturvallisuuden riskien arvioinnissa ja analysoinnissa valtioneuvoston kanslian toimintojen kannalta sopivaa ja päätöstentekoon ymmärrettävää tietoa tuottavaa menetelmää.
4.	Tietoturvallisuuden riskienhallintaa osallistuu riittävästi asiantuntijoita.
5.	Sidosryhmistä ja toimitusketjuista aiheutuvat riskit ovat huomioitu tietoturvallisuuden riskienhallinnassa.
6.	Tietoturvallisuus riskien arvioinnin ja analysoinnin tuloksia hyödynnetään turvallisuussuunnittelussa.
7.	Tietoturvallisuustoimenpiteet on mitoitettu riskiperusteisesti.
8.	Valvonta- ja turvatoimet sekä niiden perusteena ollut riskien arviointi on dokumentoitu keskeisiltä osin.

Taulukko 2: Tietoturvallisuuden riskienhallinnan toteutusesimerkki (Katakri 2020).

2.3.4 PiTuKri: Pilvipalveluiden turvallisuudenarviointikriteeristö

PiTuKri, eli pilvipalveluiden turvallisuudenarviointikriteeristö on ensisijaisesti tarkoitettu viranomaisten salassa pidettävän tiedon turvallisuuden edistämiseksi, silloin kun tietoja käsitellään pilvipalveluissa. PiTuKri on Kyberturvallisuuskeskuksen julkaisema ja viimeisin versio 1.1 julkaistiin 2020. Katakrin tavoin, PiTuKri tarjoaa vähimmäisvaatimuksia lainsäädännön ja velvoitteiden osalta. Kansallinen ja kansainvälinen lainsäädäntö ei ole kuitenkaan ajan tasalla pilviturvallisuusvaatimusten kanssa, jonka takia PiTuKri käyttää lähteinä kansainvälisesti tunnettuja pilviturvallisuuskriteeristöjä, kuten BSI:n kriteeristöä. Työkalua on tarkoitus käyttää pilvipalveluiden turvallisuuden arvioimiseen ja sitä voidaan käyttää omaehtoisen turvallisuustyön tukena. Vaikka pilvipalvelu olisi hankittu palveluntuottajalta, turvallisuutta ei kannata täysin pyrkiä ulkoistamaan heille. Tämän takia myös asiakkaan roolissa olevien organisaatiot tulisi perehtyä pilviturvallisuustarpeisiin sekä suunnitella että arvioida ne riittävällä tavalla. Valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan näkökulmasta PiTuKri ei tuo uusia vaatimuksia, mitä ei Katakri jo vaatisi. (PiTuKri 2020.)

2.3.5 Valtiovarainministeriön suositukset

Valtiovarainministeriö on tuottanut pitkään erilaisia turvallisuusohjeistuksia ja suosituksia valtionhallinnolle, joista monet myös soveltuvat yksityisten organisaatioiden käyttöön. Ministeriön kautta on tuotettu VAHTI-ohjeet sekä tiedonhallintalautakunnan suositukset.

Ohjeet ja suositukset eivät ole velvoittavia tai sitovia, vaan niissä pyritään ohjaamaan valtionhallinnon toimijoita toteuttamaan hyväksi todettuihin käytäntöihin pohjautuen lainsäädännössä säädetyt vaatimukset, esimerkiksi tietoturvallisuuden ja tiedonhallinnan osalta. (Valtiovarainministeriö 2021a.)

VAHTI on ministeriön asettama yhteistyö-, valmistelu- ja koordinaatioelin, jonka toiminnasta vastaa Digi- ja väestötietovirasto. VAHTI on toiminut nimillä: valtionhallinnon tietoturvallisuuden johtoryhmä (1992-2013), valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (2014-2016) sekä julkisen hallinnon digitaalisen turvallisuuden johtoryhmä (2017-2019). VAHTI-ohjeiden tarkoitus on pyrkiä kattamaan kaikki tietoturvallisuuden osa-alueet. Joissain ohjeissa viitataan vanhentuneeseen lainsäädäntöön, mutta niitä voidaan kuitenkin hyödyntää ottaen huomioon muuttunut lainsäädäntö. (Digi- ja väestötietovirasto 2020; Suomidigi 2020.)

VAHTI:n tavoitteena on parantaa valtiohallinnon toimintojen luotettavuutta, jatkuvuutta, laatua ja riskienhallinta varautumista tietoturvallisuutta kehittämällä. Lisäksi tavoitteena on pyrkiä saattamaan tietoturvallisuus kiinteäksi osaksi valtiohallinnon toimintaa, johtamista ja tulosohjausta. VAHTI ohjeissa nostetaan riskienhallinta tärkeäksi osaksi kutakin ohjetta. Ohjeet toteavat kuinka monet toiminnoista ja prosesseista ovat riippuvaisia riskienhallinnasta ja sen prosesseista. VAHTI-ohjeet perustuvat toiminnan riskienhallintaan, joten muissakin ohjeissa on vaikutuksia tietoturvallisuuden ja riskienhallinnan kehittämiseen kokonaisuutena. Tietoturvallisuus riskienhallintaan ja sen kehittämiseen soveltuvia VAHTI-ohjeita ovat ohje riskienhallinnasta, sovelluskehityksen tietoturvaohje sekä johdon tietoturvaopas. (Valtiovarainministeriö 2012.)

Ohje riskienhallintaan kuvaa SFS/ISO:31000 riskienhallinta standardiin pohjautuvan prosessin sekä kuvaa riskienhallinnan merkitystä johtamisen ja päätöksenteon välineenä. Ohje kuvaa tarkasti riskienhallintaprosessin ja siihen liittyvät vaiheet. Ohje esittelee riskienhallinnan viitekehystä sekä apuvälineitä kuten riskisalkku, riskienhallinnan vastuukuvausmallit ja keskeytysanalyysit. (Rousku 2017, 4.)

Vaikka sovelluskehityksen tietoturvaohje on tarkoitettu sovelluskehityksen tietoturvallisen elinkaaren kehittämiseen, ohje sisältää erilaisia suosituksia tietoturvallisuuden riskienhallintaan liittyen, joita voidaan hyödyntää muissa asiayhteydessä. Valtioneuvosto ei tee yleisesti ottaen sovelluskehitystä, mutta myös tilaajaroolissa olevien tulisi ymmärtää hyvän ja tietoturvallisen sovelluskehityksen periaatteet. (Valtiovarainministeriö 2013, 1.)

Ohjeessa on eritelty riskienhallinnan vaatimukset perus-, korotetulle sekä korkealle tasolle. Riskienhallintaprosessin yhtenä tarkoituksena on tunnistaa pahimmat mahdolliset uhkakuvat valtioneuvoston kanslian toiminta-alueiden toiminnalle ja tiedolle. Perustasolla tietoturvallisuuden riskienhallintaa tulee tehdä säännöllisesti sekä määritellä tunnistetut

riskienhallintakeinot ja sisällyttää tehtyjen toimenpiteiden vaikutuksen seuranta riskienhallintaprosessiin. Lisäksi riskien tunnistamiseen tulisi osallistua yksiköiden johdon lisäksi muut sidosryhmät. Korotetun tason vaatimuksissa on alemman tason vaatimuksien lisäksi vaatimus, että valtioneuvoston kanslian riskienhallintaprosessi tulee olla kuvattuna kirjallisesti esimerkiksi riskienhallintapolitikassa. Riskienhallintadokumentaation katselmoinnin tulisi olla säännöllistä ja sen tulisi olla vastuutettu tehtävä. Korkean tason vaatimuksiin kuuluu tietoturvallisuusriskien arviointi valtioneuvoston kanslian suurten muutosten yhteydessä ja näiden huomioon ottaminen riskienhallintaprosessissa. (Valtiovarainministeriö 2013, 35-36.)

Johdon tietoturvaopas on suunnattu valtiohallinnon johto- ja esihenkilö tehtävissä oleville henkilöille. Lisäksi se perustelee minkä takia tietoturvallisuutta tulisi toteuttaa. Valtioneuvoston kanslian tietoturvallisuuden perustaksi tarvitaan näkyvä johdon tuki, jolla varmistetaan tietoturvatyön toteuttamisen edellytykset. Tämän lisäksi tietoturvallisuuden tulisi olla integroitu osaksi kanslian johtamista ja toiminnan suunnittelua. Tietoturvaopas toteaa, että tietoturvatoimenpiteiden tulee perustua valtioneuvoston kanslian toiminnan riskien arviointiin. Kanslian johdon tehtävä on huolehtia, että säännönmukaista tietoturvallisuusriskien arviointia toteutetaan, joka on osana muuta riskienhallintaa, toiminnan suunnittelua tai laatumallia. Tietoturvallisuus integroituu riskienhallintaan tietoturvallisuusriskien arvioinnin kautta. Tietoturvallisuusriskit tulee arvioida etupainotteisesti suhteessa voimassa olevaan lainsäädäntöön, kustannuksiin sekä toimintaympäristön vaatimuksiin. Lisäksi niitä arvioidaan kanslian ydintehtävien ja niiden toteuttamiseksi asetettujen strategioiden ja tavoitteiden kautta. Valtioneuvoston kanslian riskienhallinnan toteutus tulisi olla kuvattuna kanslian tietoturvallisuuden hallintajärjestelmässä sekä Sisäisen valvonnan arviointi- ja vahvistuslausumassa. (Valtiovarainministeriö 2011, 4-16).

Tiedonhallintalautakunta on valtiovarainministeriön yhteydessä toimiva viranomainen, joka perustuu monialaiseen asiantuntijayhteistyöhön. Sen tehtävänä on ”edistää tiedonhallintalaissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tiedonhallintalain vaatimusten toteuttamista” (Valtiovarainministeriö 2021b). Lisäksi sen tehtävänä on valvoa julkishallinnon tiedonhallintalain noudattamista. Tietoturvallisuuden riskienhallintaan liittyviä suosituksia on esimerkiksi suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta sekä suositus turvallisuusluokiteltavien asiakirjojen käsittelystä. (Valtiovarainministeriö 2021c.)

Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä (2020) avaa tiedonhallintalain (906/2019) vaatimuksia sekä tiedonhallintalautakunnan suosituksia turvallisuusluokiteltavien asiakirjojen käsittelyssä. Suosituksessa perehdytään hallinnollisiin alueisiin sekä turva-alueisiin, asiakirjojen ja tietojärjestelmien suojaamiseen aiemmin mainittujen avulla,

tietojärjestelmien erotteluun sekä salausratkaisuihin. Suositukset ovat yleisesti ottaen riskiperusteisia, eli toimenpiteet ja kontrollit tulisi toteuttaa säännöllisen riskienhallintaan perustuen. (Valtiovarainministeriö 2020a.)

Suosituskokoelma tiettyjen tietoturvallisuussäädösten soveltamisesta (2020) avaa tiedonhallintalain (906/2019) vähimmäisvaatimuksia tietoturvallisuudelle sekä syventyy vahingoilta suojautumiseen, riskienhallintaan, lokitietojen keräämiseen sekä tiedon käsittelyn ja tietojärjestelmien elinkaariin. Riskienhallintaosuus perustuu pitkälti esimerkiksi VAHTI-ohjeeseen riskienhallinnasta. Suositus kuitenkin esittää kysymysmuodossa muutamia yleisiä vaatimuksien riskienhallintaan, jotka on esitelty taulukossa 3. (Valtiovarainministeriö 2020b.)

”Onko [valtioneuvoston kanslia] tunnistanut ja dokumentoinut kaiken tiedon ja kaikki tietojärjestelmät, joista se on vastuussa?”
”Onko näitä ylläpitävät ja käyttävät avainhenkilöt tunnistettu?”
”Onko tietoihin, tietojärjestelmiin ja avainhenkilöihin mahdollisesti kohdistuvat uhkatekijät tunnistettu?”
”Onko tiedoille ja tietojärjestelmille laadittu vaikutusanalyysi, jonka perusteella on mahdollista arvioida riskienhallintatoimenpiteiden oikeasuhtaisuus?”
”Ovatko riskienhallintatoimenpiteet oikeasuhtaiset riskin realisoitumisen vaikutukseen ja todennäköisyyteen nähden?”
”Ylläpidetäänkö riskirekisteriä ja arvioidaanko riskienhallintatoimenpiteiden toimivuutta säännöllisesti?”

Taulukko 3: Suosituskokoelman yleisiä vaatimuksia riskienhallinnalle (Valtiovarainministeriö 2020b, 15).

2.3.6 Tietoturvallisuuden standardit

Standardi on yleinen ratkaisu toistuvaan ongelmaan tai kun tavoitellaan tietty saavutustasoa. Nykypäivänä standardit kattavat laajan valikoiman toimintoja. Standardointi voi edellyttää muun muassa erittelyä siitä, miten tuote tulisi valmistaa tai miten tiettyä prosessia tulisi hallita. Standardit syntyvät kehittämällä yritysten ja tieteellisten laitosten asiantuntijoiden yksityiskohtaisia kuvauksia tuotteen tai palvelun erityispiirteistä. Ne edustavat yksimielisyyttä ominaisuuksista, kuten laadusta, turvallisuudesta ja luotettavuudesta, joiden tulisi olla sovellettavissa, sekä ne dokumentoidaan ja julkaistaan. Standardien kehittämisen tavoitteena

on tukea yrityksiä liiketoiminnassa. Organisaatio voi standardeja noudattamalla parantaa mainettaan. Menon Economics:in (Grimsby 2018) teettämän tutkimuksen mukaan jopa 91% vastanneista oli sitä mieltä, että standardit kasvattavat asiakkaiden luottamusta. (Disterer 2013; Grimsby 2018.)

Valtioneuvoston tietoturvallisuustarkistuksissa ja arvioinneissa voidaan hyödyntää tapauskohtaisesti myös muita standardeja, kriteeristöjä ja ohjeita. Nämä tietoturvallisuustarkistukset ja arvioinnit ovat tarkoitettu valtioneuvoston tieto- ja viestintäteknisille järjestelmille ja palveluille. Ne ovat kuitenkin osittain hyödynnettävissä tietoturvallisuuden riskienhallinnan arviointiin sekä kehittämiseen. Monet olemassa olevista ohjeista ja määräyksistä perustuvat ISO 27001 viitekehykseen. Tapauskohtaisesti muita hyödynnettäviä kriteeristöjä ovat valtioneuvoston kanslian ohjeiden mukaan esimerkiksi NIST Cyber Security Framework, Common Criteria sekä PCI DSS. (Valtioneuvoston kanslia 2019e.)

