LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoturvan kehittäminen organisaatiossa X

Mika Ruuska

2018 Laurea

Laurea-ammattikorkeakoulu

Tietoturvan kehittäminen organisaatiossa X

Mika Ruuska
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Toukokuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Turvallisuusalan koulutusohjelma (AMK)

Mika Ruuska

Tietoturvan kehittäminen organisaatiossa X

Vuosi 2018 Sivumäärä 61

Tässä opinnäytetyössä tietoturvan kehittämistä tarkastellaan tutkimus – ja kehittämisprojektin näkökulmasta. Tutkimusprojekti ja kehitysprojekti voivat kohdistua samaan sisältöön eri tavoittein ja tuloksin. Tutkimusprojektilla tavoitellaan sovelluskelpoisen tiedon löytämistä tai uuden tiedon luomista erityisen epävarmoilla alueilla ilman ennakkotietoa siitä, saadaanko tutkimuksen perusteella tuloksia tai hyötyä.

Valtioneuvosto on tehnyt periaatepäätöksen tietoturvatyön kehittämisestä, jossa johdon vastuulle linjataan tietoturvatyön resurssien ohjaaminen. Vahti -ohjeistuksen mukaan organisaatiolla tulisi olla tietoturvan hallintajärjestelmä, joka on kiinteä osa organisaation prosesseja, johtamis – ja hallintarakenteita. Tietoturvan arviointi tulisi olla normaalia johdon vastuulla olevaa johtamiseen ja tulosohjaukseen liittyvää päätöksentekoa.

Opinnäytetyössä tutkittiin, millainen on organisaatiolle X soveltuva tietoturvallisuuden hallintajärjestelmä. Tavoitteen tukemiseksi tutkittiin mahdollisuutta kehittää sovelluspohjainen tietoturvan hallintajärjestelmä organisaatiolle X. Alustana opinnäytetyön yhteydessä kokeiltiin Office 365 -ympäristössä toimivia online -pilvipalveluja. Opinnäytetyön tuloksena luotiin hahmotelma tietoturvan hallintajärjestelmästä Ms Planner -projektityökalulla, jossa ympäristö on toteutettu projektimaiseen muotoon ja on siten helposti muunneltavissa tietoturvan kehittämisprosessin etenemisen mukaan.

Opinnäytetyön tuloksena nousi esille tutkimusprojektin keinoin kysymyksiä, mahdollisuuksia sekä ongelmia liittyen tietoturvan hallintaan, tarkoituksena pohtia niiden yleisempää merkitystä organisaation X tietoturvan kannalta. Halusin hyödyntää tutkimuksessa suurimman osan VAHTI ohjeistuksesta, jotta saisin työn tukemiseksi laaja-alaisen ja kattavan kuvan valtiohallinnon tietoturvallisuuden ohjeistosta sekä VAHTI -ryhmän merkittävästä työstä tietoturvallisuuden kehittämiseksi.

Asiasanat: Tietoturva, tietoturvan hallintajärjestelmä, tietoturvan kehittäminen

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

Mika Ruuska

Abstract

Development of Information Security in Organization X

Year 2018 Pages 61

In this thesis, the development of information security is examined from the point of view of a research and development project. A research project and a development project can focus on the same content with different objectives and results. A research project seeks to map useful information or create new knowledge in particularly uncertain areas without any prior knowledge of the research results or benefits.

The Finnish Government has drawn up the Government Policy Decision on Information Security in the State Government offices, in which allocating resources of information security work is the responsibility of the management. According to the VAHTI instructions, an organization should have an information security management system, which is a fixed part of the processes of the organization and the organization's management and control structures. Evaluation of information security procedures should be a part of normal leadership and a responsibility of the management-related decision-making process and should lead to management by results.

The thesis investigated what type of an information security management system would be suitable for Organization X. The development of an application-based information security management system for Organization X was explored. As a template, online cloud services in the Office 365 environment were tested. The result of the thesis was an outline of the information security management system using the Microsoft Planner project tool, where the environment has been carried out in a project form and thus can be easily modified according to the progress of the information security development process.

As a result of the thesis, possibilities and problems were reported with the methods of research project information security management. Most of the VAHTI guidelines were exploited in the research, and it resulted in a comprehensive picture of the government administration information security guidelines and the VAHTI -group´s seminal work for information security.

Keywords: Information security, Information Security Management System, Developing of the Information Security

Sisällys

1 Johdanto

Organisaation tietoturvan rakentaminen on yksilöllistä, ja tiettyjä viitekehyksistä johtuvia perusvaatimuksia täytyy noudattaa, jotta tietoturvan hallinta olisi osoitettavissa systemaattiseksi ja arvioitavissa olevaksi toiminnaksi. Tietoturvallisuuden hallintajärjestelmän rakentamista vaikeuttaa osaltaan se, että tietoturvallisuuteen liittyviä ohjeita ja ohjeistajia on useita, eivätkä linjaukset aina ole yhtenäisiä (Valtiokonttori 2015b, 75). Tulkinnoille jää varaa, ja vaikeuksia on aiheuttanut etenkin tietoturvallisuusasetuksen (681/2010) 5 § vaatimuksista johtuva tasomalliajattelu, jonka soveltaminen on ajoittain ollut epäyhtenäistä (Valtiovarainministeriö 2017b).

Tietoturvatyön ja sen kehittämiseen liittyvien toimenpiteiden pitäisi liittyä organisaation toiminnasta lähtöisin oleviin vaatimuksiin. Painopisteinä tietoturvallisuuden kehittämisessä ovat riskienhallinta, tietoturvallisuuden hallintajärjestelmä, tietoturvan mittarit ja seuranta sekä varautuminen. (VAHTI 2/2014, 14-15.) Näihin painotuksiin nojautuen, tässä opinnäytetyössä tutkitaan organisaation X tietoturvan kehittämismahdollisuuksia suunnittelemalla sähköinen tietoturvan hallintajärjestelmä sekä tutkimalla, minkälaiset ohjausmallit organisaation X toimintaympäristössä tukevat tietoturvan kehittämistä.

Tärkeänä painopisteenä tietoturvallisuuden kehittämisessä on myös toimiva ja oikein toteutettu riskienhallinta, joka on tärkeimpiä prosesseja digitaalisen tietoturvan eli tieto – ja kyberturvallisuuden sekä tietosuojan näkökulmasta (Rousku 2017b, 4). Organisaatiolle X suunniteltavaan sähköiseen tietoturvan hallintajärjestelmään sisällytetään sähköisessä muodossa oleva riskienhallintaosio.

Sähköisen tietoturvan hallintamallin kehittämiseen on päädytty meneillään olevan digitalisaation antaman näkökulman kautta. Yksi digitalisaation tuomista mahdollisuuksista on automatisoida työtä siten, että manuaalisia ratkaisuja korvataan digitaalisilla ratkaisuilla, joka taas mahdollistaa mm. reaaliaikaisen raportoinnin. (Valtioneuvosto 2017.) Tietoturvatulkintojen yhtenäistämisen kautta pilvipalveluja voitaisiin hyödyntää tehokkaammin ja uusia palveluja voitaisiin kehittää kustannuksiltaan kilpailukykyisillä ketterillä alustoilla (Valtiokonttori 2015b, 77).

Vaikka digitalisoiminen koskettaa ennemminkin asiakkaiden suuntaan tuotettavia palvelukokonaisuuksia, on kyse myös ajattelutavan muutoksesta ja siitä, miten valtionhallinto toimii osana julkista hallintoa. Valtionhallinnon toiminnan tuloksellisessa kehittämisessä on hyvä huomioida erilaisia näkökulmia ja tarpeita, ja kaikessa toiminnan kehittämisessä digitalisaatio tulee ottaa arkipäiväiseksi työvälineeksi. Jotta tässä onnistuttaisiin, digitalisaatio pitää nähdä

myös uusien teknologioiden käyttöönottoina toiminnan ja prosessien kehittämisessä, osana organisaation kehittämistä ja arkityötä. Samalla aikaisemmista tavoista toimia ja tottumuksista on uskallettava luopua. (Valtiokonttori 2015b, 18.)

1.1 Tutkimusongelma

Tietoturvan arvioinnin, riskienarvioinnin ja dokumentoinnin suhteen joudumme usein vielä tukeutumaan asiakirjapohjaiseen dokumentointiin ja useisiin, sisällöltään monimutkaisiin Excel -taulukoihin, joka ei kannusta systemaattiseen tietoturvan kehittämiseen.

Sovelluksia tai selainpohjaisia palvelualustoja tietoturvan ja riskien arviointiin on markkinoilla, mutta niiden käyttöön saattaa liittyä kalliita lisenssi- tai käyttömaksuja, ja niiden mukautuminen asiakkaan toimintaympäristön muutoksiin riippuu palveluntarjoajan kyvystä vastata nopeisiin kehittämistarpeisiin. Joissakin tietoturvan hallintaan kehitetyissä palveluissa saattaa olla hankalasti ymmärrettäviä ja kiinteitä, arviointikehikkoihin sidottuja toiminnallisuuksia, jotka tekevät käytettävyyden vaikeaksi. Tämän takia organisaatiolle X tutkitaan mahdollisuutta luoda tietoturvan hallintajärjestelmä Office 365 -ympäristöön sekä malli sähköisen riskienhallintaprosessin käynnistämistä varten.

Tutkimuskysymyksinä ovat:

1. Millainen on organisaatiolle X soveltuva tietoturvallisuuden hallintajärjestelmä?
2. Millainen sovelluspohjainen hallintajärjestelmä voisi tukea tietoturvan hallintaa?

Työn tavoitteena tutkitaan mahdollisuutta rakentaa sovelluspohjainen tietoturvan hallintajärjestelmä oikeusministeriön hallinnonalalla toimivalle organisaatiolle X, joka on valtion talousarviosta annetun lain (423/1988) 12 a §:n (1096/2009) mukaisen kirjanpitoyksikön tulosohjattu virasto. Alustana opinnäytetyön yhteydessä kokeillaan Office 365 -ympäristössä ryhmätyöskentelyyn käytettävää Microsoft Planner -sovellusta.

1.2 Rajaus

Opinnäytetyö rajataan koskemaan hallinnollista tietoturvaa. Teknistä tietoturvaa sivutaan tässä raportissa siltä osin, kuin se tutkimuksellisuuden näkökulmasta on tarpeellista. Vahti -ohjeistus sisältää useita tietojärjestelmiin liittyviä yksityiskohtaisia vaatimuksia, jotka kohdistuvat myös vastuisiin, prosesseihin ja hallinnan menettelyihin. Yleensäkin tietoturvallisuuteen liittyvät vaatimukset eri tietoturvan osa-alueilta aiheuttavat yhdessä organisaatiolle tarpeen ylläpitää ja kehittää omaa tietoturvallisuuttaan. (Vahti 3/2012, 11.) Kappaleessa 4 tuodaan esille organisaation X tietojenkäsittely-ympäristössä esiintyviä yleisiä julkisuudessa esillä olleita tekniseen tietoturvallisuuteen liittyviä riskejä, jotka saattavat muodostaa uhkia organisaation X tietoaineistojen turvallisuudelle.

Opinnäytetyöstä rajataan pois tietosuoja ja asiakirjojen luokittelu sekä niiden integrointi tietoturvallisuuden hallintajärjestelmään, koska organisaation X hallinnonalalla on opinnäytetyöprosessin aikana kesken tietosuojan osoitusvelvollisuuteen liittyvä hanke. Tietoaineiston luokittelusta on tehty organisaation X hallinnonalalla päätös 31.12.2016, mutta asiakirjojen käsittelyvaatimusten toteuttaminen hallinnonalalla on vielä kesken.

Luokittelupäätös tulee vaatimaan suunnittelua organisaation johdon osalta hallinnollisten ja organisatoristen velvollisuuksien selvittämiseen sekä tehtävien ja vastuualueiden jakamisen osalta (VAHTI 3/2010, 16). Tämän ja 25.5.2018 voimaan astuneen EU:n yleisen tietosuoja-asetuksen johdosta salassa pidettävien asiakirjojen käsittelyä sivutaan lyhyesti riskienarvioinnin näkökulmasta kappaleessa 4 kohdassa ”päätelaitteet”.

1.3 Tutkimusnäkökulma

Tässä opinnäytetyössä tarkastellaan tietoturvan kehittämistä tutkimus – ja kehittämisprojektin näkökulmasta. Tutkimusprojekti ja kehitysprojekti voivat kohdistua samaan sisältöön eri tavoittein ja tuloksin. Tutkimusprojektilla tavoitellaan sovelluskelpoisen tiedon löytämistä tai uuden tiedon luomista erityisen epävarmoilla alueilla ilman ennakkotietoa siitä, saadaanko tutkimuksen perusteella tuloksia tai hyötyä. Vaikka tuloksena olisi tieto siitä, että tietyn uuden tekniikan soveltaminen ei onnistu, voidaan tutkimusprojekti todeta erinomaisesti onnistuneeksi. Toivottuna lopputuotoksena voidaan myös saada uusia kysymyksiä, mahdollisuuksia ja ongelmia valmiiden ratkaisuideoiden lisäksi. (Karlos ym. 2008, 26.) Kuvaan tietoturvaan liittyviä ongelmia eräänlaisena teoreettisena kontekstina, jossa koostan keskeisiä aihepiirejä siinä laajuudessa ja syvyydessä, kun tämän opinnäytetyön ja aikataulun puitteissa on relevanttia.

Opinnäytetyö on laadullinen eli kvalitatiivinen tutkimus, jossa tutkin empiiristen havaintojen kautta ongelmanasettelua, tulkitsen havaintoja sekä pohdin niiden yleisempää merkitystä tietoturvan kannalta. Merkitystä tutkittaessa tässä tutkimuksessa on otettu fenomenologinen lähestymistapa, jossa aineiston käsittely muotoutuu tutkimustilanteen mukaan, tutkijan oman käsityksen mukaan ihmisestä, kokemuksesta ja merkityksistä. (Laine 2001, 31; Varto 1992, 26-27.)

Tutkimuksen merkityskokonaisuudet ja niiden etsiminen ohjautuvat tutkijan merkitysten tajun ja tutkimusaineiston kautta. Myös tutkimusongelma ja tutkimuskysymykset ohjaavat aineiston tulkintaa ja rajaamista; mikä on olennaista organisaation X kannalta nykytilanteessa, ja mikä osa aineistosta auttaa ymmärtämään syvällisesti tietoturvaa siitä näkökulmasta, josta voisi olla apua organisaation X tietoturvan hallintajärjestelmän rakentamiseen. Ilman teoreettista viitekehystä ei voida tehdä fenomenologista tutkimusta. (Laine 2001, 39 - 43; Varto 1992, 57, 86 - 92.)

1.4 Teoreettinen viitekehys

Uusi tieto tieteellisessä tutkimuksessa tuotetaan teorian avulla, josta voidaan metodikirjallisuuden mukaan puhua teoreettisena viitekehyksenä. Jos ammattialalla on tehty vähän tieteellistä perustutkimusta ja käsitteiden muodostamista, ammatillisista käytännöistä nousee objektiiviseksi tarkastelutavaksi viitekehys, josta voidaan puhua ammatillisena tietoperustana. (Vilkka & Airaksinen 2004, 73 – 75.) Tarkoituksenmukaisuus tehtävänasettelun lähestymistavan kannalta on tutkimuksessa tärkeintä ja se, että lähestymistapa ei perustu tekijän laajaan kokemukseen tai mielipiteisiin, vaan on perustellusti valittu (Vilkka 2015, 22).

Teoreettinen viitekehys pohjautuu hermeneuttiseen tutkimusotteeseen ja analyysimenetelmään, joka tarkoittaa, että mielenkiinto kohdistetaan ihmisten ja työyhteisöjen toiminnan ymmärtämiseen ja tulkintaan tietoturvan näkökulmasta (Varto 1992, 69). Systematisoituna viitekehyksenä käytetään VAHTI - ohjeistusta sekä SFS/IEC ISO27001 - sarjan tietoturvastandardia.

2 Tietoturvan kehittäminen valtionhallinnossa

Teoreettisen viitekehyksen lisäksi tutkimuksessa käytetään usein käsitteitä, jotka voivat olla järjestelmällisen tutkimustyön tuloksena teoreettisia, yleisiä ja aika- ja paikkasidonnaisuudesta vapaita tai konkreettisia, arkikielen epätäsmällisiä käsitteitä. Konkreettiset käsitteet ovat voineet muodostua havainnoista ja kokemuksista. (Hirsijärvi ym. 2005, 138–141.) Teoreettisilla, yleisillä käsitteillä on tärkeä rooli tavassamme ajatella, koska niitä käyttäen voimme löytää samankaltaisuutta tapahtumien, merkitysten, piirteiden ja kohteiden välillä (Varto 1992, 76).

Haavoittuvuus on ohjelmistossa oleva virhe tai toiminnallinen ominaisuus, jota hyödyntämällä kyberloukkauksen tekijä voi vaarantaa ohjelmiston toteuttavan palvelun tietoturvallisuuden (Jaakonhuhta 2011).

Hallinnollinen tietoturva tarkoittaa sitä kokonaisuutta, jonka muodostavat tietoturvatoiminnan johtaminen, järjestelyt, henkilöstön vastuiden ja ohjeistuksen määrittely, koulutus sekä valvonta (VAHTI 2/2004, 13). Yleensä ensimmäisiä arvioitavia kohteita tietoturvallisuuden osa-alueista on hallinnollinen tietoturvallisuus myös silloin, kun halutaan varmistua siitä, että organisaation prosessit toimivat tietoturvallisuuden hallintajärjestelmän mukaisesti (VAHTI 8/2006, 31).

Katakri on auditointityökalu, jolla arvioidaan viranomaisen kykyä käsitellä salassa pidettävää tietoaineistoa. Katakrin on julkaissut kansallinen turvallisuusviranomainen (NSA, National Security Authority), joka Suomessa on ulkoministeriö. Katakria käytetään tietoturvallisuuden ar-

viointiperusteena silloin, kun todennetaan kansainvälisiin tietoturvallisuusvelvoitteisiin liittyviä tietoturvallisuusvaatimuksia. Kriteeristöä voidaan käyttää vaihtoehtoisesti todentamaan myös kansallisten tietoturvallisuusvaatimusten täyttymistä. (Viestintävirasto 2017, 14.)

Kirjanpitoyksikkönä tarkoitetaan valtion virastoa tai laitosta, joka ”hoitaa talousarvioasetuksessa (1243/1992) mainittuja valtion maksuliike – ja kirjanpitotehtäviä ja joka on niistä tilivelvollinen.” Tällaisia kirjanpitoyksiköitä ovat tasavallan presidentin kanslia, ministeriöt ja virastot, laitokset ja muut toimielimet, jotka muodostavat toiminnallisesti ja taloudellisesti tarkoituksenmukaisen kokonaisuuden. (Valtiontalouden tarkastusvirasto 2018)

Kontrollit voivat olla laadultaan ehkäiseviä, havaitsevia (ilmaisevia) tai korjaavia. Kontrolli on riskienhallinnan kautta syntyvä menetelmä, keino tai tavoite, jolla pyritään suojautumaan tai varautumaan tietoturvallisuuteen liittyviä haitallisia tapahtumia vastaan (VAHTI 8/2008, 53).

Kyberloukkaus on tapahtuma, jossa tekijä käyttää luvattomasti digitaalista palvelua, estää sen käyttöä tai käyttää palvelua muihin rikoksiin, kuten petokseen; tai katselee, muuttaa, poistaa tai sotkee palveluun tallennettuja tietoja tai aiheuttaa palvelulle haittaa tai tuhoa. (Valtiontalouden tarkastusvirasto 2017, 11)

Kyberturvallisuus on tietoturvallisuutta laajempi käsite, joka kattaa tiedon sekä tietoja käsittelevät ja niihin luottavat ihmiset, tietoja käsittelevät laitteet, laajemmin käsittäen koko yhteiskunnan edun ja kriittisen infrastruktuurin (Jaakonhuhta 2011).

Office 365 on pilvipalvelu, jonka Microsoft on kehittänyt erilaisia intranet-, työtila, pikaviesti, sähköposti, toimisto-ohjelma- ja kalenteripalveluja varten. Office 365 -palvelu sisältää samoja toiminnallisuuksia, kuin paikallinen Sharepoint -alusta, mutta on monipuolisempi, koska erilaisten palvelujen tarjonta päivittyy ja kehittyy jatkuvasti. (Jaakonhuhta 2011.)

SFS-ISO/IEC 27001 – standardi määrittelee organisaatioin toimintaympäristössä tietoturvallisuuden hallintajärjestelmän luomista, toteuttamista, ylläpitämistä ja jatkuvaa parantamista koskevat vaatimukset sekä tietoturvariskien arviointia ja käsittelyä koskevat vaatimukset, jotka ovat mukautettu organisaation tarpeisiin (Valtioneuvoston kanslia 2017a, 14).

Sovellus on käyttöjärjestelmän alustan, sovelluspalvelimen yms. päällä suoritettava ohjelma (VAHTI 8/2008, 14).

Tietojärjestelmä on kokonaisuus, joka muodostuu sovelluksista, laitteista ja ihmisistä ja jonka avulla toimintaa voidaan tehostaa ja kehittää (Jaakonhuhta 2011).

Tietoturvallisuus kattaa organisaatiossa käsiteltävän tiedon suojaamiseen tarkoitetut tekniset ratkaisut ja hallinnolliset prosessit, joiden avulla pyritään takamaan tiedon luottamuksellisuus, eheys ja saatavuus (VAHTI 8/2008, 111).

Tietoturvan hallintajärjestelmä on eräänlainen toimintajärjestelmä tai viitekehys, joka toteuttaa organisaation strategiaa ja jonka avulla tietoturvan toteutuminen kaikissa toimintaprosesseissa pyritään varmistamaan. Se luodaan riskienarviointiin perustuen ja se sisältää organisaatiorakenteen lisäksi erilaisia toimintamalleja, kuten politiikkoja, vastuita, kehittämistoimenpiteitä, prosessikuvauksia sekä mittareita (VAHTI 8/2008, 110).

Tietoturvapoikkeama on tahallinen tai tahaton, haitalliseksi katsottavat tapahtuma tai olotila, joka saattaa vaarantaa tai on jo vaarantanut organisaation tiedon tai palvelujen eheyden, luottamuksellisuuden tai tarkoituksenmukaisuuden (VAHTI 8/2008, 112).

Tietoturvapolitiikka on näkemys perusperiaatteista, jotka määrittelevät organisaation tietoturvan toteutuksen ja painotukset ja jonka organisaation johto on hyväksynyt (VAHTI 8/2008, 113).

Tietoturvataso tarkoittaa tiettyä tietoturva-asetuksessa määriteltyä tasoa, jonka organisaation tulee täyttää hallinnollisen tietoturvallisuuden, teknisen tietoturvallisuuden ja suojattavien kohteiden osalta (VAHTI 3/2012, 17).

Vakiointi tarkoittaa työasemien ja ohjelmistojen yhdenmukaistamista siten, että ne ovat merkittäviltä osin samanlaisia, jotta niiden ylläpito ja käyttäminen olisi helppoa. Vakioitu työasemaympäristö tarkoittaa myös niiden keskitettyä hallintaa sekä rajoituksia. (Hewlett-Packard 2005.)

Valtioneuvosto teki vuonna 2009 periaatepäätöksen, jonka tarkoituksena on ohjata tietoturvallisuuden kokonaisuutta valtionhallinnossa ja joka velvoittaa jokaisen viranomaisen huolehtimaan riittävän tietoturvan ja henkilötietojen suojan toteutumisesta oman organisaation ja sidosryhmien kanssa tehtävän yhteistyön piirissä. Periaatepäätöksessä linjataan tietoturvatyöhön liittyviä tärkeitä suuntaviivoja ja päätetään tietoturvan kehittämisen painopisteistä, kuten riskienhallinta, tietoturvan hallintajärjestelmä, seuranta ja mittarit sekä varautuminen. VAHTI 2/2014, 14.)

Valtioneuvosto ja sen ministerivaliokunnat, valtioneuvoston kanslia sekä ulkoasiainministeriö, sisäministeriö, puolustusministeriö, valtionvarainministeriö sekä liikenne – ja viestintäministeriö käsittelevät turvallisuusasioita (Valtiontalouden tarkastusvirasto 2017, 17). Valtioneuvoston johtamisen tukena toimii normaalioloissa kansliapäällikkökokous ja häiriötilanteissa lisäksi ministeriöiden valmiuspäällikkökokous (Valtioneuvoston ohjesääntö 2003/262 10 §). Valmiuspäällikkökokouksen kutsuu tarvittaessa koolle toimivaltainen ministeriö valtioneuvostossa tai

valtioneuvoston kanslia. Poikkeusoloissa valtiovarainministeriö voi valmiuslain (1552/2011) mukaisesti määrätä valtionhallinnossa tietoturvallisuuden, tietoliikenteen ja tietohallinnon järjestämisestä (VAHTI 2/2014, 24).

Valtionvarainministeriö ohjaa julkisen hallinnon tietoturvallisuuden yleistä kehittämistä ja ohjausta sekä vastaa valtionhallinnon tietoturvallisuuden ohjauksesta. ”Valtiovarainministeriön vastuulla on laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä tarkoitettujen yhteisten palvelujen palvelutuotannon yleishallinnollinen, strateginen sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaus”. Valtionvarainministeriö vastuulla on myös turvallisuusverkkotoiminnan yleishallinnollinen, strateginen, taloudellinen sekä tieto- ja viestintätekninen ohjaus ja valvonta niin varautumisen, valmiuden kuin turvallisuudenkin osalta. (Rousku 2017a.)