ISO on johtava kansainvälisten standardien myöntäjä, joka perustettu vuonna 1946. ISO 27000 kategoriaan kuuluvat standardit on kehitetty yhteistyössä International Electrotechnical Commissionin (IEC) kanssa, joka on johtava kansainvälisten standardien liikkeellelaskija elektroniikan teknologioiden alalla. Maailmanlaajuisesti käytetyt standardit ISO 27000, ISO 27001 ja ISO 27002 tarjoavat valvontatavoitteita, toimintamalleja, vaatimuksia ja ohjeita, joiden avulla valtioneuvoston kanslia voi saavuttaa standardin mukaisen tietoturvallisuuden tason. ISO 27001 on yksi yleisimmin käytetty tietoturvallisuuden standardi. Se on tietoturvallisuutta varten jäsennelty laajasti tunnustettu menetelmä, joka keskittyy eheyden, saatavuuden ja luottamuksellisuuden varmistamiseen. ISO 27001 on kuvattu hallintaprosessiksi, jota voidaan käyttää tietoturvan hallintajärjestelmän arviointiin, toteuttamiseen ja ylläpitoon. ISO 27001 sertifioitu taho on arvostettu ja sertifioidulla katsotaan olevan riittävä tietotuvallisuuden perusta, sekä ennen kaikkea turvallisuusorientoitunut asenne tietoturvallisuuden kehittämistä kohtaan. Yleisesti ottaen ISO 27001 sertifikaatti takaa sopimuksellisten tietoturvallisuuden vaatimuksien täyttämisen. (Disterer 2013; Talib, Barachi, Khelifi, Ormandjieva 2012.)

Ministeriöistä ulkoministeriö oli ensimmäinen, joka sai ISO 27001 tietoturvallisuus sertifikaatin. Ulkoministeriö sai sertifikaatin lokakuussa 2020. Ulkoministeriön valtiosihteeri Matti Anttonen kokee, että sertifikaatti vahvistaa hyviä tietoturvallisuuden johtamiskäytäntöjä sekä ylläpitää hyviä hallintatapoja, edistäen avoimuutta. Anttonen lisäksi koki, että sertifikaatti viestii ulkoministeriön sidosryhmille ministeriön luotettavuudesta sekä motivaatiosta ylläpitää ja kehittää tietoturvallisuutta. Valtioneuvoston kanslian käyttöönotettava hallintamalli tulisi mahdollisesti hyödyntämään ISO 27001 mallia viitekehyksenä. (Ulkoministeriö 2020.)

NIST:in kyberturvallisuuskehys, The Cybersecurity Framework, koostuu kolmesta pääkomponentista. Yksi komponenteista, The Core, koostuu joukosta toivottuja kyberturvallisuustoimia ja -tuloksia, jotka on järjestetty luokkiin. The Core:ssa on viisi tasoa, Identify, Protect, Detect, Respond ja Recover, jotka pitävät sisällään erilaisia teemoja, joiden alapuolella on tarkempia vaatimuksia. Erityisesti tasossa Identify on tietoturvallisuuden riskienhallintaan liittyviä vaatimuksia. Riskienhallintaan kategorioita on kolme, riskien arviointi, riskienhallinta strategia sekä toimitusketjun riskienhallinta. Cybersecurity Frameworkin vaatimukset eivät ole velvoittavia ja monet niistä ovatkin jo sisällytetty valtioneuvoston kanslian omiin tietoturvallisuusasiakirjoihin. NIST:in vaatimuksiin kuuluu käytännössä riittävästi resursoitu tietoturvallisuustoiminto, niin henkilöstön kuin tietojärjestelmien osalta. Lisäksi toiminnan tulisi olla riskiperusteista, joilla mahdolliset riskit ennaltaehkäistään mahdollisimman tehokkaasti. (NIST 2018; NIST 2020.)

Common Criteria standardi koostuu 60 turvallisuusvaatimuksesta 11 eri luokassa. Common Criteria on enemmän arviointityökalu, joka on kehitetty useamman eri standardin ja vaatimuspatteriston yhdistelmänä, helpottaakseen kansainvälisten tietoturvallisuusvaatimusten arviointia omassa organisaatiossa. Common Criteria ei kuitenkaan arvio hallinnollisia toimia eikä täten sisällä vaatimuksia tietoturvallisuuden riskienhallinnalle. (Mead 2013; Common Criteria 2017.)

Maksukorttiteollisuuden tietoturvastandardi (Payment Card Industry Data Security Standard, PCI DSS) on joukko vaatimuksia, joiden tarkoituksena on varmistaa, että luottokorttitietoja käsittelevät yritykset ylläpitävät turvallista käsittely-ympäristöä. Vaikka valtioneuvoston kanslia ei kuulu näihin, teemat ovat samankaltaiset. Yritykset käsittelevät arkaluonteista materiaalia ja se halutaan pitää suojattuna, ja tavoitteet tietoturvallisuuden osalta on samat kanslialla. PCI DSS sisältää tietojärjestelmävaatimuksia, joiden tarkoitus on taata turvallinen maksutietojen käsittely ja säilyttää asiakkaiden luottamus. PCI DSS sisällyttää jatkuvan kehittämisen periaatteita, joilla pyritään estämään tietoturvaloukkauksia sekä kehittämään IT-infrastruktuurin tehokkuutta sekä tukemaan kanslian turvallisuusstrategioita. 12 kohdan vaatimuslistan viimeinen vaatimus on että, organisaatiolla on oltava tietoturvallisuuspolitiikka. Standardi tarkentaa, että lisäksi on toteutettava vähintään vuosittain tai ison organisaationaalisen muutoksen yhteydessä riskienarviointiprosessi, jossa tunnistetaan kriittiset resurssit, uhat ja haavoittuvuudet. Tämän lisäksi tulokset ja riskianalyysi tulisi dokumentoida. (Mustoe 2020; PSI Security Standards Council 2018.)

3 Kehittämistyön menetelmät

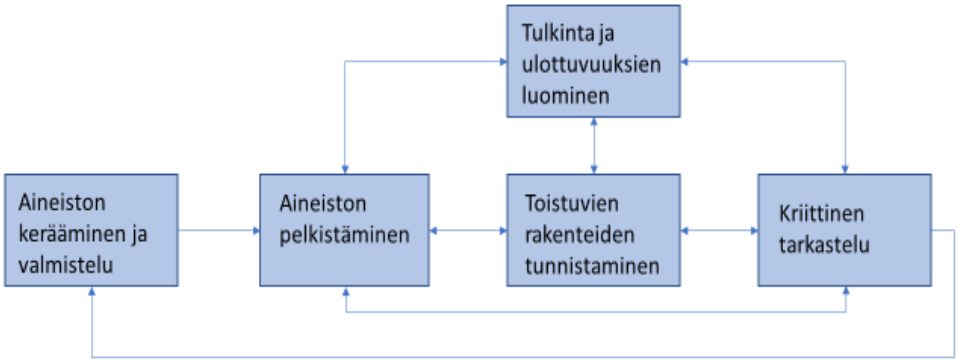
Tämän luvun tarkoituksena on esitellä ja perustella opinnäytetyössä käytettyjä kehittämistyön menetelmiä. Laadullinen kehittämisnäkökulma valittiin kehittämistyön

strategiaksi, sillä tarkoituksena on tuottaa kehittämisehdotuksia tulkittua tiedon sekä tutkimuksen keinoin. Onkin tyypillistä, että kehittämistyössä käytetään useita erilaisia menetelmiä. Kehittämiskohde on valittu käytännön tarpeen ja valtioneuvoston kanslian asetettujen tavoitteiden ohjaamana. Ensin valtioneuvoston kanslian edustajien kanssa määriteltiin kehittämisongelma. Tämän jälkeen tietoturvallisuuden riskienhallintaan perehdyttiin käytännössä ja teoriassa. Aineistoa kerättiin ja analysoitiin eri menetelmillä, ja tuloksina tuotettiin lopulta erilaisia kehittämisehdotuksia. (Ojasalo, Moilanen & Ritalahti 2015, 52-54.)

Opinnäytetyön kehittämistavoite oli, kuinka valtioneuvoston kanslian tietoturvallisuuden riskienhallintaa voitaisiin kehittää. Kehittämisehdotuksissa otettiin huomioon niiden toteutuskelpoisuus sekä tarpeellisuus. Ennen kehittämisehdotuksia, tulisi arvioida valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan nykytila. Nykytilan arviointia varten tulee selvittää valtioneuvoston kansliaan kohdistuvat vaatimukset ja velvoitteet. Nykytilan kartoitus luo pohjan kehittämistyölle ja kehittämisehdotukset voidaan kohdentaa tarpeellisiin osiin. Opinnäytetyö pyrki selvittämään mitä vaatimuksia lainsäädäntö, ohjeet sekä tilannekuva-arviot asettavat tietoturvallisuuden riskienhallinnalle. Valtioneuvoston kanslian tietoturvallisuutta määrittelevä lainsäädäntö on pirstaleinen. Lisäksi useat erilaiset asetukset, määräykset ja ohjeet luovat vaatimuksia. Selvittämällä velvoittavat ja suositellut vaatimukset on helpompi luoda tarvittava kehys ja arvioida kehittämistarpeita. Vaatimuksia kartoitettiin kirjallisuuskatsauksella sekä dokumenttianalyysilla. Lisäksi tietoturvallisuuden riskienhallinnan nykytilaa arvioitiin kyselyn sekä puolistrukturoidun haastattelun, eli teemahaastattelun avulla. Haastattelusta saadun aineiston analysoimiseen käytettiin dokumenttianalyysin menetelmiä. Käyttökelpoisia kehittämisehdotuksia tutkittiin käyttämällä dokumenttianalyysia sekä strukturoidun kirjallisuuskatsauksen menetelmiä.

3.1 Dokumenttianalyysi

Tietoperustan kokoamiseksi, vaatimusten listaamiseksi sekä tulosten tulkintaa varten hyödynnettiin dokumenttianalyysia. Dokumenttianalyysi toteutettiin ilmisisällön analyysillä, jossa pyritään kuvaamaan dokumenttien sisältöä sanallisesti, tavoitteena tunnistaa tekstin merkityksiä. Dokumenttianalyysin prosessi on samankaltainen kuin laadullisen tutkimuksen yleinen malli (kuvio 6). Dokumenttianalyysin prosessiin kuuluu aineiston kerääminen ja valmistelu, aineiston pelkistäminen, toistuvien rakenteiden tunnistaminen sekä tulkinta. Lisäksi kaikkiin vaiheisiin kuuluu kriittinen tarkastelu, jonka tarkoituksena on parantaa tulosten laatua ja luotettavuutta tunnistamalla eri vaiheissa mahdollisesti esiintyviä virheitä tai vääristymiä. Dokumenttianalyysiä menetelmänä käytettiin myös teemahaastattelujen litteroinnissa. (Moilanen, Ojasalo & Ritakoski 2015, 136-138.)



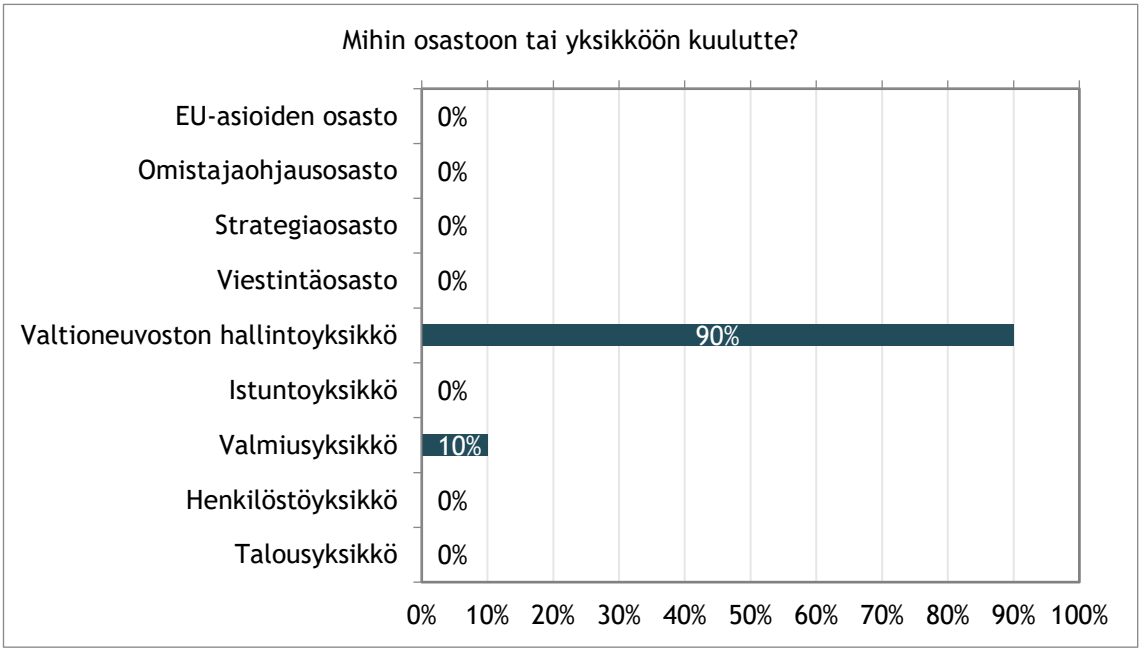
Kuvio 6: Laadullisen tutkimuksen yleinen malli (Moilanen, Ojasalo & Ritakoski 2015, 138).

Aineiston kerääminen oli paikoittain haastavaa pirstaleisuuden takia. Valtioneuvoston kansliaa koskevaa lainsäädäntöä ei ole kokonaisuudessaan avattu, vaan velvoittavaa lainsäädäntöä joutui etsimään eri määräyksistä ja ohjeista. Lainsäädännön osalta piti lisäksi vertailla lakeja keskenään ja varmistua että lait ovat edelleen ajan tasalla ja velvoittavia. Valtioneuvoston kanslian omat määräykset ja ohjeet eivät ole myöskään koostettuna aiheittain. Tietoturvallisuuden intrasivuille (2020c) on koottu merkittävimmät tietoturvallisuuteen liittyvät määräykset ja ohjeet. Muut ei velvoittavat ohjeet, kuten VAHTI-ohjeet ja standardit oli helpompi löytää, kun näihin oli viitattu kanslian dokumenteissa. Osassa VAHTI-ohjeissa haasteena on vanhentuneet lainsäädännölliset viittaukset, joista piti tulkita, miten ohjeet mukautuvat nykylainsäädäntöön. Dokumentit arkistoitiin sähköisesti.

3.2 Kysely

Kyselyn (liite 2) tarkoituksena oli selvittää valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan nykytilaa. Kysely toteutettiin Webropol sovelluksella ja sähköpostitse levitettynä internetkyselynä, jossa vastaajilla oli kaksi viikkoa vastausaikaa. Kyselyssä osin hyödynnettiin tyypillisesti kyselytutkimuksessa käytettyjä menetelmiä. Kysely koostui 12 monivalintakysymyksestä sekä kolmesta avoimesta kysymyksestä. Kyselyä oli mukautettu siten, että toinen kysymys tuli vaihtoehdoiksi vain heille, ketkä valitsivat ensimmäisessä kysymyksessä yksikön, jonka alla on yksiköitä tai osastoja. Havaintoyksikköinä olivat valtioneuvoston kanslian eri yksiköiden ja osastojen johtohenkilöt, joiden vastuulla on oman toimialansa tietoturvallisuuden riskienhallinta. Valtioneuvoston kanslian organisaatiokartasta (kuvio 1) sai muodostettua täten kattavan otantakehikon. Kyselyn perusjoukko, joille kysely lähetettiin, kattoi kattavasti kaikki valtioneuvoston kanslian organisaatioon kuuluvat toiminnot. Kyselyssä ei kysytty henkilötietoja, joten kyselystä ei ilmene ketkä ovat vastanneet. Kyselyssä kerättiin yksikkö tai osasto, josta voi kuitenkin päätellä ketkä ovat

vastanneet. Perusjoukkoon kuului 40 henkilöä, joista 10 vastasi kyselyyn (taulukko 4). Osa henkilöistä oli siirtynyt muihin tehtäviin tai virkavapaalle, mutta kyselyä ei välitetty mahdollisille sijaisille tai seuraajille, sillä otanta perustui julkisista lähteistä saatavaan organisaatiokarttaan (kuvio 1).



Taulukko 4: Kyselyn 1. kysymyksen vastaukset

Kysely perustui otantaan, jolloin tulokset olisi voinut yleistää koskemaan koko perusjoukkoa, mutta kyselyyn vastanneista 9 henkilöä edusti valtioneuvoston hallintoyksikköä. Valtioneuvoston hallintoyksikkö on suurin valtioneuvoston kanslian yksiköistä ja 24 perusjoukkoon kuuluvista ovat osa yksikköä. Valtioneuvoston hallintoyksikkö koostuu hyvin monipuolisesti eri alan toiminnoista ja sen voidaan katsoa kattavan kuitenkin hyvin valtioneuvoston kanslian toiminnot. Tavoiteltua otantaa ei kuitenkaan saavutettu ja se huomioitiin vastauksien analysoinnissa. Pienen vastausmäärän takia kyselyä ei tule tulkita kyselytutkimuksen tavoin, vaan enemmin laadullisena lomakehaastatteluna.

Epävarmuustekijöitä internetkyselyssä aiheutti se, ettei haastattelija ollut avustamassa tai valvomassa vastaamista. Lisäksi epävarmuutta aiheutti mahdollinen kyselytulva tai vastausväsymys, joka ilmeni vastausmäärissä. Haasteena oli myös perusjoukkoon kuuluvat havaintoyksiköt. Kyselyn saaneista monet ovat korkean tason virkamiehiä, joille erityisesti COVID19 -tilanne on merkittävästi lisännyt työmäärää, joka omalta osaltaan saattoi vaikuttaa vastausintoon. Vastausaikaa ei katsottu tarpeelliseksi pidentää, sillä suurin osa vastauksista tuli alle kahden tunnin sisään ensimmäisen tai toisen viestin lähettämisen jälkeen. Vain yksi vastaus tuli tämän aikaikkunan ulkopuolelta. Mahdollisesti kolmas muistutuskierros olisi

todennäköisesti nostanut kyselyyn vastanneiden määrää vain muutamalla vastaajalle. (Moilanen, Ojasalo & Ritakoski 2015, 129.)

Kyselyssä (liite 2) pyrittiin ymmärrettävään sekä yksinkertaiseen kysymystenasetteluun, joka olisi kuitenkin kehittämistehtävän kannalta kattava. Hirsjärven, Remeksen ja Sajavaaran (2004) suosituslistan mukaisesti kysely pyrittiin luomaan selkeäksi, jossa on yksiselitteisiä kysymyksiä. Kysymykset pyrittiin luomaan tarkoiksi ja ne pyrittiin pitämään lyhyinä. Kysymysten määrä pyrittiin pitämään maltillisena ja käytetty kieli ymmärrettävänä. Kysymyksissä oli ”en osaa sanoa / en ole varma” -vaihtoehto, tosin monivalintavaihtoehtoja ei käytetty, vaan ”kyllä” ja ”ei” -vaihtoehtoja. Tähän vaihtoehtoon päädyttiin, sillä katsottiin, että mikäli jokin asia ei täysin toteudu kysymyksen mukaisesti, silloin vaatimus ei toteudu. (Moilanen, Ojasalo & Ritakoski 2015, 131.)

Kyselyssä oli myös kehitettävää. Osa kysymyksistä oli muotoiltu siten, että ne koostuivat käytännössä kahdesta kysymyksestä. Tämä aiheuttaa epävarmuutta siitä, miten vastaajat ovat ymmärtäneet kysymyksen ja ovatko he esimerkiksi vastanneet vain osaan kysymyksestä. Kysymysten olisi pitänyt olla yksiosaisia, selkeämpiä, erityisesti silloin kun kyselyä ei päästä valvomaan ja tarvittaessa antamaan tarkentavia ohjeita kysymyksiin.

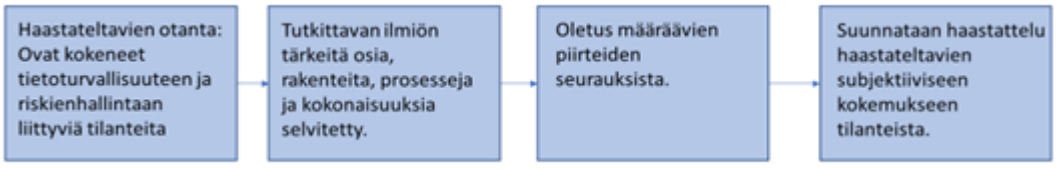
Sähköpostitse levitettävään Webropol internetkyselyyn päädyttiin kustannus-, vaivattomuus- ja nopeusetujen vuoksi. Kyselylomake testattiin ennen jakelua ja annettiin alaa tunteville henkilöille täytettäväksi. Lisäksi kyselyn mukana lähetettiin saatekirje, jossa kuvailtiin lyhyesti, mikä on kyselyn tarkoitus ja tavoite, tekijä, tulosten käytöstä, viimeinen palautuspäivämäärä, etukäteiskiitokset vastauksista ja yhteistyöstä sekä tekijän ja teettäjän nimet. Muistutuskierros toteutettiin noin viikko ennen viimeistä palautuspäivämäärää. Moilanen, Ojasalo & Ritakoski (2015) toteaa, että muistutuskierros tulisi toteuttaa mahdollisimman pian vastauskierroksen vastausajan päättymisen jälkeen. Aikatauluhaasteiden takia näin ei kuitenkaan toimittu, vaan muistutuskierros lähetettiin kesken ensimmäisen ja ainoan vastauskierroksen aikana. Saatteessa toistettiin aiemman saatteen teksti, jonka lisäksi saatteessa oli maininta, ettei jo vastanneiden tarvitse vastata, etukäteiskiitokset vastaamisesta, vastausten viimeinen palautuspäivämäärä päivämäärän ja kellonajan tarkkuudella sekä uudestaan tekijän ja teettäjän nimet. (Moilanen, Ojasalo & Ritakoski 2015, 128-134.)

3.3 Teemahaastattelu

Teemahaastattelu, tunnetaan myös puolistrukturoituna tai puolistandardoituna haastatteluna, valittiin yhdeksi kehittämismenetelmäksi, sillä sen avulla haluttiin saada syventää tietoa tietoturvallisuuden riskienhallinnasta sekä haluttiin selventää erityisesti kyselystä saatuja vastauksia tietoturvallisuuden riskienhallinnan nykytilasta. Haasteita teemahaastattelun käytössä kehittämismenetelmänä on sen viemä aika sekä virhelähteiden mahdollisuus. Lisäksi

teemahaastattelu vaatii haastattelijoilta taitoa ja kokemusta sekä molempiin rooleihin, haastattelijan sekä haastateltavan rooleihin, tulisi kouluttautua. Haastateltavat ihmiset olivat kaikki kokeneita virkahenkilöitä, ketkä ovat eri näkökulmista käsitelleet tietoturvallisuuden riskienhallintaa. Opinnäytetyötä varten haastateltiin valtioneuvoston kanslian osastopäällikköä, toimialajohtajaa, kahta yksikön päällikköä sekä palvelupäällikköä. Teemahaastattelun käyttö mahdollisti haastattelun etenemisen tietoturvallisuuden ja riskienhallinnan teemojen ympärillä, mahdollistaen henkilöiden omien tulkintojen sekä ajatuksien esille tuomisen. Kehittämismenetelmälle ominaisesti haastatteluissa oli kaikissa samat teema-alueet. (Hirsjärvi & Hurme 2008.)

Ensin valittiin haastateltavien otanta. Otantaan valikoitu johtotason henkilöstöä, ketkä ovat kokeneet tietoturvallisuuteen ja riskienhallintaan liittyviä tilanteita. Lisäksi selvitettiin aineistosta tietoturvallisuuden riskienhallintaan liittyviä prosesseja ja kokonaisuuksia ja tehdään oletus määräävien piirteiden seurauksista haastattelussa. Teemahaastattelun prosessi kuvataan kuviossa 7. Haastattelu päätetiin toteuttaa verkossa Skype-sovelluksessa johtuen voimassa olevasta laajasta etätyösuosituksesta. Videokuvaa ei käytetty. Haastatteluajat sovittiin hyvissä ajoin ennen haastatteluja. Teemahaastattelujen tarkoituksena oli täydentää kyselystä saatua pintapuolisempaa kvantitatiivista tietoa syvällisemmällä kvalitatiivisella tiedolla. Haastatteluita varten varattiin 30 minuuttia henkilöä kohden. Haastatteluun varattu aika oli lyhyt ja se näkyikin haastatteluihin käytetyssä ajassa, sillä jokainen haastattelu meni yliajalle. Aika jouduttiin pitämään henkilöiden aikataulusyistä lyhyehkönä. Haastatteluissa pyrittiin suuntaamaan haastattelu haastateltavien subjektiivisiin kokemuksiin tietoturvallisuuden riskienhallinnan eri tilanteista. Haastattelut äänitettiin ja ne litteroitiin puhekielen mukaisesti. Tämän jälkeen litteroitu aineisto analysoitiin lukemalla se useampaan kertaan, jonka jälkeen se luokiteltiin ja purettiin teema-alueittain. Saturaatiopiste saavutettiin, sillä uudet haastattelut eivät varsinaisesti tuottaneet kehittämistehtävän kannalta merkittävää uutta tietoa. Oleellisempaa olisi ollut saada lisää vastaajia kyselyyn. (Ojasalo, Moilanen & Ritalahti 2015, 106-108; Merton, Fiske & Kendall 1990, 3-4.)



Kuvio 7: Teemahaastattelun prosessi (Merton, Fiske & Kendall 1990, 3-4).

Etä- ja verkkohaastatteluilla on joitakin hyviä puolia fyysiseen haastatteluun verrattuna. Sähköisessä vuorovaikutuksessa, vaikkakin puhelussa, vastaajalla on enemmän aikaa pohtia ja

vastata kysymyksiin, ilman että se vaikuttaa poikkeavalta vuorovaikutukselta. Lisäksi esimerkiksi vaikeista asioista puhuminen, kuten tietoturvallisuudesta ja riskienhallinnasta, voi olla miellyttävämpää, kun haastattelija ei näytä tuomitsevalta. Etänä ja verkossa tapahtuvissa haastatteluissa yleensä pidetään tiukemmin kiinni ennakkoon sovituista aikatauluista, kun taas fyysisessä haastattelussa ollaan joustavampia aikataulujen suhteen. (Bampton & Cowton 2002, 3-6.)

Etä- ja verkkohaastatteluilla on kuitenkin huonojakin puolia. Mikäli haastattelussa ei käytetä esimerkiksi webkameraa, jää erilaisten ilmeiden ja eleiden havainnointi kokonaan pois. Webkameraakin käyttäessä kehonkielen lukeminen on rajatumpaa kuin kasvotusten keskusteltaessa. Tämä voi johtaa siihen, että reaktiot tiettyihin asioihin jäävät huomaamatta ja esimerkiksi haastateltavan epämukavuus ja -varmuus jää huomaamatta, jolloin haastattelija ei välttämättä ymmärrä reagoida tilanteeseen. Oman kokemukseni mukaan myös etä- ja verkkohaastatteluita tehdessä on keskityttävä tarkemmin, toisin kuin kasvotusten, jolloin keskustelu on luonnollisempaa. (Bampton & Cowton 2002, 3-6.)

3.4 Kirjallisuuskatsaus

Kirjallisuuskatsaus toteutettiin hyödyntämällä strukturoidun kirjallisuuskatsauksen menetelmiä. Kirjallisuuskatsausta ei voida pitää strukturoituna kirjallisuuskatsauksena, sillä sen toistettavuus on haasteellista sekä otantaan valittujen tutkimusten kriteeristö paikoittain joustava ja tulkinnanvarainen. Menetelmä oli kuitenkin opinnäytetyön tavoitteisiin nähden riittävä ja se tuotti riittävän määrän tietoa. (Jesson, Matheson & Lacey 2011, 36.)

Aiheena julkishallinnon tietoturvallisuuden riskienhallinnan kehittäminen ei ole kovinkaan tutkittu. Yksityisten yritysten tietoturvallisuuden sekä riskienhallinnan kehittämisestä löytyy sen sijaan hyvinkin paljon tutkimusta ja kirjallisuutta. Tutkimus ja kirjallisuus kerättiin käyttäen Google Scholar hakukonetta. Suomenkielisten hakusanojen lisäksi käytettiin vastaavia englanninkielisiä hakusanoja, sillä tietoturvallisuuteen liittyvät tutkimukset on monet kirjoitettu englanniksi. Lisäksi tietoturvallisuuden riskienhallintaan liittyvät rakenteet ja haasteet julkishallinnossa ovat kansainvälisesti vertailukelpoisia.