Valtiovarainministeriö on asettanut *valtionhallinnon tietoturvallisuuden johtoryhmän* VAHTI kehittämään ja ohjaamaan valtionhallinnon tietoturvaa. VAHTI käsittelee tietoturvallisuuteen liittyvät linjaukset ja tietoturvatoimenpiteisiin liittyvät ohjausasiat (VAHTI 2/2011, 7.) VAHTI – ryhmä toimii yhteistyö-, koordinaatio- ja valmisteluelimenä hallinnon organisaatioiden kanssa, jotka vastaavat hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta (Valtioneuvoston kanslia 2017a, 12).

VAHTI asetettiin vuonna 2017 uudelle kolmen vuoden toimikaudelle. Sen keskeisin kehittämiskohde on osana tietoturvasäädösten uusimista ja toimeenpanoa vuoden 2010 tietoturvallisuusasetuksen uudistaminen. VAHTI -toiminnassa pyritään myös uudistamaan digitaalisen turvallisuuden hallintamalli. VAHTI – ryhmälle tehtiin uudelle toimikaudelle nimenmuutos toiminnan pääpainon muuttuessa digitaaliseen toimintaan, keinoälyyn, robotiikkaan sekä henkilötietojen digitaaliseen käsittelyyn. Uusi nimi on *julkisen hallinnon digitaalisen turvallisuuden johtoryhmä* (VAHTI). (Valtiovarainministeriö 2018c.)

VAHTI – toiminta siirtyi 1.1.2018 alkaen Väestörekisterikeskuksen vastuulle valtioneuvoston 16.11.2017 antaman asetuksen (760/2017) ”Väestörekisterikeskuksen eräistä tehtävistä” myötä (Valtiovarainministeriö 2017). Asetuksen tavoitteena on ollut digitalisaation toimeenpanon entistä selkeämpi jako, jossa valtionvarainministeriö vastaa strategisista ja linjaavista tehtävistä, ja Väestörekisterikeskus virastotason toimeenpanevista ja kehittävistä tehtävistä (Valtioneuvosto 2017).

VAHTI – ryhmään kuuluu sihteeristö sekä asiantuntijaryhmien puheenjohtajat, jotka päivittävät ja valmistelevat vuosittain toimintasuunnitelmia VAHTI – johtoryhmän käsittelyä ja päätäntää varten (VAHTI 21/2017, 20).

VAHTI – ohjeistus on luonteeltaan ohjaava kokoelma valtionhallinnon tietoturvallisuutta koskevista säädöksistä, suosituksista, tavoitteista ja ohjeista. Ohjeistuksella ohjataan valtionhallinnon tietoturvatoimenpiteitä sekä tietoturvallisuuden linjauksia. (Valtioneuvoston kanslia 2017a, 12.)

2.1 Tietoturvan kehittäminen organisaatiotasolla

Nykyisessä tietokeskeisessä yhteiskunnassa organisaation tärkeimpiä tehtäviä on suojata omat tietonsa ja huolehtia tietoturvallisuudestaan. Ilman toimivia yhteyksiä tai tietojärjestelmiä organisaation toiminta voi lamaantua, tai ilman oikeita ja luotettavia tietoja päätökset voivat perustua virheelliseen tietoon, josta voi syntyä vakava vahinko organisaatiolle tai yhteiskunnan turvallisuudelle. Tietoturvallinen toimintaympäristö on ehdoton edellytys organisaation toiminnalle. Organisaation hallussa olevat tiedot voivat sisältää myös asiakkaiden ja sidosryhmien salassa pidettävää tietoa, joka pitää pystyä suojaamaan asianmukaisesti ja huomioida johdon vastuulla oleva organisaation kokonaisvaltainen tietoriskien hallinta. (VAHTI 2/2011, 11–13.)

Toiminnan jatkuvuuteen kohdistuu digitalisoituvan toimintaympäristön takia uusia tietoturvauhkia. Tietoturvatyön päämääränä tulisi olla toimintaan kohdistuvien häiriöiden vähentäminen, ja tietoturvatyön strategisena kehittämistavoitteena organisaation riskienhallinnan sisältävän tietoturvallisuuden johtamis – ja hallintajärjestelmän luominen (VAHTI 6/2006, 8 – 10.)

Tavoitteena laadukkaille toiminnoille ja palveluille on viranomaisen kyky hoitaa tietoturvaansa hyvällä tasolla. Tietoturvallisella toiminnalla turvataan tietojen käsittely, hallinta ja käyttö. Riittävän tietoturvan, varautumisen ja suojauksen tason organisaatio määrittelee säädösten ja omien toiminnallisten tavoitteiden perusteella, ottaen huomioon valtionvarainministeriön ohjeistuksen. (VAHTI 7/2009, 7.) Tietoturvallisuuden yhteisenä perustana, jokaisella organisaatiolla on valtionhallinnossa lähtökohtaisesti vastuu saattaa oma toimintansa täyttämään säädösten määrittelemien tietoturvavelvoitteiden ja valtiovarainministeriön antaman VAHTI -ohjeistuksen mukaiseksi (VAHTI 6/2006, 8).

Tarkastelun tapahtuessa organisaatiotasolla pitää pystyä myös ymmärtämään suomalaista virastorakennetta, jonka mukaisesti valtionhallinnon virastot jakaantuvat ainakin kirjanpitoyksikköihin, tulosohjattuihin virastoihin sekä työnantajavirastoihin. Kirjanpitoyksikön tehtävänä on vastata talousarvioin valmistelusta ja tilinpäätöksestä virastossa. Tulosohjattu virasto solmii ohjaavan ministeriön kanssa tulossopimuksen, joka velvoittaa virastoa saavuttamaan sovitut toimintaan liittyvät tulostavoitteet. Työnantajavirasto vastaa ”kyseisen organisaatioyksikön henkilösuunnittelusta ja seurannasta”. (Valtiovarainministeriö 2015b, 17.)

Valtiontalouden tarkastusvirasto toteaa tulosohjaukseen liittyvistä vaikuttavuustavoitteista raportissaan, että yhteisiä hallinnonalatasoisia ja laajemmin yhteen sitovia vaikuttavuustavoitteita hallinnonalalla ei ilmeisesti ole (Valtiontalouden tarkastusvirasto 2009, 27). Yhteinen, keskushallintoviranomaisen kaltainen toimeenpanoelin, on puuttunut hallinnonalalta ja johtanut siihen, että hallinonalalta puuttuu eri organisaatioita yhteisesti sitovia tavoitteita ja niiden muodostavia kokonaisuuksia. (Valtiontalouden tarkastusvirasto 2009, 9).

Tämänkaltainen organisaatiokohtainen ja toimijalähtöinen tavoitteellisuus näkyy ehkäpä samankaltaisena sirpaloitumisena organisaation X hallinnonalalla olevien virastojen yhteisten tietoturvatavoitteiden asettamisessa. Toisaalta, koko valtionhallinnon mittakaavassa 80 prosenttia valtionhallinnon organisaatioista oli vuonna 2014 ottanut tietoturvatavoitteet tulosohjauksen osaksi ja 92 prosenttia oli arvioinut omaa tietoturvallisuuttaan VAHTI -ohjeita tai standardeja vastaan (Valtioneuvosto 2015).

Tulevaisuudessa organisaation X hallinnonalan virastojen hallinnolliset toiminnot keskitetään mahdollisesti uuteen keskushallintovirastoon, joka mahdollistaa virastojen ydinosaamisen tukitoimintojen laadun parantamisen ja kehittämisen (Oikeusministeriö 2017, 8). Tilanne tietoturvallisuuden ohjaamiseen ja yhteisten tavoitteiden asettamiseen hallinnonalalla voisi kehittyä uuden viraston myötä, jossa hoidettaisiin tuomioistuinlaitosta koskevia keskushallintotehtäviä, kuten kehys – ja talousarviovalmistelu ja tietojärjestelmät (Oikeusministeriö 2017, 13).

Valtiontalouden tarkastusviraston mietintöön antamassaan lausunnossa todetaan, että viraston perustaminen mahdollistaa nykyistä vahvemman ohjausotteen kautta tuomioistuinlaitoksen ja sen toiminnan kehityksen, paremmat välineet oman vastuun alla olevien asioiden tehokkaasta käsittelystä sekä yhdenmukaisuutta menettelytapojen kehittämiseen. Tarkastusviraston mukaan kaikki yksittäiset, keskitetysti hoidettavissa olevat tehtävät, tulisi keskittää uudelle virastolle. (Oikeusministeriö 2017, 30.) Tietoturvaan liittyvästä ohjauksesta ei uutta virastoa koskevassa mietinnössä varsinaisesti puhuta.

Lausuntotiivistelmässä otetaan kantaa myös siihen, että sellaista kehityssuuntaa tulisi uuden viraston kohdalla varoa, jossa esimerkiksi tietojärjestelmien kehittämistä ja ylläpitoa suunniteltaessa pyynnöt välitetään toisaalla oleville palvelujen tosiasiallisille ylläpitäjille ja tuottajille (Oikeusministeriö 2017, 58). Sama näkökulma voisi olla myös tärkeä, jos uuden viraston tietohallinnon järjestäytymisen kohdalla pohditaan myös hallinnonalan tietoturvan ohjausta.

2.2 Tietoturvan arviointi

Viranomaisen tulee arvioida säännöllisesti tietoturvallisuuden tilaa organisaatiossaan, mutta samalla myös jo toteutettujen tietoturvaan liittyvien toimenpiteiden asianmukaisuus ja riittävyys. Arviointitoiminnalla varmistetaan organisaation tietoaineistojen sekä palvelujen turvallisuus. (VAHTI 2/2014, 11.)

Tietoturvallisuuden hallintajärjestelmää ja sen vaikuttavuutta pitää pystyä myös arvioimaan. Tietoturvan arvioinnin suhteen on viranomaisten keskuudessa esiintynyt epätietoisuutta, miten ja milloin arviointia tulisi suorittaa ja erityisesti, mitä viitekehyksiä arvioinnin apuna tulisi käyttää (VAHTI 2/2014, 14.)

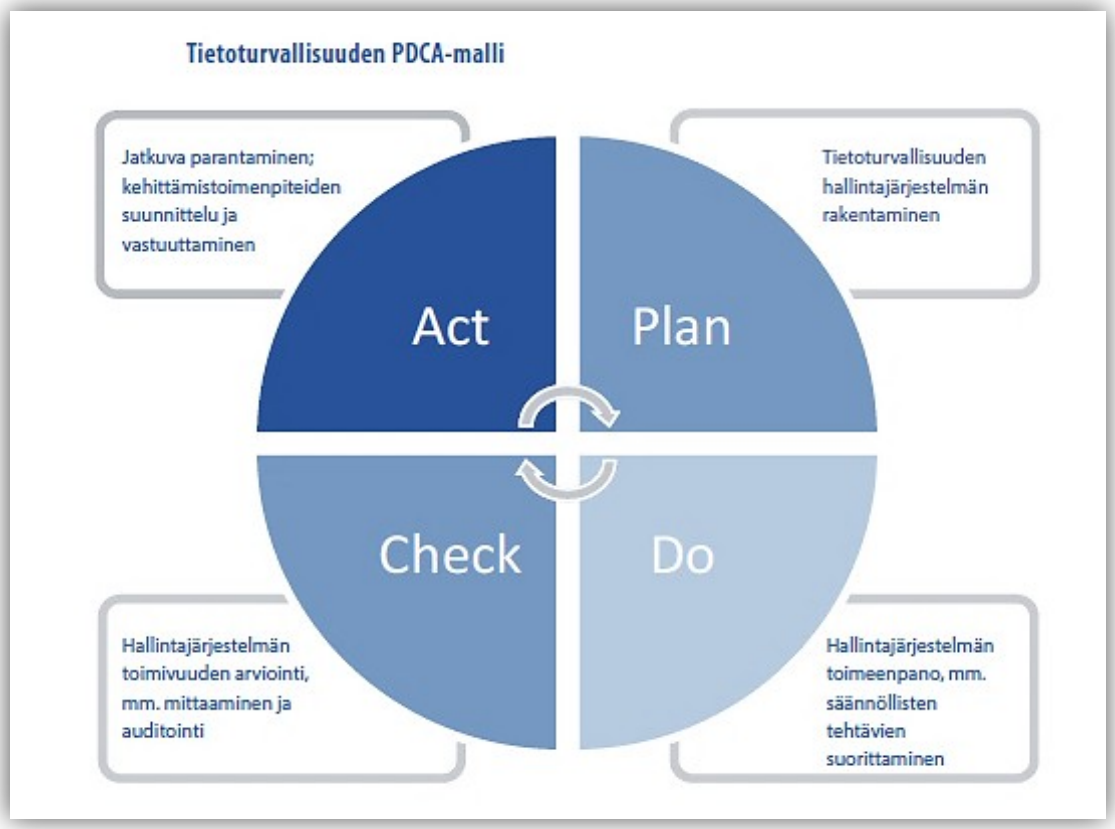
Viestintäviraston 19.5.2017 päivitetyssä ohjeessa tietoturvallisuuden arviointiin tarkoitettujen arviointikriteeristöjen soveltamisesta todetaan, että kun arvioinnin kohteena oleva organisaatio käsittelee Suomen viranomaisen salassa pidettävää tietoa ja salassapito perustuu julkisuuslakiin, tietoturvallisuuden arviointiin sovelletaan VAHTI -ohjeistusta, mutta vaihtoehtoisesti arviointiperusteena voidaan käyttää myös Katakria. (Viestintävirasto 2017, 13.)

Katakria käytetään tietoturvallisuuden arviointiin silloin, kun halutaan todentaa, täyttääkö viranomaisen tai yrityksen toiminta ja tietojärjestelmät kansalliset tai kansainväliset tietoturvavaatimukset, jota niiltä edellytetään. Jos arvioidaan kansalliseen lainsäädäntöön kuuluvan vaatimuslähteen velvoittavien sitoumusten tietoturvallisuusvaatimusten toteutumista, käytetään arviointiin myös Katakria. Tällainen vaatimuslähde on valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) ja kansainvälisenä vaatimuslähteenä EU:n neuvoston turvallisuussäännöt (2013/488/EU). (Viestintävirasto 2017, 28.)

Kyseisten kahden viitekehyksen välillä ei käytännön tasolla ole vaatimuseroja, eroavaisuuksia on lähinnä esitystavassa (Viestintävirasto 2017, 13). Katakrissa kaikki vaatimukset ovat yhdessä dokumentissa, kun taas VAHTI -ohjeistus on jakaantunut useisiin eri julkaisuihin. Viestintäviraston mukaan on suositeltavaa käyttää Katakria arvioitaessa tietojärjestelmiä, joissa käsitellään kansallista salassa pidettävää tietoa. (Viestintävirasto 2015, 1.)

Vahti -ohjeistuksen mukaan on tärkeää, että tietoturvallisuuden perustason saavuttaneet organisaatiot ohjaavat riittävästi resursseja tietoturvan arviointiin hallinnollisesta ja teknisestä näkökulmasta (VAHTI 2/2014, 5). Yhtenä kokonaisuutena tietoturva-asetuksessa (681/2010) on tietoturvallisuuden arviointi ja mittaaminen (2/2014, 11), mutta sen tuloksena syntyvän tietoturvan kehittämistoimenpiteiden tulisi perustua organisaation johdon tietoisuuteen turvallisuuden tasosta organisaatiossa (2/2014,13).

Arviointi toimii välineenä tietoturvallisuuden johtamiseen ja kehittämiseen organisaatiossa, jonka tuloksena saadaan tietoa tietoturvatoiminnan vahvuuksista ja osa-alueista, jotka on hoidettu hyvin. Tietoturvan hallintaa kehitetään jatkuvan parantamisen periaatteella; suunnittele, tee, arvioi ja mittaa sekä paranna (Plan, Do, Check, Act - PDCA). (VAHTI 2/2014, 14.)



Kuvio 1: Tietoturvallisuuden PDCA -malli (VAHTI 2/2014, 15).

Tietoturvan arviointia voi suorittaa itsearvioinnin muodossa. Arvioinnin kohteena tarkastellaan hallinnollisia toimintaprosesseja ja menettelytapoja sekä teknisten järjestelyjen riittävyyttä ja vaatimuksenmukaisuutta (VAHTI 2/2014, 16.) Ulkopuolisen arvioinnin tarkoituksena voi olla tietoturvan hallintajärjestelmän arviointi, mutta myös organisaation tietoturvallisuuden kehittäminen. Arvioinnin avulla selvitetään, miltä osin esimerkiksi tietoturva-asetuksen perustason tietoturvallisuusvaatimukset täyttyvät. (Viestintävirasto 2017, 7.)

Arviointi perustuu myös lainsäädännölliseen velvoitteeseen (VAHTI 2/2014,13), mutta se ei tarkoita yleistä velvollisuutta hakea viranomaishyväksyntää organisaation tiedonkäsittelylle tai tietojärjestelmille. Velvoitteet arvioinnille liittyvät julkisuuslain (621/1999) 18 § perusteella säädettyyn viranomaisen velvollisuuteen hyvän tiedonhallintatavan noudattamiseen, eli asiakirjojen, tietojärjestelmien ja niiden sisältämien asianmukaisen saatavuuden, käytettävyyden ja suojaamisen huolehtimisesta. Tietoturvallisuuden järjestelyt pitää olla sellaiset, että asiakirjojen, tietojärjestelmien ja niiden sisältämien tietojen suojaus, eheys ja laatu pitää turvata asianmukaisin menettelytavoin. (VAHTI 2/2014,19.)

Julkisuuslain perusteella on annettu myös asetus (1030/1999) viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta, jossa tarkennetaan julkisuuslain sääntelyä viranomaisen hyvän tiedonhallintatavan toteuttamisesta. Asetuksessa velvoitetaan viranomainen selvittämään ja arvioimaan uhat liittyen tietojärjestelmien turvallisuuteen sekä tietojen saatavuuteen, käytettävyyteen, laatuun ja suojaamiseen. Viranomaisen tulee arvioida myös keinot, kustannukset ja muut vaikutukset uhkien vähentämiseksi ja poistamiseksi käytettävissä olevien keinojen osalta. (VAHTI 2/2014,19 - 20.)

3 Tietoturvan kehittämiseen vaikuttavat ohjausmuodot

Johtaminen linjataan yhdeksi tietoturvallisuuden painopisteeksi valtioneuvoston periaatepäätöksessä valtionhallinnon kehittämisestä. Johdon tulisi ohjata tietoturvatyölle resurssit ja ohjausmekanismit, jotta organisaation tavoitteet voivat toteutua ja jotta tietoturvallisuus voisi olla kiinteä osa organisaation johtamista ja toiminnan suunnittelua. (VAHTI 2/2012, 5.)

Tietoturvallisuuden hallinnan tulisi kulkea koko organisaation läpi, ja olisi hyvä perustaa organisaatioon vastuullisen johtajan alaisuuteen ryhmä, joka koordinoi tietoturvallisuuden ohjaamista, hallintaa ja kehittämistä. Ryhmän toimintaa edustavat tietoturvallisuuden kannalta parhaiten henkilöstöryhmät, jotka ovat tekemisissä tietopalveluiden, tietojärjestelmien ja atk-tuen kanssa sekä teknisistä kehittämis - ja ratkaisutoimenpiteistä vastuussa olevat henkilöt. Erittäin tärkeää on sitouttaa näiden henkilöstöryhmien edustajat tietoturvatyöhön sekä varmistaa heidän osaaminen ja laadukas toiminta. (VAHTI 6/2006, 26.)

Tietoturvan hallintajärjestelmän tulisi olla kiinteä osa organisaation prosesseja sekä johtamis- ja hallintarakenteita (SFS-EN ISO/IEC 27001:2017, 7), ja tietoturvan arviointi organisaation johdon vastuulla olevaa normaalia johtamis-, tulosohjaus- ja päätöksentekotoimintaa, jonka tavoitteena on toiminnan luotettavuuden takaaminen (VAHTI 8/2006, 12).

3.1 Sisäinen valvonta

Valtiontalouden tarkastusvirasto on ylin valtiontalouden tilintarkastaja, joka ulkoisen tarkastajan roolissa tarkastaa sisäisen valvonnan ja riskienhallinnan riittävyyttä ja asianmukaisuutta. Tarkastusvirasto kohdistaa poikkihallinnollisluonteisia tarkastuksiaan myös tietoturvallisuuteen, jossa sisäisen valvonnan lisäksi huomioidaan tietojärjestelmät, hallinnonalan ohjausjärjestelmät ja turvallisuutta koskeva tuloksellisuus. Turvallisuutta koskevaan tuloksellisuuden arviointiin liittyy tietoyhteiskunnan, lainsäädännön, hallinnon ja teknisen infrastruktuurin arviointi. (VAHTI 2/2014, 53.)

Sisäistä valvontaa ja riskienhallintaa valtionhallinnossa ohjaa valtiovarainministeriö, Valtiokonttori puolestaan vastaa ohjeistuksesta. Valtioneuvosto on asettanut sisäisen valvonnan ja riskienhallinnan neuvottelukunnan, jonka tehtävänä on tehdä aloitteita liittyen sisäisen val-

vonnan ja riskienhallinnan kehittämiseen, ja jonka tehtävänä on seurata ja arvioida valtionhallinnon sisäisen valvonnan ja siihen liittyvien riskienhallinnan menettelyjen ja järjestämisen tilaa. Valtiovarain controller -toiminto johtaa valtiovarainministeriön yhteydessä toimivaa neuvottelukunnan työtä. (Valtiovarainministeriö 2017d, 1.)

Organisaation X hallinnonalan ministeriön kansliapäällikön alaisuudessa toimii sisäisen tarkastuksen yksikkö, jonka yhtenä tehtävänä on tukea hallinnonalalla olevia virastoja kehittämään sisäistä valvontaa, riskienhallintaa ja tietoturvaa. Ministeriö on ohjeistanut myös kirjanpitoyksikköön kuuluvia hallinnonalan virastoja vastaamaan sisäisestä valvonnasta omissa työjärjestyksissään, varmistamaan sisäisen valvonnan riittävyys ja asianmukaisuus sekä arvioimaan oman organisaation osalta sisäisen valvonnan toimivuus. Sisäisen valvonnan ja riskienhallinnan kehittämistä ja koordinoimista varten on hallinnonalalla oma yhteistyöverkosto. (Oikeusministeriö 2018, 86 - 87.)

Vuonna 1992 valtion talousarvioasetuksen perusteella annetun asetuksen (1243/1992 65a §) mukaan viraston, jolle ministeriö oli asettanut tulostavoitteita, ”tuli laatia sisäisen valvonnan arviointi – ja vahvistuslausuman sisältävän toimintakertomuksen, jos ministeriö oli laatinut sille tulostavoitteet.” Asetus kumottiin joulukuussa 2009 siten, että kirjanpitoyksikköön kuuluva virasto ei ole enää velvollinen antamaan erillistä vahvistuslausumaa toimintakertomukseen, vaan kirjanpitoyksikön toimintakertomuksessa tulee olla kuvaus riittävin ja oikein tiedoin, kaikkien siihen kuuluvien virastojen toiminnasta ja taloudesta. (Valtiokonttori 2010.)

Sisäiseen valvonnan järjestelmää kehitettäessä tulisi talousarvioasetuksen 69 a §:n (7.4.2004/254) mukaisesti huomioida yleisiä standardeja sekä suosituksia, joiksi tarkoitetaan kansainvälisen valtioiden tarkastusvirastojen yhteisen järjestön INTOSAI:n sekä toisen järjestön, The Institute of Internal Auditors Inc.(IIA) antamia suosituksia. Julkishallinnon organisaatioiden käyttöön soveltuu myös Valtiokonttorin taloussääntömääräyksen mukaisesti COSO -yhdistyksen viitekehys. (Valtiontalouden tarkastusvirasto 2017b, 13.)

Sisäisellä valvonnalla organisaation johto ja muu henkilöstö valvovat toteuttamansa prosessin keinoin organisaation toimintoihin, raportointiin ja vaatimuksenmukaisuuteen liittyviä tavoitteita. Sisäisen valvonnan prosessilla on tarkoitus saada kohtuullinen varmuus tavoitteiden saavuttamisesta. Toiminnalliset tavoitteet liittyvät tuloksellisuuteen ja toiminnan tehokkuuteen, sisältäen omaisuuden turvaamisen sekä toiminnan ja talouden tulostavoitteet. (COSO 2013.)

Organisaation raportointi koskee esimerkiksi omien periaatteiden mukaista raportointia. Raportoinnin tavoitteet liittyvät toiminnallisuuteen sekä sisäisen ja ulkoisen laskennan läpinäkyvyyteen, ajantasaisuuteen ja luotettavuuteen. Lakien ja määräysten noudattaminen muodostaa tavoitteet vaatimustenmukaisuuden valvontaan. (COSO 2013.)