Strukturoitu kirjallisuuskatsaus koostuu hausta, kriteeristön valinnasta, analysoinnista sekä lopulta tuloksista. Hakuja tehtiin jokaisen hakusanajoukon osalta kerran. Haut tehtiin loka- ja marraskuussa 2020. Google Scholarista haettu tutkimus on kerätty useammalla eri hakusana yhdistelmällä. Ensimmäinen hakusana yhdistelmä oli ”julkishallinto”, ”tietoturvallisuus” ja ”riskienhallinta”. Toinen hakusana yhdistelmä oli ”valtioneuvosto”, ”tietoturvallisuus” ja ”riskienhallinta”. Näiden kahden lisäksi haettiin vastaavia englanninkielisillä termeillä kahdella vastaavanlaisella yhdistelmällä: ”public administration” (julkishallinto), ”government” (valtioneuvosto), ”information security” (tietoturvallisuus) sekä ”risk management” (riskienhallinta). Englanninkieliset haut tuottivat suuren määrän tuloksia ja

suoraa yhteyttä julkishallintoon oli vaikea arvioida. Suurta määrää hakutuloksia tulisi pyrkiä pienentämään käyttämällä Boolean-hakua, jossa käytetään loogisia operaattoreita, kuten AND, OR, ja NOT. Boolean-haun avulla hakutuloksien määrää olisi mahdollista pienentää helpommin käsiteltävään määrään. (Jesson, Matheson & Lacey 2011, 36.)

Haut eivät tuottaneet kovinkaan montaa täsmällisesti aiheeseen sopivaa tutkimusta eikä ulkopuolisia viittauksia julkaisuihin juurikaan ollut. Haun tiedot esitellään taulukossa 5. Otantaan valittiin vuoden 2010 ja tuoreemmat julkaisut sekä vertaisarvioitu kirjallisuus. Lisäksi rajattiin pois yliopistojen kandidaattien tutkielmat sekä alemman ammattikorkeakoulututkinnon opinnäytetyöt. Hakutuloksissa esiintyä lisäksi VAHTI-ohjeita ja VAHTI toimintasuunnitelmia, jotka rajattiin pois, sillä ne kuuluvat jo tutkimusaineistoon osana tietoperustaa. Otantaan valittiin tulokset, jotka liittyivät tietoturvallisuuteen ja/tai riskienhallintaa julkishallinnon näkökulmasta.

Haku	Hakusanat	Tulokset	Otantaan
#H1	”julkishallinto”, ”tietoturvallisuus”, ”riskienhallinta”	535	3
#H2	”valtioneuvosto”, ”tietoturvallisuus”, ”riskienhallinta”	705	2
#H3	”government”,” information security”, ”risk management”	181000	3
#H4	“public administration”, ”information security”, ”risk management”	354000	9

Taulukko 5: Google Scholar hakujen tiedot

Otantaan valittuun teokset, joka esitellään liitteessä 3, perehdyttiin ja niistä muodostettiin taulukko. Taulukkoon kirjattiin teoksista lyhyt kuvaus sekä tärkeimmät avainsanat. Tämän avulla saadaan kattava yleiskuva käsitellyistä teoksista ja teemoista, joita ne käsittelevät.

Taulukoiduista avainsanoista jätettiin selkeästi tekniseen tietoturvallisuuteen liittyvät pois ja jäljelle pyrittiin jättämään hallinnolliset organisatoriset toimenpiteet, joita voisi soveltaa valtioneuvoston kansliassa. Tutkimuksista nousi esille erityisesti tietoturvallisuustietoisuuteen ja -osaamisen lisääminen organisaatiossa sekä riittävä tietoturvallisuusviestintä. Nostetuista aiheista muodostettiin erilaisia kehittämisehdotuksia, jotka esitellään luvussa 5.

Strukturoitu kirjallisuuskatsaus menetelmänä vaatii tutkittavan alan osaamista ja ymmärrystä eikä välttämättä sovi alemman ammattikorkeakoulututkinnon tasolla oleviin katsauksiin. Menetelmä on aikaa ja resursseja vaativa ja yleisesti sen toteuttaisi joukko ihmisiä, ei niinkään yksi henkilö. Katsauksessa tulisi tarkasti, systemaattisesti sekä kattavasti hakea kaikki relevantti kirjallisuus. Kirjallisuuskatsauksen tehokkuus on hyvin vahvasti sidoksissa käytettyyn sähköiseen tietokantaan ja sen rajallisuuksiin, jonka takia suositellaan useamman sähköisen tietokannan käyttöä. (Jesson, Matheson & Lacey 2011, 98.)

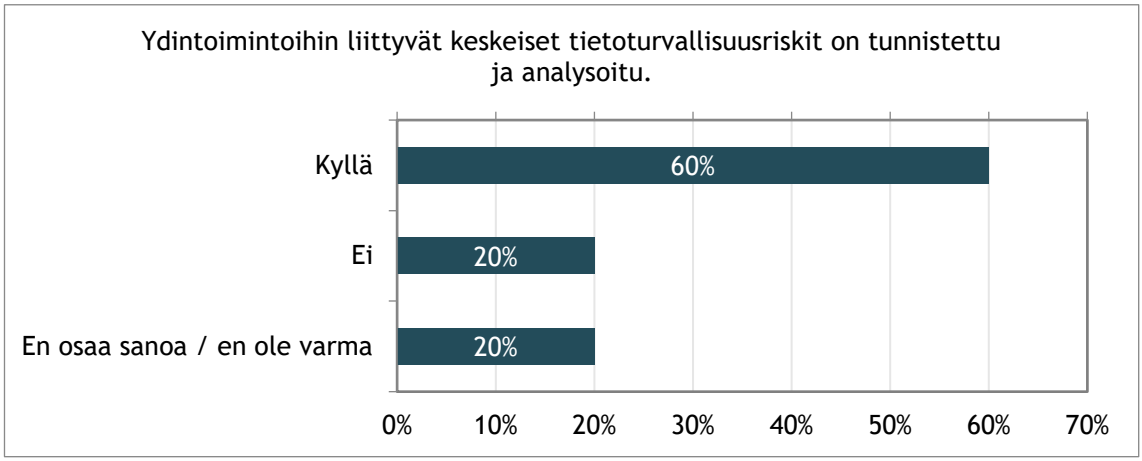
4 Tietoturvallisuuden riskienhallinnan nykytila

Kyselyllä ja teemahaastatteluilla saaduilla nykytila kartoituksen tuloksien avulla voitiin tarkastella sopivia kehittämisehdotuksia tietoturvallisuuden riskienhallinnan kehittämiselle kansliassa. Lähdemateriaaliin kuuluvasta valtioneuvoston kanslian dokumentaatiosta tulee ilmi, että dokumentit ovat kohtalaisen tuoreita, vuosilta 2017-2020, mikä viestii tietoturvallisuuden ja riskienhallinnan ajankohtaisuudesta ja siitä, että asia on tunnistettu tärkeäksi kanslian johdon toimesta.

Nykytilan kartoitus toteutettiin osastojen ja yksiköiden päälliköille suunnatulla kyselyllä, teemahaastatteluilla sekä dokumenttianalyysilla. Näistä saatuja vastauksia analysoitiin ja verrattiin voimassa oleviin vaatimuksiin. Vastaajat olivat kuitenkin keskittynyt hyvin vahvasti yhteen yksikköön, joten varmuudella ei voida päätellä tuloksien koskevan koko valtioneuvoston kansliaa. Vastaukset ovat kuitenkin suuntaa näyttäviä, ja niistä voidaan käynnistää tarvittavat jatkotutkimukset eri yksiköihin.

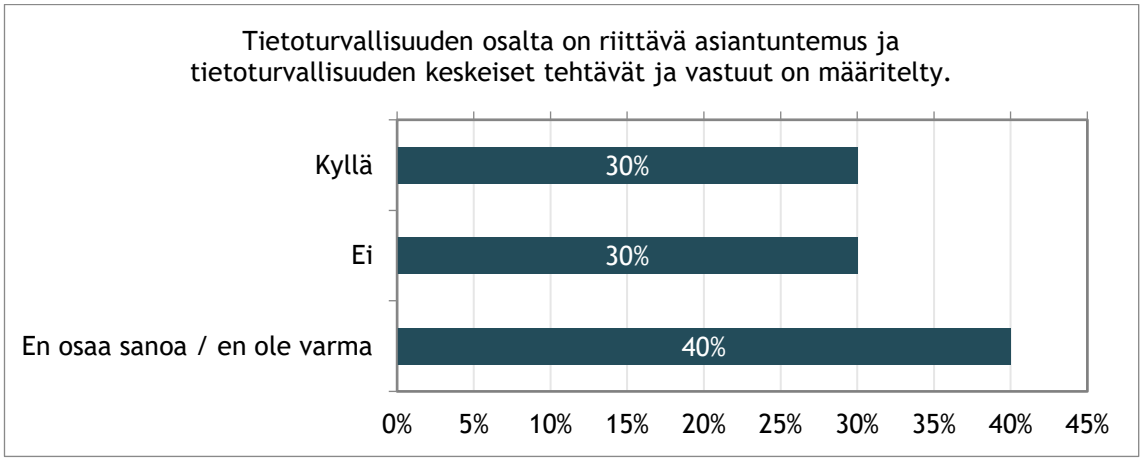
Tietoturvallisuuden riskienhallinnalle ei ole yhtenäistä prosessia, vaan jokainen yksikkö vastaa omalta osaltaan sen toteutumisesta tietoturvapolitiikan ja ohjeistuksien mukaan. Vastuut tietoturvallisuuden riskienhallinnan osalta koettiin epäselväksi ja käytännön yhteistyötä tulisi kehittää. Eri osastojen ja sidosryhmien välisessä viestinnässä on puutteita ja samoin tietoturvallisuuden tilan ymmärryksessä, erityisesti valmiusyksikön ulkopuolella. Itse riskienhallinnan prosessi koettiin epäselväksi ja siihen toivottiin koulutusta sekä tukea. Yksiköissä kuitenkin suhtaudutaan tietoturvallisuuteen vakavasti ja henkilöstö on sitoutunut toimimaan annettujen ohjeiden mukaisesti. (Yksikön päällikkö 2020; Yksikön päällikkö 2 2020.)

Kuusi kyselyyn vastanneista koki, että oman yksikön tai osaston ydintoimintoihin liittyvät keskeiset tietoturvallisuusriskit oli tunnistettu sekä analysoitu. Kaksi vastaajista ei kokenut näin tapahtuvan tai ei tiennyt varmaksi näin tapahtuvan, kuten taulukosta 6 ilmenee. Toimialajohtaja (2020) lisäksi arvioi, että osalla vastaajista saattoi olla eriävä käsitys siitä, mitä ydintoiminto tarkoittaa. Vastauksien perusteella voidaan päätellä, että vaatimus tietoturvallisuusriskien tunnistamisesta ja analysoimisesta täyttyy, mutta aiheeseen tulisi kiinnittää huomiota.



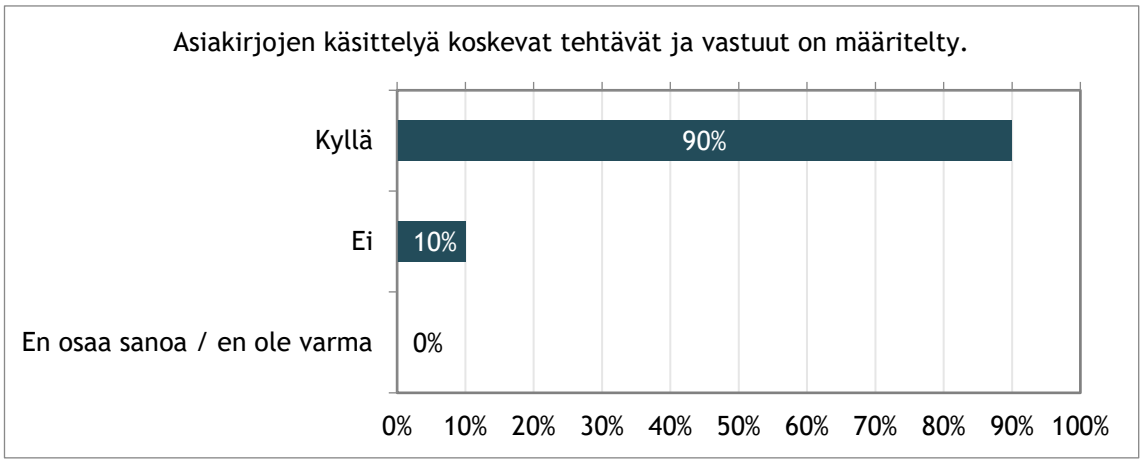
Taulukko 6: Kyselyn 3. kysymyksen vastaukset

Taulukon 7 tuloksista tulee ilmi, että vastaajien käsitys tietoturvallisuuden asiantuntemuksesta ja sen keskeisistä tehtävistä ja vastuista oli epäselvä. Suurin osa, neljä vastaajista vastasi, etteivät ole varmoja. Haastatteluissa tuli ilmi, että tämä saattaisi johtua vastuiden jaottelusta kahden eri yksikön välille sekä yleisestä tietämättömyydestä tietoturvallisuudesta. Tähän koettiin erääksi ratkaisuksi viestinnän ja tietoisuuden lisääminen tietoturvallisuuden vastuista ja tehtävistä valtioneuvoston kansliassa. Haasteina nähtiin hallinnollisen tietoturvallisuuden tarkemman kuvauksen puute kanslian työjärjestyksessä. Lisäksi palvelupäällikkö (2020) arvioi, että Valtorin rooli tietoturvallisuuden osalta on monelle epäselvä. Valtioneuvoston kanslialla on arvion mukaan riittävä asiantuntemus, vaikka kehittämiskohteita resurssien suhteen löytyy. Tietoturvallisuus kansliassa on kehittynyt ja kehittämisprojekteja on useita. Tästä voidaan päätellä, että minimivaatimukset täyttyvät, mutta asiaa tulisi tarkastella tarkemmin. (Osastopäällikkö 2020; Toimialajohtaja 2020.)