Sisäinen valvonta toimii ohjausmekanismina, jonka avulla organisaatio voi valvoa sille asetettuja tärkeitä tavoitteita, kehittää suorituskykyään ja ylläpitää sitä. Vuonna 1985 perustetun yksityisen sektorin riippumaton toimija (Noukka 2017) Committee of Sponsoring Organizations of the Treadway Commission ”COSO” on rakentanut sisäisen valvonnan kokonaisvaltaisen ajatusmallin, jonka avulla organisaatio voi kehittää omaa sisäistä valvontaansa tuloksellisesti tukemaan päätöksentekoa yhä muuttuvassa toimintaympäristössä. Ajatusmallin tarkoitus on antaa johdolle ymmärrys sisäisen valvonnan osa-alueista sekä toteuttamaan sisäiseen valvontaan liittyviä tehtäviä vähemmän ohjailevasti. (COSO 2013)

Sisäinen valvonta – kokonaisvaltainen ajatusmalli -viitekehikko voi olla periaatteellinen lähestymistapa minkä tahansa ja kokoisen toimialan organisaation sisäistä valvontaa suunniteltaessa. Organisaatio voi olla niin voittoa tavoitteleva, yleishyödyllinen kuin julkishallinnon organisaatio. (COSO 2013.)

Sisäinen valvonta ja siihen liittyvä riskienhallinta ovat olleet käsitteenäkin vielä kymmenen vuotta sitten vieraita niin valtionhallinnossa kuin organisaation X hallinnonalalla. Sisäinen valvonta ei tietyltä osin tarkoita kirjaimellisesti ”valvontaa”, eikä kaikilta osin sisällä tarkasteltavissa olevia elementtejä. Sellaisia voivat olla esimerkiksi ”johdon ote ja tavoitteenasettelu, sisäinen viestintä ja tiedonkulku, valvontatoimet ja erilaiset varmentavat kontrollit, toiminnan arviointi sekä organisaation toimintaympäristö, rakenteet ja periaatteet” (Valtiontalouden tarkastusvirasto 2015, 14.) Sisäinen valvonta kohdistuu toimintayksikön toimintaan kokonaisuudessaan, ja siihen voi sisältyä esimerkiksi erilaiset kokoukset, yhteistyöryhmät, työhön liittyvien vastuiden ja prosessien määrittely, hyväksymis- ja valtuutusmenettelyt sekä osaamisen varmistaminen. (Oikeusministeriö 2006, 5.)

Organisaation X johdon on valtion talousarviolain (13.5.1988/423) 24 b §:n tarkoittaman sisäisen valvonnan järjestämisen kautta oltava selvillä organisaation perustehtäviin liittyvistä riskeistä turvallisuuden eri osa-alueilla. Sisäisen valvonnan järjestämisestä, asianmukaisuudesta ja riittävyydestä vastaa viraston johto, jonka vastuuta sisäisestä valvonnasta on vahvistettu kaikilla hallinnon tasoilla. (VAHTI 2/2004.)

Organisaation X kohdalla sisäisen valvonnan tavoitteet ja päämäärät käydään läpi tulostavoiteasiakirjassa, jossa keskitytään toimintaan ja tuloksellisuuteen vaikuttaviin tekijöihin. Tuloksellisuuteen ja toimintaan vaikuttavat ainakin mittareina käytetyt substanssitoimintaan ja henkilöstöön kohdistuvat muutokset sekä sisäisten toimintatapojen kehitys ja muutokset. Mittareina tuloksellisuuteen käytetään erilaisia vireillä olevia prosesseja sekä niihin liittyviä erillisprosesseja ja niistä syntyviä kuormituksia ja työmääriä. Riskeinä nähdään mm. henkilökunnan vaihtuvuus, jolla on välillisiä tai välittömiä vaikutuksia organisaation toimintaan ja aikatauluihin. (TTA 2018.)

3.2 Riskienhallinta

Riskienhallinnan peruslähestymistavoista on laadittu valtionhallinnon hyvää käytäntöä kuvaava suositus valtion virastoille ja laitoksille valtioneuvoston asettaman sisäisen valvonnan ja riskienhallinnan neuvottelukunnan toimesta. Johdon työvälineeksi riskienhallinnan kehittämistarpeiden tunnistamiseen sekä sen arvioimiseksi, onko sisäisen valvonta ja riskienhallinta asianmukaista ja riittävää, on suositeltu COSO-ERM -viitekehystä, joka on yleisesti hyväksytty ja käytetty malli sisäisen valvonnan ja riskienhallinnan arvioimiseksi. COSO-ERM -mallia on kuitenkin muokattu siten, että sen sisältämät yksityiskohdat sopisivat valtionhallinnon toimintatapaan. (Valtiovarainministeriö 2005b, 3.)

Mallin tai neuvottelukunnan suositusten soveltaminen ei ole pakollista. Sisäisen valvonnan ja riskienhallinnan kehittämiseen voidaan virastoissa ja laitoksissa käyttää yleisesti hyväksyttyjä viitekehyksiä, laatumalleja, tuloskortteja tai muita työkaluja, jotka perustuvat edellisiin. Tällaisia ovat esimerkiksi CAF -itsearviointimalli, EFQM -Euroopan laatupalkintomalli ja ISO -standardit. Myös niin kutsutut BSC eli tasapainoisen onnistumisstrategian mallit ovat hyviä työkaluja. (Valtiovarainministeriö 2005, 3).

COSO-ERM on vuonna 2004 julkaistu riskienhallintaprosessin viitekehys, jonka COSO -organisaatio sai päivitettyä syksyllä 2017. Uudessa versiossa näkemys riskienhallinnasta ja sisäisestä valvonnasta yrityksen sisäisenä työkaluna on muuttunut näkemykseksi riskienhallinnasta integroituna toimintana, joka tukee yrityksen liiketoimintaa ja ennemminkin on apuna, kun strategiaa laaditaan ja lähdetään toteuttamaan. (Noukka 2017.)

Organisaatioissa saatetaan pohtia, mitä arviointikehikkoa hyödyntäen riskienhallintaa voisi lähteä kehittämään. COSO-ERM -viitekehys ja ISO 31 000 – standardi käsittelevät samoja asioita eri tavoin, mutta COSO-ERM yhdistää viitekehyksen ja prosessin ja ISO 31 000 erottelee ne. Sisäistä valvontaa varten organisaatiolla pitäisi olla tavoitteita ja päämääriä, joita valvomaan esimerkiksi COSO – malli on luotu ja joiden tehokkaasta toteutumisesta organisaation johto vastaa. (Marjamäki-Ruuskanen 2013, 34, Järvensivu 2017, 8.)

Nykytilanteessa valtionhallinnon eri virastoilla ja laitoksilla on virastokohtaisia riskienhallinnan käytäntöjä, ja etenkin virastojen vastuulla aiemmin olleiden ICT-toimintojen keskittämisen jälkeen on ollut kasvava tarve kattavampaan ja yhtenäisempään riskienhallintaan (Valtiontalouden tarkastusvirasto 2017a, 7).

Oikeusministeriössä pilotoitiin kehikkoluonnoksena COSO 2013 – mallia siten jatkomuokattuna, että se huomioi paremmin ministeriön toiminnan luonteen, terminologian ja ohjaus – ja johtamisjärjestelmän (Oikeusministeriö 2018, 87).

Riskienarviointi sisällytetään organisaation toimintaan ja tavoitteisiin kokonaisuudessaan sekä organisaation niihin tärkeisiin prosesseihin, jotka tavoitteet muodostavat. Riskienhallinnan tulokset hyväksytetään johdolla, joka vastuuttaa riskien hallintaan liittyvät toimenpiteet. Organisaation pitää selvittää oma riskinkantokykynsä ja johdon tulee hyväksyä riskienkäsittelyn tulokset myös jäännösriskien osalta. (VAHTI 3/2012, 20.)

3.3 Tulosohjaus

Väestö ja yritykset kohdistavat odotuksia julkisten palvelujen saatavuuteen. Tämän takia julkisten palvelujen laatu ja saatavuus edellyttävät, että valtion rahoittaman toiminnan vaikuttavuus, toiminnallinen tehokkuus ja tuottavuus ovat todennettavissa vuorovaikutteisen, sopimusajatteluun perustuvan ohjausmallin, tulosohjauksen, keinoin. Julkisen toiminnan tuloksia arvioidaan siitä näkökulmasta, minkälaisia yhteiskunnallisia hyötyjä toimija on aikaansaanut sekä miten tehokkaasti tai tehottomasti voimavaroja on käytetty, jotta saataisiin riittävä kuva esimerkiksi viraston toiminnasta ja tuloksellisuudesta. (Valtiovarainministeriö 2005a, 9.)

Tulosajattelun mukaisen ohjaustavan on katsottu kehittävän toiminnan tehokkuutta ja saavan aikaan haluttuja tulosvastuutavoitteiden mukaisia vaikutuksia, jossa päähuomio on tavoitteiden asettamisessa (Valtiontalouden tarkastusvirasto 2007, 8). Keskeistä tulostavoitteille hallittavuudenkin näkökulmasta on vähäinen määrä tulosta kuvaavia tavoitteita ennemmin, kuin suuri määrä epärealistisia toimenpiteitä ja tekemistä kuvaavia tavoitteita. Tavoitetasolla on hyvä olla suhteutusperusta, joka tarkoittaa sitä, että organisaatiolla on mahdollisuus suhteuttaa tavoitteitaan seuraavaan vuoteen, jos tulostavoite on edellistä vuotta vaativampi. (Valtiovarainministeriö 2005a, 24.)

Vahti -ryhmän jo 14 vuotta sitten antaman suosituksen mukaan tietoturvatyön ohjaamiseen virastokohtaisesti tulisi käyttää tietoturvakysymykset huomioiden strategia-, toiminta – ja taloussuunnitelmia sekä tulosohjauksen keinoja (VAHTI 1/2004, 11). Tietoturvallisuus tulisi olla organisaation tulosohjausprosessissa osana normaalia toiminnan kehittämistä (VAHTI 1/2004, 36).

Tulosohjausajattelun mukainen tietoturvatyön kehittäminen organisaation X kohdalla tarkoittaa sitä, että tietoturvatavoitteiden asettaminen voi liittyä suoraan tietoturvatoimintoihin, mutta ne voivat olla johdettu myös muista organisaation tietoturvallisuuteen keskeisesti liittyvistä tavoitteista (VAHTI 6/2006, 22), kuten jo toteutuneet asioiden sähköisen käsittelyn kehittäminen, sähköisten aineistojen valmistelu sekä muilla asioiden käsittelyyn ja tietojenkäsittely-ympäristöön liittyvillä kehittämistoimenpiteillä.

Tietoturvatyön tulosohjausajattelutavan mukaisten kehittämistoimenpiteiden pitäisi kohdistua prosessien lisäksi myös ihmisiin, sillä organisaation X hallinnonalallekin vaikuttavien julkis-

yhteisön säästötavoitteiden riskin hallitsemiseksi tulisi kiihtyvästi etenevän digitalisaation takia uudistaa myös toimintatapoja. Digitalisaation nopea eteneminen voidaan nähdä haasteena ja mahdollisuutena, mutta epäonnistumisella siihen liittyvien riskien hallinnassa on negatiivisia vaikutuksia toiminnalle liittyville tehostamis- ja tuottavuusvaatimuksille. (Oikeusministeriö 2018, 88.)

Tulosohjausajattelun mukainen tietoturvatyön kehittäminen liittyy suoraan myös osaamisen kehittämiseen, jonka edistämiseen organisaatio voi vaikuttaa itse kehittämällä toimintatapoja sekä panostamalla hallinnonalan henkilöstön ICT-osaamiseen liittyvien tarpeiden kehittämiseen. Tätä tärkeää työtä on tehty organisaatiossa X vuodesta 2015, jonka tuloksena hallinnonalalle on saatu sähköisten työvälineiden sekä uusien järjestelmien ja ohjelmistojen osaamiseen liittyvää koulutusta, sekä lisäksi ICT-osaamista kehittävä valtakunnallinen koulutuskonsepti. (Oikeusministeriö 2017b, 11.)

3.4 Tuloksellisuus

Tuloksellisuus viittaa tulosohjausajattelun mukaisiin organisaation kokonaistavoitteisiin ja niiden saavuttamiseen (Valtiovarainministeriö 2018b). Organisaation toiminnan tuloksia on voitava arvioida siitä näkökulmasta, miten voimavaroja käytetään ja millaisia yhteiskunnallisia hyötyjä sen toiminta saa aikaan. Näistä muodostuu toiminnan laadulliset tekijät, eli yksi tuloksellisuuden osatekijöistä. (Valtiovarainministeriö 2005a, 49.)

Tavoitteet voivat liittyä viraston kykyyn palvella asiakkaitaan ja vastata sille asetettuihin odotuksiin. Laatuun liittyvät tavoitteet liittyvät toimintaprosesseihin, esimerkiksi käsittely – tai odotusaikoihin tai läpäisyaikaan (Valtiovarainministeriö 2005a, 73). Koska tietotekniikalla on merkitys organisaation sisäisiin toimintaprosesseihin, voidaan keskeisiä tietoturvakysymyksiä tarkastella osana viraston toiminnan johtamista ja tulosohjausta (VAHTI 2/2004, 8).

Valtiovarainministeriön vuoden 2005 tulosohjauksen käsikirjassa todetaan, että julkinen talous ja toimintaan liittyvä ohjaus ovat julkiseen talouteen kohdistuvien, noususa olevien menopaineiden edessä merkittävien haasteiden edessä (2005a, 9). Kehitys julkisen talouden menopaineiden suhteen jatkuu nykytilanteessa samanlaisena, sillä oikeusministeriön hallinnonalalle näyttäisi tulevan 13 milj. euroa vähemmän määrärahoja vuoteen 2017 verrattuna (HE 106/2017 vp, 31).

Määrärahojen kaventuminen heijastuu koko hallinnonalla oleviin resursseihin ja sitä kautta kaikkiin prosessiketjussa olevien yksikköjen kykyyn toimia ydintehtävässään riittävän laadukkaasti. Tähän vaikuttaa eduskunnan ja hallinnonalan kirjanpitoyksikön päätösvallassa oleva rahoitus ja määrärahojen jakaminen, jolla on vaikutuksia taas rekrytointiin ja koulutuksiin (TTA 2018).

Määrärahojen kaventuminen saattaa heijastua negatiivisesti viranomaisen kykyyn hoitaa tietoturvaansa hyvällä tasolla sekä palvelun tai toiminnan laadun heikkenemisenä. Organisaation X hallinnonalalla esiintyvistä riskeistä keskeisimpänä nähdään julkisen talouden kasvavat säästötavoitteet, jotka toteutuessaan voivat heikentää kansalaisten oikeusturvaa ja oikeusvaltion toimintaedellytyksiä (Oikeusministeriö 2018, 87). Määrärahojen kaventuminen heijastuu myös organisaation X tulostavoitteisiin strategisina muutoksina, jonka riskinä nähdään vaikutukset organisaation perustehtävään ja asemaan. (TTA 2018).

4 Tietoturvan kehittämistyössä huomioitavia riskejä

Organisaation X ja muiden hallinnonalan virastojen työasemaympäristö käsittää yhtenäisen laitekannan ja samanlaisen, vakioidun työasemaympäristön. Käyttäjien pääsyvaltuuksia ja työasemien ohjelmisto- ja turvallisuuspäivitysjakeluja hallitaan keskitetysti. Valtiolla on käytössä yhteinen, tietoturvallinen tietoliikenneverkkoratkaisu, jossa asiakasorganisaatioille tarjotaan keskitetty palomuuripalvelu, roskapostin suodatus, haittaohjelmien suodatus, tunkeutumisenestojärjestelmä ja suoja palvelunestohyökkäysten varalta. Internetin kautta tulevaa liikennettä suodatetaan ja optimoidaan nettisuodatuksen avulla sekä sähköpostiliikenne suodatetaan roskapostien varalta. Asiakasorganisaatiot saavat käyttöpalveluita keskitetysti suojattujen konesalien ja tietoliikenneyhteyksien kautta. (Valtori 2016.)

Tietohallintopalveluita on valtionhallinnossa keskitetty palvelukeskushankkeissa yli hallintorajojen. Tämän johdosta virastot ja laitokset ovat menettäneet toimivaltaa ja sellaisia resursseja, joiden avulla toiminnan jatkuvuutta ja kybersuojausta voidaan tietohallintopalveluista riippuvaisissa organisaatioissa varmistaa. Ministeriötasolla toimii tilaaja-tuottaja -järjestelyt, joissa kybersuojaukseen liittyvät palvelut tulevat valtioneuvoston hallintoyksikön välityksellä Valtion tieto- ja viestintätekniikkakeskus Valtorilta. Valtori voi tilata palvelun myös yksityiseltä palveluntuottajalta. (Valtiontalouden tarkastusvirasto 2017, 16.)

Asiakirjojen käsittelyyn liittyy julkisuuslain puolelta vaatimus hyvän tiedonhallintatavan noudattamisesta ja siihen liittyen vaatimus asiakirjojen sekä tietojärjestelmien asianmukaisen suojaamisen huolehtimisesta sellaisin järjestelyin, että asiakirjojen ja tietojärjestelmien suojaus on turvattu asianmukaisin menettelytavoin (VAHTI 2/2014, 19). Tietoturvallisuusasetukseen (valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010) sisältyy taas vaatimus viranomaiselle estää käyttöoikeushallinnan avulla tietojen luvaton tai asiaton käsittely sekä luvaton muuttaminen (VAHTI 2/2014, 59).

ICT-palvelujen tuottajalla voi olla lähtökohtaisesti tietoturvalliset ja laadukkaat palvelut, mutta viranomaisen voi olla mahdotonta arvioida sitä, täyttääkö se julkisuuslain ja tietoturvallisuusasetuksen asettamat vaatimukset liittyen asiakirjojen ja tietojärjestelmien sisältämien tietojen suojaamiseksi silloin, kun tietojärjestelmiin liittyvä suojaus tuotetaan organi-

saation ulkopuolelta. Vaikka tietoturvallisuus kuuluu eri palveluntuottajien ydinosaamisalueeseen ja turvallisuusratkaisujen pitäisi olla riittävät, asiakasyrityksellä on harvoin keinoja tai kykyjä arvioida niitä turvallisuusratkaisuja, joita palveluntuottaja käyttää. (Sisäasiainministeriö 2012.)

Viranomaisen tulee varmistaa organisaationsa, palveluidensa ja tietoaineistonsa turvallisuus (VAHTI 2/2014, 5). Seuraavilla tietojenkäsittely-ympäristöstä tunnistetuilla riskeillä voi olla merkitystä silloin, kun arvioidaan tietoturvallisuuden tilaa organisaatiossa ja sitä, onko toteutetut tietoturvatoimenpiteet olleet asianmukaiset ja riittävät.

4.1 Sovellukset

Aloitin työni tietotekniikan parissa julkishallinnossa jo 2000 -luvun alussa, kun käytössä oli osin merkkipohjaisia työasemia ja graafisena käyttöjärjestelmänä alkoi yleistymään Windows 3.11 (Windows for Workgroups) ja myöhemmin NT/2000 -käyttöjärjestelmät. Tuohon aikaan ei vielä ollut yhtenäistettyä IT-palvelujen tuotantoa eikä keskitettyjä perustietotekniikan palveluja, ja tietoturvan hallinta oli haastavaa jo työasemien ylläpidosta lähtien. Olen työskennellyt sekä kunnan että valtion puolella tietoteknisissä työympäristöissä it-alan ammattilaisena yli 17 vuotta, joista 5 vuotta perehdyin turvallisuusjärjestelmiin pääkäyttäjän ominaisuudessa sekä turvallisuushankintojen näkökulmasta.

Vuonna 2013 havaitsin organisaatiorajat ylittävän tietoturvapoikkeaman, joka mahdollisti kirjautumisen toisten käyttäjien sähköpostilaatikoihin tietyissä olosuhteissa. Tämä tapahtuma sai minut kiinnostumaan tietoturvasta, sen kehittämisestä ja hallinnasta kokonaisuutena; miksi hyvistä teknisistä ja hallinnollisista kontrolleista huolimatta useassa organisaatiossa sivuutettiin tietoturvaan liittyvää ohjeistusta? Palveluntarjoajan pääsynvalvontaan liittyvä virheellinen ohjeistus oli yksi riskin eskaloinut tekijä, mutta poikkeaman ei teknisestikään olisi pitänyt olla mahdollista varsinkin, kun sähköpostia voitaneen pitää erittäin keskeisenä tietojärjestelmänä. Vahti -ohjeistuksessa keskeiseksi tietojärjestelmäksi määritellään sellainen tietojärjestelmä, jonka tukemien toimintojen puuttuminen tai tietojen paljastuminen lamauttaa organisaation toiminnan tai heikentää organisaation työntekijöiden turvallisuuden (Vahti 5/2004, 12). Sähköpostijärjestelmää käytetään sovelluksen kautta, mutta harvoin organisaation tietoturvaa arvioitaessa lähdetään arvioimaan jo käytössä olevien sovellusten tietoturvallisuutta, joka saattaa usein olla vaarallisen heikko lenkki tietojärjestelmässä (Vahti 5/2004, 6).

Aktiivisesta tietoturvallisuuden kehitystyöstä, hyvästä seurannasta ja hyvistä mittareista huolimatta poikkeamia voidaan havaita yllättäviltä tietoturvan osa-alueilta. Yhtenä tietoturvan kehittämistyön mittarina voidaan pitää huonotasoisten salasanojen käytön estoa (VAHTI 1/2016, 31). Hyvistä teknisistä ja fyysisistä kontrolleista huolimatta organisaatio voi olla ulkoistetun ICT-palvelujen takia osin kykenemätön huolehtimaan omasta tietoturvastaan, koska

joku muu on määritellyt ja rakentanut sen teknisen ympäristön, jossa organisaatio työskentelee. Riippuvuutta tietojärjestelmistä yhdessä palveluiden ulkoistamisen kanssa pidetään yhtenä heikentävänä tekijänä hallinnon tietoturvallisuudelle (Vahti 7/2003, 6).

Erääseen sähköpostijärjestelmään liittyvän asiakassovelluksen salasanan luontiin liittyvissä käytänteissä määritellään ja ohjeistetaan, että:

1. Sinun on käytettävä salasanaa, jonka pituus on 8 merkkiä.
2. On suositeltavaa, että salasanassasi on vähintään 10 merkkiä.
3. Käytä isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä.
4. Jos haluat, että salasana on helposti muistettavissa, käytä lausahdusta tai lausetta.
5. Vältä yksittäisten nimien tai sanakirjassa olevien sanojen käyttämistä.

Useimmiten käyttäjät noudattavat tunnollisesti salasanan luontiin liittyviä ohjeita järjestelmän pakottamana silloin, kun salasana ei täytä vaatimuksia, eikä salasanan vaihto muutoin onnistu. Entä, jos ainoa *pakollinen* vaatimus edellisessä esimerkissä on tuo listan ensimmäinen: ” Sinun on käytettävä salasanaa, jonka pituus on 8 merkkiä”. Oikeastaan ohjeesta jo näkee, että ensimmäinen lause on ainoa, joka on muodoltaan ehdoton. Muut vaatimukset eivät ole luonteeltaan ehdottomia, vaan suosituksen omaisia. Käyttäjä voi antaa siten salasanaksi vaikka 12345678, aaaaaaaa tai 11111111. Rajoituksia tai salasanahistoriaa ei ole. Salasanahistoriaa ei tarvita, koska sovellus ei koskaan pakota käyttäjää vaihtamaan salasanaa. Vaikka salasana pakotettaisiin vaihtamaan erillisen käyttövaltuushallintajärjestelmän kautta, vanhan salasanan voi vaihtaa takaisin.

Ongelmana hyvän käyttövaltuushallinnon näkökulmasta on myös organisaatiorajat ylittävä sovelluksen käyttö, kun samaa sovellusta käytetään useissa hallinnonalan virastoissa (VAHTI 9/2006, 12). Toiseen hallinonalan virastoon ja toisiin tehtäviin siirtyvien käyttäjien vanhat käyttövaltuudet jäävät kyseisen sovelluksen kohdalla voimaan jopa vuosiksi, joten mahdollinen heikko salasana voi olla pitkään käytössä.

Sovellus on vielä nykyäänkin käytössä. Ulkopuolisista tietoturvajärjestelyistä ei ole suurta hyötyä, jos esimerkiksi huonosti toteutettu sovellus avaa oikeudettoman pääsyn suoraan tietojärjestelmään sisälle, kun käyttäjä pääsee hyödyntämään vaikkapa sovelluksen virheellistä logiikkaa (Vahti 5/2004, 24).

Tietojärjestelmien, sovellusten ja päätelaitteiden kohdalla on tietysti muistettava, että suojattavia kohteita joudutaan kustannustehokkuuden ja tarkoituksenmukaisuuden näkökulmasta rajaamaan, koska tietoturvatarpeet etenkin tietojärjestelmien kohdalla ovat erilaisia. VAHTI -ohjeistuksen tarkoitus on kuitenkin tietojärjestelmien tietoturvan huolehtiminen kokonaisuutena ja siten pyrkimys vaikuttamaan siihen, että tietoturvallisuuden suunnitteluun sovelletaan vakioituja ja hyväksyttyjä menettelytapoja. (VAHTI 3/2010, 17.)

4.2 Päätelaitteet

Laitetta, jossa käsitellään sähköisessä tietojärjestelmässä tai jossakin muussa palvelussa olevaa tietoa, kutsutaan päätelaitteeksi (VAHTI 5/2013, 14). Uusien työskentelytapojen myötä valtionhallinnon organisaatioissa on otettu, ja tullaan yhä enenevissä määrin ottamaan käyttöön lisää päätelaitteita palveluineen. Päätelaitteisiin kuuluvat työasemat, kannettavat ja erilaiset mobiililaitteet, kuten älypuhelimet. Valtionhallinnon organisaatioiden tulisi päätelaitteita käyttäessään huomioida salassa pidettävän tietojen käsittelyn turvallisuuden erilaisissa tilanteissa. (VAHTI 5/2013, 9.) Tässä luvussa päätelaitteilla tarkoitetaan Windows -käyttöjärjestelmällä varustettuja pöytätyöasemia tai kannettavia tietokoneita.