Taulukko 7: Kyselyn 4. kysymyksen vastaukset

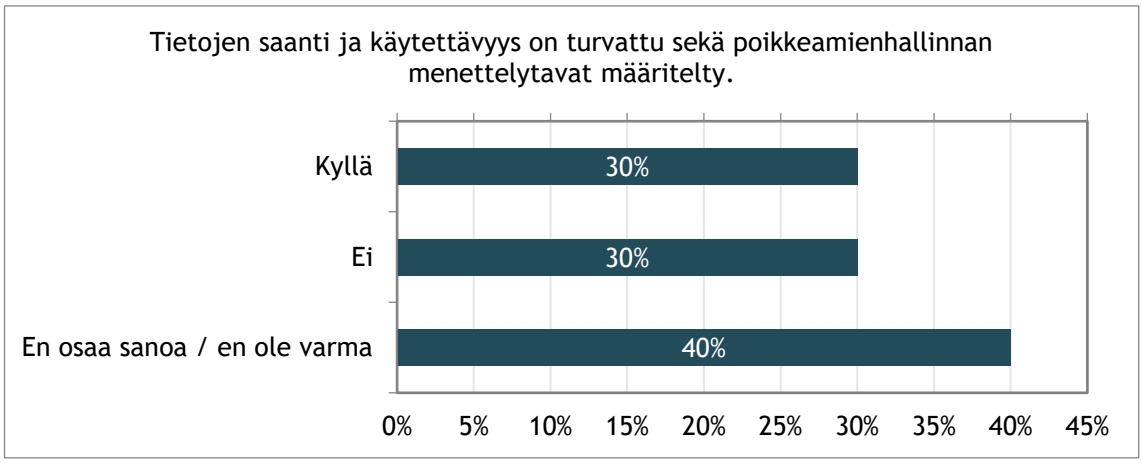
Lähes jokainen valtioneuvoston kanslian työntekijä käsittelee työssään asiakirjoja. Asiakirjojen käsittelyä koskevat tehtävät ja vastuut ovat valtioneuvoston kanslian ydintehtäviin kuuluvia asioita, ja yhdeksän koki niiden olleen määritelty (taulukko 8). Valtioneuvoston kanslian tietoaineistoturvallisuuden ohjeet ovat ajantasaiset ja käytettävät, joten vaatimus täyttyy. Kehittämiskohteita löytyy lähinnä teknisestä työasemaympäristöstä, jota kehittämällä, voisi entisestään kehittää tietoaineistoturvallisuutta. (Toimialajohtaja 2020.)



Taulukko 8: Kyselyn 5. kysymyksen vastaukset

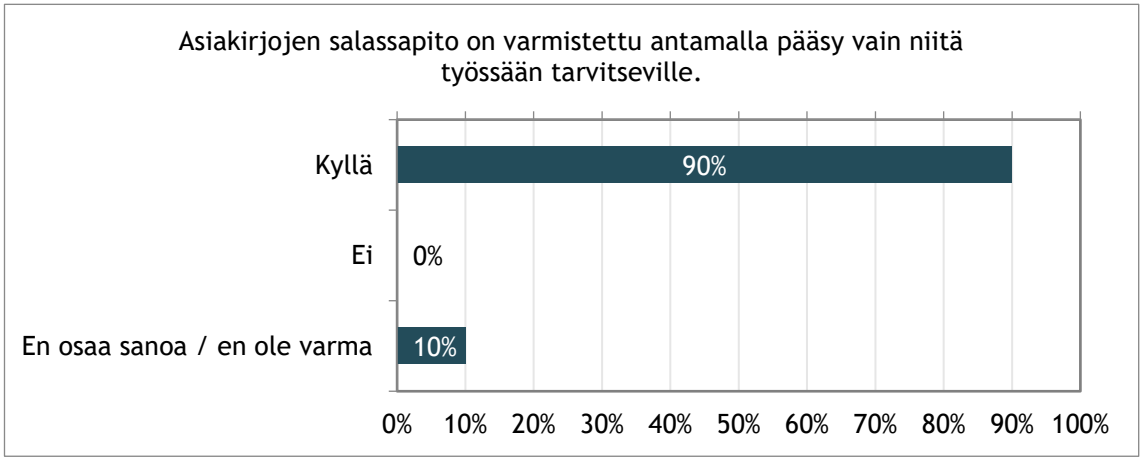
Kuten muutamatkin muutkin kysymyksen, seuraava kysymys (taulukko 9), on kyselyteknisesti hieman virheellinen. Poikkeamienhallinnan menettelytavat ovat suurimalle osalle tuntemattomia ja ne koskettavatkin ylempiä virkamiehiä ja niitä ketkä poikkeamienhallinnan prosesseissa ovat mukana. Vaikka yksittäinen käyttäjä käynnistää jonkin osan poikkeamienhallinnan prosessista, ei hän välttämättä tunne kokonaisuutta, eikä hänen tarvitsekaan. Neljä olivat epävarmoja toteutuvatko nämä ja loput menivät tasan ”kyllä” ja

”ei” vastauksille. Arvion mukaan normaalioloissa peruskäyttöön tarkoitettu tieto on hyvin saatavilla ja käytettävissä, mutta poikkeustilanteissa niiden turvaamisessa on vielä kehitettävää. (Palvelupäällikkö 2020.)



Taulukko 9: Kyselyn 6. kysymyksen vastaukset

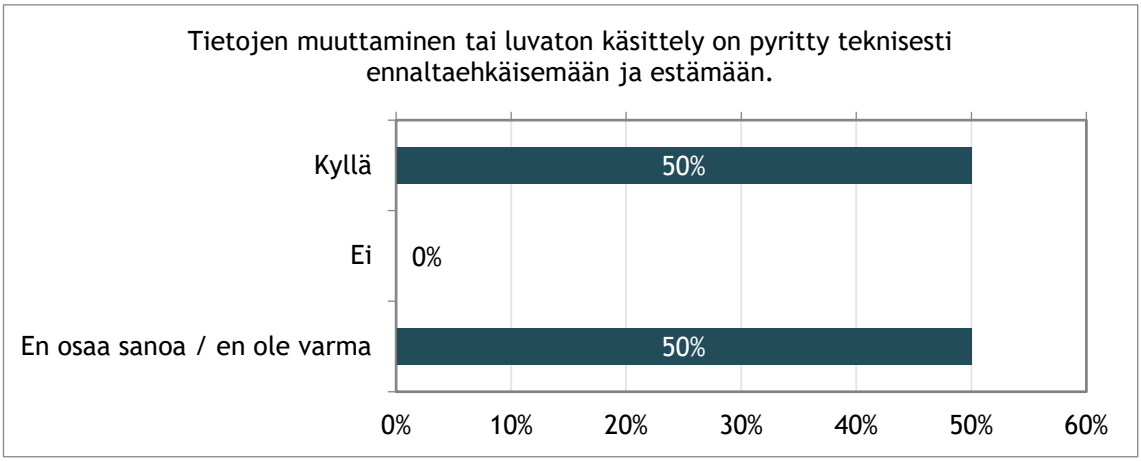
Yleisesti asiakirjojen tietoturvallisuus nähdään hyvänä (taulukko 10). Joillekin kuitenkin käsitys asiakirjasta on edelleen fyysisessä asiakirjassa, ja kysymyksen on osa ymmärtänyt koskettavan nimenomaan fyysisiä asiakirjoja, eli esimerkiksi pääsyllä tiloihin tai kassakaappiin. Kuitenkin lähes kaikki valtioneuvoston kanslia henkilökunnasta käsittelevät työssään asiakirjoja, joten usein tarve asiakirjoille on perusteltua. Asiakirjojen tietoturvallisuus onkin merkittävä aihe valtioneuvoston tietoturvallisuuskoulutuksissa. (Osastopäällikkö 2020.)



Taulukko 10: Kyselyn 7. kysymyksen vastaukset

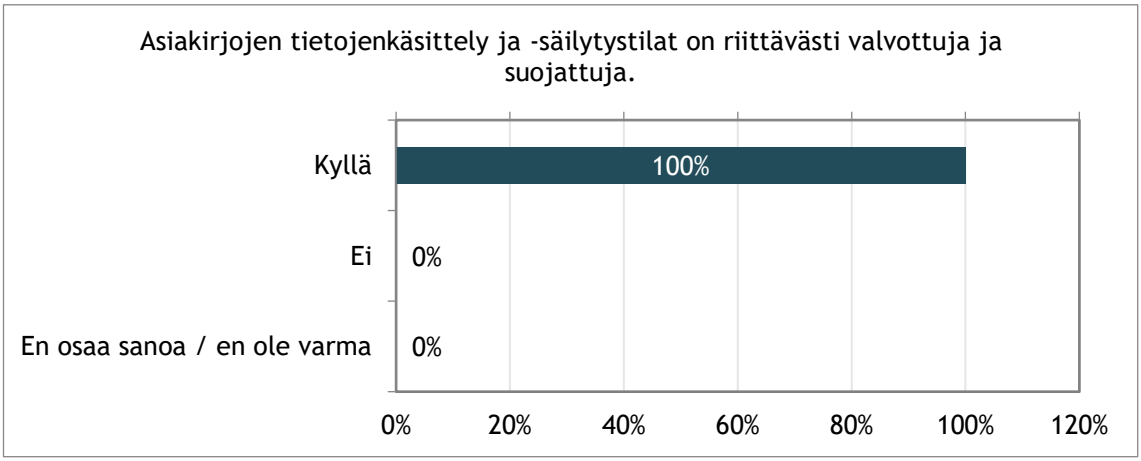
Seuraava kysymys (taulukko 11) jakoi vastaajat. Puolet vastaajista tiesi omasta mielestään, että valtioneuvoston kansliassa toteutuu teknisiä tietoturvallisuuskontrolleja. Puolet ei taas osannut tähän vastata, mikä osittain heijastaa sitä, ettei tieto käytettävistä

tietoturvallisuuskontrolleista ole kovin laajalle levinnyttä. Tämä voi osittain selittyä viestinnällisillä seikoilla: teknisestä tietoturvallisuudesta viestiminen julkishallinnon organisaatiossa ei välttämättä saavuta tavoiteltua lukijakuntaa. Lisäksi osa tiedosta liittyen erilaisiin turvallisuuskontrolleihin on salassa pidettävää ja onkin asianmukaista pitää tieto rajatun joukon tietona.



Taulukko 11: Kyselyn 8. kysymyksen vastaukset

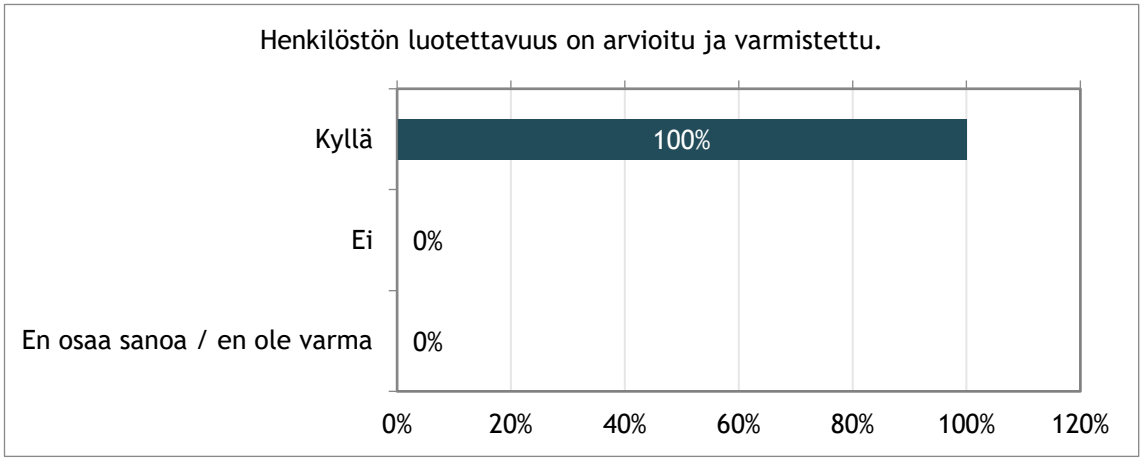
Fyysinen turvallisuus asiakirjojen tietoturvallisuuden osalta koettiin vastaajien toimesta yksimielisesti riittäväksi (taulukko 12). Fyysinen turvallisuus on tietoturvallisuuden suojaustoimenpiteistä näkyvin ja sellainen, jonka kaikki henkilökuntaan kuuluvat joutuvat lähes päivittäin käyttämään: avaamaan ovia, käyttämään kulkutunnistetta, pidettävä henkilökorttia näkyvillä. Aiheen ollessa vastaajille tutumpi ja näkyvämpi asia, on helpompi todeta sen toteutuminen.



Taulukko 12: Kyselyn 9. kysymyksen vastaukset

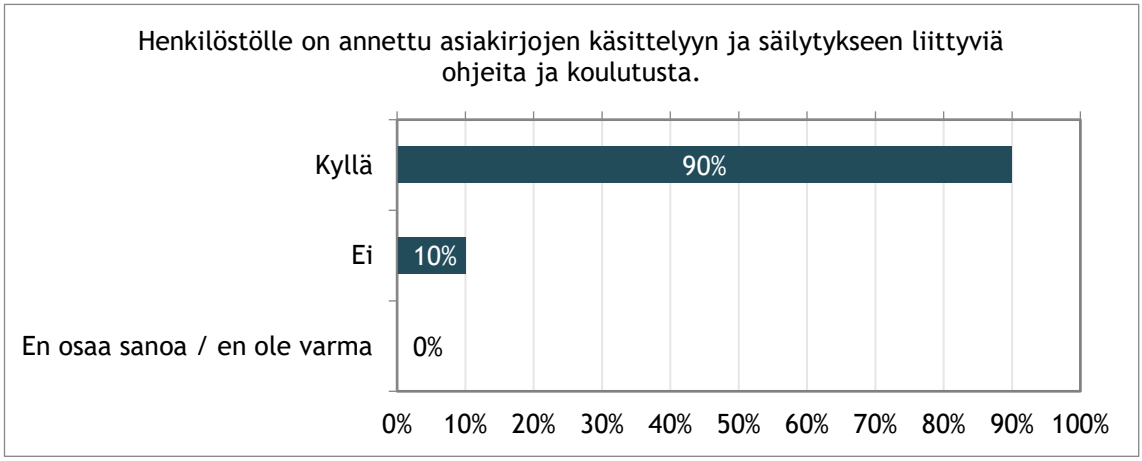
Vastaajat olivat yksimielisiä siitä, että valtioneuvoston kansliassa henkilöstön luotettavuus on arvioitu ja varmistettu (taulukko 13). Näkyvin ja julkisin tapa arvioida ja varmistua

henkilöstön luotettavuudesta on henkilöturvallisuusselvitys. Valtioneuvoston kanslia voi tehdä virkaan tai tehtävään valittavasta henkilöstä henkilöturvallisuusselvityksen.