Salassa pidettävän tiedon turvallisessa käsittelyssä päätelaitteella on keskeinen rooli varsinkin sellaisissa tilanteissa, joissa tietyssä palvelussa tai tietojärjestelmässä on puutteita, tai jos tietojärjestelmä tai palvelu ei kykene rajaamaan päätelaitteessa tapahtuvaa salassa pidettävän tiedon käsittelyä (VAHTI 5/2013, 13). Varsinainen tietojen käsittely päätelaitteessa tapahtuu laitteessa tai laitteeseen asennetussa ohjelmistossa (5/2013, 14).

Organisaation X hallinnonalalla tehtiin tietoaineiston luokittelupäätös 31.12.2016 asiakirjojen luokittelusta sekä luokiteltujen asiakirjojen käsittelyn vaatimuksista. Hallinnonalan ohjeistuksen mukaisesti salassa pidettävää aineistoa saa käyttää vain henkilökohtaisilla, virkakäyttöön annetuilla työasemilla. Aineisto on tallennettava sähköisesti siten, että ainoastaan sen käyttöön oikeutetuilla henkilöillä on aineistoon pääsy (Oikeusministeriö 2014a).

Luokittelupäätöksen myötä on tärkeää suunnitella luokittelun käyttöönotto hyvin. Luokittelun tarkoitus on helpottaa salassa pidettävien tietojen vaihtoa viranomaisten välillä etenkin silloin, kun salassa pidettävien tietojen vaihto tai vastaanottaminen on säännönmukaista tai massaluonteista. (VAHTI 3/2010, 10.)

4.3 Salassa pidettävän tiedon käsittelyyn liittyviä riskejä

Salassa pidettävien tietojen käsittely päätelaitteilla sisältää aina riskejä, jotka huomioidaan riskien arvioinnin kautta luomalla tarpeen tullen rajattu palveluiden, päätelaitteiden, tietojärjestelmien, verkkojen ja tilojen muodostama tietojenkäsittely-ympäristö. Joissakin tapauksissa päätelaitteissa voi olla tiettyjä tietojen suojaukseen tai hallintaan liittyviä puutteita, jotka voidaan kompensoida esimerkiksi tietojärjestelmään, kuten sähköpostiin, liittyvillä teknisillä ratkaisuilla. (VAHTI 5/2013, 10.)

Salassa pidettävien tietojen suojaus esimerkiksi päätelaitteiden varkaustapauksissa toteutuu hyvin erillisillä turva-ohjelmistoilla, joilla kannettavien tietokoneiden tai älypuhelimien sisältö on salattu. Edellä kuvattuja tilanteita, joissa tietojärjestelmässä on puutteita, eikä tietojärjestelmä tai palvelu kykene rajaamaan päätelaitteessa tapahtuvaa, salassa pidettävän

tiedon käsittelyä, on usein vaikea havaita tai valvoa. Tällaisia puutteita voi sisältyä esimerkiksi käytettävään sähköpostijärjestelmään.

Vahti -ohjeistuksessa mainitaan, että jos esimerkiksi suojaustason IV rajatun käsittelyn vaatimuksia ei pystytä toteuttamaan, voidaan riskienarvioinnin avulla päättää, voidaanko päätelaitteilla käsitellä tai tallentaa esimerkiksi rajatusti salassa pidettävää suojaustason IV tietoa. Organisaatio voi ohjeistaa, että sähköposteihin tai kalenterimerkintöihin ei sisällytetä salassa pidettävää suojaustason IV tietoja muutoin, kuin sähköpostin liitetiedostoina. (VAHTI 5/2013, 47.)

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999; julkisuuslaki) 18 § sisältää vaatimuksen liittyen asiakirjallisten tietojen laatuun mm. tietojen suojaamisen osalta, jonka varmistamiseksi tietojärjestelmät tulee suunnitella siten, että asiakirjallisten tietojen julkisuus voidaan toteuttaa ja erityisesti suojata salassa pidettävät tiedot (VAHTI 5/2006, 11).

Tietoaineistojen käsittelyyn liittyviä teknisiä vaatimuksia käsitellään VAHTI 3/2012 -ohjeessa ”Teknisen ICT-ympäristön tietoturvataso-ohje”. Ohje tehtiin tukemaan 1.10.2010 voimaan tulleen asetuksen tietoturvallisuudesta valtionhallinnossa täytäntöönpanon ohjausta. (VAHTI 3/2012, 5.) Ohjeen sivulla 41 käsitellään valtionhallinnon organisaatioiden päätelaitteiden vakiointia sekä koventamisperusteita (VAHTI 3/2013, 41).

4.4 Koventaminen

Koventaminen tarkoittaa käyttöjärjestelmän kohdalla ”turhan toiminnallisuuden poistamista ja turvattomien oletusarvojen muuttamista turvalliseksi” (VAHTI 5/2004, 70). Koventamisella halutaan estää kaikki sellaiset ohjelmistojen perusominaisuudet, joita normaalikäytössä ei tarvita. Se tarkoittaa myös sitä, että käyttöjärjestelmän asetuksista poistetaan sellaisia oletusasetuksia, joiden poistamatta jättäminen voisi mahdollistaa asetuksen ominaisuuden käyttämisen vääriin tarkoituksiin. Esimerkkinä voi olla tietyt käyttöjärjestelmien hakemistot ja niiden pääsyoikeuksien rajoittaminen. (Viestintävirasto 2015, 73.)

Microsoft on julkaissut tietoturvamääritysohjeita Windows – käyttöjärjestelmälleen. Osa ohjeista on tarkoitettu sovellettavaksi alueilla, joissa tarvitaan erittäin tehokasta tietoturvaa, osa on yrityksille tai kuluttajille tarkoitettuja ohjeita. Muitakin organisaatiota on, jotka julkaisevat erilaisia vapaaehtoisesti sovellettavia luokituksia, ohjeita ja tietoturvatasoja, kuten Microsoft Center for Internet Security (CIS). VAHTI ohjeissa viitataan usein National Institute of Standard and Technology (NIST) -nimiseen organisaatioon. (Microsoft 2018d.)

VAHTI 3/2010 määrittelee sisäverkon suojaamiseen liittyviksi toimenpiteiksi järjestelmien koventamisen, käyttöoikeuksien rajaamisen ja päätelaitteiden koventamisen (3/2010, 41), mutta tarkempaan ohjeistukseen liittyen viitataan yhdysvaltalaisen kauppaministeriön alai-

sen, NIST -viraston ohjeisiin (NIST 2018a). NIST -ohjeissa päätelaitteiden ja käyttöjärjestelmän lisätietoturvan kohdalla puhutaan vähimpien oikeuksien periaatteesta (least privilege), jonka mukaisesti käyttäjille annetaan pienimmät mahdolliset oikeudet tietojärjestelmän tai työaseman käyttöön. Periaatteen tarkoituksena on myös suojata ja rajoittaa haittaohjelmista syntyviä vahinkoja. (NIST 2018b.)

Kansallisen turvallisuusauditointikriteeristön (Katakri) aiemmassa ohjeistuksessa mainitaan, että ”Käyttäjillä on vain ne oikeudet, joita he tarvitsevat tehtäviensä hoitamiseen. Pääsy on rajattu vain omiin työtehtäviin liittyviin verkkoihin, tietoihin ja järjestelmiin.”, eli sama suositus vähimpien oikeuksien periaatteeseen liittyen. (KATAKRI 2011, 68.)

Katakrin vuoden 2015 päivitetyssä versiossa on vaatimus liittyen vähimmäistoimintojen ja vähimpien oikeuksien periaatteeseen, eli järjestelmäkovennuksiin. Kohdassa I 08 (5. tekninen tietoturvallisuus) suositellaan, että asennuksen yhteydessä käyttöjärjestelmiin automaattisesti luoduista tileistä (järjestelmänvalvoja, vierailija) on oikeudet rajattu minimiin tai poistettu käytöstä (Katakri 2015, 43).

Edellä mainittuja koventamiseen liittyviä käytäntöjä on tietyiltä osin jo käytössä vakioiduissa päätelaiteympäristöissä kannettavien ja pöytätyöasemien kohdalla, mutta osittaiset tiukennukset voisivat tulla harkittavaksi toukokuussa 25.5.2018 voimaan astuneen EU:n yleisen tietosuoja-asetuksen jälkeen. Asetus velvoittaa suojaamaan henkilötiedot käsittelyn, tallennuksen ja siirron aikana mm. vahingossa tai oikeudetta tapahtuvalta pääsyltä. (EUR-Lex, 2016.)

Pääosin vaatimus kohdistuu tietojärjestelmiin ja niihin liittyvään pääsyn rajaamiseen ja pääsyoikeuksien hallintaan, mutta kyse on myös siitä, miten henkilötietoja saa tallentaa pilvipalveluun, siirtää sähköpostilla sekä tallentaa siirrettäville tietovälineille. (VAHTI -raportti 1/2016, 25). Siirtäminen ja tallentaminen voi tapahtua turvallisesti, mutta loppukäyttäjän tietojenkäsittely-ympäristössä voi esiintyä tiettyjä päätelaitteissa esiintyviä toiminnallisia riskejä, joita avataan seuraavissa alaluvuissa.

4.4.1 Käytännön esimerkkejä koventamisperusteille

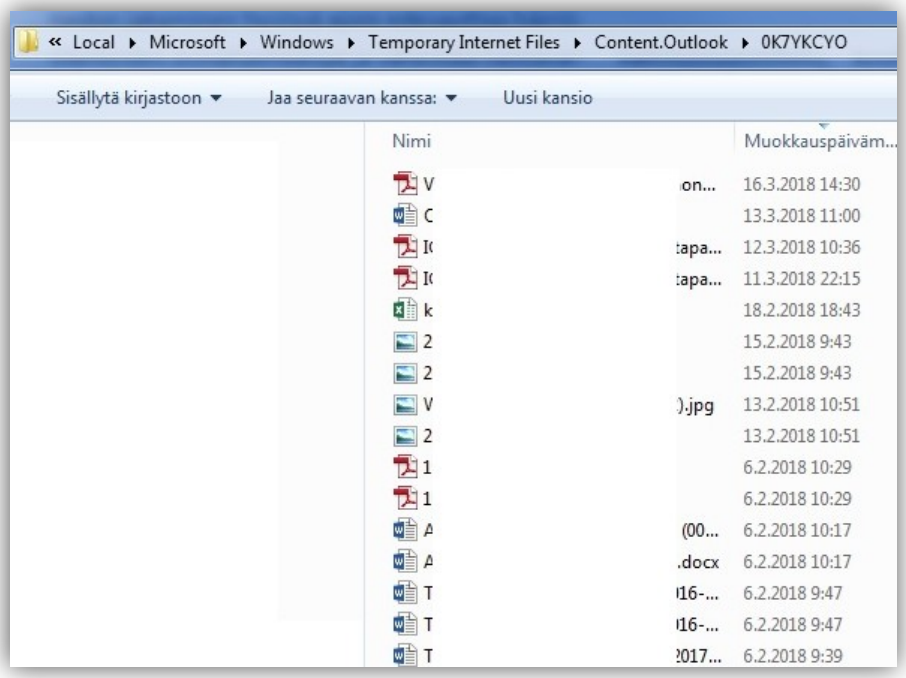
Outlook -sähköpostijärjestelmän asiakassovelluksessa on ominaisuus, jossa sähköpostiviestin turvalliseksi katsottu liitetiedosto tallentuu piilotettuun tiedostokansioon varotoimena. Outlook tarkistaa kansion sijainnin Windows -käyttöjärjestelmän rekisteristä etsimällä arvon *”HKEY_CURRENT_USER\Software\Microsoft\Office\(versio)\Outlook\Security”*.

Jos rekisteriavain sisältää kelvollisen tiedostopolun, esimerkiksi *”C:\Users\(käyttäjäprofiili)\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Outlook\(kansio)\”*, Outlook sijoittaa kyseiseen sijaintiin väliaikaiset tiedostonsa. Jos rekisteriavainta ei ole, tai osoite ei ole kelvollinen, Outlook luo uuden satunnaisesti nimetyn alihakemiston ”Temporary Internet Files” -kansion alle (Kuvio 2). (Microsoft 2012.)

Outlook -asiakassovelluksen piilotettuun väliaikaiseen kansioon liittyvä toiminnallisuus voi olla tietoturvan ja tietosuojankin kannalta ongelmallinen, koska normaalioikeuksilla (user) toimiva käyttäjä ei välttämättä osaa etsiä kansiota, tai ihannetilanteessa edes pääse kansioon, eikä siten pysty poistamaan kyseiseen kansioon tallentuvaa salassa pidettävää tietoaineistoa ja siten omatoimisesti suojaamaan salassa pidettävän tiedon vahingossa tai oikeudetta tapahtuvalta pääsyltä.

Organisaation X käyttäjiltä on tullut huolestunutta palautetta siitä, että salassa pidettäviä asiakirjoja tallentuu heistä riippumattomista syistä myös jonnekin muualle, kuin mihin oli tarkoitus. Huoli kohdistuu tilanteisiin, joissa käyttäjän päätelaite siirtyy palvelussuhteiden päättyessä toisille käyttäjille. Vaikka palvelussuhteensa päättävän käyttäjän käyttövaltuudet lopetetaan, jää esimerkiksi kannettavaan työasemaan käyttäjän paikallinen käyttäjäprofiili muiden käyttäjäprofiilien joukkoon, ellei kannettavaa asenneta uudelleen tai kiintolevyn sisältöä ylikirjoiteta päätelaitteen elinkaaren päättyessä.

Normaalioikeuksilla (user) kannettavaan kirjautuva loppukäyttäjä ei toisen käyttäjien profiileihin pääse käsiksi, mutta järjestelmänvalvojan oikeudet itselleen saanut käyttäjä pääsee käsittelemään jokaisen paikallisen profiilin sisältämiä tietoja. Outlookin väliaikaiseen kansioon voi tallentua vuosien aikana suuri määrä asiakirjoja.



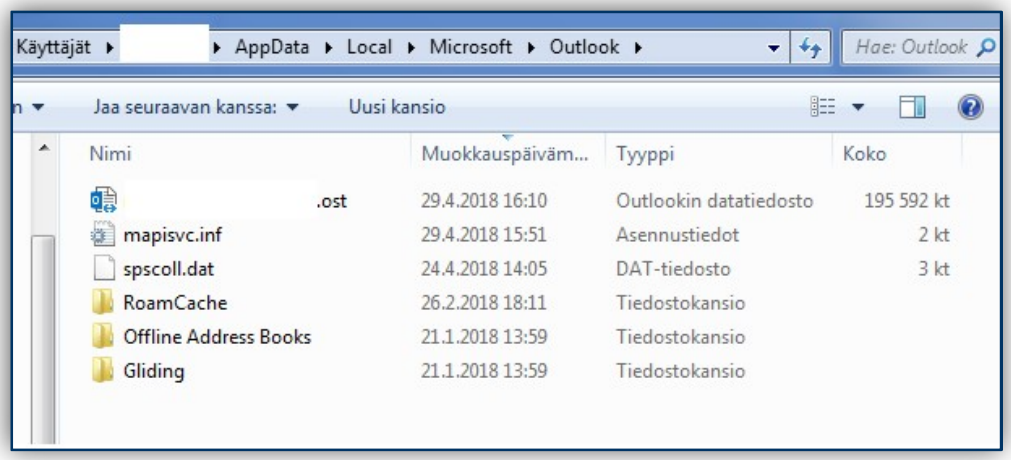
Kuvio 2: Outlook -työasemasovelluksen väliaikaisten tiedostojen sijainti

Toinen Outlook -ympäristöön liittyvä ongelma on Outlook -sovelluksen offline -toiminnallisuus. Kun käyttäjä kirjautuu esimerkiksi Windows -ympäristössä kannettavalle tietokoneelleen ja lisää sähköpostitilin Outlookiin, käyttäjän tietokoneen profiiliin tallennetaan paikallinen kopio, jotta käyttäjä voi toiminnon avulla käyttää sähköposteja, yhteystietoja, ja kalenteritietoja ilman verkkoyhteyttä. (Microsoft 2018a.)

Tällaista tiedostoa kutsutaan Outlookin offline -datatiedostoksi (.ost). Se on synkronoitu kopio sähköpostilaatikon tiedoista, jonka avulla Outlookin toiminnallisuus säilyy, vaikka yhteys postipalvelimeen keskeytyy tai verkkoyhteys kannettavaan katkeaa. Ainoastaan uusia sähköpostiviestejä ei ladata tai sähköpostiviestejä ei lähetetä, ennen kuin yhteys koneeseen palautuu. (Microsoft 2018a.)

Office datatiedosto sijaitsee piilotetussa kansiossa seuraavassa sijainnissa:

C:\Käyttäjät\käyttäjä\AppData\Local\Microsoft\Outlook (Microsoft 2018a).



Kuvio 3: Outlook ost -tiedosto

Offline -toiminnallisuuden riskiksi voi muodostua organisaation tietojenkäsittely-ympäristö, jos työaseman tai käyttöjärjestelmän kovennuksia ei ole toteutettu riittävällä tasolla. Ost-tiedoston lukeminen on mahdollista erilaisilla kolmannen osapuolen kaupallisilla sovelluksilla, mutta myös ilmaisilla, avoimen lähdekoodin sovelluksilla, jotka pystyvät lukemaan ost -tiedoston sellaisenaan vaikka muistitikulta, ilman tarvetta suorittaa ost -tiedostoa Outlook -ympäristössä. Loppukäyttäjä pystyy myös varmuuskopioimaan Outlookin toimintojen avulla sähköpostiviestit ja kalenteritiedot pst -datatiedostoksi, jonka voi avata toiseen koneeseen asennetulla Outlook -asiakasohjelmistolla.

4.4.2 Väliaikaiset kansiot

Vahti – raportissa EU-tietosuojan kokonaisuudistuksesta todetaan tietosuoja-asetuksen velvoittavan rekisterinpitäjän turvaamaan henkilötietojen käsittelyn siten, että rekisterinpitäjä toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet. Henkilötietoja pitää esimerkiksi suojata ”siirron, käsittelyn ja tallennuksen aikana” sekä ”oikeudetta ja vahingossa tapahtuvalta tuhoamiselta, muuttamiselta, luovuttamiselta tai pääsyltä.” (Valtiovarainministeriö 2016.) Väliaikaisiin kansioihin tallentuvat asiakirjat saattavat muodostaa riskin tietosuojan näkökulmasta.

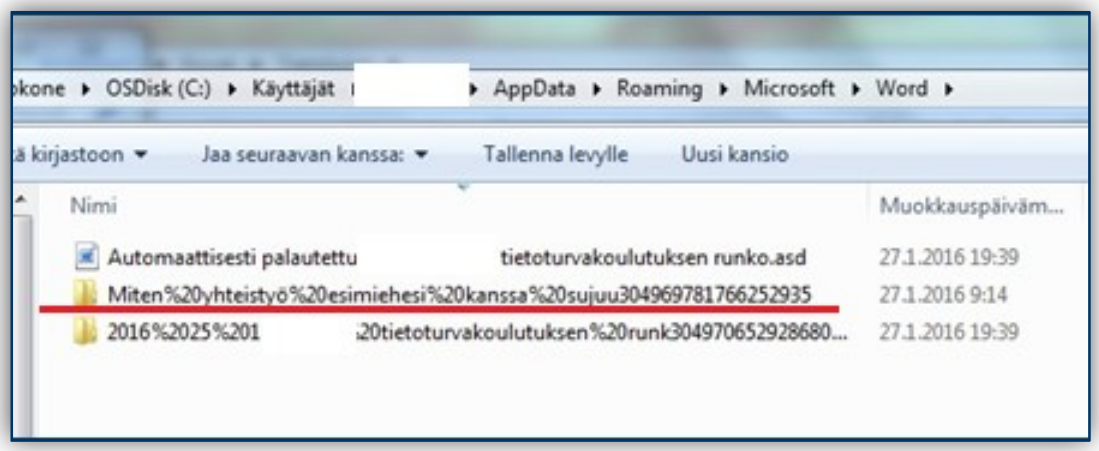
Oikeudeton pääsy henkilötietoja tai muuta arkaluonteista sisältävään tietoon voi toteutua tilanteessa, jossa työaseman paikallisen järjestelmänvalvojan salasana on saatu murrettua. Yksinkertainen esimerkki paikallisen järjestelmänvalvojan salasanaan liittyvään haavoittuvuuteen on Microsoft Server 2008 -version julkaisu, jonka mukana tuli ryhmäkäytäntöihin liittyviä uusia ominaisuuksia, joita käyttämällä paikallisen järjestelmänvalvojan salasana saatiin asetettua palvelimille ja toimialueella sijaiseville työasemille. (Microsoft 2017)

Tätä ei nykyisin suositella, koska jo vuonna 2009 oli laajasti tiedossa, että mainitulla tekniikalla hallinnoidut salasanat olivat heikosti salattu AES 32-bittisellä salauksella, ja helposti paljastettavissa takaisinmallintamalla. Se oli kuitenkin parempi vaihtoehto, kuin erilaisilla skripteillä, eli komentosarjojen avulla selväkielisenä tallennetut salasanat. (Microsoft, 2017.)

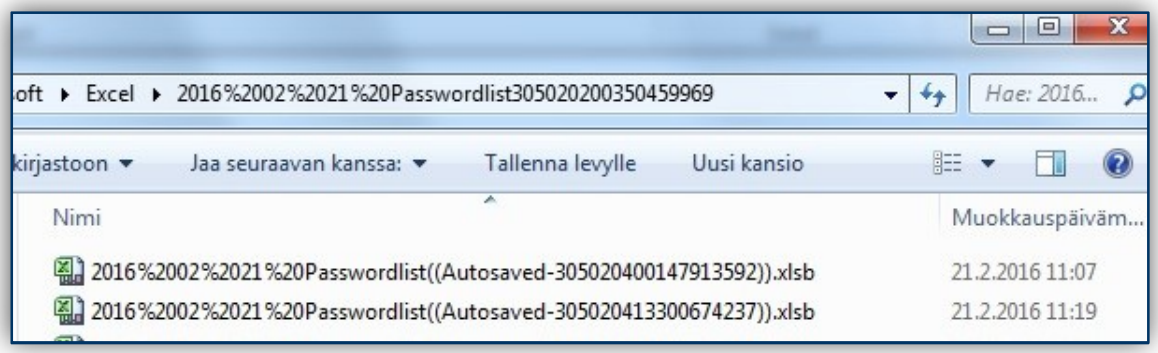
Microsoft on varoittanut käyttämästä Group Policy Preferences -nimistä hallintakonsolia salasanojen hallinnoimiseen. Hallintakonsoli on jo vuosia näyttänyt varoituksen salasanan tallentamisesta, koska se tallentuu palvelimen aktiivihakemistossa sijaitsevaan SYSVOL -hakemistoon, johon kaikilla toimialueen käyttäjillä on lukuoikeudet. Sittemmin Microsoft on julkaissut (13.3.2014) hotfix -päivityksen MS14-025, joka estää salasanojen konfiguroinnin Group Policy Preferences -laajennuksen avulla. (Microsoft 2017.)

Kaikilla Windows -työasemilla on sisäänrakennettu paikallisen järjestelmänvalvojan tili, ja järjestelmänvalvojan salasanan vaihtaminen on useissa organisaatioissa tietoturvallisuuden perusvaatimuksia. Yleinen käytäntö on ollut jakaa paikallisen järjestelmänvalvojan salasana ryhmäkäytännöillä (GP) suureen määrään työasemia, mutta riskinä toimintatavassa on se, että tällöin kaikissa työasemissa yli organisaatiorajojen on sama paikallisen järjestelmänvalvojan salasana käytössä. Jos kahdessa tai useammassa Windows -työasemassa on saman niminen paikallinen tili ja salasana, se avaa järjestelmänvalvojan tilin murtaneelle hyökkääjälle pääsyn kaikkiin työasemiin, joissa on samat paikallisen järjestelmänvalvojan tunnistetiedot. (Active Directory Security 2015) Microsoftin Baseline Security -hallinnon ohjeiden mukaisesti paikallisten tilien etäkäyttö Active Directory ympäristössä tulisi estää (Microsoft 2018, Microsoft 2014).

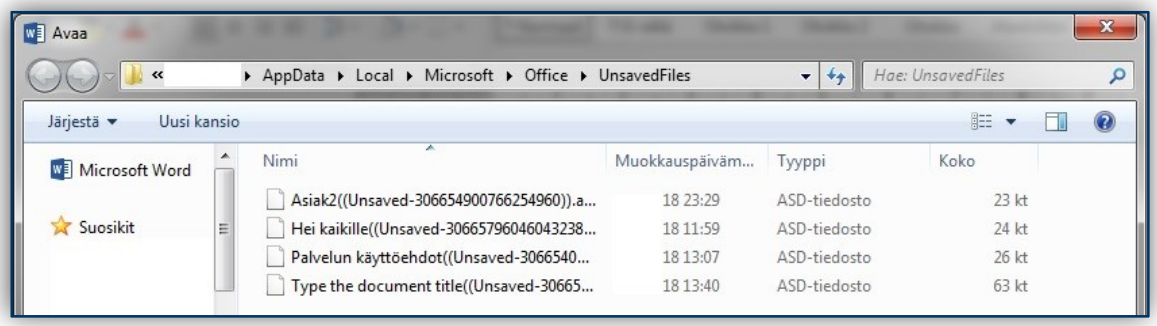
Oikeudeton päästy työasemien paikallisiin resursseihin (C$) mahdollistaa oikeudettoman pääsyn taas toisten käyttäjien paikallisiin käyttäjäprofiileihin tallentuneisiin tietoihin. Kuvioissa 4 – 7 on esimerkkejä käyttäjän paikallisessa profiilissa olevista kansioista, joihin MS Office -sovellukset (Word, Excel, PowerPoint) tallentavat automaattiseen tallennukseen sekä automaattiseen tiedoston palautukseen liittyvien toiminnallisuuksien kautta tiedostoja, joista saattaa löytyä paljon hyödyllistä tietoa hyökkääjälle, jolla on paikallisen järjestelmänvalvojan tunnukset käytössään.



Kuvio 4: Käyttäjän profiiliin tallentunutta tietoaineistoa (Word)



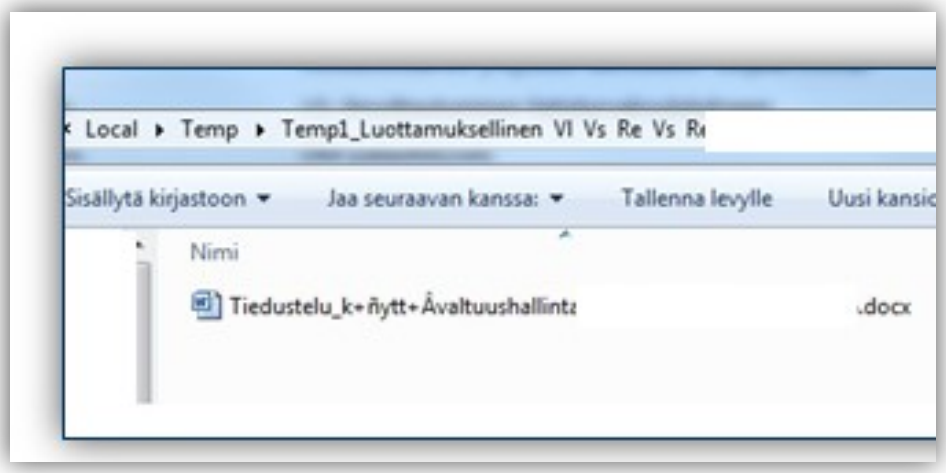
Kuvio 5: Käyttäjän profiiliin tallentunutta tietoaineistoa (Excel)



Kuvio 6: Käyttäjän profiiliin tallentunutta tietoaineistoa (Word palautus)

4.4.3 Turvaposti

Organisaation X hallinnonalan ohjeistuksessa ohjeistetaan salassa pidettävän aineiston tallentaminen henkilökohtaiseen kotihakemistoon ja virkasähköpostiin sähköisesti siten, että pääsy aineistoon on ainoastaan sen käyttöön oikeutetuilla henkilöillä (Oikeusministeriö 2014a). Salassa pidettävän tiedon turvalliseen siirtoon voidaan käyttää ulkopuolisen palveluntarjoajan käyttämiä ratkaisuja. Huolimatta siitä, että itse viesti tallennetaan suojatusta sähköpostijärjestelmästä omaan kotihakemistoon tai suojattuun sijaintiin, siitä voi tallentua kopio käyttäjän työaseman paikalliseen kansioon, kuten kuviossa 7 on tapahtunut.



Kuvio 7: Luottamuksellinen dokumentti tallentunut Turvapostista avatusta liitetiedostosta käyttäjäprofiilin väliaikaiseen kansioon.

Edellä kuvatut esimerkit voivat muodostaa riskin julkisuuslain hyvän tiedonhallintatavan mukaisen asiakirjojen suojaamisen ja tietoturvallisuusasetuksen tietojen luvattoman tai asiattoman käsittelyn vaatimusten suhteen, mutta työasemaympäristö tulisi nähdä myös tietojenkäsittely-ympäristönä, jossa käsitellään tietosuoja-asetuksen tarkoittamia henkilötietoja sekä

erityisesti arkaluonteisia, yksityiselämään kuuluvan henkilötietojen suojan ytimeen kuuluvia tietoja. Tällaisiksi katsotaan esimerkiksi organisaation X sähköisissä asiakirjoissa esiintyviä tietoja rikollisista teoista, rangaistuksista ja muista rikoksen seuraamuksista (Perustuslakivaliokunta 2013).

5 Tietoturvan hallintajärjestelmän rakentaminen

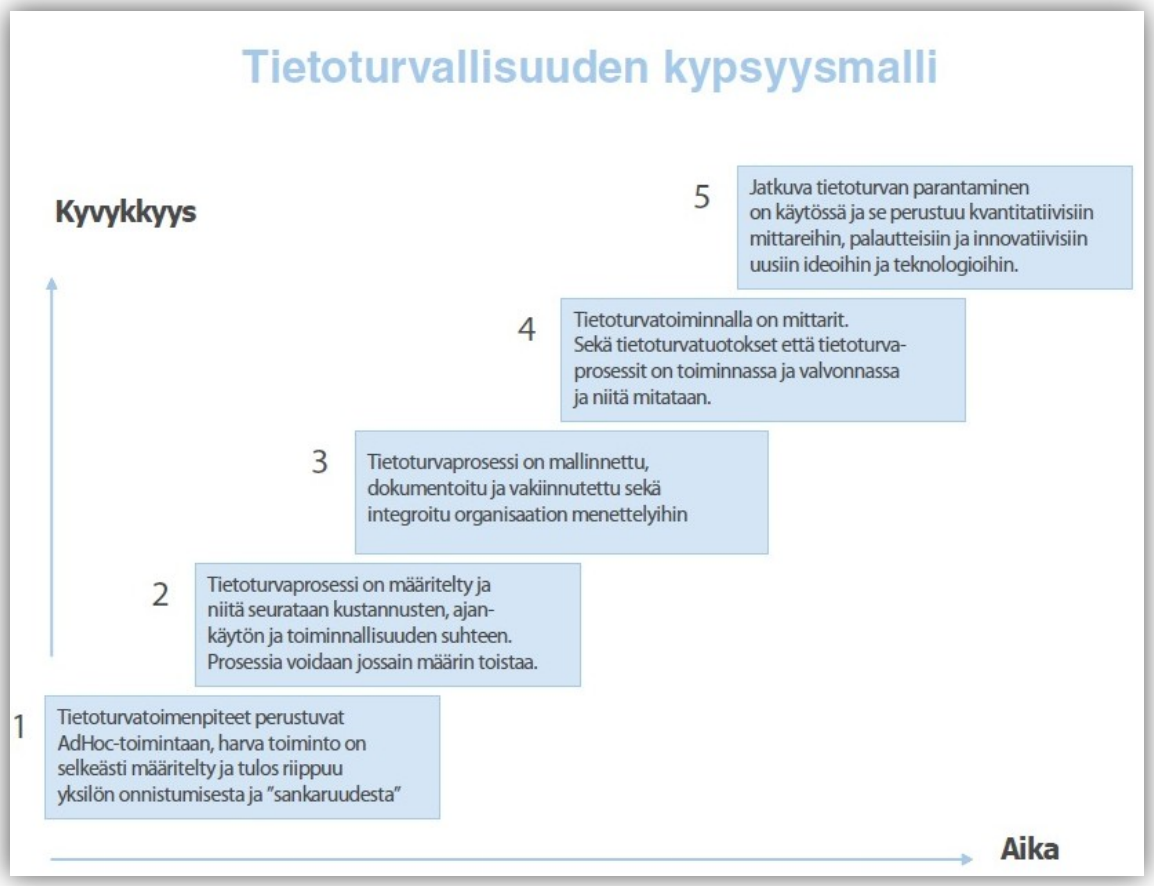
Tietoturvallisuuden hallintajärjestelmän perustus on organisaation toimintastrategiassa ja hallintajärjestelmä on luonteeltaan viitekehys. Se on organisaatiokohtainen, ja hallintajärjestelmän rakenne riippuu organisaation tietoturva-asioiden kehitysvaiheesta. (VAHTI 6/2006, 17.) Organisaation X tietoturvan hallintajärjestelmä toteutetaan tietoturva-asetukseen (TTA 681/2010) pohjautuvien tietoturvatasovaatimusten mukaan, sillä vahtiohjeistuksen (VAHTI 2/2010) mukaan ja näin toteutettuna se on yhteensopiva ISO/IEC27001 -standardin mukaisen hallintajärjestelmän kanssa (Vahti 3/2013, 24). Organisaation johto voi standardin mukaisella toiminnalla osoittaa sitoutuneisuutensa pitkäjännitteiseen tietoturvallisuuden kehittämiseen (VAHTI 6/2006, 17).

Organisaation tietoturvatyön päämääränä on sen omaan toiminaan kohdistuvien häiriöiden ja tietoturvariskien vähentäminen sekä toiminnan laadun varmistaminen. Tästä päämäärästä voidaan johtaa strategiseksi kehittämistavoitteeksi organisaation toimintaan liittyvän hyvän hallintotavan (corporate governance) vaatimuksen ja riskienhallinnan merkityksen korostaminen, joka osoitetaan sidosryhmille luomalla organisaation riskienhallintaa tukeva tietoturvallisuuden hallintajärjestelmä. Sen avulla varmistetaan organisaation kokonaisvaltainen riskien hallinta, laadunhallinta ja niihin liittyvien tavoitteiden toimeenpano. Se osoittaa organisaation toiminnallisen vastuun näkökulmasta, että organisaatiossa tehdään järjestelmällistä työtä tietoturvallisuuden kehittämiseksi (VAHTI 6/2006.)

Tietoturvan hallintajärjestelmän rakentamiselle ei ole estettä, jos riskienhallintaa ei vielä ole tarkasteltu organisaatiotasolla. Tietoturvan hallintajärjestelmän kehittäminen kestää useita vuosia, ja varsinaista tietoturvatyötä organisaatiossa voidaan johtaa samoilla keinoilla, kuin tulosohjauksessa. Tällöin kehittämiseen voidaan asettaa vuositavoitteita, ja tavoitteiden vaikutuksia mitataan ja arvioidaan laadullisten tai määrällisten näkökulmien avulla. (VAHTI 6/2006.)

Laadulliset näkökulmat liittyvät esimerkiksi arviointiin, onko tietoturvan kehittäminen osa viraston toimintaa, miten ja mistä näkökulmasta organisaation riskejä tunnistetaan ja onko tietoturvaa kehitetty lainsäädännön edellyttämien vaatimusten mukaisesti. Määrälliset näkökulmat liittyvät esimerkiksi suoritettuihin tietoturvakoulutuksiin, tietoturvallisuustyöhön käytettyihin työtunteihin tai henkilötyöpäiviin tai tietoturvakatselmointien lukumääriin kohteittain. (VAHTI 6/2006.)

Tietoturvallisuuden ja riskienhallinnan kehittäminen on jatkuvaa prosessia, jossa tietoturvan hallintajärjestelmän kypsyys kehittyy erilaisissa kehitysvaiheissa. Kun ensimmäisessä vaiheessa toiminta, ohjeistus ja vastuut ovat vielä hajanaisia, toisessa kehitysvaiheessa tietoturvaan liittyvässä hallinnassa on jo säännöllisyyttä. Toisessa vaiheessa organisaatiolla tulisi olla jo tietoturvapolitiikka, ja tietoturvallisuuden systemaattisen kehittämisen tuloksena tietoturvallisuuden kehittämissuunnitelma. Kolmannessa vaiheessa tietoturvaprosessit ja tavoitteet ovat yleensä jo määritelty ja organisaatiolla on kattava tietoturvaohjeisto. Tietoturvallisuuden kehityssuunnitelma on laadittu ja otettu käytäntöön ja tietoturvan hallintajärjestelmä on toteutunut. Neljännessä vaiheessa organisaation toiminta on tietoturvan hallintajärjestelmän mukaista ja toiminta seuraa tuloksellisuudelle ja kehittämistarpeille asetettuja mittareita. Neljännessä vaiheessa organisaatio voi jo viestiä, että tietoturvallisuuden johtamis – ja hallintajärjestelmä on jo olemassa. Viidennessä vaiheessa hallintajärjestelmä on optimoitunut organisaation oppimisen ja kokemuksen kautta ja organisaation toimintakulttuuriin on kytketty turvallisuusasiat osana organisaation toimintaa. (VAHTI 6/2006, 20.)



Kuvio 8: Tietoturvallisuuden kypsyysmalli (VAHTI 6/2006, 19).

5.1 Tietoturvallisuuden tason määrittely

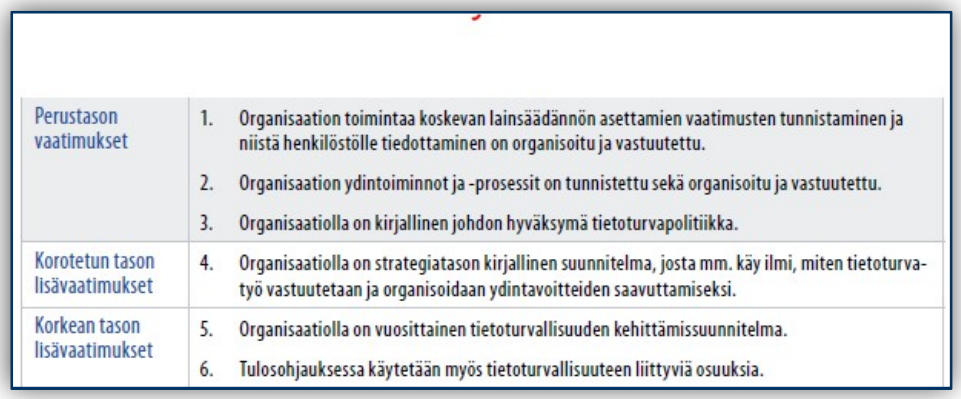
Organisaatiolle ja sen tietojenkäsittely-ympäristölle voidaan määritellä teknisiä ja hallinnollisia vaatimuksia tietoturvallisuustasojen avulla, joilla kuvataan valtionhallinnon organisaation tietoturvatoimintaan ja -prosesseihin liittyviä toteuttamisvelvollisuuden sisältämiä vaatimuksia (VAHTI 2/2010, 15). Tietoturvatasoja on kolme; perustaso, korotettu taso ja korkea taso, joista alimman eli tietoturvallisuuden perustason tulisi jokaisen valtionhallinnon viraston täyttää salassa pidettävien asiakirjojen käsittelyn osalta. Korotetun tietoturvallisuustason vaatimuksia noudatetaan lähtökohtaisesti valtionhallinnon viranomaisen toiminnassa silloin, kun asiakirjat ovat yhteiskunnan elintärkeiden toimintojen kannalta kriittisiä. (VAHTI 3/2012, 28.)

Yhteiskunnan elintärkeitä toimintoja ovat ”Valtion johtaminen, kansainvälinen toiminta, valtakunnan sotilaallinen puolustaminen, sisäisen turvallisuuden ylläpitäminen, talouden ja infrastruktuurin toimivuus, väestön toimeentuloturva ja toimintakyky ja henkinen kriisinkestävyys” (Puolustusministeriö 2006, 4).

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen arvioinnista annetun lain (1406/2011) ja tietoturvallisuuden arviointilaitoksista annetun lain (1405/2011) perusteella tietoturvallisuusasetuksen 5§ tietoturvatasovaatimukset soveltuvat arvioinnin perustaksi, jos organisaatiossa käsitellään julkisuuslakiin perustuvaa salassa pidettävää tietoa (Vahti 2/2010, 27).

Tietoturvatasoa määriteltäessä on syytä huomata, että viranomaisen on tietoturva-asetuksen 23§ mukaan saatettava tietojenkäsittely vastaamaan 5 § perustason vaatimuksia. Korotetun ja korkean tason vaatimukset liittyvät asiakirjojen suojaamista koskeviin vaatimuksiin ja kohdistuvat siis yhteiskunnan kannalta elintärkeisiin tietojenkäsittely-ympäristöihin, mutta viime kädessä arvioinnin kohteen omistaja päättää riittävästä tasosta ja sen saavuttamisesta sekä hyväksyy jäännösriskit yksittäisten toteutumatta jääneiden tietoturvavaatimuksen kohdalla. (VAHTI 2/2014, 29)

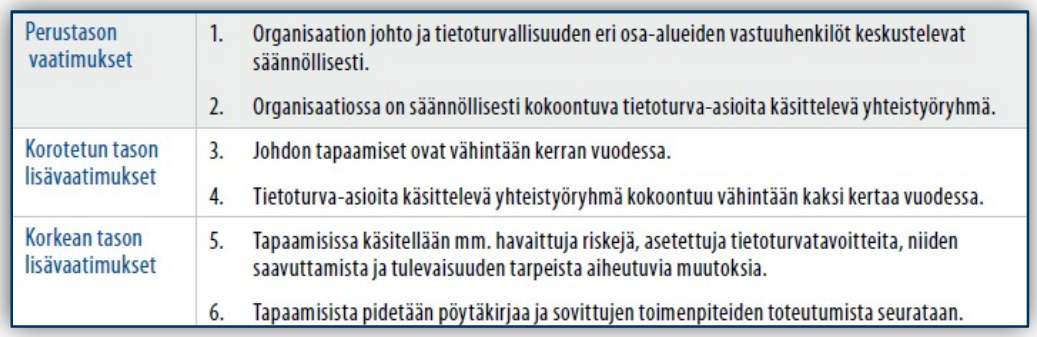
Toisaalta, organisaatiossa voidaan myös yksittäisen tietoturvallisuustason osa-alueen kohdalla soveltaa korotetun tai korkean tason vaatimuksia. Esimerkiksi kuviossa 9 esitytetyt strategisen ohjauksen osa-alueen korotetun tason vaatimukset *”Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi”* ja korkean tason vaatimus *”Organisaatiolla on vuosittainen tietoturvallisuuden kehittämisohjelma”* voivat sidosryhmien näkökulmasta tuoda lisää uskottavuutta organisaation tietoturvan hallintaan.



Perustason vaatimukset	1.	Organisaation toimintaa koskevan lainsäädännön asettamien vaatimusten tunnistaminen ja niistä henkilöstölle tiedottaminen on organisoitu ja vastuutettu.
	2.	Organisaation ydintoiminnot ja -prosessit on tunnistettu sekä organisoitu ja vastuutettu.
	3.	Organisaatiolla on kirjallinen johdon hyväksymä tietoturvapolitiikka.
Korotetun tason lisävaatimukset	4.	Organisaatiolla on strategiatason kirjallinen suunnitelma, josta mm. käy ilmi, miten tietoturvatyö vastuutetaan ja organisoidaan ydintavoitteiden saavuttamiseksi.
Korkean tason lisävaatimukset	5.	Organisaatiolla on vuosittainen tietoturvallisuuden kehittämissuunnitelma.
	6.	Tulosohjauksessa käytetään myös tietoturvallisuuteen liittyviä osuuksia.

Kuvio 9: VAHTI 2/2010 Liite 5; 1.1.1 strateginen ohjaus

Osa-alueen ”Yhteistyön koordinointi” johdon ja tietoturvan vastuuhenkilöiden kommunikointiin liittyvät korotetun ja korkean tason vaatimukset eivät aiheuttane kohtuutonta lisätyömäärää organisaatiossa (Kuvio 10 alla).



Perustason vaatimukset	1.	Organisaation johto ja tietoturvallisuuden eri osa-alueiden vastuuhenkilöt keskustelevat säännöllisesti.
	2.	Organisaatiossa on säännöllisesti kokoontuva tietoturva-asioita käsittelevä yhteistyöryhmä.
Korotetun tason lisävaatimukset	3.	Johdon tapaamiset ovat vähintään kerran vuodessa.
	4.	Tietoturva-asioita käsittelevä yhteistyöryhmä kokoontuu vähintään kaksi kertaa vuodessa.
Korkean tason lisävaatimukset	5.	Tapaamisissa käsitellään mm. havaittuja riskejä, asetettuja tietoturvatavoitteita, niiden saavuttamista ja tulevaisuuden tarpeista aiheutuvia muutoksia.
	6.	Tapaamisista pidetään pöytäkirjaa ja sovittujen toimenpiteiden toteutumista seurataan.

Kuvio 10: VAHTI 2/2010 Liite 5; 1.1.3 Yhteistyön koordinointi

Tietoturvallisuuden hallintajärjestelmän ja yksittäisten suojattavien kohteiden kehittämisen osana, organisaation tulisi etukäteen tarkkaan rajata ja selvittää, miten sen kannattaa toteuttaa perus – ja korotetun tietoturvatason tekniset ympäristöt, jotta ne vastaisivat tietoturvatasojen vaatimuksia (VAHTI 3/2012, 12).

Suojattavat kohteet muodostavat sen kokonaisuuden, joka organisaatiossa luokitellaan jollekin tietoturvatasolle tietoturvallisuusasetuksen ja VAHTI 2/2010 -ohjeistuksen mukaan. Yksittäiset suojattavat kohteet voivat olla esimerkiksi jokin fyysinen tila, tietojärjestelmä, työasema tai asiakirja, jolla on organisaation toiminnan kannalta merkitystä (VAHTI 3/2012, 15).

Toisaalta organisaation ydintoiminta ja sisäiset toimintaprosessit voivat olla sellaisia, että koko toimintaympäristön voidaan katsoa olevan suojaustasoltaan samankaltaista ympäristöä.

Organisaation X tietoturvataso voidaan toteuttaa perustason mukaisesti valtionvarainministeriön 19.10.2010 julkaiseman ohjeen ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta” perusteella. Ohjeiden mukaisella toiminnalla organisaation on ollut mahdollista saavuttaa toiminnassaan ja yhteistyössään 1.10.2010 voimaan tulleen tietoturva-asetuksen mukainen tietoturvallisuuden perustaso (Vahti 2/2010, 5).

Vahti 2/2010 -ohjeen viidennen liitteen tietoturvallisuustasojen yksityiskohtaiset vaatimukset ovat selkeät ja sovellettavissa olevat arviointiohjeet organisaatiolle, jonka tietojenkäsittelyympäristölle riittää perusvaatimuksena pidettävä tietoturvallisuuden perustaso. Liitteen tietoturvatasojen vaatimukset ovat selkeästi ja ymmärrettävästi esitetty muodossa, jossa vaatimuksia voi siis käyttää sellaisenaan apuvälineenä tietoturvan hallintajärjestelmää luotaessa. Vaatimuksia voi soveltaa ylemmältä tasolta, jos toiminnan katsotaan tietyin osin käsittävän yhteiskunnan elintärkeiden toimintojen kannalta kriittisiä viranomaisen asiakirjoja (Vahti 2/2010, 44).

5.2 Tietoturvan hallintajärjestelmän tekninen toteutus

Erilaisia kaupallisia sovelluksia tai selainpohjaisia palvelualustoja tietoturvan ja riskien arviointiin on markkinoilla, joista muutamaa olen päässyt kokeilemaan itsekin. Näen ongelmana kokeilemissani palveluissa sen, että osassa niistä on vielä teknisesti hankalasti ymmärrettäviä rakenteita ja joidenkin sähköisten alustojen käytettävyys on vaikeaa. Standardien ja eri viitekehysten tarkoitus on tarjota malli tietoturvan hallintaan ja hallintajärjestelmän rakentamiseen (Vahti 7/2003, 23), mutta standardit ja viitekehykset ovat kokonaisuutena tulkinnallisesti vaikeita. Kaupallisen tietoturvan arviointiin tarkoitettujen sovelluksen käyttölogiikka saattaa olla sidottu olemassa olevien standardien ja viitekehysten (VAHTI, Katakri) mukaisiksi rakenteisiksi malleiksi, joten käyttäjä ei välttämättä pysty jättämään pois sellaisia hallintakeinoja, joihin organisaatio ei voi vaikuttaa.

Yksi merkittävä ongelma kaupallisissa palvelualustoissa on toisaalta sekin, että organisaatio ei välttämättä halua palvelun kautta avata kriittisimpiä tietoturva-ongelmiaan ulkopuolisen osapuolen luettavaksi. Yhdessä kokeillussa tietoturvan hallintaan tarkoitetussa Saas – palvelussa palvelutuottajalla oli pääsy asiakkaan tuotantoympäristöön, joka lienee yleistä ja on palvelun kehittämisen näkökulmasta normaali käytäntö, mutta asettaa asiakasorganisaatiolle haasteita palveluun tuottamansa ja jakamansa luottamuksellisen tiedon suhteen. Ohjelmistoresurssipalvelumalli, eli Software as a Service (SaaS) on palveluna yksinkertainen ottaa käyttöön, mutta palvelun tekniseen tietoturvaan ja toteutukseen on loppukäyttäjäpuolella vähän vaikutusmahdollisuuksia (Viestintävirasto 2018b, 5). Käyttäjän on voi olla vaikea ilman erillisiä sa-

lassapitosopimuksia varmistua siitä, ettei palveluntarjoajan henkilökunta, joilla ei ole oikeutta päästä asiakkaan luottamukselliseen tai arkaluonteiseen tietoon, pääse sellaiseen käsiksi (Viestintävirasto 2018b, 7).