Taulukko 13: Kyselyn 10. kysymyksen vastaukset

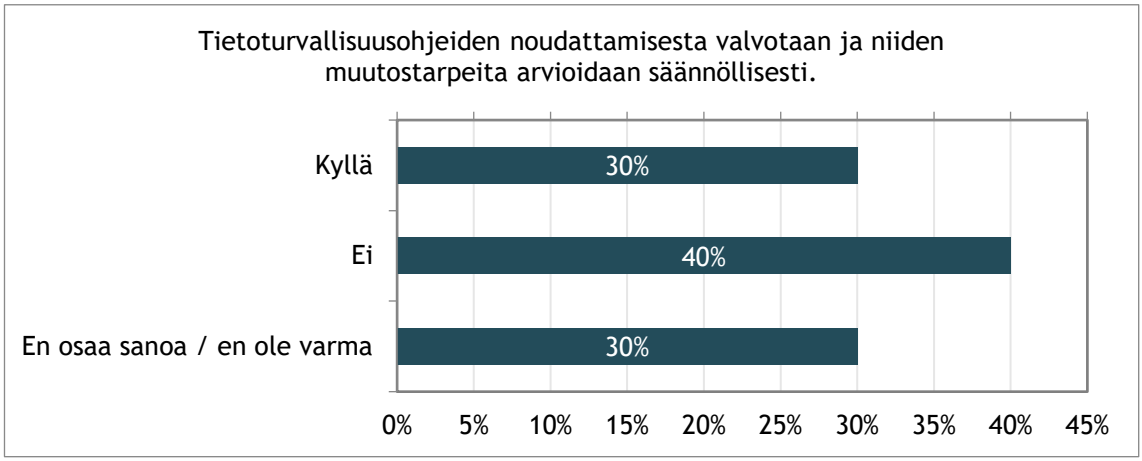
Yhdeksän vastaajista koki, että henkilöstölle on annettu asiakirjojen käsittelyyn ja säilytykseen liittyviä ohjeita ja koulutusta (taulukko 14). Asiakirjojen käsittelyyn ja säilytykseen liittyvä koulutus on pakollinen uusille työntekijöille. Koulutusta järjestetään säännöllisesti yhteistyössä tiedonhallinta- ja tietoturvallisuusasiantuntijoiden toimesta. Täten voidaan päätellä, että vaatimus koulutuksen antamisesta toteutuu. Koulutuksen sisältöön tai sen kehittämistarpeisiin ei oteta tässä kantaa.



Taulukko 14: Kyselyn 11. kysymyksen vastaukset

12. kysymyksen (taulukko 15) asettelu oli haastava, sillä kysymys pitää sisällään kaksi kysymystä, ”noudatetaanko tietoturvallisuusohjeiden noudattamista” sekä ”arvioidaanko niiden muutostarpeita säännöllisesti”, jonka takia ei voida yleistää vastanneiden vastanneen molempiin joko ”kyllä” tai ”ei”. Valtioneuvoston kanslia on asiantuntijaorganisaatio, jossa tietoturvallisuusvastuita on sekä esimiehellä että henkilöstöllä itsessään. Kyselyyn

vastanneista kuitenkin vain kolme koki, että tietoturvallisuusohjeiden noudattamista valvotaan ja että niiden muutostarpeita arvioidaan säännöllisesti. Neljä vastasi, ettei koe näin tapahtuvan ja toiset kolme vastasi, ettei tiedä tai osaa sanoa. Haastatteluiden perusteella oli epäselvää, miten tarkalleen valvontaa on ajateltu toteutettavan ja että ohjeistus sen toteuttamisesta on hyvinkin vaihtelevaa eri yksiköissä. Tietoturvallisuusohjeiden muutostarpeita ei juurikaan arvioida valmiusyksikön ulkopuolella. Vastauksista ei voi päätellä täyttyykö vaatimus, vaan asiaa tulisi selvittää syvällisemmin. (Toimialajohtaja 2020.)



Taulukko 15: Kyselyn 12. kysymyksen vastaukset

Kyselyn avoimissa kysymyksissä kysyttiin, miten tietoturvallisuuden riskienhallinta näkyy vastaajien jokapäiväisessä työssä, mikä on tietoturvallisuuden riskienhallinnan nykytilan ja miten sitä voisi kehittää. Vastauksista selviää, että vastaajat kokevat asian tärkeänä ja että asiasta on enemmissä määrin keskusteltu työyhteisössä. Lisäksi muutokset ja tapahtumat toimintaympäristössä vaikuttavat henkilöstön tietoisuuteen ja asioiden kehittymiseen. Nykytila nähtiin riittävän hyvänä, mutta ongelmia katsottiin myös olevan. Puutteelliset resurssit, epäselvyydet vastuunjaoissa kanslian sisällä sekä myös Valtorin roolista, sekä yhtenäisten toimintamallien ja käytäntöjen vähyys aiheuttavat huolia vastaajissa. Kehittämistoimina nähdään henkilöstön tietoisuuden kehittäminen, säännöllinen tietoturvallisuuden riskiarviointi sekä yhteisten käytänteiden jalkauttamista yhteisesti koko organisaatiolla.

Uudet nousevat teknologiat ja esimerkiksi pilvipalveluiden lisääntyminen aiheutti vastaajissa huolta, ja he toivoivatkin parempia ja selkeämpi ohjeita niihin liittyen. Valtioneuvoston kanslia ei ole välttämättä ottanut jotakin tiettyä teknologia käyttöön, mitä joku sidosryhmä tai henkilöstö omassa arjessaan käyttävät. Tällaiset tilanteet saattavat aiheuttaa hämmennystä osassa käyttäjissä, sillä ohjeistusta siitä, miten tiettyä teknologiaa tulisi käyttää, ei välttämättä ole vielä tehty valtioneuvoston kanslian toimesta.

Teemahaastatteluista tuli ilmi samansuuntaisia ajatuksia. Yleisesti ottaen valtioneuvoston tietoturvallisuuden tilaa pidettiin hyvänä ja tietoturvallisuusriskejä säännöllisesti arvioidaan. Haastatteluista nousi kuitenkin esiin huoli epäselvistä vastuista, kuten esimerkiksi kenen vastuulla on tietoturvallisuus. Lisäksi nousi esiin huoli riittävien resurssien turvaamisesta tietoturvallisuuden osalta, niin henkilöstön kuin tietojärjestelmienkin osalta. Haasteina nähtiin muutoksen kiihtyvä tahti ja se, kuinka valtioneuvoston kanslia pysyy muutoksen tahdissa mukana, tietoturvallisesti.

5 Johtopäätökset

Haasteena on löytää riittävät ja tarpeelliset kontrollit, prosessit sekä käytänteet. Lainsäädännön muodostaessa minimivaatimukset, voidaan pohtia, onko lainsäädäntö kuinka ajantasaista tieto- ja kyberturvallisuuden osalta. Yritysmaailmassa käytettävät käytänteet vaihtelevat suuresti ja turvallisuusalan toimijoita on useita, myös kansainvälisiä, ketkä tuovat mukanaan ovat edut, sekä haasteet. Tämän lisäksi meillä on kansalaisia, myös valtionhallinnon henkilöstöä, ketkä ovat aktiivisesti muuttamassa käyttäytymistään verkossa ja digitaalisessa elinympäristössä. Tämä muutos käytöksessä ja käytänteissä, työ- ja arkielämän lähentyminen digitaalisessa mielessä, luo uuden näkökulman tietoturvallisuuden riskienhallintaan, jota tulisi myös pohtia osana suurempaan tietoturvallisuusstrategiaa.

Kehittämistyön osalta, jatkokehitettävää on erityisesti tietoturvallisuuden riskienhallinnan prosessien räätälöimisen ja jalkauttamisen kanssa. Lisäksi tulisi tehdä erillinen katsaus riskienhallinnan eri osa-alueiden nykytilaan ja niiden kehittämiseen, kuten riskien arviointiin ja käsittelyyn. Tulevissakin kehittämistöissä tulisi ottaa huomioon mahdolliset luottamukseen liittyvät riskit. Mikäli kehittämismenetelmänä käytetään haastattelua sekä kyselyä, on riskinä, että henkilöstö ei myönnä mahdollisia puutteita ja virheitä omissa toiminnoissaan. Tätä riskiä voidaan pienentää tutustumalla syvällisemmin toimintoihin sekä tarkkailemalla heidän prosessejansa ja käytänteitä.

Kehittämisehdotukset on koottu kyselystä ja teemahaastatteluista ilmi tulleista ehdotuksista sekä kirjallisuuskatsauksesta saaduista ehdotuksista. Kehittämisehdotuksissa on pyritty ottamaan huomioon toteutuskelpoisuus sekä tarpeellisuus. Toteutuskelpoisuuden osalta arvioidaan erityisesti tarvittavat resurssit. Tarpeellisuutta arvioidaan valtioneuvoston kanslian julkishallinnon viranomaisen näkökulmasta. Opinnäytetyössä ei ole tutkittu ja arvioitu tarkemmin suojattavia resursseja, vaan ne arvioidaan lähteiden antamien tietojen mukaan. Monet kehittämisehdotuksista vaativat toimialarajojen ylittäviä toimenpiteitä ja mahdollisten johtoryhmien hyväksyntää, jonka takia näitä ehdotuksia tulisi tarkistella ja arvioida tarkemmin erikseen ennen mahdollista käyttöönottoa tai toimeenpanoa. Opinnäytetyössä ei oteta kantaa eikä ole tiedusteltu, mikäli ehdotuksista on jo mahdollisesti käynnissä olevaa

tiedonkeruuta tai markkinatutkimusta. Taloudellisuutta ja kustannusarvioita on arvioitu henkilötyöpäivä arvioilla, ottamatta kantaa minkä tason asiantuntija kyseistä tehtävää suorittaa. Yksi henkilötyöpäivää vastaa noin 7,5 tuntia töitä. Kehittämisehdotuksissa arvioidaan ehdotuksen toteuttamiseen tarvittava työmäärä sekä jatkuvan palvelun tuottamiseen tarvittava työmäärä.

Yleisesti ottaen kehitettävää oli valtioneuvoston kanslian henkilöstön turvallisuustietoisuuden kehittämisessä. Kokonaisvaltainen turvallisuustietoisuus parantaa organisaation eri turvallisuuden osa-alueita, kuten tietoturvallisuutta ja sen riskienhallintaa. Opinnäytetyön kehittämisehdotukset kaikki omalta osaltaan auttavat kehittämään turvallisuustietoisuutta. Kehittämisehdotukset osin liittyvät myös toisiinsa siten, että yksi kehittämisehdotus saattaa toimia paremmin, mikäli toinen on jo otettu käyttöön. Eräs tietoturvallisuuden riskienhallinnan kehittämisen lopputuloksista olisikin, että toiminnot pystyisivät omalla henkilöstöllään ja osaamisellaan huolehtimaan tietoturvallisuus- ja riskienhallinta vastuistaan sekä velvollisuuksistaan. Valtioneuvoston kanslian tietoturvallisuusasiantuntijat olisivat taustalla tukemassa tätä työtä, mutta eivät päätoimisesti olisi vastuussa toimintojen omasta päivittäisestä tietoturvallisuudesta.

5.1 Tietoturvallisuus- ja riskienhallintakoulutus

Isona osana tietoturvallisuuden riskienhallinnan kehittämistä on henkilöstön yleisen tietoturvallisuuden ja riskienhallinnan osaaminen. Valtioneuvoston kanslialla on paljon velvoitteita henkilöstölle näiden osalta, mutta tarjottavaa koulutusta on suhteessa selkeästi vähemmän. Opinnäytetyön tulosten perusteella valtioneuvoston kansliassa on tahtotilaa sekä tarvetta lisätä eri tasoista ja kohdennettua tietoturvallisuus- ja riskienhallintakoulutusta.

Henkilöstöllä tulisi olla pakollinen säännöllinen tietoturvallisuuskoulutus, joka käydään esimerkiksi työsuhteen alussa, jonka jälkeen kerran vuodessa. Tämän lisäksi olisi räätälöityjä tietoturvallisuuskoulutuksia eri tason tehtäviin ja eri projekteihin. Esimerkiksi henkilön siirtyessä esihenkilö tehtäviin tai osaksi jotakin turvallisuusluokiteltua projektia, hänen tulisi käydä tehtävään räätälöity tietoturvallisuuskoulutus. Nämä koulutukset voisi olla osa jo muuta olemassa olevaa koulutusta.

Tietoturvallisuuskoulutuksia voisi pyrkiä pelillistämään, kuten Digi- ja väestötietoviraston lokakuussa 2020 julkaisema Digiturvallinen elämä -mobiilipeli, jonka tarkoituksena on ”elävöittää digiturvan kouluttamista” (Digi- ja väestötietovirasto 2020). Tietoturvallisuuskoulutuksien pelillistämisellä voidaan aktivoida henkilöstöä osallistumaan koulutukseen sekä auttaa heitä tarkastelemaan tietoturvallisuutta uusista näkökulmista. Esimerkiksi vertailemalla videopelien vihollinen vastaan puolustaja asetelmaa voisi pyrkiä hyödyntämään pelillistetyssä tietoturvallisuuskoulutuksessa. Pelinomaisilla yleisen tason

tietoturvallisuuskoulutuksissa voidaan täydentää täsmällisempää valtioneuvoston kanslian toimintaan liittyvää tietoturvallisuuskoulutusta. (Saviaro 2021.)

5.2 Tietoturvan vuosikello toimintoihin

Valtioneuvoston kanslian tietoturvatoiminnolla on jo käytössään vuosikello, mistä tulee ilmi vuositasolla tehtävät vastuutetut tehtävät. Osana isompaa organisatorista kehittämistä, jokaiselle toiminnolla luodaan yhteistyössä tietoturvallisuusasiantuntijoiden kanssa, toiminnon oma tietoturvallisuuden vuosikello. Kun suunnittelutyöhön otetaan toiminnon henkilöstö, vuosikello saadaan parhaan mukaan noudattamaan toiminnon muuta aikataulua, jolloin ei tule aikatauluhaasteita ja henkilöstö saadaan osallistumaan tietoturvallisuustyöhön. Tällöin tietoturvallisuusasiantuntijat toimivat ainoastaan koordinoivassa roolissa. Tietoturvan vuosikello voi olla osana toiminnon muuta vuosikelloa, mikäli sellainen on jo käytössä. Johtamisen ja päätöksenteon helpottamiseksi, vuosikellojen tulisi olla yhdenmukaisia ja pitää sisällään vaatimuksen mukaiset velvoitteet tietoturvallisuuden osalta.

Toiminnon oma tietoturvallisuuden vuosikello edesauttaa tietoturvallisuuden muovautumista osaksi valtioneuvoston kanslian arkea. Vuosikelloon voisi määritellä esimerkiksi tietoturvallisuusviestinnän aikataulu, auditoinnit ja muut säännölliset tietoturvallisuuteen liittyvät tapahtumat. Tällöin ihmiset osaavat varautua ja odottaa niitä, sekä yleinen tietoisuus ympärillä tehtävästä tietoturvallisuus työstä kasvaa. (Remes 2016.)

Vuosikellon tausta- ja laatimistyöhön tulisi varata arviolta yksi henkilötyöpäivä, jonka lisäksi tulisi varata arviolta puolikas tai kokonainen henkilötyöpäivä vuosittain toimintoa kohden vuosikellon katselmointiin. Tarvittaessa aikaresurssia tulisi lisätä, mikäli isompia korjauksia tai lisäyksiä tulee. Tavoite olisi, että toiminto itse pystyisi ylläpitämään vuosikelloansa, tietoturvallisuusasiantuntijat olisivat tukena tarvittaessa.