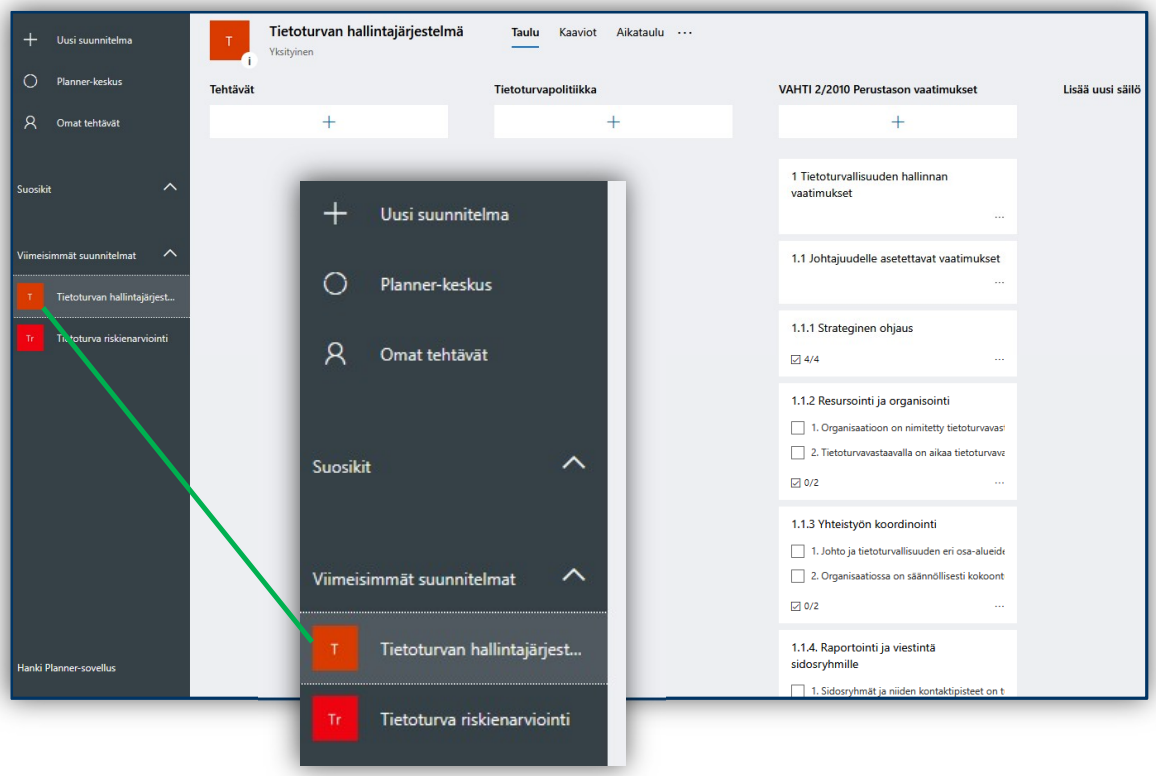
Office 365 – ympäristössä toimiva Ms Planner -sovellus on ketteriin projekteihin tarkoitettu työkalu, joka on todella helppokäyttöinen, graafisesti miellyttävän visuaalinen ja yksinkertainen käyttölogiikaltaan (Inmics Oy 2018). Ms Planner -sovelluksen avulla rakennettu tietoturvan hallintajärjestelmä eroaa nykyisistä kaupallisista toteutuksista käyttäjälähtöisyytensä ja muokattavuutensa takia. Ympäristö on toteutettu projektinhallinnan muotoon ja on siten muunneltavissa ja muokattavissa projektin etenemisen mukaan. Tietoturvan kehittäminen on jatkuvaa projektinomaista prosessointia, joten Planner -ympäristössä organisaatio pystyy kehittämään tietoturvaansa toimintaympäristöönsä kohdistuvien VAHTI -ohjeistuksen ja vaatimusten muutosten edellyttämällä tavalla ja aikataululla itsenäisesti, huomioiden esimerkiksi tulevan tiedonhallintalain aiheuttamat muutokset tietoturvan hallintaan ja VAHTI -ohjeistukseen.

Tammikuussa 2018 pidetyssä tietoturvallisuuden standardisointiverkoston kokouksessa Kimmo Rousku totesi, että tietoturvallisuusasetus tulee korvautumaan tietohallintolain myötä, ja tietoturvallisuustasot tulee korvaamaan tietoturvallisuuden vähimmäistaso. Muutoksen myötä VAHTI – ryhmässä tullaan kehittämään täysin uusi vaatimuskehikko, VAHTI 100, joka tulee sisältämään organisaatioon, tietojärjestelmiin ja hankintoihin kohdistuvia vaatimuksia sekä auditointikriteerit, jotka mahdollistavat auditoinnin ja tarkastuksen. (Rousku 2018, 23.)

Tällaiset suuret muutokset vaatimuskehikkoon olisi hankalampi toteuttaa nopealla aikataululla ulkopuolisen palveluntarjoajan palvelussa, kun taas nyt luodussa Planner -ympäristössä muutokset voidaan toteuttaa heti organisaation omasta toimesta. Perinteinen ohjelmistokehityksen projektimalli on ”vesiputousmalli”, joka reagoi huonosti muutoksiin, kun taas Plannerin edustama ketterä projektimalli mahdollistaa vaikka kesken projektin tapahtuvat nopeat muutokset. (Inmics Oy 2018.)

Suojattavia kohteita määriteltäessä Ms Planner mahdollistaa jokaisen yksittäisen suojattavan kohteen kohdalla vastuuhenkilön nimeämisen, organisaation X toimintaympäristössä jopa omien organisaatiorajojen ulkopuolelta, joten hallintajärjestelmän ylläpitäjä voi esimerkiksi riskienhallintakeinon kohdalla siirtää riskin hallintatoimenpiteet arvivoitavaksi toiseen asiantuntijaorganisaatioon tai palveluntarjoajalle.

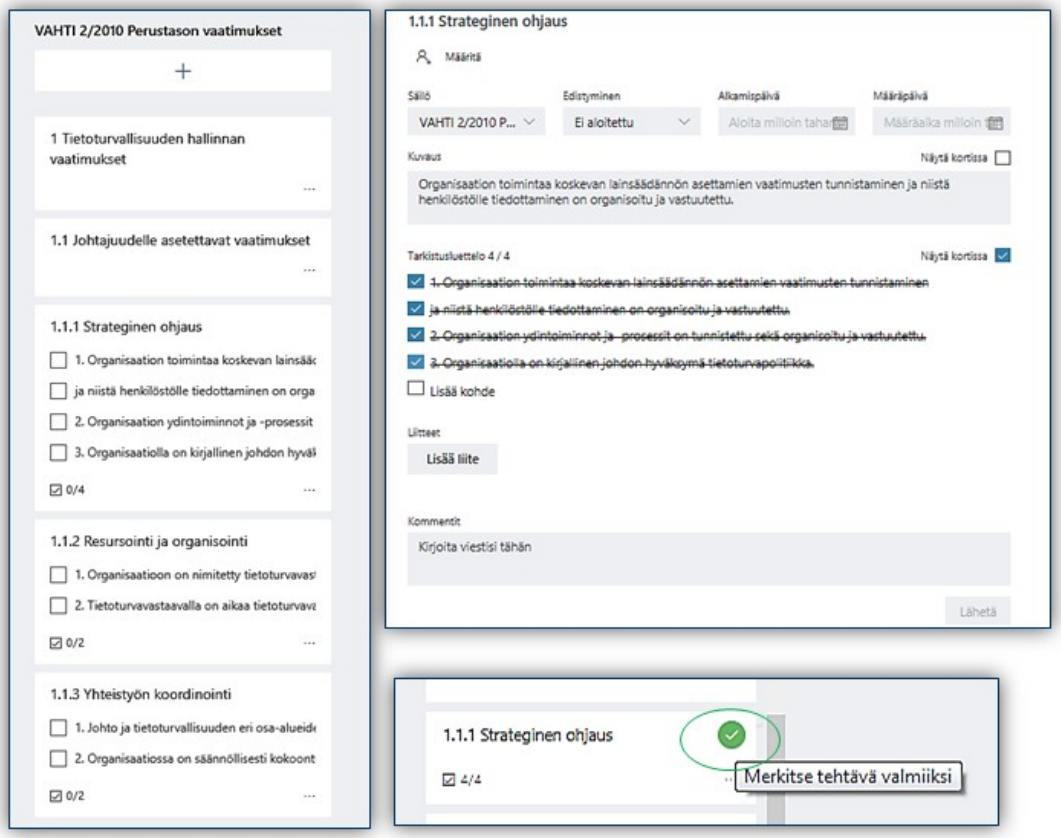
Tietoturvan hallintajärjestelmä voidaan muodostaa yksittäisenä suunnitelmana, johon perustettaviin kehitysjonoihin (säilöihin) voidaan määritellä ”työjonoiksi” tietoturvaan liittyviä kokonaisuuksia, esimerkiksi yhteen työjonoon VAHTI 2/2010 perustason vaatimukset, toiseen jonoon tietoturvapolitiikka (Kuvio 11).



Kuvio 11: Planner -keskuksen aloitusnäkymä

Eri osa-alueiden vaatimukset voidaan jaotella uusina ”tehtävinä” ja vaatimuksiin liittyvät kontrollit saa helposti lisättyä ”tarkistusluetteloina” listaksi. Tarkistusluettelosta voidaan hyväksyä kontrollit toteutuneeksi laittamalla oikein-merkki kontrollin kohdalla olevaan ruutuun (Kuvio 12).

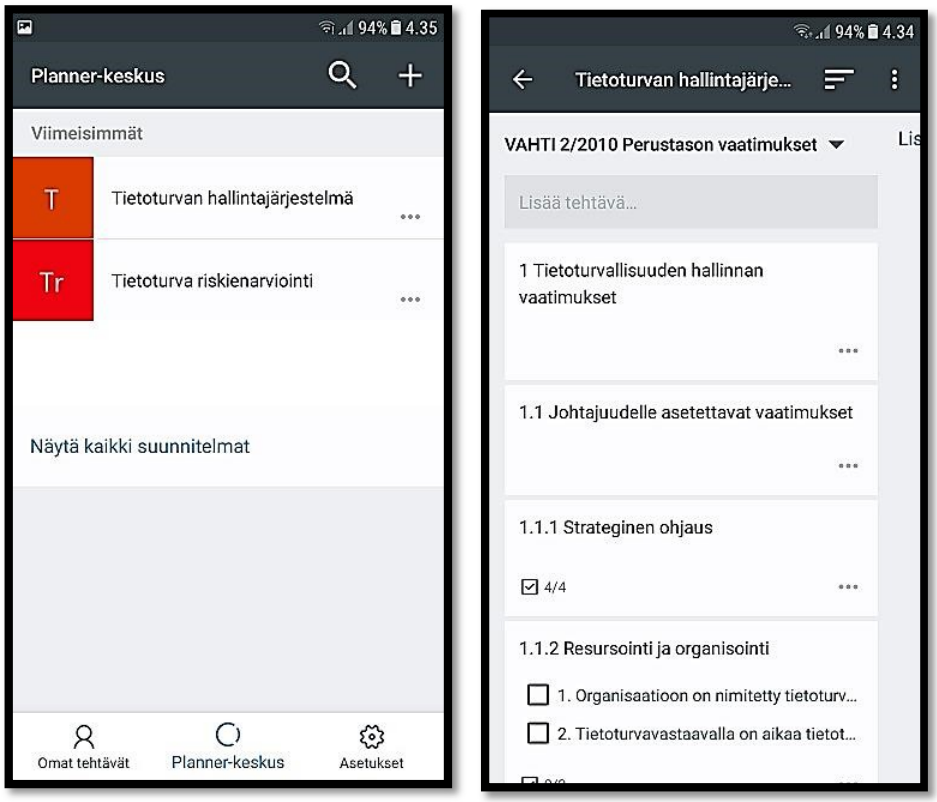
Osa-alueen voi myös vastuuttaa tai nimetä tietylle henkilölle, jolloin tietoturvan hallinnasta voi parhaimmillaan saada työyhteisöä sitouttavan projektin. Ympäristö toimii myös ”digitaalisena seinänä”, joka mahdollistaa esimerkiksi maantieteellisesti hajautuneet tiimit sekä etätyöskentelyn. Tehtävän voi aikatauluttaa, ja kun osa-alue katsotaan olevan kunnossa, se voidaan merkitä valmistuneeksi (Kuvio 12).



Kuvio 12: Planner tehtävänäkymä

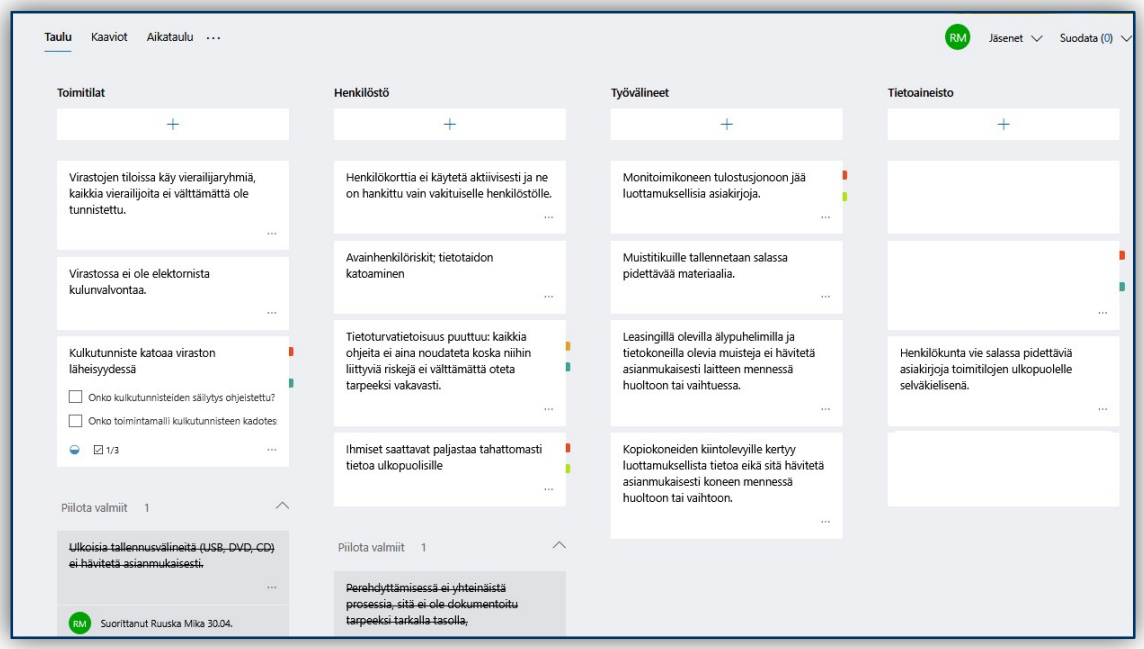
Planner – sovellus on helppo asentaa omalle mobiililaitteelle (esimerkkinä Android), jolloin tietoturvan hallintajärjestelmän katselmointi on helppoa ja organisaation johto voi koska tahansa tarkistaa omalta laitteeltaan tietoturvan tilannekuvan, tai lisätä omia huomioitaan ajasta tai paikasta riippumatta.

Kuvio 13: Android -puhelimen näkymä



5.3 Riskienarvioinnin integroiminen

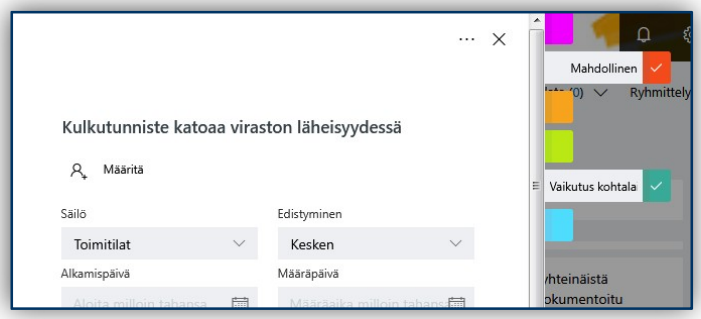
Riskienarvioinnin voi myös rakentaa Ms Planner -sovelluksella. Kuvion 14 näkymään on jaoteltu vahinkoriskejä, kukin omaan säilöönsä. Planneriin voi perustaa oman ”suunnitelman” jokaiselle riskiluokalle; strategiset, operatiiviset, taloudelliset ja vahinkoriskit, näin näkymä ja jaottelu pysyvät selkeänä ja riskien seuranta sekä katselmointi on helpompaa.



Kuvio 14: Riskienhallintanäkymä, esimerkki yleislaatuisista riskeistä.

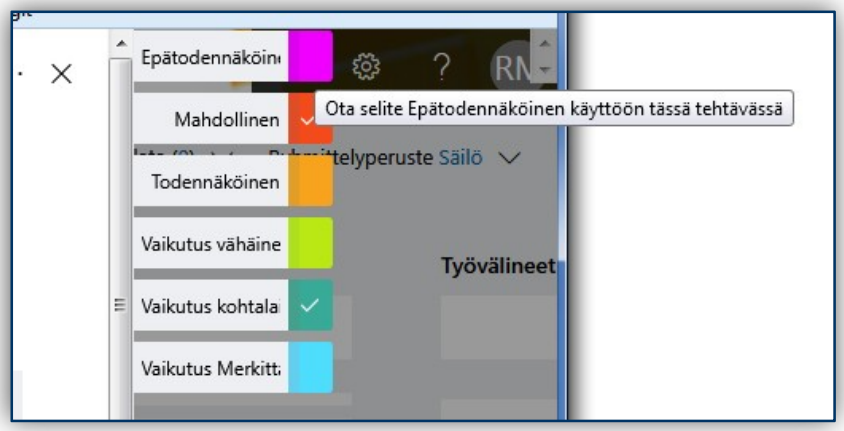
Kuvioissa 15 ja 16 riskin vaikutuksia arvioidaan yleisestä käytetyllä 3 -portaisella asteikolla, jossa riskit arvioidaan luonteeltaan epätodennäköiseksi, mahdolliseksi ja todennäköiseksi sekä vaikutuksiltaan vähäiseksi, kohtalaiseksi tai merkittäväksi. Planner -ympäristön rajoittava tekijä riskienarviointiin liittyen on se, että selitteiden määrä rajoittuu toistaiseksi kuuteen.

Siten esimerkiksi valtiovarainministeriön riskienhallinnan ohjeen (Rousku 2017, 24 - 25) mukaista neliportaista asteikkoa riskikohtaisten todennäköisyyksien ja vaikutusten arvioinnille ei voida käyttää. Toisaalta ohjeessa todetaan riskianalyysin kohdalla (2017, 24), että riskien käsittelyyn vaikuttavat todennäköisyyksien ja vaikutusten arviot ovat subjektiivisia näkemyksiä, jolloin yhteisen käsityksen muodostaminen riskien tasosta voi olla vaikeaa.



Kuvio 15: Riskin todennäköisyyden ja vaikutusten arviointi

Kuvioissa 15 ja 16 esimerkkeinä olevia selitteitä voi muokata haluamakseen. Kuvion 16 riskien selitteet riskin seurausten vakavuudesta voisivat olla myös vähäinen, merkittävä ja huomattava.



Kuvio 16: 3 X 3 riskimatriisin asteikot

Petri Lundahl toteaa Aaltoyliopistossa tekemässään tutkimuksessaan, että todennäköisyyden arviointi tehdään akateemisten tutkimusten ja käytännön perusteella epävarmoista lähtökohdista. Riskin todennäköisyyden arvioimisen toistaminen on vaikeaa, vaikka sillä on vaikutusta toimenpiteiden valintaan. Lundahlin mukaan riskiympäristön muutokset ovat vieneet organisaatioiden riskienhallintaa abstraktimpaan suuntaan ja itse riskienhallinta on aiemmasta asiantuntijatyöstä poiketen yhä enemmän linjaorganisaation työtä (Lundahl 2011, 2.)

Organisaation X toimintaympäristössä linjaorganisaation työnä suoritettava riskienhallinta on ongelmallista, koska riskienhallinta ja siihen liittyvät riskien käsittelykeinot ovat rajallisia. Etenkin virastotasolla organisaatio ei välttämättä voi määritellä tai muuttaa itse strategisia tavoitteitaan tai luopua tehtävistä, jotka ovat laissa säädetyt. Virasto ei voi vakuuttaa omaisuuttaan, jota se hallitsee. Edellä mainituista syistä riskienhallinta on valtionhallinnossa hajaantunut organisaatiokohtaisiksi vastuiksi ja toiminnoiksi, joihin virasto ei voi omalla päätöksellään vaikuttaa. (Valtiontalouden tarkastusvirasto, 2017b, 13.)

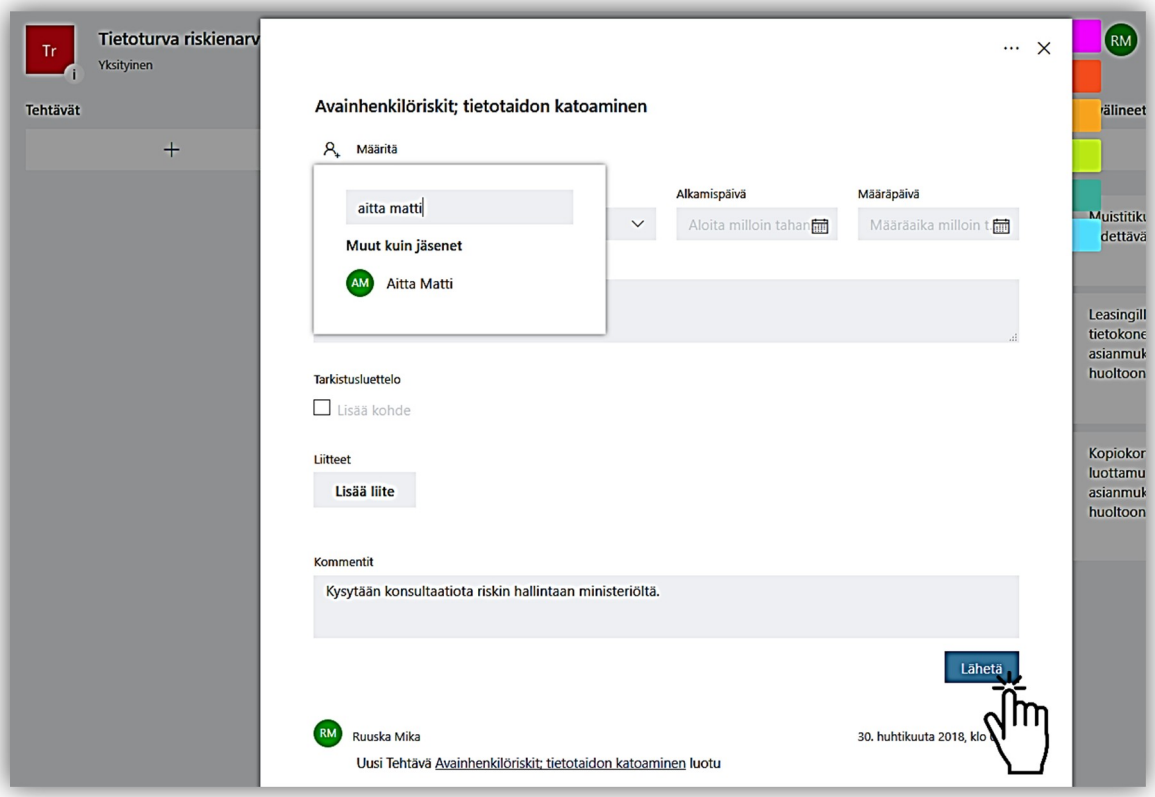
Riskienhallintaan liittyvä vastuutus ja päätökset valtionhallinnossa ovat osittain muodostuneet epäselväksi, koska riskit voivat jakautua eri organisaatioihin hallinnonalalla ja esimerkiksi tietojärjestelmä voi olla hajautettu usealle toimijalle ja sen kehittäminen sekä siihen liittyvät käyttöpalvelut on ulkoistettu. (Valtiontalouden tarkastusvirasto, 2017b, 13.)

Kimmo Rouskun mukaan epävarmuuksien vaikutusta toimintaan on mahdotonta hallita täydellisesti ja keskeistä onkin saada määriteltyä tarvittavat hallintatoimenpiteet arvioinnin kautta

löydetyille merkittävimmille riskeille. Toinen tärkeä asia on toteuttaa sovitut hallintatoimenpiteet ja varmistaa toimenpiteiden eteneminen. (Rousku 2017, 17.) Nämä voisivat olla ydinajatuksena organisaation X riskienhallintaan, myös edellä mainituista valtionhallinnon riskienhallintaan liittyvistä epävarmuustekijöistä johtuen.