5.3 Säännölliset työpajat

Valtioneuvoston kanslian toimintaympäristö muuttuu jatkuvasti ja yhä kiihtyvällä tahdilla. Valtioneuvoston kanslian tietoturvallisuusasiantuntijoiden on liki mahdotonta hahmottaa jokaisen yksittäisen toiminnon tietoturvallisuuden tilaa ja sen mahdollisesti muuttuneita vaatimuksia sekä vaikutuksia. Tietoturvallisuuden riskienhallinnan kehittämiseksi tulisi järjestää säännöllisesti, esimerkiksi kerran vuodessa tai silloin kun toimintoon kohdistuu merkittäviä muutoksia, tietoturvallisuus ja riskienhallinta työpaja. Työpajassa käsitellään toiminnon tietoturvallisuusriskejä sekä keskustellaan mahdollisesti toiminnon näkökulmasta muuttuneesta toimintaympäristöstä.

Säännöllisten työpajojen avulla tietoturvallisuusasiantuntijat perehtyvät syvällisemmin toimintoihin, jolloin he kykenevät yhä paremmin hahmottamaan valtioneuvoston kansliaa

kokonaisuutena tietoturvallisuuden näkökulmasta. Lisäksi työpajoista saadaan tukea toiminnoille räätälöidyille koulutuksille sekä määräyksille ja ohjeille. Työpajan avulla on mahdollista lisäksi pienimuotoisesti varmentaa henkilöstön aiemmin saatua tietoturvallisuuskoulutusta ja -perehdytystä. Työpajat lisäksi antavat turvallisen ja asiantuntevan foorumin kysyä ja pohtia toiminnon henkilöstöä askarruttavia turvallisuusasioita. Työpajan ja sen materiaalin valmisteluun tulisi varata arviolta yksi henkilötyöpäivä. Tämän lisäksi tulisi varata yksi henkilötyöpäivä työpajaan ja sieltä saadun materiaalin analysointiin ja raportointiin.

5.4 Tietoturva-chat

Opinnäytetyön tuloksista tuli ilmi, että valtioneuvoston tietoturvallisuustoiminto nähtiin paikoittain etäisenä ja monille hieman tuntemattomana. Tietoturvallisuustoiminnossa on jo nimetyt henkilöt eri osa-alueille, mutta joillakin voi silti olla korkea kynnys lähteä kysymään turvallisuuteen liittyviä kysymyksiä henkilöstökohtaisesti. Tämän tueksi voisi ottaa käyttöön tietoturvan chat-palvelun. Chat-sovellus voisi olla tekoälypohjainen, joka osaisi vastata yksinkertaisiin tietoturvallisuuteen ja riskienhallintaan liittyviin kysymyksiin. Lisäksi he osaisivat ohjata asian oikealle tietoturvallisuusasiantuntijalle. Kevyt chat-palvelu täydentäisi tietoturvallisuuskoulutuksessa saatua osaamista ja tietoisuutta sekä madaltaisi henkilöstön kynnystä kysyä heitä askarruttavia turvallisuuskysymyksiä.

Hieman vastaavanlaisia chat-palveluita on jo olemassa valtioneuvoston kansliassa. Chat-sovelluksen tulisi toimia sekä työasemalla että mobiililaitteella. Chat-sovellus olisi kustannustehokkainta hankkia ulkoiselta palveluntoimittajalta. Chat-sovelluksen hinnalle ei ole hinta-arviota.

5.5 Turvallisuuspoikkeama- ja riskienhallintasovellus

Osana tietoturvallisuuden arkistamista tulisi kriittisimmät tehtävät, kuten turvallisuuspoikkeamista ja riskeistä ilmoittaminen tehdä helpoksi ja vaivattomaksi. Mikäli niistä ilmoittaminen on liian aikaa vievää ja vaivalloista, se jää tekemättä. Helpoksi ja yksinkertaiseksi suunniteltu turvallisuuspoikkeama ja riskien ilmoituskanava on yksi keino varmistaa kriittisempien tietoturvallisuusriskien ja -tapahtumien päätyminen tietoturvallisuusprosessiin. Lisäksi sovellukset auttavat tapahtumien tilastoinnissa sekä jatkoraportoinnissa. Sovelluksen tulisi toimia sekä työasemalla että mobiililaitteella.

Sovellus olisi kustannustehokkainta hankkia ulkoiselta palveluntoimittajalta. Sovelluksen hinnalle ei ole hinta-arviota. Henkilöstön aikaresursseja tulisi varata riittävästi projektin käynnistämiseen ja loppuunsaattamiseen. Projektiin vaadittavat aikaresurssi voi olla hyvinkin suuri, riippuen tarjottavasta sovelluksesta ja siihen kohdistuvista vaatimuksista. Tämän lisäksi

varata riittävästi aikaa palveluntoimittajan yhteistyöhön. Valmis sovellus tulisi osaksi muuta tavanomaista tietoturvallisuustyötä, eikä sen pitäisi lisätä aikaresurssien tarvetta.

5.6 Toiminnoille räätälöidyt vastuut ja velvollisuudet

Eräs havaittu asia oli valtioneuvoston kanslian tietoturvallisuutta koskevan dokumentaation, määräyksien, ohjeiden ja vaatimusten pirstaleisuus. Niitä ei ole kootusti saatavilla, kuin muutamien tärkeimpien tietoturvallisuuden määräyksien ja ohjeiden osalta tietoturvallisuustoiminnon osalta. Tuloksista selvisi osin, etteivät kaikki olleet täysin varmoja siitä, että minkälaisia vaatimuksia ja vastuita heidän toiminnollansa on. Kehittääkseen tietoturvallisuuden riskienhallintaa, tulisi jokaiselle toiminnolle luoda oma räätälöity tietoturvallisuusdokumentaatio, missä tulee esille sen vastuut ja velvollisuus tietoturvallisuuden osalta, sekä siihen tulisi liittää aiemmin mainittu tietoturvallisuuden vuosikello. Jokaisen toimintoon kuuluvan henkilön tulisi olla tietoinen näistä vastuista ja velvollisuuksista sekä heidän tulisi olla tietoinen tietoturvallisuusyhteyshenkilöistä.

Selvitys ja laatimistyöhön tulisi varata arviolta viisi henkilötyöpäivää, jolloin asiantuntija perehtyy tarvittavilta osin lainsäädäntöön ja muihin vaatimuksiin toiminnon näkökulmasta yhdessä toiminnon henkilöstön kanssa. Tämän jälkeen tulisi varata arviolta puolikas tai kokonainen henkilötyöpäivä vuosittain toimintoa kohden dokumentaation katselmointiin ja tarvittaessa lisätä aikaresurssia, mikäli isompia korjauksia tai lisäyksiä tulee.

5.7 Vastuiden jalkauttaminen organisaatioon

Valtioneuvoston kanslian määräykset ja ohjeet määrittelevät selkeästi vastuut tietoturvallisuuden osalta organisaatiossa, mutta käytäntö osoittaa, että monet olettavat tietoturvallisuustoiminnon olevan vastuussa tietoturvallisuudesta kokonaisuudessa. Selkeästi haastavin kehittämisehdotus onkin tietoturvallisuusvastuiden jalkauttaminen organisaatioon vähintään määräysten ja ohjeiden mukaiselle tasolle. Osittain vastuun jalkauttaminen liittyy tietoturvallisuustietoisuuteen, jota aiemmat kehittämisehdotukset pyrkivät omalta osaltaan kehittämään. Keskiössä tietoturvallisuuden riskienhallinnan kehittämisessä on valtioneuvoston kanslian ylimmän johdon sekä muun esihenkilöstön tahtotila sen kehittämiseksi. Tahtotila tulisi näyttää omalla aktiivisella esimerkillä sekä resursoimalla riittävästi tietoturvallisuuden riskienhallinnan kehittämiseen valtioneuvoston kansliassa sekä sen eri toiminnoissa. Tahtotilaa on esitetty esimerkiksi valtioneuvoston kanslian tulostavoitteissa, mutta jalkauttaminen esihenkilöstölle hieman uupuu. Räätälöidyt tietoturvallisuuskoulutukset ja -dokumentaatio toimintoihin sekä esihenkilöille vahvistavat vastuiden jalkauttamista, mutta tämän lisäksi, se vaatii ylimmän johdon näyttävämpää tahtotilan osoittamista.

Tälle kehitykselle ei varsinaisesti voi arvioida tarvittavaa työmäärää eikä resursseja, sillä kyseessä on suuri ja hidas prosessi. Muiden kehittämisehdotuksia ja muun kehittämistyön

ohella sekä jälkeen tulisi jälleen arvioida miten vastuut ja velvollisuudet ovat jalkautuneet eri toimintoihin. Tällöin voidaan ottaa kehittämiskohteeksi yksittäisiä toimintoja. Kehittäminen tulee kulkemaan käsi kädessä tietoturvallisuuden hallintamallin käyttöönoton sekä muun tietoturvallisuuden riskienhallinnan kehittämisen kanssa.

Lähteet

Painetut

Bampton, R. & Cowton, C. 2002. The E-Interview. Forum: Qualitative Social Research. 3(2), Art. 9.

Common Criteria. 2017. Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1.

Disterer, G. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security Vol. 4 No. 2, 92-100.

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

Hirsjärvi, S. Remes, P. & Sajavaara, P. 2004. Tutki ja kirjoita. 10. painos. Helsinki: Tammi.

Hirvonen, A. 2011. Mitkä metodit?. Opas oikeustieteen metodologiaan. 1. painos. Helsinki: Yleisen oikeustieteen julkaisuja.

Jesson, J. Matheson, L. & Lacey, F. 2011. Doing Your Literature Review. Traditional and Systematic Techniques. 1. Painos. Lontoo: Sage Publications Ltd.

Katakri. 2020. Tietoturvallisuuden auditointityökalu viranomaisille. Kansallinen turvallisuusviranomainen. Ulkoministeriö.

Merton, K. Fiske, M. & Kendall, P. 1990. The Focused Interview. A Manual of Problems and Procedures. New York: The Free Press.

NIST. 2018. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1.

Ojasalo, K. Moilanen, T. & Ritalahti, J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. 3.-4. painos. Helsinki: Sanoma Pro.

PCI Security Standards Council. 2018. Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures. Version 3.2.1.

PiTuKri. 2020. Traficomin julkaisuja 13/2020. Kyberturvallisuuskeskus. Liikenne- ja viestintävirasto Traficom. Versio 1.1.

Raggad, B. 2010. Information Security Management. Concepts and Practice. 1. painos. Boca Raton: CRC Press.

Rousku, K. 2017. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Valtiovarainministeriö. Helsinki: Lönnberg Print & Promo.

SFS-EN ISO/IEC 27002. 2017. Tietoturvallisuuden hallintakeinojen menettelyohjeet. 1. painos. Helsinki: Suomen Standardisoimisliitto.

Stoneburner, G. Goguen, A. & Feringa, A. 2002. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. Falls Church: Booz Allen Hamilton Inc.

Talib, M. Barachi, M. Khelifi, A. & Ormandjieva, O. 2012. Guide to ISO 27001: UAE Case Study. Zayed University.

Vacca, J. 2013. Computer and Information Security Handbook. 2. painos. Waltham: Morgan Kaufmann Publishers.

Valtiovarainministeriö. 2011. Johdon tietoturvaopas. Helsinki: Tampereen Yliopistopaino Oy.

Valtiovarainministeriö. 2012. ICT-varautumisen vaatimukset. Helsinki: Suomen Yliopistopaino Oy.

Valtiovarainministeriö. 2013. Sovelluskehityksen tietoturvaohje. Helsinki: Juvenes Print – Suomen Yliopistopaino Oy.

Valtiovarainministeriö. 2020a. Suositus turvallisuusluokiteltavienasiakirjojen käsittelystä. Helsinki.

Valtiovarainministeriö. 2020b. Suosituskokoelma tiettyjen tietoturvallisuus-säädösten soveltamisesta. Helsinki.

Vilkka, H. 2015. Tutki ja kehitä. 4. painos. Jyväskylä: PS-Kustannus.

Wheeler, E. 2011. Security Risk Management. Building an Information Security Risk Management Program from the Ground Up. 1. painos. Waltham: Syngress.

Yeboah-Boateng, E. 2013. Cyber-Security Challenges with SMEs in Developing Economies: Issues of Confidentiality, Integrity & Availability (CIA). Aalborg Universitet. 1. Painos.

Sähköiset

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999. Viitattu 28.9.2020. https://www.finlex.fi/fi/laki/ajantasa/1999/19991030

Digi- ja väestötietovirasto 2020. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä VAHTI. Viitattu 30.9.2020. https://dvv.fi/vahti

Digi- ja väestötietovirasto. 2020. Tänään julkaistava Digiturvallinen elämä -mobiilipeli elävöittää digiturvan kouluttamista. Viitattu 15.5.2021. https://dvv.fi/-/tanaan-julkaistava-digiturvallinen-elama-mobiilipeli-elavoittaa-digiturvan-kouluttamista

Grimsby, G. 2018. The Influence of Standards on The Nordic Economies. Viitattu 4.10.2020. https://www.sfs.fi/files/8515/Nordic_market_study_-_influence_of_standards_FINAL.pdf

Laki julkisen hallinnon tiedonhallinnasta 906/2019. Viitattu 28.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2019/20190906

Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004. Viitattu 28.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2004/20040588

Laki valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 1226/2013. Viitattu 18.3.2021. https://www.finlex.fi/fi/laki/alkup/2013/20131226

Laki valtioneuvostosta 175/2003. Viitattu 27.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2003/20030175

Laki yksityisyyden suojasta työelämässä 759/2004. Viitattu 29.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Mead, N. 2013. The Common Criteria. Cybersecurity & Infrastructure Security Agency. Viitattu 19.1.2020. https://us-cert.cisa.gov/bsi/articles/best-practices/requirements-engineering/the-common-criteria

Mustoe, L. 2020. What is PCI Compliance?. Digital Guardian. Viitattu 15.1.2021. https://digitalguardian.com/blog/what-pci-compliance

NIST 2020. An Introduction to the Components of the Framework. Cybersecurity Framework. Viitattu 19.1.2020. https://www.nist.gov/cyberframework/online-learning/components-framework

Remes, M. 2016. 5 tapaa saada työntekijäsi kiinnostumaan tietoturvasta. Kauppalehti. Viitattu 15.5.2021. https://blog.kauppalehti.fi/vieraskyna/isoworks-5-tapaa-saada-tyontekijasi-kiinnostumaan-tietoturvasta

Saviaro, M. 2021. Pelillistämisestä voi saada apua myös tietoturvallisuuteen. Core Service. Viitattu 15.5.2021. http://blog.coreservice.fi/pelillist%C3%A4misest%C3%A4-voi-saada-apua-my%C3%B6s-tietoturvallisuuteen

Suomidigi 2020. VAHTI-ohjeet. Viitattu 30.9.2020. https://www.suomidigi.fi/ohjeet-ja-tuki/vahti-ohjeet

Turvallisuusselvityslaki 726/2014. 29.9.2020. https://www.finlex.fi/fi/laki/alkup/2014/20140726

Ulkoministeriö 2021. Kansallinen turvallisuusviranomainen. Viitattu 18.3.2021. https://um.fi/kansallinen-turvallisuusviranomainen

Ulkoministeriö. 2020. Ulkoministeriön tietoturva sai sertifikaatin. Viitattu 15.1.2021. https://um.fi/uutiset/-/asset_publisher/GRSnUwaHDPv5/content/ulkoministeri-c3-b6n-tietoturva-sai-sertifikaatin

Valtioneuvosto 2020. Valtioneuvoston toiminta. Viitattu 10.9.2020. https://valtioneuvosto.fi/tietoa/toiminta

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019). Viitattu 29.9.2020. https://www.finlex.fi/fi/laki/alkup/2019/20191101

Valtioneuvoston asetus valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä 132/2014. Viitattu 18.3.2021. https://www.finlex.fi/fi/laki/alkup/2014/20140132

Valtioneuvoston asetus valtioneuvoston kansliasta 393/2007. Viitattu 27.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2007/20070393

Valtioneuvoston kanslia 2020a. Johto ja organisaatio. Viitattu 27.9.2020. https://vnk.fi/ministerio/johto-ja-organisaatioo

Valtioneuvoston kanslia 2020b. Kansliapäällikkökokous. Viitattu 27.9.2020. https://vnk.fi/yhteensovittamistehtavat/kansliapaallikkokokoukset

Valtioneuvoston kanslia. 2019a. Valtioneuvoston kanslian tulostavoitteet vuodelle 2019. Viitattu 20.9.2020. https://vnk.fi/fi/ministerio/tulossuunnitelmat

Valtioneuvoston kanslia. 2019b. Valtioneuvoston kanslian tulostavoitteet vuodelle 2020. Viitattu 20.9.2020. https://vnk.fi/fi/ministerio/tulossuunnitelmat

Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 162/2015. Viitattu 20.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2015/20150162

Valtioneuvoston kanslian asetus valtioneuvoston kanslian työjärjestyksestä 162/2015. Viitattu 27.9.2020. https://www.finlex.fi/fi/laki/ajantasa/2015/20150162

Valtioneuvoston ohjesääntö 262/2003. Viitattu 27.9.2020.
https://www.finlex.fi/fi/laki/ajantasa/2003/20030262

Valtiovarainministeriö 2021a. Tiedonhallintalautakunnan suositukset. Viitattu 15.5.2021.
https://vm.fi/suositukset

Valtiovarainministeriö 2021b. Tiedonhallintalautakunnan tehtävät. Viitattu 15.5.2021.
https://vm.fi/tiedonhallintalautakunnan-tehtavat

Valtiovarainministeriö 2021c. Tiedonhallintalautakunta. Viitattu 15.5.2021.
https://vm.fi/tiedonhallintalautakunta

Valtori 2021. Tietoa Valtorista. Viitattu 18.3.2021. https://valtori.fi/tietoa-valtorista.

Julkaisemattomat

Osastopäällikkö. 2020. Osastopäällikön haastattelu 14.12.2020. Valtioneuvoston kanslia. Helsinki.

Palvelupäällikkö. 2020. Palvelupäällikön haastattelu 17.12.2020. Valtioneuvoston kanslia. Helsinki.

Toimialajohtaja. 2020. Toimialajohtajan haastattelu 14.12.2020. Valtioneuvoston kanslia. Helsinki.

Valtioneuvoston kanslia. 2017. Valtioneuvoston kanslian riskienhallintapolitiikka. Tulostettu 2.9.2020.

Valtioneuvoston kanslia. 2018. Tietoturvallisuuden hallinta valtioneuvostossa ja sen ministeriöissä. Tulostettu 2.9.2020.

Valtioneuvoston kanslia. 2019c. Tietoturvallisuuden hallinta valtioneuvoston kansliassa. Tulostettu 2.9.2020.

Valtioneuvoston kanslia. 2019d. Tietoturvariskien hallintaohje. Tulostettu 1.9.2020.

Valtioneuvoston kanslia. 2019e. Tietoturvatarkastukset ja arvioinnit valtioneuvoston tieto- ja viestintäteknisille järjestelmille ja palveluille. Tulostettu 2.9.2020.

Valtioneuvoston kanslia. 2020c. Tietoturvallisuuden intrasivut. Viitattu 1.10.2020.

Yksikön päällikkö 2. 2020. Yksikön päällikön haastattelu 4.12.2020. Valtioneuvoston kanslia. Helsinki.

Yksikön päällikkö. 2020. Yksikön päällikön haastattelu 27.11.2020. Valtioneuvoston kanslia. Helsinki.

Kuviot

Taulukot

Liitteet

Liite 1: Lainsäädännön asettamat vaatimukset valtioneuvoston kanslian tietoturvallisuuden riskienhallinnalle

Laki	Pykälä	Vaatimukset
1)	1 §	Kumottu lainsäädäntö, mutta perusvaatimukset ovat edelleen hyvin paikkaansa pitävät. Valtioneuvoston kanslian tulee varmistaa tietoturvallisuus sekä suorittaa tietoturvallisuuden riskienhallintaa.
2)	12 §	Valtioneuvoston kanslian tulee tunnistaa ne tehtävät, joissa henkilöiltä vaaditaan erityistä luotettavuutta. Luotettavuutta voidaan arvioida ennaltaehkäisevin toimin kuten: • Henkilöturvallisuusselvitys • Henkilön luottotietojen tarkistuksella • Huumausainetesti Säädösperusta toimille: turvallisuusselvityslaki 726/2014 ja laki yksityisyyden suojasta työelämässä 759/2004.
2)	13 §	Valtioneuvoston kanslian on tehtävä säännöllistä tietoturvallisuuden riskienhallintaa aineistojen ja järjestelmien elinkaaren ajan.
2)	13 §	Valtioneuvoston kanslian tulee säännöllisellä testauksella varmistaa oleellisten tietojärjestelmien vikasietoisuus ja käytettävyys.
2)	13 §	Valtioneuvoston tulee varmistua hankinoissaan toteutuneista tietoturvallisuustoimenpiteistä.
2)	15 §	Valtioneuvoston kanslian on varmistettava tiedon eheys, luotettavuus ja käytettävyys. Tietoa saa käsitellä ja säilyttää ainoastaan tiloissa, joiden fyysinen tietoturvallisuus on varmistettu. Saatavuuden osalta: • Tietojen saatavuutta saa rajoittaa vain, jos se on laissa rajoitettu (esimerkiksi turvallisuusluokiteltu tieto). • Tiedot voidaan tarpeellisin osin arkistoida.

3)	6 §	”Erityissuojattava tietoaineisto on pidettävä salassa, jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu”. Ainoastaan henkilöillä, joilla on työperusteinen tarve tietoon, tulisi saada oikeudet siihen.
3)	7 §	Valtioneuvoston kanslian henkilöstölle ja sen alihankkijoilla on vaitiolovelvollisuus ja tiedon hyväksikäyttökielto.
3)	8 §	Turvallisuusluokiteltuun materiaaliin tulee merkitä sen turvallisuusluokka.
3)	9 §	Valtioneuvoston kanslian tulee huolehtia, että turvallisuusluokiteltua tietoa käsitellään sitä vastaavan käsittelyvaatimuksien mukaisesti.
3)	10 §	Valtioneuvoston kanslia tulee huolehtia, että turvallisuusluokiteltua tietoa säilytetään tiloissa, joissa kansainvälisistä tietoturvallisuusvelvoitteista voidaan huolehtia.
4)	7 §	Valtioneuvoston kanslian on toteutettava turvallisuusluokiteltujen asiakirjojen monitasoista suojausta. Suojausta vaarantavia tekoja tulee: • Ennaltaehkäistä, estää ja rajata • Havaita ja jäljittää Lisäksi niiden vaikutusta tulisi vähentää palauttamalla turvallisuustaso.
4)	9 §	Valtioneuvoston kanslian on määriteltävä fyysisesti suojatut turvallisuusalueet: • ”hallinnolliset alueet, joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa” • ”turva-alueet, joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle”

1) Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999), osin kumottu.
2) Laki julkisen hallinnon tiedonhallinnasta (906/2019)
3) Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

4) Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019)

Liite 2: Tietoturvallisuuden riskienhallinta VNK:ssa -kysely

Kyselyn tavoitteena on selvittää valtioneuvoston kanslian tietoturvallisuuden riskienhallinnan nykytila. Kysely on julkinen, joten salassa pidettävää aineistoa ei saa lähettää. Vastaattehan viimeistään perjantaina 4.12.2020 klo 16 mennessä. Lisätietoja Anthony Baxter, suunnittelija: anthony.baxter@vnk.fi.

Vastaattehan oman toimintonne näkökulmasta.

1.Mihin osastoon tai yksikköön kuulutte?

- EU-asioiden osasto
- Omistajaohjausosasto
- Strategiaosasto
- Viestintäosasto
- Valtioneuvoston hallintoyksikkö
- Istuntoyksikkö
- Valmiusyksikkö
- Henkilöstöyksikkö
- Talousyksikkö

2. Mihin yksikköön tai toimialaan kuulutte?

- Yleisten EU-asioiden yksikkö
- EU-politiikkayksikkö
- EU-tiedonhallintayksikkö
- Yhteiskuntapolitiikan suunnitteluyksikkö
- Hallituspolitiikan yksikkö
- Käännös- ja kielitoimiala sekä sisäisen viestinnän ja tietotuen toimiala
- Tietotoimiala
- Tila- ja virastopalveluyksikkö

3. Ydintoimintoihin liittyvät keskeiset tietoturvallisuusriskit on tunnistettu ja analysoitu.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

4. Tietoturvallisuuden osalta on riittävä asiantuntemus ja tietoturvallisuuden keskeiset tehtävät ja vastuut on määritelty.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

5. Asiakirjojen käsittelyä koskevat tehtävät ja vastuut on määritelty.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

6. Tietojen saanti ja käytettävyys on turvattu sekä poikkeamienhallinnan menettelytavat määritelty.

- Kyllä

- Ei
- En osaa sanoa / en ole varma

7. Asiakirjojen salassapito on varmistettu antamalla pääsy vain niitä työssään tarvitseville.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

8. Tietojen muuttaminen tai luvaton käsittely on pyritty teknisesti ennaltaehkäisemään ja estämään.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

9. Asiakirjojen tietojenkäsittely ja -säilytystilat on riittävästi valvottuja ja suojattuja.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

10. Henkilöstön luotettavuus on arvioitu ja varmistettu.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

11. Henkilöstölle on annettu asiakirjojen käsittelyyn ja säilytykseen liittyviä ohjeita ja koulutusta.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

12. Tietoturvallisuusohjeiden noudattamisesta valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti.

- Kyllä
- Ei
- En osaa sanoa / en ole varma

13. Lyhyesti, kuvaile miten tietoturvallisuuden riskienhallinta näkyy työssäsi.

14. Teidän oma näkemys toimintonne tietoturvallisuuden riskienhallinnan nykytilasta?

15. Miten mielestänne tietoturvallisuuden riskienhallintaa voisi toiminnossanne kehittää?

Liite 3: Strukturoidun kirjallisuuskatsauksen otantaan valittu kirjallisuus

#H1.1	Moilanen, A. 2018. Tietoturvallisuuden mittaaminen julkishallinnon organisaatiossa. Seinäjoen ammattikorkeakoulu.
#H1.2	Lagerblom, V-P. 2014. ICT-varautumisen analyysi ja kehittäminen julkisen sektorin virastossa. Lappeenrannan teknillinen yliopisto.
#H1.3	Scherf, A. 2012. Riskienhallinta osaksi eduskunnan kanslian johtamista. Laurea-ammattikorkeakoulu.
#H2.1	Marjamäki-Ruuskanen, S. 2013. Hallinnon tietotekniikkakeskuksen kokonaisvaltaisen riskienhallinnan kehittämissuunnitelma. Laurea-ammattikorkeakoulu.
#H2.2	Kiviharju, V. 2015. Onko turvallisuusjohdon sijoittumisella organisaatiorakenteessa vaikutusta turvallisuuden toteuttamiseen ja toteutumiseen?. Aalto PRO.
#H3.1	Khidzir, N. Mohamed, A. & Arshad, N. 2010. Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing. 2010 Second International Conference on Network Applications, Protocols and Services. 234-239.
#H3.2	Paquette, S. Jaeger, P. & Wilson. S. 2010. Identifying the Security Risks Associated with Governmental Use of Cloud Computing. University of Maryland.
#H3.3	Ali, O. Shrestha, A. Chatfield, A. & Murray, P. 2019. Assessing Information Security Risks in The Cloud: A Case Study of Australian Local Government Authorities. University of Southern Queensland.
#H4.1	Białas, A. 2013. Information Security and Business Continuity Issues and Solutions With OSCAD-Case Studies in Public Administration. Instytut Technik Innowacyjnych EMAG.
#H4.2	Ahmed, Z. Shah, M. & Ahmed, J. 2015. Information security management needs more holistic approach: A literature review. University of Central Lancashire.
#H4.3	Albrechtsen, E. & Hovden, J. 2009. Improving Information Security Awareness and Behaviour Through Dialogue, Participation and Collective Reflection. An Intervention Study. Norwegian University of Science and Technology.

#H4.4	Coppolino, L., D'Antonio, S. Mazzeo, G. Romano, L. & Sgaglione, l. 2018ö. How to Protect Public Administration from Cybersecurity Threats : The COMPACT Project. 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA).
#H4.5	Ebot, E. & Check, N. 2018. Information Systems Security Audits in Cameroon's Public Administration. ICEGOV '18: Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance. Sivut 312-317.
#H4.6	Safa, N. & Solms, R. 2016. An information security knowledge sharing model in organizations. Nelson Mandela Metropolitan University.
#H4.7	Ikaneng, B. 2018. Assessment on The Level of Information Security Awareness at The Government Pensions Administration Agency (GPAA). University of the Witwatersrand.
#H4.8	Flores, W. Antonsen, E. Ekstedt, M. 2014. Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. Royal Institute of Technology.
#H4.9	Hohan, A. Olaru, M. & Pirnea, I. 2011. Case Study Regarding the Implementation of An Integrated Risk Management System in Local Public Administration. Quality - Access to Success.