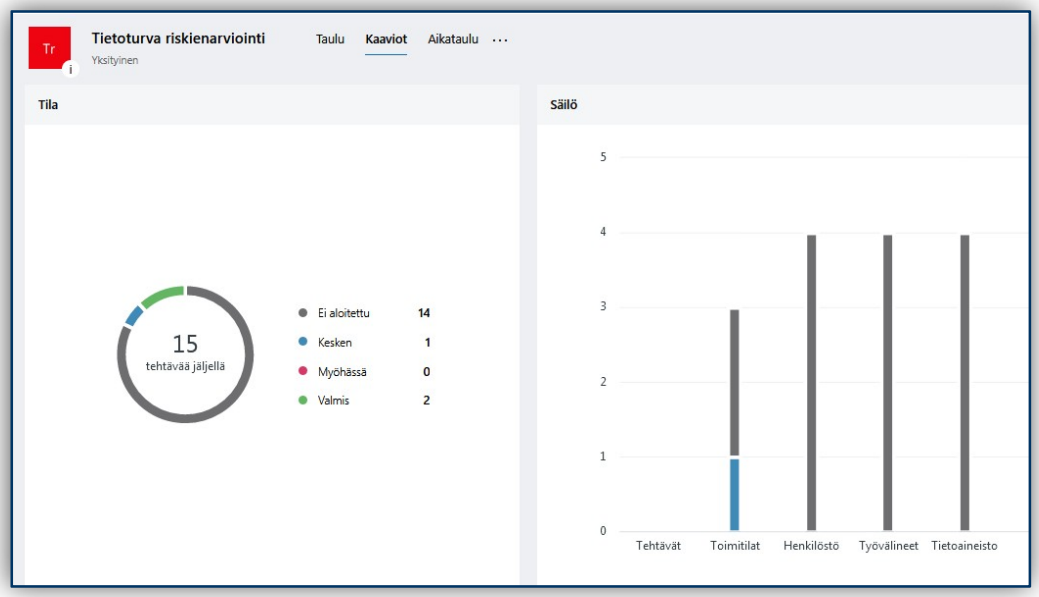
Tärkeää on myös ymmärtää organisaation X toimintaympäristön määrittelyn kautta keskeisimmät riskit, millaiset riskit kannattaa riskianalyysiin sisällyttää mukaan ja mitä riskejä voidaan jättää riskienarvioinnin ulkopuolelle. Tämä määrittelytyö ja sen perusteella tehtävät rajaukset riskien arviointiin on keskeinen asia organisaation X riskien arviointiprosessin kannalta. (Valtiovarainministeriö 2017c, 29.)

Planner -ympäristössä riskin hallintatoimenpiteet voidaan esimerkiksi organisaation X toimintaympäristössä vastuuttaa organisaatiorajojen yli (Kuvio 17), koska Valtorin Active Directory hakemisto käsittää lähes kaikki valtionhallinnon virastot. Tehtävien muodossa olevia riskejä voi lähettää esimerkiksi kommentointia varten toisen viraston asiantuntijalle.



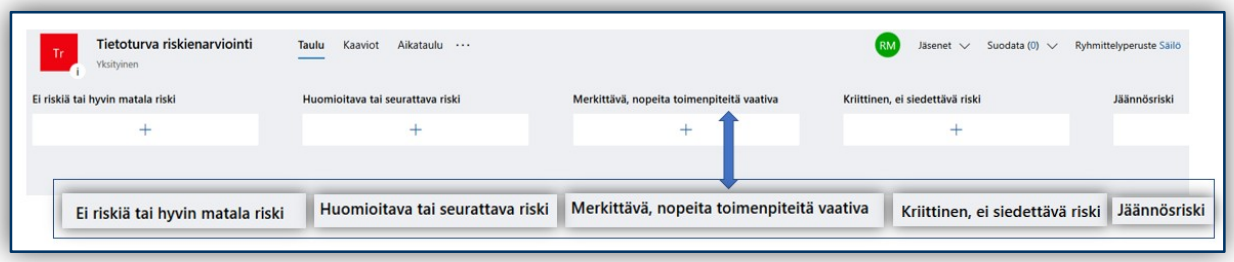
Kuvio 17: Riskin hallintatoimenpiteiden siirtäminen organisaatiorajan yli, esim. konsultaatiota varten.

Planner -sovelluksessa on raportointia varten tehtävien tilasta kertova koontinäkymä. Näkymä on yksinkertainen, mutta kun tietoturvan hallintajärjestelmään saadaan kehitystyön aikana kattavasti tehtäviä, koontinäkymä tarjoaa järkevän näkymän seurantaa varten. Tehtäviin kannattaakin laittaa tilamerkintä (Aloittamatta, Työn Alla, Valmis), aikatauluttaa tehtävät sekä nimitä niille vastuuhenkilöt. Kun tehtäville asetetaan jakson loppupäivä määräpäiväksi, raportissa näkyy myöhässä olevat tehtävät. (Inmics Oy 2018.)

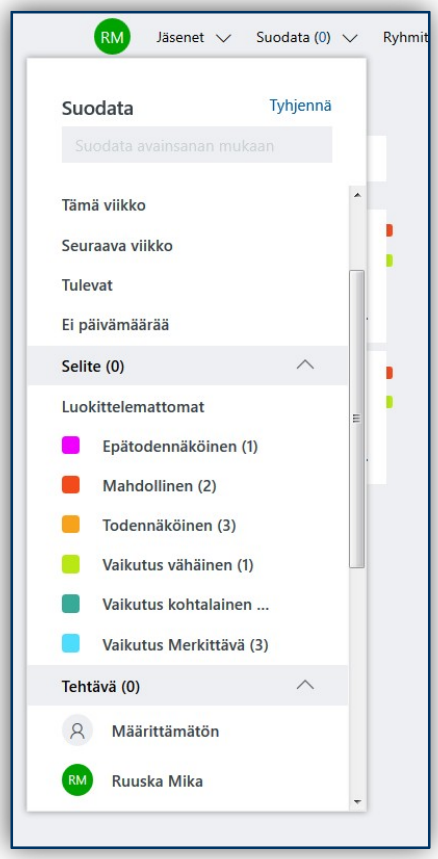


Kuvio 18: Plannerin koontinäkymä.

Riskienhallinnan suhteen Planner ei kokonaisuutena yllä vielä joidenkin kaupallisten riskienhallintasovellusten tasolle, koska se ei mahdollista automaattisesti riskien merkitysten arviointia laskemalla esimerkiksi neliportaisella asteikolla riskien suuruusluokkaa (R=T x V), mutta pienen organisaation riskienhallinnan läpiviemiseksi merkityksen arvioinnin voi suorittaa nimeämällä uudet säilöt riskin merkityksen mukaan: Kriittinen, merkittävä, huomioitava, ei riskiä, jäännösriski (Kuvio 19). Tällöin Plannerissa olevalla suodattimella voi suodattaa näkyville esimerkiksi vain kriittiset riskit. Olennaistahan riskien käsittelyn kannalta on priorisoida riskit päätöksentekoa varten ja erottaa joukosta ainakin välittömiä tai nopeita toimenpiteitä vaativat riskit sekä jäännösriskiksi hyväksytyt riskit.

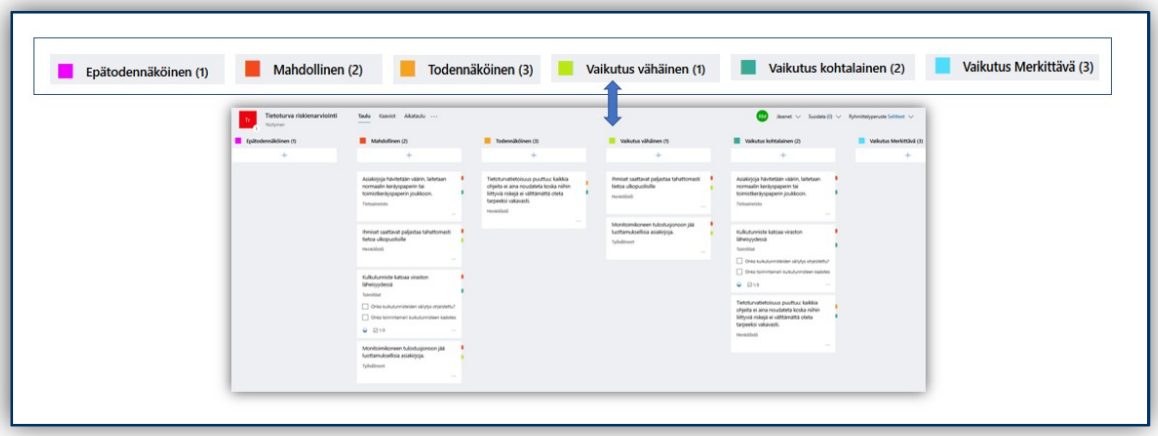


Kuvio 19: Planner säilöt riskien luokittelua varten.



Kuvio 20: Suodattaminen selitteiden perusteella.

Plannerissa saa myös suodattamalla selitelajin mukaan näkymän riskin todennäköisyyden tai vaikutuksen perusteella.



Kuvio 21. Riskit lajiteltuina todennäköisyyden tai vaikutuksen mukaan eri tehtäväjonoihin.

6 Pohdinta ja päätelmät

Opinnäytetyössä tietoturvan kehittämistä tarkasteltiin tutkimus – ja kehittämisprojektin näkökulmasta. Tutkimisprojektin tavoitteena oli löytää sovelluskelpoista tietoa ja uutta tietoa erityisen epävarmoilla alueilla ilman ennakkotietoa siitä, saadaanko tutkimuksen perusteella hyötyä tai tuloksia. Tutkimusprojektin näkökulmasta löysin paljon sovelluskelpoista tietoa organisaation X käytettäväksi tietoturvan kehittämistyötä varten. Uutena tietona opinnäytetyö tuo esille Office 365 -ympäristössä olevan Ms Planner -sovelluksen ja sen käyttömahdollisuuden tietoturvan projektinomaiseen hallintaan. Planner -työkalun kohdalla olen vahvasti toiveikas sen soveltuvuudesta organisaation X tietoturvan hallintaan, mutta käyttökelpoisuuden varmistaminen vaatii vielä käyttöönottoprosessin ja pilotoinnin, kun Valtorin pilvipalvelut tulevat hallinnonalalle tuotantokäyttöön.

Tietoturvallisuuden tutkiminen oli erittäin haastavaa siinä laajuudessa, joka opinnäytetyössä saavutettiin. Alkutilanteessa oli tarkoitus keskittyä enimmäkseen hallinnolliseen tietoturvaan ja tietoturvan hallintajärjestelmän rakentamiseen liittyviin vaatimuksiin ja ohjeisiin. Opinnäytetyöprosessin aikana aloin kuitenkin laajentamaan aihepiiriä ja lähestymistapaa, koska oli selvää, että minun oli saatava työhöni myös johtamisen toimintaympäristössä esiintyviä elementtejä sisällytettyä mukaan.

Tutkimuksen aihepiirin laajentamisella halusin ymmärtää itse, miltä tietoturvan johtaminen näyttäytyy johdon näkökulmasta ja minkälaisilla valtionhallinnon ohjausmekanismeilla voi olla vaikutusta tietoturvan hallintaan organisaatiotasolla. Tähän kannusti myös valitsemani kvalitatiivinen tutkimusnäkökulma ja siihen liittyvä havaintojen tulkinta sekä tulkintojen muodostama yleisempi merkitys tietoturvan näkökulmasta.

Aiempi taustani tietotekniikan ja tietoturvan puolella on puhtaasti teknisellä tasolla ja kokemukseni pohjautuu kunnallishallinnon ohjausmalleihin, joten tätä taustaa vasten sain mielestäni hyvin selvitettyä, miten ohjaussuhteet ja vastuut valtionhallinnossa voivat vaikuttaa organisaation X tietoturvan hallintaan ja kehittämistyöhön. Organisaatio X on kirjanpitoyksikön tulosohjauksessa oleva virasto, jonka olemassa olevat johtamis – ja hallintarakenteet toimivat valtionhallinnon tulosohjausajattelun mukaisesti, joten organisaation X tietoturvan kehittämistyötä voidaan edistää sisällyttämällä tulosohjauksen keinoja siten, kun organisaation koko ja toimintapäämäärät huomioiden on järkevää.

Tärkein toimenpide kehittämistyöhön liittyen olisi lisätä tulossopimukseen organisaation X toiminnalliseksi tavoitteeksi tietoturvallisuus (VAHTI 1/2004, 37). Tulosohjausajattelun mukainen tietoturvatyön kehittäminen organisaation X kohdalla tarkoittaa sitä, että tietoturvatavoitteiden asettaminen voi liittyä suoraan tietoturvatoimintoihin, esimerkiksi tietoturvakoulutukseen osallistuneiden määrä. Tavoitteet voidaan johtaa myös muista organisaation tavoitteista, kuten jo toteutuneet asioiden sähköisen käsittelyn kehittäminen, sähköisten aineistojen valmistelu sekä muilla asioiden käsittelyyn ja tietojenkäsittely-ympäristöön liittyvillä kehittämistoimenpiteillä.

Puutuin työssäni yksityiskohtaisesti työn alkuvaiheessa pois rajaamaani tekniseen tietoturvaan, mutta kuten VAHTI 3/2012 ohjeessa (Teknisen ICT -ympäristön tietoturvataso-ohje) todetaan; tietojärjestelmiin liittyvät yksityiskohtaiset vaatimukset kohdistuvat myös hallinnan vastuisiin, prosesseihin ja menettelyihin. Tietyt teknisessä ympäristössä esiintyvät puutteet voivat tulevaisuudessa antaa aihetta muuttaa linjauksia tai olemassa olevia käytäntöjä esimerkiksi käyttöjärjestelmän koventamisen suhteen. Nyt esille tuomani väliaikaisiin tiedostoihin ja Outlook -asiakassovellukseen liittyvät ongelmat näyttäytyvät yksittäisen organisaation kohdalla pieniltä, mutta jos samat toiminnallisuudet esiintyvät koko hallinnonalalla, ongelma voi muuttua opinnäytetyössä mainittujen julkisuuslain vaatimusten, tietosuojan toteutumisen ja tietoturvan hallinnan näkökulmasta merkittävämmäksi.

Opinnäytetyössäni mainitsemani sovelluksiin ja työasema-ympäristöön liittyvät riskit perustuvat omiin kokemuksiini ja havaintoihini 13 vuoden ICT-tukityön aikana. Kaikki esitetyt riskit ovat yleisesti tiedossa ja löydettävissä internetin julkisista tietolähteistä, eivätkä ne liity välttämättä organisaation X tietojenkäsittely-ympäristöön miltään osin. Koventamiseen liittyvistä vaatimuksista ja ohjeistuksista oli todella vaikea löytää selkeää lähdemateriaalia, eikä opinnäytetyön aikataulu mahdollistanut syvällisempää perehtymistä esimerkiksi NIST -organisaation tai Microsoftin tietoturvamäärityksistä kertoviin ohjeisiin. Jokaisella organisaatiolla ja ICT-palvelujen tuottajilla on omat käytäntönsä ja politiikkansa teknisen ICT -ympäristön suojaamiseen, ja esimerkiksi organisaation X hallinnonalalla etenevä valtion perustietotekniikkaratkaisun (VALTTI -työasemapalvelu) myötä työasemien vakiointi ja tietoturva kehittyvät eteenpäin.

Painotin tarkoituksellisesti opinnäytetyön teoreettista viitekehystä VAHTI -ohjeisiin, sillä olen aina halunnut käydä ohjeiston kokonaisvaltaisesti läpi, mutta aikataulut eivät ole sitä mahdollistaneet. VAHTI -ohjeisto on laaja, monipuolinen ja erinomaisesi laadittu, mutta tutkimuksellisuuden näkökulmasta työläs lukea läpi. Ohjeita on monesta eri näkökulmasta liittyen tietoturvallisuuden eri osa-alueisiin. Mieleeni tuli, että olisi mielenkiintoista koota ohjeistosta yksi yhtenäinen VAHTI -kirja, joka sisältäisi loogisena kokonaisuutena tärkeimmät voimassaolevat ohjeet tietoturvan eri osa-alueilta. Mielenkiinnolla odotan uutta VAHTI -100 arviointikehikkoa ja sen valmistumista.

Tietoturvan jalkauttaminen organisaatioon vaatii johdon panostusta, mutta myös työntekijöiden sitoutumista. Tämä vaatii henkilöstöltä taas motivaatiota, joka voidaan hakea tietoturvatasojen vaatimusten, eri ohjeistusten ja normatiivisen sääntelyn kautta, mutta nykyisessä muuttuvassa ympäristössä ja muutosten johtamisessa myös tietoturvan osalta pitää ottaa huomioon sellaiset työelämän laatutekijät, kuten työtyytyväisyys, työhyvinvointi, ihmisten väliset vuorovaikutustekijät ja henkilöstön osaamisen kehittäminen. Tavoitteellinen ja oikealla tavalla toteutettu osaamisen johtaminen auttaa viemään myös organisaation strategiat käytäntöön. (Rovaniemen Koulutuskuntayhtymä 2016, 4.)

Organisaation johtamista voidaan mitata ja kehittää johtamisen laatujärjestelmän ja sen arviointikriteeristön avulla, ja samanlaista ohjausmekanismia voidaan käyttää myös tietoturvan johtamiseen tietoturvavaatimusten nykytilan ja kehittämisen tukena. Näillä keinoin voidaan arvioida tietoturvan johtamisen vaikuttavuutta sekä tarvittavia kehittämistoimia. (VAHTI 2/2012, 24.) Periaatteita voitaisiin ottaa vaikkapa valtionhallinnon ohjeistuksesta hyvän henkilöstöstrategian toteutumiseksi. Henkilöstövoimavaroihin kohdistuvilla toimenpiteillä on strateginen merkitys organisaation toimintaan ja tulosten saavuttamiseen, ja se tukee organisaation strategiaan liittyvien tehtävien toteuttamista sekä organisaation kokonaisjohtamista. (Valtionvarainministeriö 2013, 5.)

Tietoturvan jalkauttaminen organisaatioon on iso muutos ja pitkäkestoinen prosessi. Toimintaympäristö muuttuessa jatkuvasti nopealla tempolla, osaamisvaatimuksia vaaditaan lisää, haastaen samalla myös työntekijät sekä johdon, mutta toimintaympäristön muutokset avaavat myös mahdollisuuksia. Yksi menestyvän organisaation avaintekijä on omaksua nopeasti uusia toimintatapoja, jonka saavuttamisen keskeisin tekijä on henkilöstön osaaminen. (Rovaniemen Koulutuskuntayhtymä 2016, 4.)

6.1 Päätelmät

Haasteena opinnäytetyön tekemisessä koin jo johdannossa mainitsemani ohjeiden ja ohjeistajien runsaan määrän, joka omalta osaltaan näkyi myös opinnäytetyöprosessissa ja lisäsi työmäärää merkittävästi siihen nähden, että työn tarkoituksena oli saada supistettua tietoturvan hallintajärjestelmään liittyvä kokonaisuus mahdollisimman yksinkertaisiin raameihin. Kokonaisuutena olen erittäin tyytyväinen omaan oppimisprosessiini ja opinnäytetyön tuloksiin. Toimeksiantajan palautteen mukaan opinnäytetyö hyödyntää organisaation X tietoturvan kehitystyötä johdon tukena sen sisältämän aihepiiriä koskevan tiedon, sääntelyn ja ohjeistuksen ansiosta.

Opinnäytetyössä esitettiin ensimmäisenä tutkimuskysymyksenä, millainen tietoturvan hallintajärjestelmä voisi soveltua organisaatiolle X. Toisena tutkimuskysymyksenä esitettiin, millainen sovelluspohjainen tietoturvan hallintajärjestelmä voisi tukea organisaation X tietoturvan kehittämistyötä.

6.2 Millainen on organisaatiolle X soveltuva tietoturvallisuuden hallintajärjestelmä?

Organisaatiolle X soveltuvan tietoturvan hallintajärjestelmän rakenne sisältää VAHTI 2/2014 ohjeistuksen mukaisesti tietoturvallisuusasetuksen (681/2010) 5 §:ssä mainitut kymmenen tietoturvallisuuden perustason vaatimusta projektinomaisina tehtävinä, jotka vastuutetaan ja aikataulutetaan. Tietoturvallisuusasetuksen 5 § perustason vaatimuksia täydentämään lisätään tietoturvan hallintajärjestelmään VAHTI 2/2010 liitteen 5 perustason vaatimukset samalla tavalla tehtäväluettelona, jotka vastuutetaan ja aikataulutetaan. Koska mainitut tietoturvallisuusasetuksen vaatimukset kohdistuvat ennemminkin prosesseihin ja menettelytapoihin, täydennetään tietoturva hallintajärjestelmää pitkän aikavälin suunnitelmalla soveltuvin osin muilla Viestintäviraston tietoturvavaatimusten arviointiin ja toteuttamiseen suosittelemia VAHTI -ohjeita. (Viestintävirasto 2018a, 12.)

VAHTI 2/2010 tasovaatimusten kohdalla huomioidaan tulevan tietohallintalain aiheuttamat muutokset, ja vaatimuksia tullaan korjaaman siten, kuin valtiovarainministeriö ja VAHTI tulevat ohjeistamaan uuden VAHTI 100 -vaatimuskehikon myötä (Rousku 2018). Tietosuoja oli rajattu tästä opinnäytetyöstä pois, mutta tietoturvan hallintajärjestelmään voi myöhemmin sisällyttää kontrollitavoitteet, jotka tarvitaan tietosuoja-asetuksen vaatimusten täyttämiseksi.

6.3 Millainen sovelluspohjainen tietoturvan hallintajärjestelmä voisi tukea organisaation X tietoturvan kehittämistyötä

Office 365 -ympäristössä toimiva projektinhallintatyökalu Microsoft Planner ja sillä luotu tietoturvan hallintajärjestelmä voisi tukea organisaation X tietoturvan kehittämistyötä mahdollistamalla käyttäjäystävällisen, projektinhallinnan muodossa olevan sähköisen ympäristön. Tutkittuihin kaupallisiin sovelluksiin verrattuna Ms Planner -sovellus eroaa edukseen juuri käytettävyyden näkökulmasta, sillä eri ”säilöihin” on todella helppo rakentaa erilaisia VAHTI -vaatimuksiin perustuvia rakenteita. Säilöihin tehtäviksi muokattuja kontrolleja pystyy liikuttelemaan horisontaalisesti säilöstä toiseen. Muokattavuus on erinomainen, ja Office 365 ympäristö mahdollistaa myös reaaliaikaisen raportoinnin johdolle, sillä Plannerin saa asennettua esimerkiksi mobiililaitteeseen, josta käsin johto voi seurata tietoturvan kehittymistä ja saada reaaliaikaista tilannekuvaa organisaation tietoturvan tilasta.

Microsoft Planner -työkalulla toteutetun tietoturvallisuuden hallintajärjestelmän voi tulevaisuudessa toteuttaa Office 365 pilvipalvelussa kokonaisuudessaan (pois lukien mahdolliset salassa pidettävät dokumentit), kun Valtorin pilvipalvelut tulevat käyttöön hallinnonalalla. Valtorin tarjoamat pilvikapasiteettipalvelut tuotetaan globaalisti julkisesta pilvipalvelusta, mutta palvelu on mahdollista saada myös luotetun yhteyden kautta (Valtori 2017). Pilvipalvelut on mahdollista toteuttaa myös yksityisessä pilvessä rajattuna, yksityisenä ympäristönä ja luotetun tietoliikenneyhteyden kautta. (Salmi 2017, 16.)

7 Jatkotutkimustarve

Ms Planner vaikutti erittäin lupaavalta jatkotutkimusta ja -kehittämistä ajatellen. Office 365 -ympäristöä en päässyt kokonaisvaltaisesti tutkimaan, koska Valtorin Office 365 -verkkopalveluympäristö ei vielä ole hallinnonalalla käytössä. Ensimmäisenä jatkotutkimustarpeena olisi selvittää, millaisena palveluna Valtori tulee Office 365 -ympäristön tarjoamaan asiakasorganisaatiolleen. Toisena jatkotutkimustarpeena on selvittää, millaiset käyttövaltuudet voitaisiin ylläpitoa varten luoda. Tietoturvan hallintajärjestelmän ylläpitoa varten ei mielellään saisi luoda yksittäiseen henkilöön sidottua käyttövaltuutta. Riskiksi voisi muodostua ylläpitäjän siirtyminen organisaation ulkopuolelle toisiin tehtäviin ja käyttäjätunnuksen lakkauttaminen, sen jälkeen muut ryhmän jäsenet eivät mahdollisesti pääse enää kirjautumaan tuotantoympäristöön.

Haasteena Planner -ympäristössä on sen suojaaminen muutoksilta. Ympäristöön tehtyä hallintajärjestelmää ei organisaatio itse pysty varmuuskopioimaan, mutta Valtorin tuottamat pilvipalvelut tuotetaan kolmen eri teknologiatoimittajan kanssa; Microsoft Azure, Amazon Web Services ja Fujitsun K5 (Valtori 2017), joten datan suojaus toteutuu luotettavien palveluntoimittajien varmistusratkaisujen kautta. Kolmantena jatkotutkimusaiheena pitäisi selvittää varmuuskopioinnin periaatteet ja tiedon käytettävyyteen ja eheyteen liittyvät riskit, sekä miten

ympäristön voisi suojata tahattomilta muokkauksilta. Esimerkiksi Googlen pilviympäristössä voi jakamilleen kansioille luoda muokkaus- tai ainoastaan katseluoikeudet. Microsoft Ms Planner –yhteisössä (Microsoft 2018c) on kuitenkin hyvin aktiivinen kehitystyö meneillään mm. tallennuksen ja tulostamisen suhteen, joten kyseinen sovellusympäristö kehittyy jatkuvasti ominaisuuksiltaan.

Mielenkiintoinen jatkotutkimuksen jatkotutkimusaihe on myös ryhmätyöskentelytila Microsoft Teams, joka tulee korvaamaan Microsoftin ilmoituksen mukaan Skype for Business -sovelluksen (Tahto Group 2018). Teams integroituu hyvin myös Ms Planneriin, ja Teams -sovelluksen kautta tietoturvatietoisuuden lisääminen onnistuisi huomattavasti aiempaa helpommin. Teams -sovelluksessa organisaatio voi viestiä asioista siten, että keskustelut säilyvät yhdessä paikassa. Teams -sovelluksen osalta pitäisi tutkia, miten sen toiminnallisuudet sopivat yhteen Plannerin kanssa.

Kuten Ms Planner -sovelluksessa on mahdollisuus, myös Teams on käytettävissä heti mobiililaitteissa iOS – ja Android -alustoilla. Teams – palvelussa on mahdollisuus tallentaa yhteisiä tiedostoja, käyttää keskustelun muistikirjaa sekä perustaa kanavia tiedon jakamista varten. (Sulava 2018.) Ehkäpä näillä työvälineillä voisi jo innostua tietoturvan hallinnasta ja etenkin sen jalkauttamisesta!

Lähteet

Hirsijärvi, S., Remes, P. & Sajavaara, P. 2005. Tutki ja kirjoita. 11. uudistettu painos. Helsinki: Tammi.

Jaakonhuhta, Hannu. 2011. Tietotekniikan sanakirja. Vaajakoski: Bookwell OY.

SFS-EN ISO/IEC 27001:2017 Standardikokokoelma.

Laine, T. 2001. Miten kokemusta voi tutkia? Fenomenologinen näkökulma. Teoksessa J. Aaltola & R. Valli (toim.) Ikkunoita tutkimusmetodeihin II. Näkökulmia aloittelevalle tutkijalle tutkimuksen teoreettisiin lähtökohtiin ja analyysimenetelmiin. Jyväskylä: PS-kustannus, 26-43.

Varto, J. 1992. Laadullisen tutkimuksen metodologia. Helsinki: Kirjayhtymä.

Vilkka, H. 2015. Tutki ja kehitä. PS-kustannus. 4. uudistettu painos. ISBN 978-952-451-756-0

Vilkka, H & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Sähköiset

Active Directory Security. 2015. Finding Passwords in SYSVOL & Exploiting Group Policy Preferences. Viitattu 29.4.2018. https://adsecurity.org/?p=2288

Active Directory Security. 2018. Securing Windows Workstations: Developing a Secure Baseline. Viitattu 16.5.2018. https://adsecurity.org/?p=3299

COSO. 2013. Committee of Sponsoring Organizations of the Treadway Comission. Internal Control – Integrated Framework Executive Summary. Suomenkielinen käännös: Sisäiset tarkastajat ry ammatillisten asioiden toimikunta. Sisäisen valvonnan kokonaisvaltainen ajatusmalli. Viitattu 15.4.2018. https://theiia.fi/wp-content/uploads/2016/12/coso_exsum_translation_into_fi_final_2.pdf

EUR-Lex. 2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Viitattu 12.5.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL

Finlex. 2018. Laki (1226/2013) valtion yhteisten tieto – ja viestintäteknisten palvelujen järjestämisestä. Viitattu 28.1.2018. https://www.finlex.fi/fi/laki/alkup/2013/20131226

HE 106/2017 vp. Hallituksen esitys eduskunnalle Valtion talousarvioksi vuodelle 2018. Viitattu 15.4.2018. https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_106+2017.pdf

Hewlett-Packard 2005. Standardize your desktop hardware to reduce TCO. Viitattu 28.1.2018. http://www8.hp.com/in/en/pdf/How-to-reduce-your-ownership-cost_tcm_188_993801.pdf

Inmics Oy. Ketterä projektinhallinta Office 365:ssä. Viitattu 25.4.2018. https://www.inmics.fi/blogi/kettera-projektinhallinta-office-365ssa/

Järvensivu, J. 2017. Kohti kokonaisvaltaista riskienhallintaa ISO 31 000 -standardin avulla. Pirkkalan kunnan riskienhallinnan kehittäminen. Tampereen ammattikorkeakoulu. Opinnäytetyö (YAMK). Viitattu 14.4.2018. https://www.theseus.fi/bitstream/handle/10024/132551/Jarvensivu_Johanna.pdf?sequence=1&isAllowed=y

Karlos, A. Martinsuo, M., Kujala, J. Projektiliiketoiminta. Viitattu 14.4.2018. http://pbgroup.aalto.fi/en/the_book_and_the_glossary/projektiliiketoiminta.pdf

Katakri 2011. Viitattu 16.5.2018. http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Katakri. 2015. Viitattu 16.5.2018. https://www.defmin.fi/files/3165/Katakri_2015_Tietoturvallisuuden_auditointityokalu_viranomaisille.pdf

Limnéll, Jarno. 12/2014. Aalto-yliopiston julkaisusarja ”TIEDE + TEKNOLOGIA. Kyber rantautui Suomeen”. Viitattu 28.1.2018. https://aaltodoc.aalto.fi/bitstream/handle/123456789/14606/isbn9789526060224.pdf?sequence=1

Lundahl, P. 2011. Riskinelonen – vaihtoehto riskin suuruuden määrittelyyn. Turvallisuusjohdon koulutusohjelma. Aaltoyliopisto. Viitattu 12.5.2018. https://www.aaltopro.fi/media/aalto-pro-publications/tjk/tjk11_tutkielma_petri_lundahl.pdf

Marjamäki-Ruuskanen, S. 2013. Hallinnon tietotekniikkakeskuksen kokonaisvaltaisen riskienhallinnan kehittämissuunnitelma. Laurea-ammattikorkeakoulu. Turvallisuusosaamisen koulutusohjelma. Opinnäytetyö (YAMK).

Microsoft. 2012. Artikkeli 817878. Viitattu 25.4.2018. https://support.microsoft.com/en-us/help/817878/attachments-remain-in-the-outlook-secure-temporary-file-folder-when-yo

Microsoft. 2014. Blocking Remote Use of Local Accounts. Viitattu 16.5.2018. https://blogs.technet.microsoft.com/secguide/2014/09/02/blocking-remote-use-of-local-accounts/

Microsoft. 2017. Ms14-025. Microsoft Security Bulletin MS14-025 https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2014/ms14-025

Microsoft. 2018a. Outlook datatiedostojen (.pst ja .ost) esittely. Viitattu 29.4.2018. https://support.office.com/fi-fi/article/Outlookin-datatiedostojen-pst-ja-ost-esittely-222eaf92-a995-45d9-bde2-f331f60e2790

Microsoft. 2018b. Outlookin datatiedostojen esittely. Viitattu 25.4.2018. https://support.office.com/fi-fi/article/outlookin-datatiedostojen-pst-ja-ost-esittely-222eaf92-a995-45d9-bde2-f331f60e2790

Microsoft. 2018c. Planner uservoice community. Viitattu 16.5.2018. https://techcommunity.microsoft.com/t5/Planner/ct-p/Planner

Microsoft. 2018d. Tietoturvamääritysohjeiden tuki. Viitattu 16.5.2018. https://support.microsoft.com/fi-fi/help/885409/security-configuration-guidance-support

NIST. 2018a. National Institute of Standards and Technology. Viitattu 16.5.2018. https://www.nist.gov/

NIST. 2018B. AC-6 Least Privilege. Viitattu 16.5.2018. https://nvd.nist.gov/800-53/Rev4/control/AC-6

Noukka, L. 2017. Riskiblogi. COSO ERM uudistui – eroon kuutioajattelusta. Viitattu 12.5.2018. https://riskiblogi.fi/?p=429

OM 5/016/2014. Oikeusministeriö. Ohje salassa pidettävien ja luokiteltujen tietoaineistojen käsittelystä oikeusministeriössä. Viitattu 22.4.2018. https://tietopyynto.fi/files/foi/346/Tietoaineistojenksittelyohje.pdf

Oikeusministeriö. 2014a. Ohje salassa pidettävien ja luokiteltujen tietoaineistojen käsittelystä oikeusministeriössä. Viitattu 22.4.2018. https://tietopyynto.fi/files/foi/346/Tietoaineistojenksittelyohje.pdf

Oikeusministeriö. 2017. Mietintöjä ja lausuntoja. Tuomioistuinviraston perustaminen. Lausuntotiivistelmä. Viitattu 14.4.2018. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80786/OMML_41_2017_Tuomioistuinvirasto_Lausuntotiivistelm%C3%A4.pdf?sequence=1&isAllowed=y

Oikeusministeriö. 2017b. ICT-osaamisen kehittämisen konsepti. Mietintöjä ja lausuntoja 55/2017. Viitattu 19.5.2018. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160540/OMML_55_2017_ICT_Koulutus.pdf?sequence=1&isAllowed=y

Oikeusministeriö. 2018. Oikeusministeriön kirjanpitoyksikön (KPY 150) tilinpäätös vuodelta 2017. Viitattu 14.4.2018. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160617/OMTH_10_2018_OMn_tilinpaatos_2017.pdf?sequence=1&isAllowed=y

Perustuslakivaliokunta. 2013. Perustuslakivaliokunnan lausunto PeVL 37/2013 vp. Viitattu 5.5.2018. https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_37+2013.pdf

Puolustusministeriö. 2006. Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia. Viitattu 27.5.2016. https://www.defmin.fi/files/815/YETT_2006.pdf

Rousku, K. 2017a. VAHTIn kesäseminaari 5.6.2017. Viitattu 22.4.2018. http://vm.fi/documents/10623/1898625/VAHTI-kes%C3%A4seminaari+kooste/da928575-7c94-4853-a5f9-acf31a87eae2/VAHTI-kes%C3%A4seminaari+kooste.pdf

Rousku, K. 2017b. Ohje riskienhallintaan. Valtiovarainministeriön julkaisuja 22/2017. Viitattu 12.5.2018. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80013/VM_22_2017.pdf?sequence=1

Rousku, K. 2018. Tietoturvallisuuden standardisointiverkoston kokous 1/2018 – VAHTI 100. Viitattu 24.4.2018. https://www.viestintavirasto.fi/attachments/esitykset/Tiesta_kokous_01_2018_liite_3_VAHTI_100.pdf

Rovaniemen Koulutuskuntayhtymä. 2016. Osaamisen johtaminen. Osaamisen ennakoinnista osaamisien kehittämiseen. SOTE-tuotantoalueen osaamisen kehittämisen toimintamalli. Viitattu 14.4.2018. http://www.redu.fi/loader.aspx?id=283831a3-dbf6-4ce2-82cd-7251322e8b03

Salmi, A. 2017. Microsoft Azure -pilvipalvelun käyttöönotto valtion yhteisessä tietoliikennepalvelussa. Viitattu 27.5.2018. http://www.theseus.fi/bitstream/handle/10024/123922/ont_arttu_salmi_final.pdf?sequence=1&isAllowed=y

Sisäasiainministeriö. 2012. Liiketoimintaa turvallisesti. Viitattu 28.1.2012. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79435/sm_302012.pdf

Sulava 2018. Microsoft Teams – Mikäs tämä nyt on? Viitattu 29.4.2018. https://www.sulava.com/microsoft-teams-mikas-tama/

Tahto Group Oy. 2018. Microsoft Teams ratkaisee monta ongelmaa. Viitattu 29.4.2018. https://tahtogroup.fi/microsoft-teams-ratkaisee-monta-ongelmaa/

VAHTI 2/2004. Tietoturvallisuus ja tulosohjaus. Viitattu 19.5.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=d67f9f1e-74e3-4a74-af67-71f7552f9f38&groupId=10128

VAHTI 6/2006. Tietoturvatavoitteiden asettaminen ja mittaaminen. Viitattu 26.4.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=b3a59fa6-570f-4cd6-9a67-79e34f3c4b38&groupId=10128

VAHTI 7/2006. Muutos ja tietoturvallisuus, alueellistamisesta ulkoistaimiseen – hallittu prosessi. Viitattu 24.4.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=3f4ff661-4b63-488b-8103-a0af508c67c8&groupId=10128

VAHTI 3/2007. Tietoturvallisuudella tuloksia. Viitattu 24.2.2018. https://www.VAHTIohje.fi/

VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. Viitattu 24.2.2018. https://www.VAHTIohje.fi/

VAHTI 2/2011. Johdon tietoturvaopas. Viitattu 4.4.2018. https://www.VAHTIohje.fi/c/document_library/get_file?uuid=6068ca18-6214-4244-8ce6-dffe952e3e8e&groupId=10229

VAHTI 3/2012. Teknisen ympäristön tietoturvataso-ohje. Viitattu 24.2.2018. https://www.VAHTIohje.fi/.

VAHTI 1/2013. Sovelluskehityksen tietoturvaohje. Viitattu 24.2.2018. https://www.VAHTIohje.fi/

VAHTI 5/2013. Päätelaitteiden tietoturvaohje. Viitattu 24.2.2018. https://www.VAHTIohje.fi/

VAHTI 2/2014. Tietoturvallisuuden arviointiohje. Viitattu 14.4.2018. https://www.VAHTIohje.fi/

VAHTI 1/2016. VAHTIn toimintakertomus vuodelta 2015. Valtiovarainministeriö. Viitattu 14.4.2018. http://vm.fi/documents/10623/307681/VAHTIn+toimintakertomus+vuodelta+2015/dd8a0178-3957-4fc1-b591-011af92a015e

VAHTI 3/2016. Henkilöstön ja johdon tietoturvabarometri. Viitattu 18.3.2018. http://julkaisut.valtioneuvosto.fi/handle/10024/79060

VAHTI 21/2017. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä. Toimintasuunnitelma vuosille 2017- 2019. Viitattu 22.4.2018. http://urn.fi/URN:ISBN:978-952-251-860-6

VAHTI 24/2017. VAHTIn toimintakertomus 2016. Valtiovarainministeriö. Viitattu 18.3.2018. http://julkaisut.valtioneuvosto.fi/handle/10024/80014

Valtiokonttori. 2010. Toimintakertomuksen laatiminen. Dnro VK 510/03/2010. Viitattu 19.5.2018. http://www.valtiokonttori.fi/kasikirja/Public/download.aspx?ID=81869&GUID=%7B41E4930D-1FF4-4C8A-9E72-E7EB8E1C9AFC%7D

Valtiokonttori. 2015a. Valtion talous- ja henkilöstöhallinnon käsikirja. Viitattu 27.1.2018. http://www.valtiokonttori.fi/kasikirja/public/download.aspx?ID=84664&GUID=%7BF74D76EE-9231-4001-A4FB-C253222F1B70%7D

Valtiokonttori 2015b. Valmiina digikiriin. Digitalisaatio ja virastojen tuottavuuspotentiaali. Viitattu 22.4.2018. http://www.valtiokonttori.fi/download/noname/%7B8B28514D-E7AA-4384-A6D6-6B85615A3D93%7D/92716

Valtioneuvosto. 2015. Valtionhallinnon tieto – ja kyberturvallisuus on kehittynyt myönteisesti ja kehittämistä jatketaan. Viitattu 26.5.2018. http://valtioneuvosto.fi/artikkeli/-/asset_publisher/valtionhallinnon-tieto-ja-kyberturvallisuus-on-kehittynyt-myonteisesti-ja-kehittamista-jatketaan?_101_INSTANCE_3wyslLo1Z0ni_groupId=10623

Valtioneuvosto. 3/2017. Julkishallinnon digitalisaatio – tuottavuus ja hyötyjen mittaaminen. Viitattu 2.3.2018. http://vnk.fi/julkaisu?pubid=16202

Valtioneuvosto. 2017. Valtioneuvoston asetus Väestörekisterikeskuksen eräistä tehtävistä. Valtioneuvoston yleisistunto 16.11.2017 13.00. Viitattu 24.4.2018. http://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f8056c00e
Liite 1 muistio: http://valtioneuvosto.fi/delegate/file/34261

Valtioneuvosto. 2018. Digitalisaatio, kokeilut ja normien purkaminen. Viitattu 26.2.2018. http://valtioneuvosto.fi/hallitusohjelman-toteutus/digitalisaatio

Valtioneuvoston kanslia. 2017a. Valtioneuvoston rakenteisten asiakirjojen käsittely. Kohdearkkitehtuurikuvaus. Viitattu 22.4.2018. https://api.hankeikkuna.fi/asiakirjat/fa1a69b2-c881-4655-a7e4-48d7d63c24c2/300a5128-f6af-48e5-bb66-bbefd493fb02/RA-PORTTI_20170626092615.pdf

Valtioneuvoston ohjesääntö 2003/262. Viitattu 10.3.2018. https://www.finlex.fi/fi/laki/ajantasa/2003/20030262#L2P2

Valtiontalouden tarkastusvirasto. 2007. Valtiontalouden tarkastusviraston toiminnantarkastuskertomus 150/2007. Tulosohjauksen tila. Viitattu 14.4.2018. https://www.vtv.fi/files/108/1502007_Tulosohjauksen_tila_NETTI.pdf

Valtiontalouden tarkastusvirasto. 2009. Valtiontalouden tarkastusviraston tuloksellisuustarkastuskertomus 197/2009. Viitattu 14.4.2018. https://www.vtv.fi/julkaisut/tuloksellisuustarkastuskertomukset/2009

Valtiontalouden tarkastusvirasto. 2014. Valtiontalouden tarkastusviraston vuosikertomus eduskunnalle VTV K 18/2014 vp. Pääjohtajan katsaus. https://www.vtv.fi/files/4126/K_18_2014_vp.pdf. Kouvo, Antti. 2014. Luottamuksen lähteet. Vertaileva tutkimus yleistynyttä luottamusta synnyttävistä mekanismeista, Turun yliopisto, sarja C381, Turku (2014). Viitattu 15.4.2018.

Valtiontalouden tarkastusvirasto. 2015. Valtiontalouden tarkastusviraston vuosikertomus eduskunnalle toiminnastaan 2015 valtiopäiville. Viitattu 26.5.2018. https://www.eduskunta.fi/FI/vaski/Kertomus/Documents/K_18+2015.pdf#%5B%7B%22num%22%3A47%2C%22gen%22%3A0%7D%2C%7B%22name%22%3A%22FitR%22%7D%2C-65%2C283%2C563%2C686%5D

Valtiontalouden tarkastusvirasto. 2017a. Kybersuojauksen järjestäminen. Viitattu 10.3.2018. https://www.vtv.fi/files/5862/16_2017_Kybersuojauksen_jarjestaminen.pdf

Valtiontalouden tarkastusvirasto. 2017b. Sisäisen valvonnan ja riskienhallinnan tila valtionhallinnossa. Viitattu 20.5.2018. https://www.vtv.fi/files/5821/13_2017.pdf

Valtiontalouden tarkastusvirasto. 2018. Käsitteitä. Viitattu 27.1.2018. https://www.vtv.fi/toiminta/tilintarkastus/kasitteita

Valtiovarainministeriö. 2005a. Tulosohjauksen käsikirja. Viitattu 14.4.2018. http://vm.fi/documents/10623/307545/Tulosohjauksen+k%C3%A4sikirja.pdf/b7f9a7f9-2b46-4dbb-bb66-85bf1074b88a

Valtiovarainministeriö. 2005b. Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta. Viitattu 14.4.2018. http://www.vm.fi/vm/fi/03_tiedotteet_ja_puheet/01_tiedotteet/2005/20051229Suosit/98830.pdf

Valtionvarainministeriö. 2013. Valtionvarainministeriö ja valtion työmarkkinalaitos. Henkilöstövoimavarojen johtamisen kehittämishankkeen kehittämisryhmä. Edita Prima Oy. ISBN 978-951-37-5255-2

Valtiovarainministeriö. 2015. Valtiovarain controller -toiminto. Päivitetty 23.1.2015. Valtion viraston ja laitoksen sekä rahaston sisäinen valvonta ja riskienhallinta – Laaja arviointikehikko. Viitattu 19.5.2018. http://vm.fi/documents/10623/307569/Valtion%20viraston%20ja%20laitoksen%20sek%C3%A4%20rahaston%20sis%C3%A4inen%20valvonta%20ja%20riskienhallinta%20-%20Laaja%20arviointikehikko/d1a86b32-c320-447a-9a65-5ba7072fb0be

Valtiovarainministeriö. 2015b. Keskus – ja aluehallinnon virastoselvityshankkeen yhteinen koontiraportti VIRSU. Valtiovarainministeriön julkaisuja 5/2015. Viitattu 26.5.2018. http://vm.fi/documents/10623/360852/VIRSU+koontiraportti/5a128c1d-12f2-4aca-bb9c-722b8e956a8b

Valtiovarainministeriö. 2016. Julkisen hallinnon tiedonhallinnan sääntelyn kehittämistä selvittävän työryhmän asettaminen. 17.11.2016. Viitattu 10.5.2018. https://api.hankeikkuna.fi/asiakirjat/351707bb-fcc5-437b-94bd-57fcab83d609/d7549487-f0cb-458c-a909-c135e2f9b499/ASETTAMISPAATOS_20161121061501.PDF

Valtiovarainministeriö. 2016. Vahti -raportti 1/2016. EU-tietosuojan kokonaisuudistus. Viitattu 23.4.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Valtiovarainministeriö. 2017. Digitalisaatiota tukevia asiantuntijatehtäviä siirretään Väestörekisterikeskukseen 1.1.2018 alkaen. Viitattu 24.4.2018. http://vm.fi/artikkeli/-/asset_publisher/digitalisaatiota-tukevia-asiantuntijatehtavia-siirretaan-vaestorekisterikeskukseen-1-1-2018-alkaen

Valtionvarainministeriö. 2017a. Hallinnon rakenteet. Viitattu 19.11.2017. http://vm.fi/hallintopolitiikka/hallinnon-rakenteet

Valtiovarainministeriö. 2017b. Tiedonhallinnan lainsäädännön kehittämislinjaukset. Työryhmän raportti. Viitattu 5.5.2018. http://vm.fi/documents/10623/306884/37_2017_Tiedonhallinnan+lains%C3%A4%C3%A4d%C3%A4nn%C3%B6n+kehitt%C3%A4mislijaukset.pdf/c1f679f5-a26b-4308-9162-c395b3f5d093

Valtiovarainministeriö. 2017c. VM 22/2017 Ohje riskienhallintaan – LIITTTEET 1 – 6. Viitattu 23.5.2018

Valtiovarainministeriö. 2017d. Sisäisen valvonnan arviointikehikko. Lausuntopyyntö 19.12.2017. VM036:01/2015,VM/533/00.01.00.01/2015. Viitattu 19.5.2018. https://api.hankeikkuna.fi/asiakirjat/a186ec44-405e-4ff9-a943-10ff9a0f7d68/f2484ef5-45ce-4403-8ee3-4a86ce4d7679/LAUSUNTOPYYNTO_20171219101000.PDF

Valtiovarainministeriö. 2018a. Tiedonhallintalain valmistelu jatkuu hallitusohjelman tavoitteiden mukaisesti. Viitattu 22.4.2018. http://vm.fi/artikkeli/-/asset_publisher/tiedonhallintalain-valmistelu-jatkuu-hallitusohjelman-tavoitteiden-mukaisesti

Valtiovarainministeriö. 2018b. Mitä on tuloksellisuus. Viitattu 30.5.2018. http://vm.fi/mita-on-tuloksellisuus-

Valtori. 2016. Valtion yhteiset tietoliikennepalvelut (VY-verkko). Uutinen Valtorin verkkosivuilla 30.12.2016. Viitattu 24.2.2018. http://www.valtori.fi/fi-FI/Palvelut/Tyoskentely-ympariston_palvelut/Tietoliikennepalvelut/Valtion_yhteiset_tietoliikennepalvelut_VY-verkko

Valtori. 2017. VAKA-Pilvi: Pilvikapasiteettipalvelut osaksi Valtorin palveluvalikoimaa. Viitattu 27.5.2018. http://www.valtori.fi/fi-FI/VAKA-Pilvi_Pilvikapasiteettipalvelut_osa

Valtiovarainministeriö. 2018b. Sisäinen valvonta ja riskienhallinta. Viitattu 5.5.2018. http://vm.fi/hallintopolitiikka/sisainen-valvonta-ja-riskienhallinta

Valtiovarainministeriö. 2018c. VAHTI -toiminnan organisointi. Viitattu 24.2.2018. http://vm.fi/vahti-toiminnan-organisointi

Viestintävirasto. 2015. Ohje arviointikriteeristöjen tulkinnasta. Kansalliset arvioinnit. Viitattu 28.4.2018. https://www.viestintavirasto.fi/attachments/tietoturva/Ohje_arviointikriteeristojen_tulkinnasta.pdf

Viestintävirasto. 2015. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. Viitattu 16.5.2018. https://www.viestintavirasto.fi/attachments/tietoturva/TeollisuusautomaationTietoturva.pdf

Viestintävirasto. 2017. Ohje tietoturvallisuuden arviointilaitoksille. Julkaistu 28.6.2013. Päivitetty 19.5.2017. Viitattu 29.4.2018. https://www.viestintavirasto.fi/ohjausjavalvonta/ohjeetjajulkaisut/ohjeidentulkintojensuositustenjaselvitystenasiakirjat/ohjetietoturvallisuudenarviointilaitoksille.html

Viestintävirasto. 2018a. Ohje tietoturvallisuuden arviointilaitoksille 210/2016 O. Versio 7 23.4.2018 uusi ohje. Viitattu 12.5.2018.

Viestintävirasto. 2018b. Pilvipalveluiden turvallisuus. Mitä organisaatioiden tulisi huomioida pilvipalveluja hyödyntäessä. Viitattu 16.5.2018. https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Julkaisemattomat

TTA 2018. Organisaation X tulostavoiteasiakirja vuodelle 2018.

Kuviot